服务网址：www.Router.net.cn

中文域名：软件路由器

服务范围：软件路由器开发、改写，路由器配件电子硬盘、CF-IDE、服务器网卡、服务器主板、SCSI卡、工控机箱等。

免费技术热线：0771-2577076

ISP级软件路由器之王

RouerOS 宽带接入服务器

用户手册

——配置指南

RouerOS 系列宽带接入服务器配置指南内容摘要

一．概述

RouerOS 宽带接入服务器是基于嵌入式专用网络操作系统而设计的，具有丰富的网络接口，具备多数常见的网络设备功能，处理能力超群，运行十分稳健，性价比极高。

1．RouerOS 宽带接入服务器的网络接口类型

1.1 4 个10/100M 以太网接口，可选10/100/1000M 接口

4 个RJ45 以太网接口机箱上标注名称分别为“ETH0”、“ETH1”、“ETH2”、“ETH3”，在系统中对应名称为“ETH0”、“ETH1”、“ETH2”、“ETH3”。由于物理接口较多，虚拟接口（如VLAN、PVC 等）更多，因此不像一般防火墙上用“内网接口”、“外网接口”、“停火区接口”等作为标示。在配置防火墙功能或其它网络功能时由用户灵活运用。可选以下接口：

☐ ※ 无线网络（Wireless LAN）接口（2.4G,5.2G,5.8G 无线网）；
☐ ※ MOXA C101 同步接口；
☐ ※ MOXA C502 同步接口；
☐ ※ 串行异步接口；
☐ ※ IP 电话接口；
☐ ※ ISDN 接口；
☐ ※ 帧中继PVC 接口；
☐ ※ E1/T1 接口。

2．RouerOS 宽带接入服务器具有以下网络功能

当然，有些功能需要单独的许可证。

1 路由器功能（支持RIP1、RIP2、RIPng、OSPF、OSPFv6、BGP4 路由协议）支持IPv4、IPv6 协议。
2 PPPOE 服务器和客户端功能支持RADIUS 认证和计费，支持基于用户帐号的带宽管理和访问控制策略。
3 PPTP/VPN 服务器和客户端功能支持RADIUS 认证和计费，支持基于用户帐号的带宽管理和访问控制策略，支持PAP、CHAP、MSCHAP、MSCHAPv2 认证协议，支持MPPE 链路加密。
4 L2TP/VPN 服务器和客户端功能支持RADIUS 认证和计费，支持基于用户帐号的带宽管理和访问控制策略，支持PAP、CHAP、MSCHAP、MSCHAPv2 认证协议，支持链路加密。
5 基于IPIP 的VPN 功能与CISCO 等厂家的IPIP 功能兼容，与各种类UNIX、UNIX 系统的IPIP 功能兼容。
6 基于IPSEC 的VPN 功能支持AH/SEP 模式，支持多种哈稀（HASH）算法和加密算法。
7 基于EoIP(Ethernet over IP)的VPN 功能提供高性能线速VPN 功能，支持基于PPTP、L2TP、IPSEC 的链路加密应用。
8 HOTSPOT（WEB 认证）服务器功能支持在有线局域网和无线局域网上的WEB 认证；支持RADIUS 后台认证计费，支持MD5-CHAP 认证协议以保证用户口令的安全传输；用户无需安装客户端软件，并可动态显示连接时长和上网流量。
9 无线接入服务器（ACCESS POINT，AP）功能支持2.4GHZ、5.2GHZ 、5.8GHZ 无线网络，在无线链路上可使用PPPOE 、PPTP 、L2TP 、IPIP 、IPSEC、HOTSPOT 等接入方式。
10 集成WEB-CACHE 功能和代理服务器功能支持WEB-CACHE 和透明代理功能。
11 状态防火墙功能和NAT 功能支持IP 共享、基于源地址的NAT 转换、基于目的地址的NAT 转换、IP 端口重定向等功能。
12 DHCP 服务器和客户端功能支持IP-MAC 绑定。
13 DNS CACHE 功能提供基于缓存的DNS 服务器功能。

14 NTP 时间服务器和客户端功能作为NTP 时间服务器，可以为其它网络设备和系统提供时间基准；作为NTP 时间服务客户端，可以保持网络设备的时间同步。
15 IP 电话网关功能通过增加IP 电话接口卡，具备IP 电话网关功能。
16 流量整形和带宽管理功能提供多种模式的流量整形和带宽管理功能，提供固定分配的带宽管理、基于RADIUS 授权的带宽管理等多种管理方式。
17 网桥功能方便地以二层网络的方式连接各种网络。
18 VLAN（802.1Q）功能可以划分多达4096 个802.1Q VLAN，提供网络细分的能力。
19 STP（Spanning Tree Protocol）功能可以为网络提供环型拓扑保护机制。
20 RADIUS 客户端功能用以完成PPP 连接的RADIUS 认证和HOTSPOT 的RADIUS 认证
21 SNMP 网管功能可以让设备整体的网络管理环境。
22 UPS 监视功能可以自动发现UPS 电源设备掉电或重大故障，并采取相应动作保护网络设备。
RouerOS 宽带接入服务器可以通过GUI 图形界面进行配置管理，也支持使用命令行（CLI）方式进行配置和管理。使用CLI 方式时，可以通过TELNET 远程登录、SSH 安全加密远程登录、CONSOLE 本地控制台登录进入RouerOS 宽带接入服务器进行配置管理。

二．基本的配置管理

1．系统的缺省帐号

缺省帐号为"admin"，没有密码直接回车即可，该帐号具有最大权限。

2．登录方式

2.1 通过console 口进行管理

利用我们提供的专用console 线连接RouerOS2 与计算机，在计算机的串行通信口设置为9600-8-N-1，无流控。

2.2 通过远程telnet 登录管理

须在/ip service 下设置允许telnet 登录的客户IP 地址范围，缺省为允许所有IP 登录。为安全起见，要严格设置可登录地址范围。

2.3 通过专用客户端"winbox.exe"，以GUI 方式登录管理

须在/ip service 下设置允许GUI 登录的客户IP 地址范围，缺省为允许所有IP 登录。为安全起见，要严格设置可登录地址范围。

2.4 通过SSH 客户端登录管理

SSH 是基于证书/口令链路加密的登录方式，具有极高的安全性，不需要限制登录IP 地址范围。如果确实需要，可以通过防火墙策略实现。

3．命令行配置的基本操作在任何路径下或命令行中输入一个问号，可以提示你随后的选项。

1 RouerOS2 登录后的提示符为：[admin@RouerOS] > # 这里admin 是登录用户名如果进入到某个

配置子项（如IP Address），则提示符变为：[admin@RouerOS] IP Address>

3.2 命令行的基本格式为：

“路径树命令参数名=参数值”其中，路径树由具有层次结构的路径节点组成，节点与节点间用空格符分隔；命令与参数名之间也用空格符号分隔；参数名与参数值之间用“=”连接。RouerOS2 支持命令补全（用“TAB”键补全），支持问号“？”求助，支持命令回滚，支持路径名/命令名/参数名缩写，使用非常方便。通过输入全路径树，在根路径上可以完成所有的命令行操作；也可以进入某一路径进行相关操作。从父路径进入子路径，只要输入子路径名即可；从子路径返回父路径，只要输入“..”即可。输入“/”将从任何路径下返回根路径。

2 常用命令有print，add，set，enable，disable，epxort 等。“print”用于显示相关配置参数或状态信息，用于新增配置项，用于修改配置参数，、

“add”“set”“enable”

“disable”用于相关项目的允许/禁止，“export”用于导出配置脚本。

一个功能的设置有时需要在几个路径中进行配置，以后会有详细说明。

4. RouerOS 远程管理-权限管理

4.1 管理员账号管理

1 路径：/user

2 功能：增加、删除、禁止、开启用户帐号；设置帐号密码、组；修改用户名；设置允许用户进入系统的客户端IP 地址；编辑注释信息。

4.1.3 示例：a）修改用户属性/user set 0 name=hi address=0.0.0.0 netmask=0.0.0.0 group=sys password=dfusjke commet=yourname disable=no

上面命令行中红色的“0”代表用户的编号（见下面网管截屏中的“#”项）。在其它配置项目中，如有多个同样的配置项目，也都是用编号来区分的，在配置中要注意！

网管截屏：

```
[admin@Freed] user> pri
Flags: X - disabled
 #   NAME                            GROUP                   ADDRESS
 0   ;;; system default user
     admin                           full                    0.0.0.0/0
 1   ;;; manager_user
     ming                            write                   0.0.0.0/0
```

4.2 访问控制列表

网管截屏:

```
[admin@Freed] ip service> print
Flags: X - disabled, I - invalid
 #   NAME                                 PORT  ADDRESS
 0   telnet                               23    192.168.1.238/32
 1 X ftp                                  21    0.0.0.0/0
 2   www                                  80    0.0.0.0/0
 3   hotspot                              8088  0.0.0.0/0
```

1　　设置可telnet（或ssh、web 等）网管的地址：[admin@RouerOS] ip service> set 0 address=192.168.1.238 netmask=255.255.255.255
2　　禁用某种登录方式：如禁用ftp [admin@RouerOS] ip service> set 1 dis=yes

4.3 在防火墙规则中实现访问限制

[admin@xinhua] ip firewall rule input> pr Flags: X - disabled, I - invalid, D - dynamic 4 src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:!22 out-interface=all protocol=tcp icmp-options=any:any tcp-options=any connection-state=new flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=drop log=no

注：上述规则中的“!22）表示除了22 号端口外禁止通过所有其它端口对RouerOS 本身的连接。

5. 日志管理

1　　路径：/system logging
2　　功能

记录方式定义：facility，分为local，remote，none 三类，对应本地记录、远程记录、不记录。记录内容：facility，共分为16 种日志信息。[admin@RouerOS] system logging facility> pri # FACILITY LOGGING PREFIX REMOTE-ADDRESS REMOTE-PORT 0 Firewall-Log remote firewall 172.16.1.254 514 1 PPP-Account none 2 PPP-Info none 3 PPP-Error none 4 System-Info none 5 System-Error none 6 System-Warning none 7 Telephony-Info none 8 Telephony-Error none 9 Prism-Info none 10 ISDN-Info none 11 Hotspot-Account none 12 Hotspot-Info none 13 Hotspot-Error none 14 IPsec-Warning none 15 IKE-Info none

5.3 命令示例：

/system logging set 0 logging=remote remote-address=172.16.1.254 remote-port=514

5.4 为了将日志信息分类，以便于LOG 服务器分析处理，可以设置log 信息的“prefix”参数，对不同的日志信息进行标示。

/ system logging facility set Firewall-Log logging=remote prefix="fw" remote-add=172.16.1.254 remote-p=514 set PPP-Account logging=remote prefix="pppoe" remote-add=172.16.1.254 remote-p=514

日志信息一定不要设置成写在本地FLASH 中，否则，MT2 的性能将显著下降。

6. 机器名称管理

1 路径：/system identity
2 功能：设置/修改系统名

6.3 示例：/system identity set name=gggggg

7. 系统时间设置

1 路径：/system clock
2 功能：设置系统时间和时区

8. 系统热启动

/system reboot

三. 物理接口的配置管理

1. 进入接口子路径：

[admin@RouerOS] interface ethernet> enable

2. 端口使能与禁用：

[admin@RouerOS] interface ethernet> enable <int_num>

或使用命令：

/int eth <int_num> disabled=yes(no)

1 禁用启动时检查网络端口状态：
2 修改端口名称

[admin@RouerOS] interface ethernet> set <numbers> disable-running-check=yes(no)

[admin@RouerOS] interface ethernet> set <numbers> name=(int-name)

网管截屏：

```
[admin@Freed] > interface ethernet
[admin@Freed] interface ethernet>Ethernet interfaces
      print  Show ethernet interfaces
        get  get value of item's property
       find  Find interfaces
        set  Change interface properties
     enable  Enable inteface
    disable  Disable inteface
     export  Export ethernet interfaces settings
      blink  Generate traffic to blink leds
    monitor
```

```
[admin@Freed] interface ethernet> pri
Flags: X - disabled, R - running
 #    NAME                MTU   MAC-ADDRESS          ARP
 0  R eth0                1500  00:90:27:74:AD:C6 enabled
 1  R eth1                1500  00:90:27:74:AD:C7 enabled
 2  R eth2                1500  00:90:27:74:AD:C8 enabled
 3  R eth3                1500  00:90:27:74:AD:C9 enabled
```

四. 查看当前配置

4.1 查看全部配置

/export 或/print

4.2 查看子项配置

如查看ip 子项的配置：/ip export

或

/ip print

五. IP 参数配置

1. 路径：

[admin@RouerOS] IP Address>

2. 功能：

配置IPAddress 、Route、Policy-routing 、DHCPclient 、DNS、Firewall、Hotspot 、IPPool 、IP Service 等等。IP 参数配置命令：

```
[admin@Freed] ip>
        accounting   Traffic accounting
           address   Address management
               arp   ARP entries management
               dns   DNS settings
          firewall   Firewall management
          neighbor   neighbors
           packing   Packet packing settings
              pool   IP address pools
             route   Route management
           service
    policy-routing
        dhcp-client   DHCP client settings
        dhcp-server   DHCP server settings
         dns-cache
           hotspot   HotSpot management
             ipsec
         telephony   IP Telephony interface
            export
```

3. 配置IP 地址及路由

3.1 配置IP Address：[admin@RouerOS] ip address>

add addr=61.155.135.1 netm=255.255.255.252 int=eth3 删除IP Addr：ip address> remove <numbers> # numbers=执行print 命令后显示的内容中的“Flags”项。

3.2 路由配置

ip route> add dst-address=0.0.0.0/0 preferred-source=0.0.0.0 \ gateway=10.255.255.1 distance=1 comment="" disabled=no

删除某条静态路由：

ip route> remove <numbers>

3.3 基于源地址的策略路由

假设某网络有3 个出口。主出口到吉通网，网关是10.255.255.1/24，PPPoE 源地址池为172.16.1.0/24；第二出口到网通网，网关是192.168.1.1/24，PPPoE 源地址池是172.16.1.0/24；[admin@RouerOS] ip policy-routing>

a) 新建路由表名：

ip policy-routing> add name=jitong

可用print 命令查看结果：

```
[admin@Freed] ip policy-routing> pri
Flags: D - dynamic
  #    NAME
  0    jitong
  1    wangtong
  2 D main
```

b) 进入路由表：

[admin@RouerOS] ip policy-routing table jitong> 添加路由项（命令见上述第3.2 项）配置结果示例如下：

```
[admin@Freed] ip policy-routing table jitong> pri
Flags: X - disabled, I - invalid, D - dynamic, R - rejected
  #    TYPE    DST-ADDRESS     G   GATEWAY       DISTANCE   INTERFACE
  0    static  0.0.0.0/0         r   192.168.1.1   1          eth0

[admin@Freed] ip policy-routing table main> pri
Flags: X - disabled, I - invalid, D - dynamic, R - rejected
  #    TYPE    DST-ADDRESS     G GATEWAY       DISTANCE   INTERFACE
  0    static  0.0.0.0/0       r 10.255.255.1  1          eth1
  1 D  connect 192.168.1.0/24  r 0.0.0.0       0          eth0
  2 D  connect 10.255.255.0/24 r 0.0.0.0       0          eth1
```

c) 配置策略路由规则：[admin@RouerOS] ip policy-routing rule> add dst-a=0.0.0.0 dst-n=0.0.0.0 src-a=172.16.2.0 src-netmask=255.255.255.0 act=lookup inte=all flow=wt table=wangtong

配置结果示例：

```
[admin@Freed] ip policy-routing rule> pri
Flags: X - disabled, I - invalid
 #   SRC-ADDRESS     DST-ADDRESS     INTE... FLOW   ACTION     TABLE
 0   172.16.1.2/32   0.0.0.0/0       all            lookup     main
 1   172.16.1.0/24   0.0.0.0/0       all     ji     lookup     jitong
 2   0.0.0.0/0       0.0.0.0/0       all            lookup     main
 3   172.16.2.0/24   0.0.0.0/0       all     wt     lookup     wang...
```

除Table main 外，其它路由表中的路由策略必须配置Flow 参数（见上表）。

§策略路由也可用下面的方法配置：

```
ip policy-routing table jitong add dst-address=0.0.0.0/0 gateway=192.168.1.1
preferred-source=0.0.0.0 \ comment="" disabled=no / ip policy-routing table main add
dst-address=0.0.0.0/0 gateway=10.255.255.1 preferred-source=0.0.0.0 \ comment="" disabled=no
```

1 基于目的地址的策略路由

2 **4. 配置Firewall**

建议用GUI 终端配置Firewall 。针对某种应用的更详细的配置参见本手册后面的“防火墙配置”章节。

4.1 防火墙对包的处理方式

```
/ ip firewall
set input name="input" policy=accept comment=""
set forward name="forward" policy=accept comment=""
set output name="output" policy=accept comment=""
```

4.2 配置**mangle**（策略路由用到）

```
/ ip firewall mangle add src-address=172.16.1.0/24:0-65535 in-interface=all \
dst-address=0.0.0.0/0:0-65535 protocol=all tcp-options=any \ icmp-options=any:any flow=""
src-mac-address=00:00:00:00:00:00 \ limit-count=0 limit-burst=0 limit-time=0s action=accept
mark-flow=ji \ tcp-mss=dont-change comment="" disabled=no add
src-address=172.16.2.0/24:0-65535 in-interface=all \ dst-address=0.0.0.0/0:0-65535
protocol=all tcp-options=any \ icmp-options=any:any flow="" src-mac-address=00:00:00:00:00:00
\ limit-count=0 limit-burst=0 limit-time=0s action=accept mark-flow="" \ tcp-mss=dont-change
```

```
comment="" disabled=yes
```

4.3 开放防火墙端口

```
/ ip firewall service-port set ftp ports=21
disabled=no set irc ports=6667
disabled=yes
```

4.4 配置**NAT**

```
/ ip firewall src-nat
add src-address=172.16.1.0/24:0-65535 dst-address=0.0.0.0/0:0-65535 \
out-interface=eth0 protocol=all icmp-options=any:any flow=ji \
limit-count=0 limit-burst=0 limit-time=0s action=masquerade \
to-src-address=172.16.1.3-172.16.1.254 to-src-port=0 comment="" \
disabled=no
add src-address=172.16.2.0/24:0-65535 dst-address=0.0.0.0/0:0-65535 \
out-interface=eth1 protocol=all icmp-options=any:any flow="" \
limit-count=0 limit-burst=0 limit-time=0s action=masquerade \
to-src-address=172.16.2.3-172.16.2.254 to-src-port=0 comment="" \
disabled=no
```

§ src-nat（原地址转换）是将数据包中的原地址进行转换；

§ dst-nat（目的地址转换）是将数据包中的目的地址进行转换。它用于让互联网用户访问私网内部的服务器（如WEB server 、FTP server），对私网上的WEB 服务器IP 进行重定向。

§ 如果action 选择masquerade （地址伪装），则to-src-address 不用设置！该选项是指将用户地址转换为该指定的地址，而不是public 端口的地址。

5. 配置**IP Service**，限定远程管理**RouerOS** 的地址和方式

```
/ ip service set telnet port=23 address=0.0.0.0/0 disabled=no set ftp port=21 address=0.0.0.0/0
disabled=no set www port=80 address=0.0.0.0/0 disabled=no set hotspot port=8088
address=0.0.0.0/0 disabled=no / ip policy-routing add name="jitong"
```

6. 配置**Hotspot**（**WEB** 认证）

```
/ ip hotspot
```

```
set hotspot-address=(ip_addr) status-autorefresh=1m auth-mac=no \
auth-mac-password=no auth-http-cookie=no http-cookie-lifetime=1d
/ ip hotspot profile
set default name="default" session-timeout=0s idle-timeout=0s only-one=yes \
tx-bit-rate=0 incoming-filter="" outgoing-filter=""
/ ip hotspot radius-client
set enabled=no accou=yes primary-serv=(ip_addr) secondary-serv=(ip_addr)\
shared-secret="" authentication-port=1812 accounting-port=1813 \
interim-update=0s
```

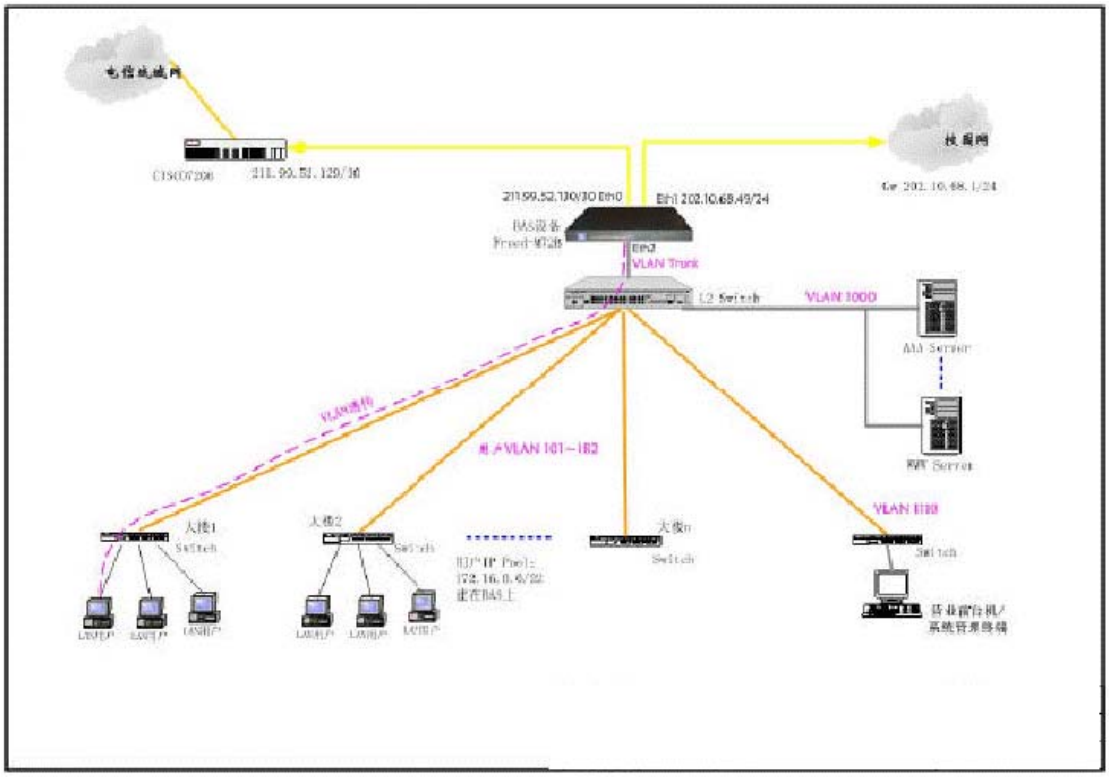
7. 配置**IP Pool**

```
/ ip pool add name="jitong" ranges=172.16.1.3-172.16.1.254 add name="dianxin"
ranges=172.16.2.3-172.16.2.254
```

8. 启用**NAT** 后的策略路由配置

应用拓扑见下面的示意图。某校园网络有教育和电信两个出口，网关分别是：202.10.68.1 和211.99.52.129。首先按正常情况配置好IP 地址、基本路由、防火墙、NAT 等。基本路由配置如下（即主路由表main）：[admin@RouerOS] ip route> pr Flags:X -disabled,I -invalid,D -dynamic,J -rejected,C -connect,S -static, r - rip, o - ospf, b -bgp

#	DST-ADDRESS	G GATEWAY	DISTANCE	INTERFACE
0	S 0.0.0.0/0	r 211.99.52.129	1	eth0
1	S 10.10.4.0/24	r 10.10.1.2	1	cdjw
2	DC 211.96.0.0/14	r 0.0.0.0	0	eth0
3	DC 202.116.68.0/22	r 0.0.0.0	0	eth1
4	DC 10.255.254.0/29	r 0.0.0.0	0	eth3
5	DC 10.10.1.0/24	r 0.0.0.0	0	cdjw
6	DC 10.5.4.0/22	r 0.0.0.0	0	v12



一个策略路由配置实例

8.1 在/ip policy-routing 下建多个路由表

其中“main”表为系统根据在/ip route 中配置的路由自动生成的。

[leitcomm@RouerOS] ip policy-routing> add ?

Creates new item with specified property values. copy-from Item

number name The name of the routing table

[leitcomm@RouerOS] ip policy-routing> pri

Flags: D - dynamic

NAME

0 jiaoyu 1 D main 这里“jiaoyu”表的配置如下:

[leitcomm@RouerOS] ip policy-routing> tab jiao [leitcomm@RouerOS] ip policy-routing table jiaoyu> pri

Flags: X - disabled, I - invalid, D - dynamic, R - rejected

TYPE DST-ADDRESS G GATEWAY DISTANCE INTERFACE

0 static 0.0.0.0/0 r 202.116.68.1 1 eth1

8.2 建立策略路由规则

[leitcomm@RouerOS] ip policy-routing rule> add ?

Creates new item with specified property values.

action Rule action

comment Set comment for items

copy-from Item number

disabled Defines whether the rule is disabled or not

dst-address Destination address

dst-netmask Destination mask

flow Flow mask of the packet to be mached by this rule

interface The name of the interface

place-before Item number

src-address Source address

src-netmask Source mask

table Routing table

[leitcomm@RouerOS] ip policy-routing rule> pri

Flags: X - disabled, I - invalid

SRC-ADDRESS DST-ADDRESS INTERFACE FLOW ACTION TABLE

0 0.0.0.0/0 202.10.68.49/32 all lookup main

1 0.0.0.0/0 0.0.0.0/0 all jiaoyu lookup jiaoyu

2 0.0.0.0/0 0.0.0.0/0 all lookup main

注意为使用指定的路由表打上flow 标记。

8.3 在防火墙src-nat 中配置相应规则

[leitcomm@RouerOS] ip firewall src-nat> pri

Flags: X - disabled, I - invalid, D - dynamic

0 src-address=172.16.0.0/22:0-65535 dst-address=0.0.0.0/0:0-65535 out-interface=eth0 protocol=all icmp-options=any:any flow="" connection="" content="" limit-count=0 limit-burst=0 limit-time=0s **action=nat** to-src-address=211.96.14.194 to-src-port=0-65535 1src-address=0.0.0.0/0:0-65535dst-address=0.0.0.0/0:0-65535out-interface=eth1 protocol=all icmp-options=any:any **flow=jiaoyu** connection="" content="" limit-count=0 limit-burst=0 limit-time=0s **action=nat to-src-address=202.116.68.49** to-src-port=0-65535 注：**action** 选**nat**，到非缺省目的地的路由**flow** 要标记。并定义**to-src-address**。

2 ;;; masquerade hotspot temporary network src-address=192.168.0.0/22:0-65535 dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=all icmp-options=any:anyflow=""connection=""content=""limit-count=0limit-burst=0 limit-time=0s action=nat to-src-address=211.96.14.194 to-src-port=0-65535 3 ;;; masquerade hotspot network src-address=10.5.4.0/22:0-65535 dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=all icmp-options=any:anyflow=""connection=""content=""limit-count=0limit-burst=0 limit-time=0s action=nat to-src-address=211.96.14.194 to-src-port=0-65535

8.4 配置防火墙**mangle**

[leitcomm@RouerOS] ip firewall mangle> pri Flags: X - disabled, I - invalid, D - dynamic 0 src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=202.116.68.49/32:0-65535 protocol=all tcp-options=any icmp-options=any:any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=accept mark-flow="" tcp-mss=dont-change mark-connection="" 1 src-address=0.0.0.0/0:0-65535 in-interface=all **dst-address=202.112.0.0/16**:0-65535 protocol=all tcp-options=any icmp-options=any:any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=accept **mark-flow=jiaoyu** tcp-mss=dont-change mark-connection="" 2 src-address=0.0.0.0/0:0-65535 in-interface=all **dst-address=116.111.0.0/16**:0-65535 protocol=all tcp-options=any icmp-options=any:any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=accept **mark-flow=jiaoyu** tcp-mss=dont-change mark-connection="" 3 src-address=0.0.0.0/0:0-65535 in-interface=all **dst-address=202.117.0.0/16**:0-65535 protocol=all tcp-options=any icmp-options=any:any flow="" connection="" content=""

src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=accept **mark-flow=jiaoyu** tcp-mss=dont-change mark-connection="" 4 src-address=0.0.0.0/0:0-65535 in-interface=all **dst-address=202.116.0.0/16**:0-65535 protocol=all tcp-options=any icmp-options=any:any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=accept **mark-flow=jiaoyu** tcp-mss=dont-change mark-connection="" 5 src-address=0.0.0.0/0:0-65535 in-interface=all **dst-address=162.105.0.0/16**:0-65535 protocol=all tcp-options=any icmp-options=any:any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=accept **mark-flow=jiaoyu** tcp-mss=dont-change mark-connection="" 注：必须针对每一目的地址段做**mangle** 策略。

六. 配置**ppp** 参数

[admin@RouerOS] ppp> secret profile active radius-client export Description of settings: [admin@RouerOS] ppp secret> add create new item comment adds comment to item disable disables items enable enables items find finds items by value get get value of item's property set change item properties print print values of item properties remove remove item export [admin@RouerOS] ppp secret> add creates new item with specified property values. caller-id comment short description of the item copy-from item number disabled local-address name password profile remote-address routes service

1. 配置PPP 模板

```
/ ppp profile
add name="dianxin_p" local-address=172.16.2.2 remote-address=dianxin \
session-timeout=0s idle-timeout=0s use-compression=no \
use-vj-compression=no use-encryption=no require-encryption=no only-one=no \
tx-bit-rate=0 rx-bit-rate=0 incoming-filter="" outgoing-filter=""
add name="jitong_p" local-address=172.16.1.2 remote-address=jitong \
session-timeout=0s idle-timeout=0s use-compression=no \
use-vj-compression=no use-encryption=no require-encryption=no only-one=no \
tx-bit-rate=0 rx-bit-rate=0 incoming-filter="" outgoing-filter=""
```

2. 配置Radius-client

/ ppp radius-client set enabled=yes accounting=yes primary-server=10.255.255.62 \

secondary-server=0.0.0.0 shared-secret="11198001" \

authentication-port=1812 accounting-port=1813 interim-update=5m 设置PPPoE 认

证在本机上：

□ ①禁用Radius 项[admin@RouerOS] ppp radius-client> set ena=no [admin@RouerOS] ppp radius-client> pri enabled: no accounting: yes primary-server: 10.255.255.62 secondary-server: 0.0.0.0 shared-secret: "11198001" authentication-port: 1812 accounting-port: 1813 interim-update: 5m

□ ②设置新的认证项

[admin@RouerOS] ppp secret> add name=lei pass=lei serv=any [admin@RouerOS] ppp secret> pri det

Flags: X - disabled 0 name="lei" service=any caller-id="" password="lei" profile=dianxin_p

local-address=0.0.0.0 remote-address=0.0.0.0 routes=""

关于pppoe 帐号容许同时在线认证的次数，与接入网关无关，只与Radius 服务器的配置和认证程序设计有关。在Radius 的Radchek 库表中，为用户增加属性项目Simultaneous-Use，其参数符为“：”，参数值为数字。

如果采用BAS 本地认证，则MT2 的 /PPPProfile 配置项下的only-one 参数设置为yes 时，标示账号只容许唯一在线。

七. PPPoE 配置配置步骤：

□ ①确定pppoe 用户端口和vlan、认证通过后的出口和vlan；

□ ②配置 /IP pool。Pool 长度可以大于256Hosts；

□ ③配置 /PPP Profile；

□ ④配置 /ppp radius-client；

□ ⑤配置 / int pppoe-server server；

□ ⑥配置 /ip firewall src-nat，对ip pool 中的地址进行转换或路由。注意掩码要正确。

□ ⑦配置 /radius，必须指定authication-port 和accounnting-port 号。/ interface pppoe-server server add service-name="jitong" interface=eth2 mtu=1492 mru=1492 \ authentication=chap keepalive-timeout=10 default-profile=jitong_p \ disabled=no add service-name="dianxin" interface=eth2 mtu=1492 mru=1492 \ authentication=chap keepalive-timeout=10 default-profile=dianxin_p \ disabled=no add service-name="crcnet" interface=user mtu=1492 mru=1492 \ authentication=chap keepalive-timeout=10 default-profile=crcnet_p \ disabled=no

PPPoE 的mtu 值必须设置为1492！mru 值必须与mtu 值一致。PPPoE 认证方式选chap，不能选mschap2。

interface 是pppoe 用户接入的vlan 或端口。如果用户分布在多个vlan 或ports，则应

为每个vlan 或port 做上述相应配置。对于vlan 模式，MT2 与边缘接入交换机对接的端口（如上述例子中的eth2）应配置为vlan trunk，即同属于多个用户vlan。

如果要将pppoe 认证改在MT2 本机上进行，则需在/ppradius-client 下禁用radius，然后在/ppp secret 下做相应配置。

配置pppoe-s serv 时必须注意要设置disabled=no；配置ip route 时gateway 必须是对端路由器接口的ip 地址；PC 终端网卡的IP 不能设置为RouerOS 中的某个接口地址段中的地址，否则该PC 可能不能正常访问该地址段的网络。

«上部完，下部稍候推出，请关注，谢谢。»

ISP级软件路由器之王

RouerOS 宽带接入服务器

用户手册(下部)

——配置指南

RouerOS 系列宽带接入服务器配置指南内容摘要

八. HOTSPOT 配置

Hotspot 的工作原理是：用户打开浏览器，浏览器将地址解析请求发给DNS 服务器，DNS 完成地址解析后反馈给客户端所以在保证BAS 的Hotspot 配置正确的情况下，要令客户端在打开浏览器时弹出认证窗口，必须保证BAS 与DNS 的路由畅通。

方法一. 使用setup 向导：

[admin@RouerOS] ip hotspot>

reset-html Reset current hotspot HTML page

active HotSpot active user list

profile HotSpot user profile management

user HotSpot local user list

server HotSpot DHCP profile management

aaa AAA (Authentication, Authorization and Accounting) configuration

cookie HotSpot active HTTP cookie list

print Print current configuration and status

get Get value of configuration property

set Change hotspot configuration

export Export hotspot settings

setup Setup wizard for hotspot configuration

universal Universal client configuration

在配置第一个hotspot 接口时建议使用向导，这样可以快速的完成配置。注意，如果要通过AAA 服务器计费，则需配置/radius 和/ip hotspot aaa。

方法二. 手工配置：可以使用add copy-from 命令,下面蓝色部分为新增加的配置。

在完成第一个接口的配置后，后续的接口配置只能以手工的方式进行。

□ 1. 配置/ip hot profile //认证账户属性要关联profile [admin@RouerOS] ip hotspot profile> pri Flags: * - default 0 * name="default" session-timeout=0s idle-timeout=0s only-one=yes

□ tx-bit-rate=0 rx-bit-rate=0 incoming-filter="" outgoing-filter="" mark-flow="hs-auth" login-method=smart keepalive-timeout=2m hotspot 认证使用动态ip 还是静态ip 在profile 中由login-method 配置。

□ 2. 配置/ip pool [admin@RouerOS] ip pool> pri # NAME RANGES 0 hs-pool-temp 192.168.0.2-192.168.3.254 1 hs-pool-real 10.5.4.1-10.5.5.0 10.5.5.2-10.5.7.254

□ 新增加一个ip pool：[admin@RouerOS] ip pool> add name=hs-pool-real1 ranges=10.25.25.2-10.25.25.254

□ 3. 配置/ip add 在Hotspot 接口上配置IP，作为客户端的静态网关或dhcp_serv 的网关：

[admin@RouerOS] ip address> pri Flags: X - disabled, I - invalid, D - dynamic # ADDRESS NETWOR

BROADCAST INTERFACE 0 10.255.255.200/24 10.255.255.0 10.255.255.255 eth0 1 ;;; hotspot temporary network 192.168.0.1/22 192.168.0.0 192.168.3.255 v12 2 ;;; hotspot network 10.5.5.1/22 10.5.4.0 10.5.7.255 v12

☐ 3 10.25.25.1/24 10.25.25.0 10.25.25.255 eth1

☐ 4. 配置/ip dhcp-server [admin@RouerOS] ip dhcp-server> pri Flags: X - disabled, I - invalid 0 name="hs-dhcp-server" interface=v12 lease-time=14s address-pool=hs-pool-temp netmask=22 gateway=192.168.0.1 src-address=0.0.0.0 dns-server=202.103.96.112 domain="" wins-server="" add-arp=yes

☐ # 新增加一个dhcp-server，注意gateway 参数1 name="hs-dhcp-s1" interface=eth1 lease-time=14s address-pool=hs-pool-real1 netmask=24 gateway=10.25.25.1 src-address=0.0.0.0 dns-server=202.103.96.112 domain="" wins-server="" add-arp=no

2 5. 配置/ip hot server //可以不用增加配置[admin@RouerOS] ip hotspot server> pri 0 name="hs-server" dhcp-server=hs-dhcp-server lease-time=1m login-delay=10s address-pool=hs-pool-real netmask=22 gateway=10.5.5.1

1 name="hs-s1" dhcp-server=hs-dhcp-s1 lease-time=1m login-delay=10s

address-pool=hs-pool-real1 netmask=22 gateway=10.25.25.1

6. 配置防火墙规则 //可以不用配置

① /ip fire rule forw：[admin@RouerOS] ip firewall rule forward> pri Flags: X - disabled, I - invalid, D - dynamic 0 ;;; limit access for unauthorized hotspot clients

src-address=192.168.0.0/22:0-65535 in-interface=v12 dst-address=0.0.0.0/0:0-65535

out-interface=all protocol=all icmp-options=any:any tcp-options=any connection-state=any

flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0

limit-time=0s action=jump jump-target=hotspot-temp log=no

下面是新增加的接口eth1 1 ;;; limit access for unauthorized hotspot clients

src-address=10.25.25.0/24:0-65535 in-interface=eth1 dst-address=0.0.0.0/0:0-65535

out-interface=all protocol=all icmp-options=any:any tcp-options=any connection-state=any

flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0

limit-time=0s action=jump jump-target=hotspot-temp log=no

2 ;;; account traffic for authorized hotspot clients src-address=0.0.0.0/0:0-65535

in-interface=all dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=all

icmp-options=any:any tcp-options=any connection-state=any flow="" connection=""

content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s

action=jump jump-target=hotspot log=no

②配置/ip fire rule hotspot-temp: [admin@RouerOS] ip firewall rule hotspot-temp> pri Flags: X - disabled, I - invalid, D - dynamic 0 ;;; return, if connection is authorized src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=all icmp-options=any:any tcp-options=any connection-state=any flow=hs-auth connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=return log=no 1 ;;; allow ping requests src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=icmp icmp-options=any:any tcp-options=any connection-state=any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=return log=no 2 ;;; allow dns requests src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:53 out-interface=all protocol=udp icmp-options=any:any tcp-options=any connection-state=any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=return log=no 3 ;;; reject access for unauthorized hotspot clients src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=all icmp-options=any:any tcp-options=any connection-state=any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=reject log=no

7. 配置防火墙NAT

① src-nat：[admin@RouerOS] ip firewall src-nat> pri Flags: X - disabled, I - invalid, D - dynamic 0 ;;; masquerade hotspot temporary network src-address=192.168.0.0/22:0-65535 dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=all icmp-options=any:any flow="" connection="" content="" limit-count=0 limit-burst=0 limit-time=0s action=masquerade to-src-address=0.0.0.0 to-src-port=0-65535 1 ;;; masquerade hotspot network src-address=10.5.4.0/22:0-65535 dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=all icmp-options=any:any flow="" connection="" content="" limit-count=0 limit-burst=0 limit-time=0s action=masquerade to-src-address=0.0.0.0 to-src-port=0-65535

2 ;;; masquerade hotspot network src-address=10.25.25.0/24:0-65535 dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=all icmp-options=any:any flow="" connection="" content="" limit-count=0 limit-burst=0 limit-time=0s action=masquerade to-src-address=0.0.0.0 to-src-port=0-65535

□ ② dst-nat：[admin@RouerOS] ip firewall dst-nat> pri Flags: X - disabled, I - invalid, D - dynamic 0 ;;; accept authorized connections

src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:0-65535 protocol=all icmp-options=any:any flow=hs-auth connection="" content="" src-mac-address=00:00:00:00:00:00

limit-count=0 limit-burst=0 limit-time=0s action=accept to-dst-address=0.0.0.0 to-dst-port=0-65535 1 ;;; redirect unauthorized hotspot clients to hotspot service src-address=192.168.0.0/22:0-65535 in-interface=v12 dst-address=0.0.0.0/0:0-65535 protocol=tcp icmp-options=any:any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=redirect to-dst-address=0.0.0.0 to-dst-port=80

下面是新增加的配置项eth1。可以使用add copy-from 命令：2 ;;; redirect unauthorized hotspot clients to hotspot service src-address=10.25.25.0/24:0-65535 in-interface=eth1 dst-address=0.0.0.0/0:0-65535 protocol=tcp icmp-options=any:any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=redirect to-dst-address=0.0.0.0 to-dst-port=80

九. VLAN 配置

/ interface vlan add name="acc" mtu=1500 arp=enabled vlan-id=100 interface=eth3 disabled=no

结果示例：

```
[admin@Freed] interface vlan> pri
Flags: X - disabled, R - running
 #     NAME                MTU   ARP        VLAN-ID INTERFACE
 0   R acc                 1500  enabled        100 eth3
 1   R office              1500  enabled        101 eth3
 2   R finance             1500  enabled        102 eth3
```

给vlan 分配IP：在/ip address 子路径下配置/ip address add addr=192.168.5.1/24 int=acc

注意MT2 将vlan 当做物理接口，上述命令中interface 参数是vlan 的名称，而不是“vlan+ID”。结果示例：

```
[admin@Freed] ip address> pri
Flags: X - disabled, I - invalid, D - dynamic
 #     ADDRESS            NETWORK         BROADCAST       INTERFACE
 0     192.168.1.239/24   192.168.1.0     192.168.1.255   eth0
 1     10.255.255.10/24   10.255.255.0    10.255.255.255  eth1
 2     192.168.4.1/24     192.168.4.0     192.168.4.255   acc
 3     192.168.5.1/24     192.168.5.0     192.168.5.255   office
 4     192.168.6.1/24     192.168.6.0     192.168.6.255   finance
```

表中interface 项的acc、office、finance 均为vlan 名称。

十. VPN 配置

10.1 PPTP VPN

10.1.1 PPTP Server

□ ① [admin@RouerOS] interface pptp-server server> set enabled=yes authentication=chap,mschap1,mschap2 default-profile=pppoe mru=1484 mtu=1484 [admin@RouerOS] interface pptp-server server>pr enabled: yes mtu: 1484 mru: 1484 authentication: mschap2,mschap1,chap default-profile: pppoe

□ ② [admin@RouerOS] interface pptp-server> add name=pptp-s user=vinson disabled=no [admin@RouerOS] interface pptp-server> pr Flags: X - disabled, D - dynamic, R - running # NAME USER MTU CLIENT-ADDRESS UPTIME ENCODING 0 pptp-s vinson

10.1.2 PPTP Client

[admin@RouerOS] interface pptp-client> add name=pptp-c connect-to=61.234.253.126 user=lei password=woyhj998 profile=default disabled=no [admin@RouerOS] interface pptp-client> pr Flags: X - disabled, R - running 0 name="pptp-c" mtu=1460 mru=1460 connect-to=61.234.253.126 user="lei" password="woyhj998" profile=default add-default-route=no

10.2 EOIP VPN

①在/int eoip 创建eoip 隧道接口：

[leitcomm@RouerOS] interface eoip> add Creates new item with specified property values. arp Address Resolution Protocol copy-from Item number disabled Defines whether eoip interface is disabled or not mtu Maximum Trasfer Unit name Tunnel name remote-address Remote address of tunnel tunnel-id Tunnel identity [leitcomm@RouerOS] interface eoip> pri Flags: X - disabled, R - running 0 R name="cdjw" mtu=1500 arp=enabled remote-address=218.75.129.134 tunnel-id=10

②给建立的EoIP 接口添加IP：

[leitcomm@RouerOS] ip address> pri Flags: X - disabled, I - invalid, D - dynamic # ADDRESS NETWORK BROADCAST INTERFACE 5 10.10.1.2/24 10.10.1.0 10.10.1.255 cdjw

十一. DHCP 配置

11.1 DHCP Server

[admin@RouerOS] ip dhcp-server> DHCP protocol allows dynamic configuration of IP addresses of hosts on the network. Router can run DHCP service to provide hosts on attached networks with

IP addresses. print Show DHCP settings find Find DHCP interfaces set Change DHCP settings add create new item remove remove item enable enables items disable disables items export Export DHCP settings lease DHCP leases 在端口eth3 上创建一个名叫“eth3”的新的DHCPServer，使用地址池（在ippool 中预先定

义）pool1=172.16.1.5-172.16.1.254，网关为该段地址中的172.16.1.1：[admin@RouerOS] ip dhcp-server> add name=”eht3” inter=eth3 leas=14000 address-p=pool1 gate=172.168.1.1

[admin@RouerOS] ip dhcp-server> pri Flags: X - disabled, I - invalid 0 name="eth3" interface=eth3 lease-time=3h53m20s address-pool=pool1 netmask=0.0.0.0 gateway=172.16.1.1 src-address=0.0.0.0 dns-server="" domain="" wins-server="" add-arp=no

1 **MAC 地址(及IP 地址)与端口绑定**

2 **1. 将指定端口的arp 设置为“reply-only”**

[admin@RouerOS_ZSU] interface ethernet> set 3 arp=reply-only [admin@RouerOS_ZSU] interface ethernet> pr Flags: X - disabled, R - running # NAME MTU MAC-ADDRESS ARP 0 R eth0 1500 00:90:27:74:AD:AA enabled 1 R eth1 1500 00:90:27:74:AD:AB enabled 2 R eth2 1500 00:90:27:74:AD:AC enabled 3 R eth3 1500 00:90:27:74:AD:AD reply-only

2. 手动添加MAC 地址（IP 地址）表一对静态地址方式

在/ip arp 子项下添加：

[admin@RouerOS_ZSU] ip arp> add addr=10.255.255.58 mac-address=00:07:AA:39:11:B8 int=eth3 disabled=no

[admin@RouerOS_ZSU] ip arp> pr

Flags: X - disabled, I - invalid, H - DHCP, D - dynamic

#	ADDRESS	MAC-ADDRESS	INTERFACE
0 D	211.97.52.74	00:06:28:8A:F4:07	eth0
1 D	202.116.68.1	00:30:6D:D6:71:40	eth1
2 D	211.97.117.147	00:06:28:8A:F4:07	eth0
3 D	211.96.187.155	00:06:28:8A:F4:07	eth0
4 D	211.96.31.245	00:06:28:8A:F4:07	eth0
5	10.255.255.58	00:07:AA:39:11:B8	eth3

3. 自动绑定MAC 地址一DHCP 方式

在/ip dhcp-server 项下设置“add-arp=no”：[admin@RouerOS_ZSU] ip dhcp-server> pr Flags: X - disabled, I - invalid 0 name="hs-dhcp-server" interface=v12 lease-time=14s address-pool=hs-pool-temp netmask=22 gateway=192.168.0.1 src-address=0.0.0.0 dns-server=202.103.96.112 domain="" wins-server="" add-arp=no

十二．防火墙配置

12.1 防“冲击波”病毒

/ip fire rule forword> [admin@xinhua] ip firewall rule forward> pr Flags: X - disabled, I - invalid, D - dynamic 0 src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=all icmp-options=any:any tcp-options=any connection-state=established flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=accept log=no 1 src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:135-139 out-interface=all protocol=tcp icmp-options=any:any tcp-options=any connection-state=any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=drop log=no 2 src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:445 out-interface=all protocol=tcp icmp-options=any:any tcp-options=any connection-state=any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=drop log=no 3 src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:135-139 out-interface=all protocol=udp icmp-options=any:any tcp-options=any connection-state=any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=drop log=no 4 X src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=icmp icmp-options=any:any tcp-options=any connection-state=any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=drop log=no 第1，2，3 条规则用于防止冲击波病毒对内网的攻击。[admin@xinhua] ip firewall rule input> pr Flags: X - disabled, I - invalid, D - dynamic 0 src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:135-139 out-interface=all protocol=tcp icmp-options=any:any tcp-options=any connection-state=any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=drop log=no 1

src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:445 out-interface=all protocol=tcp icmp-options=any:any tcp-options=any connection-state=any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=drop log=no 2 X src-address=0.0.0.0/0:0-65535 in-interface=all dst-address=0.0.0.0/0:0-65535 out-interface=all protocol=icmp icmp-options=any:any tcp-options=any connection-state=any flow="" connection="" content="" src-mac-address=00:00:00:00:00:00 limit-count=0 limit-burst=0 limit-time=0s action=drop log=no 第0，1 条规则用于防范冲击波病毒对RouerOS 本身的攻击。

十三. 配置文件的备份与恢复

1 1. 显示文件系统

2 2. 备份配置文件

/file print

方法一：

/system backup> save name <file_name> 这种方式备份的文件为压缩文件，不能用Windows 的notepad 打开。方法二：

/export file=<file_name> 这种方式保存的文件为.rsc 文件，可以用 notepad 打开。

另外在每个子路径下可以用"Export"命令以文本文件的方式备份该子路径下的配置，如：/ip > export file=ip # 这里"ip"是定义的文件名

3. 恢复配置文件

/system backup> load name =<file_name> 或/import <file_name>

4. 配置文件上载与下载

从可以远程登录到RouerOS2 的PC 上用ftp 方式上载和下载配置文件。备份的配置文件保存在根目录下。注意下载时应切换到二进制模式（bin）。

ftp> get <file_name>

5. 配置复位

将配置清空恢复到缺省配置：

/system reset

6. 查看系统资源状况

/system resource monitor

7. 监视端口流量

/int monitor-traffic eth0 interval=4

Reference：

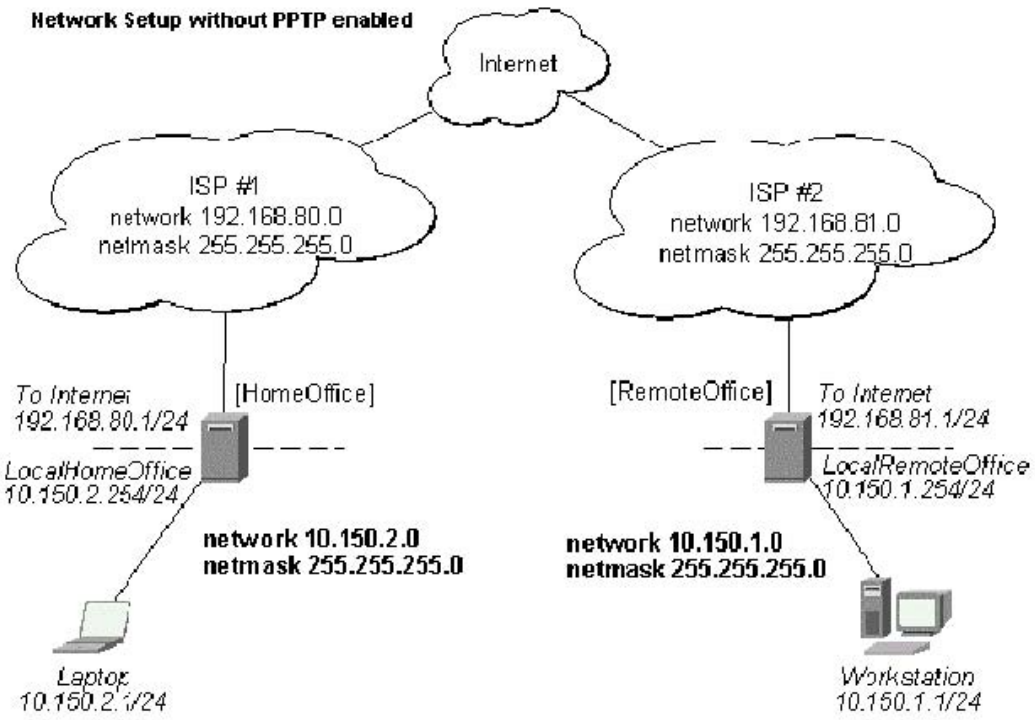
1 1. 用户带宽限制，需要与Radius 服务器配合。如果采用RouerOS 本地认证，则可以在相应的profile 中设置一组用户的带宽。
2 2. 基于用户名的访问控制：在接入网关的① ppp profile 中设置incoming-filter 和 outgoing-filter；

□ ②在firewall rule 中设置ppp 的相应规则；
□ ③在Radius 中用“filter-ID”返回给接入网关，接入网关据此执行相应filter。

3. 在vlan 中禁用arp，可以防止用户配置静态IP 而不用PPPoE 认证上网。

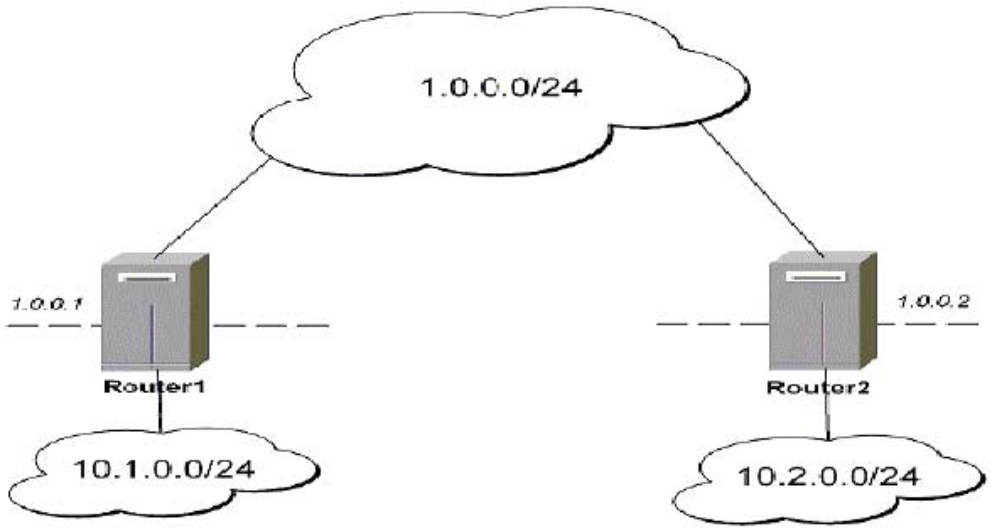
4. VPN

①移动VPN，使用pptp 或L2tp（v2.6.10 以后版本支持）

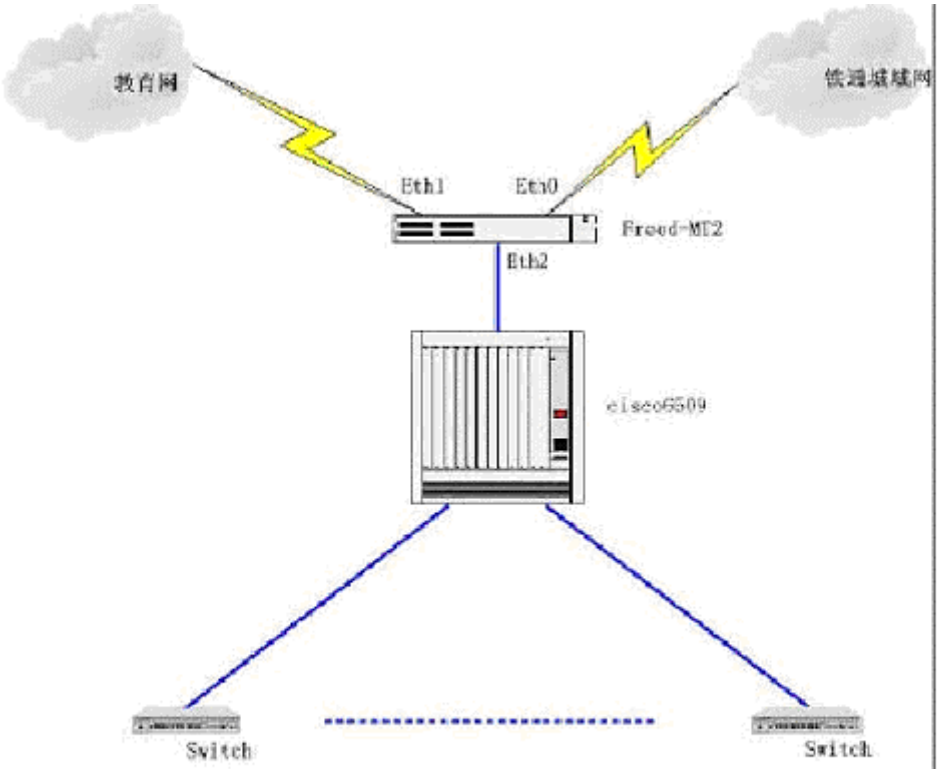


② 点对点 VPN（局域网远程互联）

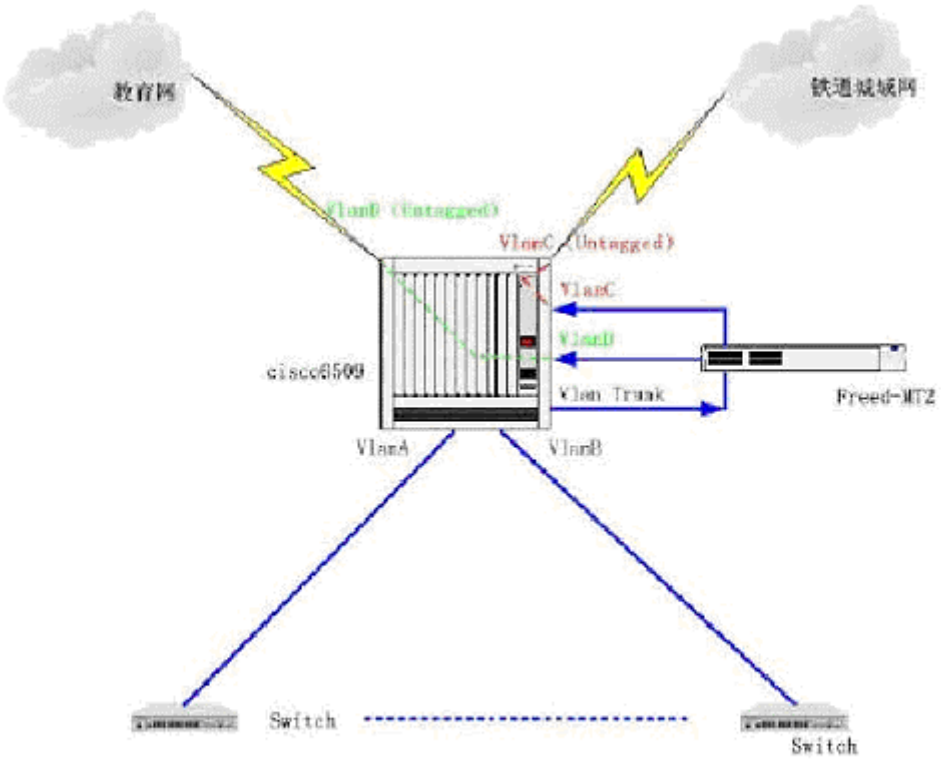
有三种方式：IPIP，EoIP，IPSec。



5. Rouer0S2 的两种应用模式（策略路由的一个例子）



RouterOS 应用模式一



RouterOS 应用模式二

6. 检测端口利用情况：[admin@xinhua] interface> monitor eth0 interval 4

received-packets-per-second: 1228 received-bits-per-second: 7.6Mbps

sent-packets-per-second: 985

sent-bits-per-second: 784kbps

7. RouerOS 提供的内置工具在子路径/tool 下。

《全文完，谢谢阅读，RouterOS原版说明书正在翻译中，敬请期待》

服务网址：www.Router.net.cn

中文域名：软件路由器

服务范围：软件路由器开发、改写，路由器配件电子硬盘、CF-IDE、服务器网卡、服务器主板、SCSI卡、工控机箱等。

免费技术热线：0771-2577076