ws RouterOS 常见问题 2017 版

编: 余松 Web: <u>www.irouteros.com</u> 更新日期 2017-06-12



目	录	1
什么,	是 MikroTik RouterOS?	5
1、	RouterOS 是什么?	5
2、	在购买 MikroTik RouterOS x86 平台许可前是否可以测试该软件?	5
3、	能否使用 MikroTik 路由器连接一个运营商设备的 T1, T3 或者其他高速接口?	5
4、	运行速度如何?	5
5、	MikroTik RouterOS 是否支持多 CPU 处理?	6
6、	MikroTik RouterOS 是否支持 SATA、USB 和 SCSI 安装	6
7、	软件路由相对于 Cisco 路由器如何?	6
8、	MikroTik RouterOS 支持那些硬件平台,有什么区分?	6
9、	MikroTik RouterOS 是否需要其他 OS (操作系统) 支持?	6
10	、安装后路由器的安全如何?	6
11	、MikroTik RouterOS script(脚本)有什么作用?	6
13	、什么是 CHR?	6
14	、为什么在 CHR 虚拟平台是基于 64bit 处理器构架?	7
15	、CHR 系统要求是什么?	7
16	、MikroTik 的 RouterBOARD、CCR 和 CRS 等产品是什么?	7
12	、为什么 RouterBOARD 的 1.2GHz 处理器在数据转发能力超过我的 2GHz PC 处理器?	7
17	、MikroTik 硬件产品采用哪些平台?	7
Route	erOS 安装	8
1、	RouterOS 的安装方式有那些?	8
2、	安装 MikroTik RouterOS 支持多大的硬盘空间?	8
3、	MikroTik RouterOS 是否支持多个硬盘?	9
5、	在 PC 上安装完成后,为什么 RouterOS 引导失败无法正常启动?	9
6、	在 RouterOS 的原有硬盘上,我是否可以覆盖安装其他操作系统?	9
Route	erOS 登录和密码	9

Vu	c
ru	э.

1,	第一次登录路由器的管理帐号和密码是什么?	9
2	如何使用 Winbox 登录 RouterOS	9
÷	推荐使用 Winbox v3 版本	.13
3、	我如何恢复丢弃的密码?	.16
4、	当 MikroTik RouterOS 启动失败,如何处理?	.16
5、	如果的 LAN 接口被禁用,如何访问路由器?	.16
Route	erOS 正版注册问题	.16
1,	RouterOS 正版有哪些等级?	.16
2、	注册软件后,是否可以改变注册码等级?	.17
3、	MikroTik RouterOS 注册许可什么?	.17
4、	如何购买正版许可	.17
5、	注册许可是否有期限?	.18
6、	在没有丢失我的软件许可码时,如果重新安装 MikroTik RouterOS?	.18
7、	CHR 许可是什么	.18
8、	我能否将 MikroTik RouterOS 使用到不同的硬件上?	.18
9、	如果我安装 MikroTik RouterOS 的硬盘坏掉了,我应该怎么处理?	.19
10	、我如何导入软件注册码?	.19
11	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19
11 12	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19
11 12 升级	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19
11 12 升级 1、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .19
11 12 升级: 1、 2、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .19 .19
11 12 升级 1、 2、 3、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .19 .19 .19
11 12 升级 1、 2、 3、 4、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .19 .19 .19 .21
11 12 升级 1、 2、 3、 4、 5、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .19 .19 .21 .21
11 12 升级 1、 2、 3、 4、 5、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .19 .21 .21 .22 .22
11 12 升级 1、 2、 3、 4、 5、 6、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .19 .21 .21 .22 .24 .24
11 12 升级 1、 2、 3、 4、 5、 6、 Route	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .19 .21 .21 .22 .24 .24 .25
11 12 升级 1、 2、 3、 4、 5、 6、 Route 1、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .19 .21 .21 .22 .24 .25 .25
11 12 升级 1、 2、 3、 4、 5、 6、 Route 1、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .19 .21 .21 .22 .24 .24 .25 .25 .26
11 12 升级 1、 2、 3、 4、 5、 6、 Route 1、 1、 2、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .21 .21 .22 .24 .24 .25 .25 .26 .26
11 12 升级 1、 2、 3、 4、 5、 6、 Route 1、 1、 2、 3、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?	.19 .19 .19 .19 .21 .21 .22 .24 .24 .25 .25 .26 .26 .26
11 12 升级 1、 2、 3、 4、 5、 6、 Route 1、 1、 2、 3、 4、	、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办? 、如果我丢失了 RouterBOARD,是否能给一个注册码到其他系统上的 RouterOS? 与降级	.19 .19 .19 .19 .21 .21 .22 .24 .25 .25 .26 .26 .26 .26

Va	C
ıи	о.

fus	
6、我的 RB750/G 系统损害,要重新通过 Netinstall 安装软件,但没有 Console 口该怎么	办?27
7、如何升级 RouterBOARD 的固件	27
8、RouterOS 添加 IP 地址后,路由器的网卡和我的电脑在同一局域网,且在同一网段, 能 ping 通路由器	但为什么不
9、我有两张网卡在 RouterOS 上,并能正常运行,同时能在路由器上 ping 通两个网络, 个网络 ning 到另外一个网络或到互联网,我并没有设置防火墙规则?	但无法从一 28
12 我能否在 DHCP 中继完每个田户的 IP 和 MAC 抽址?	28
13、加何能隐藏两个不同子网段到不同的两个外网 IP 地址?	28
14、当我使用 PPPoF 上网时,为什么不能正堂的访问某些网站?	28
什么是 Fast Path?	
TT 公定 Fust Fut T	29
1、RouterOS 简单上网配置	29
第一步,网络接口配置	30
第一步: 四相及口配量	30
第二步: 添加 II 22	31
第四步,NAT 地址转换	
第五步, DNS 配置	
10、如何修改我的 telnet 或者 HTTP 服务的 TCP 端口?	
18、如何备份或导入 RouterOS 配置	
2、如何设置端口映射?	
3 、如何设置单机带宽控制?	
4、如何设置 ADSL/PPPoE 拨号配置?	
5、如何配置 DHCP 客户端	
6、如何配置 DHCP 服务器	
7、如何设置 ARP 绑定?	41
19、RouterOS 策略路由方式有那些?	42
8 、如何做端口策略路由:	42
9 、如何配置网关断线处理?	44
23、firewall filter 里如何理解 input、foreword 和 ouput 的过滤规则?	45
16、如何使用防火墙过滤指定的端口?	46
15、如何禁止 192.168.0.11 的 IP 地址上网?	47
17、我如何导出防火墙配置,并用到其他 RouterOS 上?	47
16、如何使用 L7 脚本	47
11、如何配置 PPTP 和 L2TP 服务器	50
12、创建 PPPoE Server	53

YuS

YuS	
13、如何配置 Hotspot 认证	58
14、如何使用 Log Downloader 下载并记录访问日志	66
15、如何配置 Web 代理	67
24、如果理解 mangle 标记,什么是 prerouting,有什么作用?	69
17、如何配置 PCC 的 mangle 路由标记	69
20、Nth 和 PCC 有什么区别?	69
21、什么是 PCQ 动态流控?	70
10、如何设置 simple queue 里的 PCQ 限速	70
22、什么是 HTB?	72
如何配置两张网卡的二层桥接?	73
Wlan 无线应用 FAQ	73
1、 应该把中心 AP 放在那里?	73
2、构建一个中心基站需要什么?	73
3、一个中心基站能连接多少个客户端?	73
4、我需要连接一个客户端的网络,应该怎么做?	73
5、每个系统的传输速度如何?	74
6、能否限制每个用户的带宽?	74
7、中心基站与客户端之间无线传输最大距离能达到多少?	74
8、我能否从设备使用更长的馈线连接到天线?	74
9、我是否使用功率放大器增加距离?	74
10、无线连接是否要求在视线范围内?	74
11、什么是 Fresnel 区?	74
12、我是否可以将两个无线网络桥接?	75
13、安装一个 Wlan 无线系统需要多长时间?	75
14、Wlan 运行在 Station 模式下是否能做桥接?	75
15、Wlan 桥接模式一般使用哪种?	75
16、802.11n 或 ac 能使用 wds 模式吗?	75
17、RouterOS 最大的 5G 传输带宽能达到多少	75
18、mode=bridge 模式支持那种连接方式	75
19、什么是 Nstreme	75
20、什么是 Nstreme Dual	75
21、什么是 Nv2 协议	76
21、WLAN 与 WiFi 区别	76
22、RB751U 天线选择问题	76

802.11	无线配置	.76
1、女	四何配置无线点对点	.76
2 、女	四何设置 RouterOS 无线 AP 覆盖上网	.80
3、女	四何隐藏 WLAN 的 SSID	.84
4、女	如何使用 Access-list 控制客户端	.84
5、女	四何创建虚拟 AP(VAP)	.87

什么是 MikroTik RouterOS?

1、RouterOS 是什么?

802.11ac 双频共享 SSID

RouterOS 是路由操作系统,是拉脱维亚的 MikroTik 公司基于 Linux 核心开发,兼容 x86 PC 的路 由软件,将普通 PC 变为高性能路由器,在发展过程中逐步移植到了基于 MIPS、PPC、ARM 和 Tile GX 等平台。RouterOS 开发和应用上不断的更新和发展,软件经历了多次更新和改进,使其功能在不断增强 和完善。特别在 Wlan 无线、认证、策略路由、带宽控制和防火墙过滤等功能上有着非常突出的功能,其 极高的性价比,受到许多网络人士的青睐。

可以认为 RouterOS 和 Android 一样,只是 RouterOSd 的开发平台是封闭的,APP(应用功能包) 由 MikroTik 独立开发。MikroTik 为 RouterOS 提供 nkp 的功能包,根据需要选择你自己需要的功能进 行安装或卸载。MikroTik 的官方网主要包括: www.mikrotik.com (<u>www.routeros.com</u>), www.routerboard.com

2、在购买 MikroTik RouterOS x86 平台许可前是否可以测试该软件?

是的,基于 x86 版本的 RouterOS 是 32bit Linux 内核,你可以从官网下载 ISO 镜像安装文件,并可以 通过安装文件建立自己的 MikroTik 路由器,路由器在未注册前,所有的功能可以测试 24 小时,有足够的 时间测试,因为时间是根据系统运行时间记录的,如果你每天测试 8 个小时,一共可以测试 3 天。

2016 年后, MikroTik 官方提供了基于虚拟机平台的 CHR(Cloud Host Router), CHR 版本的 RouterOS 是 64bit Linux 内核,该版本提供免费的测试环境,提供所有 RouterOS 功能,但免费版本网络接口只有 1Mbps,付费版本有 P1, P2 和 P-U 三个版本,网络接口分别是 1Gbps, 10Gbps 和无限制,也可以申请 60 天试用版本,需要登录 <u>www.mikrotik.com</u> 注册帐号在线申请。

3、能否使用 MikroTik 路由器连接一个运营商设备的 T1, T3 或者其他高速接口?

是的,你可以安装各种 NIC (网络接口卡)在 MikroTik RouterOS 路由器上,并得到你想要的边缘路 由、骨干路由、防火墙、带宽管理、VPN 服务器、无线 AP、Hotspot 热点认证和更多功能。你可以查看我 们的技术支持和支持的各种接口。

4、运行速度如何?

使用普通 PC 的 RouterOS 处理能力相对于多数路由器都要快,随着 x86 构架的 PC 不断发展 CPU 处理速度和性能也在不断提升。MikroTik 官方陆续已经推出各种基于 MIPS, ARM 和 Tile GX 平台的硬件路由器,由于这些平台的硬件优化更加深入,某些方面已经超过了高性能的 x86 处理器。

5、MikroTik RouterOS 是否支持多 CPU 处理?

在 RouterOS 3.0 版本后支持多 CPU 运行, 3.0-4.0 版本支持 8 核心处理器, 早期的版本不支持多 CPU。 5.0 版本后支持 16 核心处理器, 特别是在 6.0 版本对多核 CPU 做了更好的优化, 解除了 CPU 数量限制。

6、MikroTik RouterOS 是否支持 SATA、USB 和 SCSI 安装

RouterOS 3.0 版本支持 SATA 和 USB 安装,早先版本不支持,SCSI 不支持,v6.39 以后支持 NVMe SSD 驱动。

7、软件路由相对于 Cisco 路由器如何?

对于早期 RouterOS 基于 x86 平台开发的软路由,能实现专业路由器大部分的功能,成本却是他的很小一部分,更灵活处理和方便升级,相对简易的管理与维护,但随着 MikroTik 产品的不断发展,现在已经成为专业无线、路由、交换设备的生产厂商。

8、MikroTik RouterOS 支持那些硬件平台,有什么区分?

RouterOS 现在基于多种平台,但已经逐渐从 PC 的 x86 构架向硬件平台的 RouterBOARD、CRS、CCR 等过度,这些硬件平台包括 MIPS、PPC、Tilera 和 ARM 等构架的处理器,软件和硬件的相互优化能有效的发挥 RouterOS 性能。

9、MikroTik RouterOS 是否需要其他 OS (操作系统) 支持?

不需要任何操作系统的支持, MikroTik RouterOS 独立的操作系统。RouterOS 是基于 Linux 内核,并 且非常稳定。你的硬件驱动将会被 RouterOS 自动识别(需 RouterOS 所支持的驱动),安装在 PRIMARY MASTER HDD(即 IDE1 主盘或 SATA 接口)、Flash 硬盘或 USB 硬盘,外接硬盘只为 Web 缓存。

10、安装后路由器的安全如何?

访问路由器需要通过用户名和密码,通过添加用户或分配用户组管理用户登录路由器,远程访问可以 通过用户的 IP 地址限制。防火墙过滤能很好的保护你的路由器和你的网络。

11、MikroTik RouterOS script(脚本)有什么作用?

脚本是 RouterOS 路由系统重要组成部分,即 RouterOS 内部语言,可以通过脚本编写将不同应用功能联系在一起,完成指定的工作,实现路由器运行的智能化。

13、什么是 CHR?

Cloud Hosted Router (CHR) 是基于虚拟主机开发的 RouterOS 版本,对 x86 平台的重新定义其使用 方式,基于 64bit CPU 构架,能运行在 VMWare, Hyper-V, VirtualBox, KVM。虽然 CHR 版本的 RouterOS 没有功能等级限制,但在网络接口速率上做了限制,免费版本是 1Mbit 的网络接口速率,也提供不速率的网络 接口,但需要购买。MikroTik 对 CHR 的特点定义为:

CHR 的特点如下:

- 可做各种功能的实验;
- 可让你在培训课程做 RouterOS 教学演示;
- 没有 24 小时或 Demo 许可限制;
- 发挥 x86 平台虚拟化技术,实现一机多用;
- 支持 64 位构架,性能能进一步释放。

14、为什么在 CHR 虚拟平台是基于 64bit 处理器构架?

传统 RouterOS 在 x86 硬件平台采用 32bit 构架,这点应该和硬件平台多样化有关系,涉及到要求兼容驱动过多等因素等关系,毕竟虚拟化平台就那几个硬件驱动优化也不是难事,因此 CHR 的版本出现了 64bit 构架,且 32bit 构架内存仅支持 4G 不到,而 64bit 内存支持方面是客观的。

15、CHR 系统要求是什么?

最低配置要求:

- 虚拟主机要求支持 64 位 CPU
- CHR 运行要求提供最低 128 MB RAM
- CHR 存储空间最低要求 128 MB

CHR 已测试平台包括如下:

- 基于 Linux 和 OS X 的 VirtualBox 5
- 基于 OS X 的 VMWare Fusion 7 和 8
- 基于 OS X 的 Qemu 2.4.0.1
- 基于 Windows Server 2012 的 Hyper-V (暂时仅支持第一代 Hyper-V 支持)
- 基于 VMware Esxi v5

16、MikroTik的 RouterBOARD、CCR 和 CRS 等产品是什么?

RouterBOARD、CCR(Cloud core Router)和CRS(Cloud Router Switch)是 MikroTik 硬件产品,基于 MIPS、PPC、Tilera 和 ARM 等平台开发的硬件,采用的是基于 Linux 内核开发的 RouterOS 系统,即将 RouterOS 变成了硬件。就如 Cisco 的路由器使用的是 IOS,基于 Unix 开发; Juniper 基于 FreeBSD 开发的 JunOS 系统。 MikroTik 的路由器则使用的是 RouterOS,都是由硬件和操作系统软件组成,可以理解为他们之间仅仅是硬件和 软件的不同,所以 RouterBOARD 是硬件路由器,而这样的路由器针对的是低功耗、高稳定性的无线网络和中小 型有线网络。后期 MikroTik 又开发了两款新品一个是基于 Tilera 构架的 Core Cloud Router(CCR 系列)和仍 然基于 MIPS 构架的 Cloud Router Switch(CRS 系列),CCR 基于高端路由,CRS 基于路由交换,在这里仍 然把两款产品归到 RouterBOARD 中介绍。

12、为什么 RouterBOARD 的 **1.2GHz** 处理器在数据转发能力超过我的 **2GHz** PC 处理器?

- 1. RouterBOARDS 的 CPU 设计为网络应用, x86 作为通用 CPU 采用总线不同, CPU 和内存在一条总线 上, 内存能直接访问快速读取数据, 连接通过以太网 Switch-chip, 即硬件交换芯片, 通过 PCI-E 总线 交换最大线速的转发以太网数据
- 2. 硬件加速功能(如当使用 IPSec 时, RB1000 系列可以通过硬件加速提高性能)
- 3. 网络交换 IC 芯片的性能优化

17、MikroTik硬件产品采用哪些平台?

<u>MIPS 平台</u>

- MIPS 4kc MIPS RouterBOARD 500 (532, 512 和 511)与 RouterBOARD 100 (133、133c、150、192)
- Atheros 24kc MIPS RouterBOARD 400(411/411A/411AH、433/433AH/433UAH、450/450G、493/493AH)
- Atheros 24kc MIPS RouterBOARD 700(711、711A、750/750G、750UP、751 系列,SXT、Groove、OmniTik)
- Atheros –74kc MIPS RouterBOARD2011 系列
- QCA 24kc MIPS hAP 系列
- QCA –74kc MIPS RouterBOARD900 系列(911、951、912)
- MTK7621 1004kc MIPS RB750Gr3, RB-M11, RB-M22

<u>PPC 平台</u>

- RouterBOARD1000、RouterBOARD1100、RouterBOARD800、RouterBOARD600、RouterBOARD333
- RouterBOARD1100AH/AHX2, RouterBOARD1200

<u>Tilera 平台</u>

- 系统支持 Tile-GX CCR1009、CCR1016、CCR1036 和 CCR1072(Tile-GX 系列是专门针对高端服务器市场,例如 大型数据中心和云计算等网络应用产品。Tile-GX 为 64 位 RISC 架构处理器, Tilera Tile-GX 采用台湾台联电 40nm 晶圆,处理器功耗从 15w~48w)
- 基于除了 CCR1016、1036 和 1072 平台的 RouterOS 是 64bit Linux,其他都是 32bit 系统

<u>ARM 平台</u>

- RouterBOARD3011 是第一款基于高通 ARM 平台的 IPQ-8064 处理器
- RB1100×4 采用 Annapurna 公司的 Alpine AL21400 处理器

RouterOS 安装

1、RouterOS 的安装方式有那些?

RouterOS 安装支持多种方式, x86 和 RouterBOARD 也不相同, 具体分为:

- 通过 ISO 镜像文件刻录到光盘引导安装(用于 x86 系统):即支持 AMD、Intel、VIA 和其他 x86 系统,硬盘支持 IDE、SATA 硬盘接口(不支持 SAS 和 RAID 卡), ISO 镜像文件小于 30M,所以 建议安装到 SSD 或 FLASH 硬盘上,如果没有特殊需求,建议系统硬盘不超过 32G。
- 2. 使用 U 盘安装基于 X86(限 3.0 版本后)
- 3. 使用 netinstall 网络安装程序,主要用于 RouterBOARD、CRS 或 CCR 平台,也适用于支持 PXE 的 x86 平台。

以上具体安装参见本人编写的《RouterOS 入门到精通》。

2、安装 MikroTik RouterOS 支持多大的硬盘空间?

-8- 编写:余松

MikroTik RouterOS 系统需要至少 32Mb 空间,RouterOS 通常硬盘支持到 120GB,更大的硬盘不建 议使用。普通机械硬盘容易出现坏道损伤,推荐使用 8~16G 的 Flash 硬盘或 SSD 固态硬盘,有利于提高 使用寿命。

3、MikroTik RouterOS 是否支持多个硬盘?

一套 RouterOS 系统只能安装到一个硬盘上,软件和硬盘是做了绑定。在使用中可以扩展其他硬盘存储,如使用 IDE、SATA 或 USB 外接存储,v6.39 以后支持 NVMe SSD 驱动。这些主要扩展应用于 web-proxy 缓存功能、User-Manager 数据存储、The Dude 网络管理数据存储、SMB 文件共享,FTP 文件存储等。

4、安装 PC 时,为什么 CD 安装有时停止在某处,不能通过安装?

随着 MikroTik 开发方向不再以 x86 平台为主, PC 硬件的支持和兼容也在逐步弱化, CD 安装可能对某些主板支持不完善,如果出现这样的情况,请跟换光驱或者其他早期硬件平台尝试安装好后,再返回现有 PC 硬件平台启动 RouterOS。

5、在 PC 上安装完成后,为什么 RouterOS 引导失败无法正常启动?

该问题,也和 CD 安装类似,同样涉及到 x86 硬件平台兼容问题,一般请检查硬盘或者 Flash 存储设备安装是否正常(硬盘或者 Flash 存储只能安装到 IDE 或 SATA 接口,不能安装到 RAID 卡),BIOS 启动选择 IDE 兼容模式,如果正确安装可能是硬件兼容问题,大多情况下是更换主板。

对于 4,5 问题,当前来说,是一个很常见的现象,RouterOS 发展方向已经不再以 x86 为重点,所 以必然会存在各种兼容问题,官方已经推出 CHR 基于虚拟化平台的 RouterOS,大家不妨尝试下,基于虚 拟机运行 RouterOS,个人预测基于 x86 硬件的 RouterOS 将来会被放弃。

6、在 RouterOS 的原有硬盘上,我是否可以覆盖安装其他操作系统?

不能,因为 RouterOS 安装完成后将许可写入了硬盘分区,如果用其他操作系统安装会破坏许可,造成结果是你的 RouterOS 授权许可无法找回,导致无法正常使用正版 RouterOS

RouterOS 登录和密码

1、第一次登录路由器的管理帐号和密码是什么?

第一次登陆,默认管理帐号是 'admin', 密码为空,你可以通过命令行'/password'命令修改密码,或者 进入/user 修改和添加账号。 Winbox 和 webfig 中进入/system user 菜单下修改。

2 如何使用 Winbox 登录 RouterOS

Winbox 是用于 MikroTik RouterOS 的管理和配置,使用图形管理接口(GUI):

	Yu	S			
S MikroTik Win	Box Loader v2	2.2.18			٢.
Connect To: 00:0	C:42:E2:0E:84		[Connect	
Login: adm	in				
Password: ***	***				
K K	eep Password		_	Save	
Secure Mode			Remove		
V L	oad Previous Sea	ssion		Tools	
Note: Mikr	oTik				_
Address (Liese	Nata			
Address 2	admin	MikroTik			ĥ.
00:0c:42:e2:0e:7f	admin	MikroTik			Ε
1					Ŧ

Winbox 支持 IP 地址、域名和 MAC 地址登陆管理路由器。MAC-telnet 功能,即使用 MAC 地址登陆管理路由器,MAC-telnet 是在路由器没有 IP 地址的情况下或者配置 IP 防火墙参数后无法连接路由器,通过路由器网卡 MAC 地址登录的方式。MAC-telnet 仅能使用在来自同一个广播域中(因此在网络中不能有路由的存在), 且路由器的网卡应该被启用。注:在 Winbox 中嵌入了通过 MAC 地址连接路由器的功能,并内置了探测工具。这样在管理员忘记或复位了路由器后,同样可以通过 MAC 登陆到 RouterOS 上,进行图形界面操作。

注: 在 winbox2.2.12 后增加了可选择的 MAC 登陆或者 IP 登陆的功能,同时需要提醒大家当打开迅雷下载软件后,会占用 MAC 扫描的 UDP 端口,所以建议使用 winbox 的 MAC 登陆时,关闭掉迅雷下载。

通过连接到 RouterOS 路由器的 HTTP(TCP 80 端口)欢迎界面下载 Winbox.exe 可执行文件,也可以 登陆 www.mikrotik.com 的 download 页面去下载 ,下载后保存在你的电脑中,之后直接在你 Windows 电脑上运行 Winbox.exe 软件,无需安装。

下面是对相应的功能键做介绍:

• •

搜索和显示 MNDP (MikroTik Neighbor Discovery Protocol) 或 CDP (Cisco Discovery Protocol) 设备。可以通过该功能键搜索同一子网内 MikroTik 和 Cisco 设备。并能通过 MAC 地址登陆到 MikroTik RouterOS 进行操作。

			YuS			
ĺ	🔲 WinBox L	oader v2.2.15				
	Connect To:	00:0C:42:53:84:53		Connect		
I	Login:	MAC Address	IP Address	Identity	Version	Boa
I	Login.	00:00:42:13:24:08	10.200.15.1	MikroTik Deelwe VDN	2.9.51	
I	Password:	00:00:42:16:FF:60	0.0.0.0 10.200.100.71	Backupven MikroTik	2.9.51	BB4
I		00:0C:42:41:69:BF	10.200.15.124	MikroTik	3.30	RB4
I		00:00:42:53:84:52	10.200.100.2	office	4.3	RB4
I						
	Note:					
I						
I	Address 🛆					
I	00:00:42:13:24					
	00.00.42:03:84					
		•				- Þ.
l	L					

注: 在 winbox2.2.12 后的版本增加了 MAC 地址和 IP 地址选择功能,可根据搜索内容选择使用 MAC 地址连接或是 IP 地址连接。

Connect

通过指定的 **IP** 地址(默认端口为 **80**,不许特别指定,如果你修改了端口需要对具体访问端口做自定) 或 **MAC** 地址(如果路由器在同一子网内)登陆路由器。

<u>S</u>ave

保存当前连接列表(当需要运行它们时,只需双击)

Remove

删除从列表中选择的项目

Tools...

删除所有列表中的项目,清除在本地的缓存,从 wbx 文件导入地址或导出为 wbx 文件

WinBox Loader v2.2.15	
Connect To: 00:0C:42:53:84:53	Connect
Login: admin	
Password: XXX	Save
Secure Mode	Remove
Load Previous Session	Tools
Note: nat_office	Remove All Addresses
Address 🖉 User Note	Clear Cache
00:0C:42:13:24:D8 admin office2 00:0C:42:53:84:53 admin nat office	Export Addresses
-	Import Addresses

YuS

- Secure Mode (安全模式):提供保密并在 winbox 和 RouterOS 之间使用 TLS (Transport Layer Security)协议
- Keep Password (保存密码):保存密码到本地磁盘的文本文件中

Winbox 控制台使用 TCP 8291 端口,在登陆到路由器后可以通过 Winbox 控制台操作 MikroTik 路由器的配 置并执行与本地控制台同样的任务。

接口概述

Winbox 接口被设计为直观的界面,接口包括以下:

- 工具栏在顶部用户可以添加一些工具,如 CPU、内存使用和工作时间,新的版本中加入了当前日期和时间。
- 菜单栏在左侧,所有功能列表菜单和子菜单,这个列表根据安装功能包不同而增减变化,例如 IPv6 功 能没有添加,此时 IPv6 菜单和他的子菜单将不会被显示在左侧栏。
- 工作区域,显示所有工作的窗口



标题栏显示路由器身份信息,显示格式如下:

[用户名]@[Router's IP 或者 MAC] ([RouterID]) - Winbox [RouterOS 版本] on [RB 型号] ([平台])

从截图上我们能看到用户通过账号 admin 登陆,连接 IP 地址 10.1.101.18,路由器的身份 ID 是 MikroTik,当 前安装 RouterOS 版本是 v5.0beta1, RouterBOARD 型号 RB800,平台是 PowerPC

在左边工具栏有 undo 和 redo 按钮,快速撤销和恢复操作

右边工具栏:

- Winbox 传输指示显示一个绿色栏
- 指示 winbox 连接使用 TLS 加密
- 复选框 Hide password.这个复选框替换所有敏感信息为"*"(如: 各种密码, PPP secret Passwords)

推荐使用 Winbox v3 版本

MikroTik 对 winbox 版本也在不断更新, winbox v3 做出了相应的改动, 主要集中在安全和使用功能上。

提示: 后期的 RouterOS v6 版本新功能都需要 winbox v3 版本支持,原有的 winbox v2 版本部分功能不支持,会导致无法登陆 RouterOS

YuS

新的 winbox 3 如下特点:

- 增加了组功能,可对各类 RouterOS 设备分组管理,增大了设备保存列表条目
- 在邻居发现功能中能对 IP 地址、MAC、RouterOS 版本分类
- 能过滤搜索,具备邻居(Neighbors)发现功能
- Winbox 能自动升级新版本
- 新增了当连接丢失,提供重新连接功能,并能保存连接会话
- 增加了设备管理密码验证功能

S WinBox v3.0rc6 (Addresses)	
File Tools	
Connect To: 192.168.88.1 Login: admin Password: Session: C:\Users\yus\AppData' 7 Browse	 Keep Password Secure Mode Autosave Session Open In New Window
Note: MikroTik Group: Add/Set Conned	Ţ.
Managed Neighbors - Master Password - Password: 0K	Find all Ŧ
Address User Session	🛆 Group 🛛 🕇 🕶
	•

在 winbox v3 版本将 _____ 按钮键取消,代替这个功能的是 Neighbors 邻居发现列表,当点击开 Neighbors 列表后,会自动搜索当前局域网内的 MikroTik 设备,如下图:

) WinBox v3	.0rcб (А	ddresses)			X
File Tools					
Connect To: Login: Password:	192.16 admin	8. 88. 1		 ✓ Keep Passw ✓ Secure Mod ✓ Autosave S Open In Ne 	ord e ession w Window
Session: Note: Group:	C:\Use MikroT	rs\yus\AppData' ∓	Browse		
Add/Set Connect					
Managed Neighbors					
MAC Address	A	IP Address	Identity	Version	Boar 🔻
	4D · 40	192 168 70 1	MikroTik	6.27	CRS125
D4:CA:6D:FA:	40.43	102.100.10.1			010120

YuS

增加了连接 Session 保存目录和 Group 设备分组选项,并添加了设备分组管理后的密码验证管理

WinBox v3.0r	сб (Addresses)		- • ×
File Tools			
Connect To: [Login: a Password:	92.168.88.1 dmin		 ✓ Keep Password ✓ Secure Mode ✓ Autosave Session Open In New Window
Session: C	:\Users\yus\AppDat	a' 🐺 Browse	会话保存目录
Note: M Group:	ikroTik Add/Set	Connect	设备分组
Managed Neight	oors		
😑 🍸 Set	Master Password	设置管理密码	Find all Ŧ
Address	Vser	Session	🛆 Group 🛛 🕽 🔻
	yus admin admin	<own> <own> <own></own></own></own>	▲
	root yus	<own> <own></own></own>	

打开 Tools 菜单,可以找到 Check For Updates 选项,可以通过连接 MikroTik 服务器,检查版本更新情况:

🔘 Wir	Box v3.0rc6 (Addresses)		
File [Tools		
Con	Import Export		✓ Keep Password ✓ Secure Mode
P	Move Sessions Folder		✔ Autosave Session □ Open In New Window
	Check For Updates)wse	
	Note: MikroTik		
	Group:	₹	
	Add/Set	Connect	

3、我如何恢复丢弃的密码?

如果你忘记了密码,不能恢复密码,如果是基于 PC 的 RouterOS 必须重新安装。如果你是 RouterBOARD,可以同 netinstall 程序重新复位系统或者通过主板上的 reset 跳线短路复位。

4、当 MikroTik RouterOS 启动失败,如何处理?

如果你在启动 RouterOS 失败,启动停止在某处,这种情况可能是非正常启动造成的文件丢失,你可以通过 RouterOS CD 或者 Netinstall 方式重新安装 RouterOS。

5、如果的 LAN 接口被禁用,如何访问路由器?

你只能通过本地的显示器和键盘操作或者通过 console 连接控制路由器,在命令行下进入 interface 菜 单使用 enable 命令+网卡名或者编号。

如果是 RouterBOARD 可以直接通 console 进行设置,如果没有 Console 接口情况下,只能复位 RouterBOARD 设备。

RouterOS 正版注册问题

1、RouterOS 正版有哪些等级?

你可以购买 Level3、4、5、6,四种等级,不同等级有不同的区别(Level3 等级一般是代理商能获得, 并提供)

等级 / 功能	Level 0 试用	Level3	Level 4	Level 5	Level 6
无线 AP	24 小时	不支持	支持	支持	支持
无线桥接和客户端	24 小时	支持	支持	支持	支持
RIP,OSPF,BGP 协议	24 小时	支持	支持	支持	支持
EoIP 隧道在线用户	24 小时	1条	无限制	无限制	无限制
SSTP 隧道在线用户	24 小时	1条	200	无限制	无限制
PPTP 隧道在线用户	24 小时	1条	200	无限制	无限制
PPPoE 隧道在线用户	24 小时	1条	200	500	无限制

YuS

		YuS			
L2TP 隧道在线用户	24 小时	1条	200	无限制	无限制
Hotspot 认证在线用户	24 小时	1条	200	500	无限制
VLAN	24 小时	1条	无限制	无限制	无限制
P2P 防火墙规则	24 小时	1条	无限制	无限制	无限制
NAT 规则	24 小时	无限制	无限制	无限制	无限制
Radius 客户端	24 小时	支持	支持	支持	支持
Queue 流量控制规则	24 小时	无限制	无限制	无限制	无限制
Web 代理	24 小时	支持	支持	支持	支持
User Manager 在线用户	24 小时	10	20	50	无限制

2、注册软件后,是否可以改变注册码等级?

不能升级更高等级,如果你希望升级到新的等级,只能重新购买相应的等级。所以你在第一次购买注 册码时,请注意根据你的情况正确选择。

3、MikroTik RouterOS 注册许可什么?

RouterOS 系统安装完成后,都会生成一个软件 ID,用于注册许可,获得许可码,也就是购买正版 RouterOS,每套 RouterOS 只有唯一的软件 ID 和唯一的许可码。如下图中 RouterOS 的 system-license 菜单下,可以找到软件 ID

License		
Software ID:	F3UJ-EC6K	OK
Level:	6	Paste Key
features:		Import Key
		Export Key
		Update License Key
		Upgrade/Get New Key

4、如何购买正版许可

购买许可可以登录官方网站 <u>www.mikrotik.com</u>注册帐号后,在自己的账户中申请购买,或找代理商, 提供软件 ID 购买许可。

下图是通过官网购买许可,对应等级许可和价格:

			Ŷ	ʻuS					
Mikro Tik	Home	Buy	About	Jobs	Hardware	e Software	Support	Training	Account
My account								Log out	yusong
ACCOUNT INFORMATION Home Balance	Purcha	ase	key						
Edit account details MUM registration history Hardware orders	1. Select	t key	/ leve	I					
WEB ORDER S Your orders and invoices	License	e L4	/P1	Lic	ense	L5/P10	Lic	ense L	6/PU
ROUTEROS KEYS Search and view all keys	USD	45.00			USD 9	95.00	0	USD 250.0	0
Account Purchase a key Make a demo key	2. Select	t key	/ type						
CHR LICENCES	• License ke	ey S	Software	ID		Prepaid key	y Sel	lect amount	•

5、注册许可是否有期限?

通过获取许可码永远不会到期,路由器可以一直运行。但许可码有升级限制,如果升级期限过后,不 再提供升级许可。不同等级软件都有不同升级期限和升级版本。

6、在没有丢失我的软件许可码时,如果重新安装 MikroTik RouterOS?

如果你是 PC 你必须通过 CD、软盘或者网络安装安装 RouterOS 到以前的 RouterOS 的硬盘上(硬盘 或者其他载体保证没有更换,硬盘或者其他载体被其他程序格式化,因为他们会删除你的注册信息),需要使用相同的 BIOS 设置到你的硬盘或者其他载体。

7、CHR 许可是什么

CHR 有 4 种许可:

许可	接口限制	价格		
Free	1Mbit	免费		
P1	1Gbit	45 USD		
P10	10Gbit	95 USD		
P-Unlimited	Unlimited	250 USD		

除了以上 4 种许可,还可以获取 60 天免费试用许可,该许可能用于所有的付费许可等级,申请 60 天免费 试用必须登录 <u>www.mikrotik.com</u>,注册 MikroTik 账号。

当运行 CHR 主机,通过 MikroTik 的账户访问更新许可,如果 CHR 无法更新许可或者许可失效,将无法 升级 RouterOS 最新版本。具体购买操作可以参考《RouterOS 入门到精通》v6.3.6 版本或官方网站

8、我能否将 MikroTik RouterOS 使用到不同的硬件上?

是的,只要保证 RouterOS 安装的载体(硬盘、CF 卡、U 盘或者 Flash 电子盘不变)你可以使用不同的硬件(如主板、各种网卡等,但必须使用同样的硬盘或其他载体),在移动其他硬件时不需要重新安装系统。当你在支付注册费用时,请考虑清楚,注册后注册码不能被用到其他硬盘或载体上。

9、如果我安装 MikroTik RouterOS 的硬盘坏掉了,我应该怎么处理?

如果你已经支付注册费用,你写信给 support@mikrotik.com,并描述具体情况,我们可能需要你将损坏的硬盘寄送到 MikroTik 总部,证明出现的问题,MikroTik 会提供替换注册码。

10、我如何导入软件注册码?

通过控制台(FTP 传输注册码文件)命令行导入:导入注册文件通过命令: '/system license import'(你 应首先通过 FTP 上传注册文件)。在一个 telnet 窗口通过复制/粘贴(不用考虑路径)。确定拷贝的注册码 包含"--BEGIN MIKROTIK SOFTWARE KEY--" and "--END MIKROTIK SOFTWARE KEY--"

导入注册码通过 winbox 或 webfig: 使用'system -> license' 目录下的'Paste' 或者 'Import the key'

11、如果在购买许可时候,输入软件 ID 时候字符输入错误,应该怎么办?

如果你输入的软件 ID 号,与正确的软件 ID 号相差 1-2 个字符,通过发送邮件到官方邮箱说明情况 (support@mikrotik.com 或 sales@mikrotik.com),官方可以给你修复,并提供正确的注册码(超过 2 个字符错误,不能提供修复)。

12、如果我丢失了 RouterBOARD,是否能给一个注册码到其他系统上的 RouterOS?

RouterBOARD 包含了 RouterOS 软件,即软件是免费的。你不能用到其他系统上。

升级与降级

1、如果添加 RouterOS 功能包操作?

你必须使用相同版本的功能包(功能包扩展名.npk),使用/system package print 命令查看已安装的功能包列表,使用/system resource print 命令检查剩余磁盘空间,是否有足够空间用于上传功能包。 保证你在上传完功能包后,保证有 2MB 的剩余空间给路由器运行!

如需要增加动态路由协议支持如 BGP、OSPF 或 RIP 需要上传 routing.npk 文件,使用 FTP 或 winbox 的 files 文件上传,上传完成后通过**/system reboot** 命令重启路由器,安装进度会显示在屏幕上,RouterBOARD 可以通过 console 显示,重启完成后,再次通过**/system package print** 查看 routing 功能 包安装是否成功。

2、RouterOS 功能包(Packages) 是什么?

RouterOS 提供了各种功能包的安装和管理,功能包可以从 http://www.mikrotik.com/download.html 页面下载,提供了 http 方式下载,管理员可以根据需要安装功能包,对于 RouterOS 而言正确的安装使用功能 包有助于系统维护和减小系统开销。

RouterOS 安装和管理时每个功能包的组成:

- 19 - 编写:余松

	YuS
功能包	包含功能
advanced-tools (mipsle, mipsbe, ppc, x86, tile)	包含各种工具 ping、netwatch、ip-scan、sms tool 和 wake-on-LAN
calea (mipsle, mipsbe, ppc, x86, tile)	数据收集功能,指定适用于在美国标准的"Communications Assistance for Law Enforcement Act"
dhcp (mipsle, mipsbe, ppc, x86, tile)	动态主机控制协议客户端和服务器
gps (mipsle, mipsbe, ppc, x86, tile)	支持全球定位系统设备
hotspot (mipsle, mipsbe, ppc, x86, tile)	HotSpot 热点认证系统
ipv6 (mipsle, mipsbe, ppc, x86, tile)	支持 IPv6
mpls (mipsle, mipsbe, ppc, x86, tile)	多协议卷标交换(Multi Protocol Labels Switching)
multicast (mipsle, mipsbe, ppc, x86, tile)	组播协议支持; IGMP(Internet Group Managing Protocol)- 代理 Proxy
ntp (mipsle, mipsbe, ppc, x86, tile)	网络对时协议客户端和服务端
Openflow (mipsle, mipsbe, ppc, x86, tile)	Openflow 协议,当前 RouterOS 支持 Openflow v1.0.0
ppp (mipsle, mipsbe, ppc, x86, tile)	PPP、PPTP、L2TP、PPPoE, ISDN PPP 客户端和服务器
routerboard (mipsle, mipsbe, ppc, x86, tile)	访问和管理 RouterBOOT 固件,仅支持 RouterBOARD 硬件
routing (mipsle, mipsbe, ppc, x86, tile)	动态路由协议如 RIP, BGP, OSPF 和路由管理如 BFD 和路由过滤
security (mipsle, mipsbe, ppc, x86, tile)	IPSEC、SSH 和 winbox 加密连接
system (mipsle, mipsbe, ppc, x86, tile)	路由器基本功能,如静态路由、ip 地址、sNTP、telnet、API、queue、 firewall、web-proxy、DNS 缓存、TFTP、IP 地址池、SNMP、sniffer、 e-mail 工具、graphing、Bandwidth 测试、torch、EoIP、IPIP、 桥接、VLAN、VRRP,在RouterBOARD 平台也包含 MetaROUTER 虚拟器
ups (mipsle, mipsbe, ppc, x86, tile)	支持 APC ups
user-manager (mipsle, mipsbe, ppc, x86, tile)	MikroTik User Manager 类 RADIUS 系统
wireless (mipsle, mipsbe, ppc, x86, tile)	Wireless 接口支持,802.11abgn
isdn (x86)	支持 ISDN
lcd (x86)	支持 LCD 显示面板
radiolan (x86)	支援 RadioLan 网卡

-

VuS

3、RouterOS 的升级文件名称区别

早期MikroTik 官方每次发行新版本提供了所有硬件合计的BT下载,如"Routeros-ALL-6.0rc6"里面有多个档,每个文件对应不同的硬件做升级和降级设置,但 2015 年下半年官方已经取消了 BT 下载,仅提供主升级包和扩展升级包下载,如下截图:

	6.34.6 (Bugfix only)	6.36.3 (Current)	5.26 (Legacy)	6.37rc36 (Release candidate)
MIPSBE	CRS, NetBox, NetMetal, PowerBox OmniTik, Groove, Metal, Sextant,	, QRT, RB9xx, hAP, mAP, RE RB7xx	34xx, cAP, hEX, wAP, BaseBox, Dyr	aDish, RB2011, SXT,
Main package	4	.↓_	4	4
Extra packages	\checkmark	.↓.	.↓.	.↓

Main package 和 Extra packetages,两种功能个包都可以用于升级 RouterOS,Main package 能用于 netinstall 的安装,Extra packages 为 zip 压缩文件,里面包含基本的系统包和各种功能扩展包,不能用于 netinsatll 的安装。

在版本上官方也提供了多种选择,当前版本除上一代 RouterOS v5 版本以外,v6 一共有三个版本可以选择,包括 Bugfix only、Current 和 Release candidate,如上图显示 v6.34.6 为对之前一个版本的 bug 修正,v6.36.3 为当前发行版本,v6.37rc36 为开发中的候选版本。也就是用户可以选择三种不同的版本,rc 开发候选版本一般会有新功能加入,喜欢尝鲜的朋友可以更新测试,而 bugfix 类似于稳定版,Current 是当前比较稳定的版本。

下面是 Extra packetages 功能名称对应的各种 RouterOS 硬件型号,以下信息仅供参考,具体请参考官 方信息 <u>www.mikrotik.com/download</u>

- all_packages_mipsbe 对应所有 Atheros 芯片的 RB400、700、900、2011 系列产品和 RBSXT、OmniTIK、 Groov 等采用 MIPS-BE
- all_packages_mipsle 对应 RB100 系列和 RB500 系列(RB133、RB133c、RB150、RB192、RB532) MIPS 4Kc 芯片
- all_packages_ppc 对应 RB300、RB600、RB800 和 RB1000 系列 (RB333、RB600、RB800、RB1000、 RB1100/AH/AHx2 和 RB1200) PowerPC 芯片
- all_packages_x86 对应所有 x86 构架的 PC 设备(AMD、Intel、VIA 和其他 x86 PC)
- **all_packages_tile** 对应基于 tilera-gx 构架的 CCR1016 和 CCR1036 系列
- all_packages-smips 对应 hAP 设备,如 hAP lite 和 hAP ac 等
- all_packages-arm 对应 ARM 芯片的 RB3011 设备

其他文件:

mikrotik-x.x.iso 光盘镜像文件,用于 x86 平台安装。

4、如果我升级 RouterOS,我的配置是否会丢失?

一般不会,所有配置都会被保存下来。如果你是通过 CD 升级 RouterOS 版本,安装时会有是否保存 老配置的提示,按照提示操作即可。注意:在某些版本升级后,一些配置存在丢失情况,比如 2.8 升级到

2.9,会出现 ip firewall filter 路径的变化,使防火墙配置丢失,这是因为版本在功能和特性上作了修改。但 **3.0**版本后各个版本功能路径几乎没有变动,因此无需担心配置丢失。

5、MikroTik RouterOS 如何升级或降级?

方法一、在线升级,当 RouterOS 连接到互联网后,可以在/system package 菜单下找到 check for updates,点击后如果有最新版本,可以点击下载升级。

Package List					
T Check For U	pdates	Check For Update	s		
Name /	Version	Current Version:	6.28		OK
@routeros-m	6.28	Latest Version:	6.28	- r	
🗃 advance	6.28		0.20		Check For Updates
🗃 dhep	6.28				
🗃 hotspot	6.28			*	
Э іруб	6.28				
🗃 mpls	6.28				
🗃 ррр	6.28				
routing	6.28				
🗃 security	6.28				
🗃 system	6.28	11			
🗃 wireless	6.28	11			
🗃 wireles	6.28	11			
		11			
12 items					
		11			

方法二、种方式通过 RouterOS 的 CD 或者 netinstall 安装新版本或老版本 RouterOS,软件注册码会 被自动保存下来,当然会提示你是否保持原有配置,只要你不通其他程序或者工具格式化硬盘。

方法三、种方式通过上传升级或降级版本的功能包,降级使用/system downgrade 命令降级。

根据你使用 RouterOS 的情况不同,选择上传的升级包文件(注: system-x.x.x.npk 的升级包是必须要, 否则无法升级)。如何来确定你当前使用的功能包,可以通过在 system package>的目录中查询对照如下 图:

Terminal [?] Gives the list of available commands ٠ Gives help on the command and list of arguments command [?] Completes the command/word. If the input is ambigous, [Tab] a second [Tab] gives possible options Move up to base level Move up one level . . /command Use command at the base level [admin@MikroTik] > sys [admin@MikroTik] /system> package [admin@MikroTik] /system package> print Flags: X - disabled SCHEDULED NAME VERSION # 0 system 6.0rc6 1 routing 6.0rc6 2 security 6.0rc6 3 6.0rc6 ppp 4 user-manager 6.0rc6 5 dhcp 6.0rc6 6 advanced-tools 6.0rc6 7 hotspot 6.0rc6 8 ipv6 6.0rc6 [admin@MikroTik] /system package> ٠

建议根据自己的需求安装或升级功能包(无线选择 wireless、PPPoE 认证选择 PPP 等等),过多的安装 功能会影响路由器的性能

根据你在 system package 中的功能包选择,并选择对应的功能包进行升级,记住 system 功能包是必须选择安装。

选择好对应的 RouterOS 功能包后,通过"FTP://路由器 IP 地址"上传功能包,或者直接打开 Winbox 的 Files 目录,通过拖放的方式将升级报上传到 RouterOS 根目录下:

🕎 Switch	File List
°C <mark>8</mark> Mesh	
255 IP 🗅	
🛒 IPv6 🗈	File Name ∧ Type Size Creation ▼
🎲 System 🗈	☐ ipv6-6. Orcl1-mipsbe. npk package 256. 1 KiB Jan/02/1970
🗬 Queues	ppp=6. Orc11-mipsbe. npk package 184. 0 KiB Jan/02/1970
📄 Files	
📄 Log	Uploading Files
🥵 Radius	Uploading system=6.0rc11-m (811.7 KiB of 8.8 MiB at 157.7 kb)
🎇 Tools 🛛 🗅	
🛅 New Terminal	
🔜 MetaROUTER	
🏉 Partition	
] Make Supout.rif	
😯 Manual	◆ 3 items 14.3 MiB of 64.0 MiB used 77% free

功能包上传完成后,通过 System Reboot 命令正常重启路由器,并升级版本:

YuS

System 🗅	Auto Upgrade
Queues	Certificates
Files	Clock
Log	Console
Radius	Drivers
Fools D	Health
New Terminal	History
MetaROUTER	Identity
Make Supout.rif	License
Manual	Logging
Exit	NTP Client
	NTP Server
	Packages
	Password
	Ports
	Reboot

RouterOS 在重启时,同时也在执行功能包的安装,重启后根据路由器性能不同会花费十几秒到1分钟的升级时间,如果是 PC 或者通过串口连接的 RB 设备可以在显示屏上看到安装进度条。重启完路由器后回 看到路由器已经升级为新的版本。

降级选项

在 system package 中可以看的右上角有一个 Downgrade 的命令,这个将高版本降级到低版本的选项 (需要同样将低版本的功能包上传到 RouterOS 的 FTP 的 files 中)。

Pacl	age List								
7	T Check For Vpdates Enable Disable Vninstall Vnschedule Downgrade								
	Name 🗡	Version	Build Time	Scheduled		-			
	🗃 advanced-t	6.0rc13	Apr/08/2013 14:25:10						
	🗃 dhep	6.0rc13	Apr/08/2013 14:25:10						
	🗃 hotspot	6.0rc13	Apr/08/2013 14:25:10						
	🗃 ipv6	6.0rc13	Apr/08/2013 14:25:10						
	🗃 openflow	6.0rc13	Apr/08/2013 14:25:10						
	🗃 ррр	6.0rc13	Apr/08/2013 14:25:10						
	routing	6.0rc13	Apr/08/2013 14:25:10						
	🗃 security	6.0rc13	Apr/08/2013 14:25:10						
	🖨 system	6.0rc13	Apr/08/2013 14:25:10						
	🖨 user-manager	6.0rc13	Apr/08/2013 14:25:10						
	🗃 wireless	6.0rc13	Apr/08/2013 14:25:10						

注意:如果是 3.25 以上版本,即 8 位 ID 降级到 3.25 以下需要 7 位 ID 的注册序列号,如果没有特殊 情况建议降级不低于 3.25 版本

6、RouterOS v6 在线升级

RouterOS 6.x 具备在线升级的选项,只要你的 RouterOS 配置网络后能正常连接网络(DNS 配置正确),可以直接从官方下载并升级 RouterOS 最新版本,当前 RouterOS 的版本划分为开发版本、稳定版本和 bug 修复版本三类。

- Bugfix only bug 修正版本,即对前一个版本的 RouterOS 做 bug 修复
- Current 当前版本,即当前发行的相对稳定版本
- Release candidate 候选开发版本,即正在开发的版本,主要提供测试。

因此在你选择版本升级时,一定要考虑使用哪一个版本,并看清楚官方的 changelog 信息,是否有你需要修复 bug 的地方或者你感兴趣的功能等。

下面是 RouterOS 进入 system -> package 目录下选择 check for updates 的升级接口,当你选择好你需要升级 的版本,并点击 Download&Install, RouterOS 会自动连接远程的 MikroTik 升级服务器。

Package List							
T Check For	Updates	Enable	Disable	Uninstal	11	Unschedule	Downgrade
Name /	Check For	Updates					
🗃 advanced-t 🖨 dhcp		Channel:	current		₹	ОК	
a hotspot	Installe	d Version:	6.33			Downlo	ad
€mpls €ppp	Lates	t Version:	6.34.1		Download &	Install	
<pre> frouting security system suser-manager wireless-cm2 </pre>	What's r 14:08): *) inter 8x small *) traff were 8x *) smips boards f What's r	new in 6.34 face - fix er; fic-monitor smaller; s - properl for winbox new in 6.34	l.1 (2016-F eed stats t - fixed s .y detect s & webfig. l (2016-Jan	•			
11 items	<pre>10:25):</pre>	e - archit (last full - The repo en greatly - and x86 (- package :MR images:	ecture sup y supporte exaggerate iterOS pack (CHR) archi included b	port d version death d; age added tecture; y default			

RouterOS 常见问题

1、RouterOS 帐号如何管理

修改 admin 帐号密码,在 CLI 命令行下直接进入 user 菜单下修改 admin 的密码,如下面修改 admin 的密码 为 123456。

[<mark>admin@MikroTik</mark>] > user										
[admin@MikroTik] /user> print										
[admin@MikroTik] > user [admin@MikroTik] /user> print Flags: X - disabled # NAME GROUP ADDRESS LAST-LOGGE 0 ;;; system default user admin full may/02/201											
# NAME	GROUP	ADDRESS	LAST-LOGGE								
Flags: X - disabled # NAME GROUP ADDRESS LAST-LOGGE 0 ;;; system default user admin full may/02/201											
admin	full	ma	ay/02/201								
[admin@MikroTik] /user> set admin pa	assword=123456									

下面是通过 winbox 创建一个 yusong 的账号, Group 为 full, allowed-address=192.168.88.0/24 即只允 许从 192.168.88.0/24 的网段登陆访问 RouterOS, 其他地址段将会被拒绝。

Vser List					
Users Groups	SSH Keys SSH Pr	ivate Keys Active	Users		
+- 🛛	× 🖻 🍸 🛛	AAA			Find
Nane	∧ Group Allowed	Address	Last I	.ogged In	-
;;; system	default user full			May/02/2	013 17:10
	New User				
	Name	yusong		OK	
	Group	full		Cancel	
	Allowed Address	: 192.168.88.0/24	•	Apply	
	Last Logged In	:		Disable	
	Password	; xoxoxox		Comment	
	Confirm Password	жжжж		Сору	
•			[Remove	•
1 item					
	enabled				

1、如何使用 Console 口连接 RouterOS 的终端控制:

通过标准的 DB9 的 Console 线连接到路由器, PC 的串口连接的默认设置为每秒位数: 9600 bits/s (RouterBOARD 系列串口是 115200 bits/s),使用终端仿真程序(如在 windows 中的超级终端或 SecureCRT, UNIX/Linux 的 minicom)连接到路由器。

2、如何连接和登陆 RouterOS

RouterOS 提供了多种登陆方式,从协议上分类包括 IP、MAC 登陆,从接口上分类有 console 连接、 以太网卡连接、显示器键盘连接;从应用程序上有 web 登陆、telnet 登陆、winbox 登陆、SSH 登陆、API 访问登陆等;

第一次登陆 RouterOS,初始化的 RouterOS 一般情况默认 IP 为空,或者是 192.168.88.1。RouterOS 登陆完全不用考虑 IP 方式,最好的登陆方式是下载一个 winbox 软件,使用 winbox 通过 MAC 地址登陆,且不需要修改本地电脑的 IP 地址,当然你的是基于 PC 安装的 RouterOS 可以用显示器和键盘登陆操作,或使用 console 口的用超级终端连接登陆。

3、如何通过命了复位 RouterOS?

进入 RouterOS 的终端控制台(CLI 命令行),在命令行输入以下命令

```
[admin@MikroTik] /system> reset-configuration
Dangerous! Reset anyway? [y/N]:
```

4、如果 RouterOS 密码丢失或者系统故障如何处理:

- 26 - 编写:余松

这个问题需要分2部分:

如果密码丢失,如果是 PC 可以通过 RouterOS 光盘重新安装回复出厂设置,也可以通过我公司的 U 盘复位软件删除密码,删除后默认账号是 admin,密码为空。如果是 RouterBOARD 可以通过 Netinstall 软件或者主板上的 reset 圆形铜片复位,如下图:



RouterBOARD 的复位

当系统出现故障无法正常启动或者允许,PC 通过 RouterOS 光盘重新安装系统,如果是 RouterBOARD 也通过 Netinstall 安装

5、我的 RB750/G 密码忘记该怎么复位?

RB750/G 在前面板都有复位按钮,开机通电安装复位按钮,直到 RouterOS 自检(设备灯连续闪烁两次)完成即复位

6、我的 RB750/G 系统损害,要重新通过 Netinstall 安装软件,但没有 Console 口该 怎么办?

RB750/G 不需要 Console 口也可以安装 RouterOS,只需要在本地电脑上打开并配置好 Netinstall 软件,通过网线连接到 RB750/G 的 ether1 口,启动时同时安装 reset 按钮不放,则可以在 Netinstall 上显示 RB750/G 的安装信息,这时你便可以安装

7、如何升级 RouterBOARD 的固件

RouterBOARD 的固件不定期进行更新,通常我们需要进行升级,操作时要求能连接到互联网,一般用 winbox 操作即可,通过命令行设置,配置参数如下

[admin@MikroTik] /system routerboard> upgrade Do you really want to upgrade firmware? [y/n] y firmware upgraded successfully, please reboot for changes to take effect! [admin@MikroTik] /system routerboard>

8、RouterOS 添加 IP 地址后,路由器的网卡和我的电脑在同一局域网,且在同一网段, 但为什么不能 ping 通路由器

这个问题可能是你的路由器 IP 地址的子网掩码没有设置正确,例如 192.168.1.1/24 的 IP 地址设置到 路由器,可能你没有设置子网掩码直接输入的是 192.168.1.1,这样路由器则认为 IP 地址是 192.168.1.1/32, 这样的问题需要你重新设置网络地址和广播地址,保证路由器和局域网在同一子网段。

9、我有两张网卡在 RouterOS 上,并能正常运行,同时能在路由器上 ping 通两个网络, 但无法从一个网络 ping 到另外一个网络或到互联网,我并没有设置防火墙规则?

这是一个典型的问题,你没有设置路由的网关,你需要将的数据传输到互联网,需要告诉路由器一个 出去的网关。如果你需要通过路由器隐藏你的内部网络上网,需要在 ip firewall nat 设置 Masquerading 操 作。具体的操作请你查看基本操作首册。下面是如何隐藏内网的 nat 操作

[admin@MikroTik] ip firewall nat> add chain=srcnat action=masquerade out-interface=Public [admin@MikroTik] ip firewall nat> print Flags: X - disabled, I - invalid, D - dynamic chain=srcnat out-interface=Public action=masquerade

12、我能否在 DHCP 中绑定每个用户的 IP 和 MAC 地址?

是的,你可以添加静态租约到 DHCP 服务器的 leases 菜单下设置,从安全性考虑,最好的方法是通过 PPPOE 认证分配 IP 地址,同样也可以根据账号绑定 MAC 地址。

13、如何能隐藏两个不同子网段到不同的两个外网 IP 地址?

进入/ip firewall nat 后,添加规则 chain=srcnat action=src-nat,设置好 src-address 的内网子网段后,指定 to-src-address 的值为需要隐藏的外网 IP 地址,如果选择 action=masquerade,则 to-src-address 不 会能选择,外网 IP 地址将由路由器自动选择

14、当我使用 PPPoE 上网时,为什么不能正常的访问某些网站?

这个问题比较常见,请在/ip firewall mangle 添加一条 change MSS 的规则,至少小于你连接 MTU 值的 40bytes,如果你加密的 PPPoE 连接 MTU 是 1492,设置 mangel 规则如下

/ ip firewall mangle

add chain=forward protocol=tcp tcp-flags=syn action=change-mss new-mss=1448

在 RouterOS 4.x 后的版本,系统会自动添加该策略,无需手动配置

什么是 Fast Path?

RouterOS 基于开发的硬件产品大部分支持 Fast path,该功能允许数据报转发不在经过 Linux 内核处理, 直接由 IC 芯片处理后转发,进一步提升转发速度。RouterOS 将添加更多关于 Fastpath 的功能更新,例如桥 接和 forward 过滤,当前的 Fastpath 还有较多的限制条件(v6.0rc10)。

RouterOS 实例配置

1、RouterOS 简单上网配置

通过下面一个简单的网络拓扑作为配置实例,根据该网络需要通过 RouterOS 完成配置:



在当前的实例中我们涉及到两个网络,即接入 ISP 网络的 WAN 外网和 LAN 内网:

- LAN 内网使用地址为: 192.168.0.0 子网淹码 24-bit (255.255.255.0)。路由器的地址在这个网络中为 192.168.0.254
- 接入 ISP 的外网 WAN 为 10.0.0.0 子网淹码 24-bit (255.255.255.0)。路由器的地址是在网络中为 10.0.0.217
- 外网 DNS 为 61.139.2.69, 202.98.68.96

配置 RouterOS 实现内网访问 ISP 网络,我们的步骤一共分为五步

- 首先: 启动设备后, 检查 interface 接口网口连接是否正常, 并定义网口名称
- 第二: 配置对应网口的 IP 地址
- 第三: 配置默认网关路由
- 第四: 配置 nat 地址转换规则
- 第五: 配置 DNS 服务器

第一步: 网络接口配置

在/interfaces 列表中修改 ether1 为 ether1-wan, 定义为外网接口;修改 ether2 为 ether2-lan 定义为内网 接口,如图:



同样将 ether2 修改为 ether2-lan,指定内网接口:

第二步:添加 IP 地址

在/ip address 中添加 IP 地址和选择网卡接口,添加内网和外围的 IP 地址如图:

		Y	ľuS				
🔚 Interfaces 😹 Bridge 🚅 PPP		_					
🕎 Switch	ARP	(G	ress List	- 7			Find
E mesn	Accounting	Ĭ	Address + 10.0.0.217/2	∧ Netw 4 10.0	ork .0.0	Interfa etheri-	се ▼ ¥ал
IPv6 D	Addresses DHCP Client		宁 192, 168, 0, 254	4/24 192.	168.0.0	ether2-3	lan
Leven and the second se	DHCP Relay		Address <192.16 Address: 192	8. 0. 254/2 . 168. 0. 25	4> 4/24		
Files	DNCF Server DNS		Network:			✓ Car	ncel
Andius Radius	Firewall Hotspot		Interface: eth	er2-lan	:	₹ Ap	ply
🔀 Tools 🗈	Neighbors					Dis	able
MetaROUTER	Packing	_				Com	ment
Partition Make Supout.rif	Routes	•				Rer	vove
a Manual	SMB	2 i	enabled				

第三步:添加默认网关

在/ip routes 里添加默认网关 10.0.0.1, 开启 check-gateway=ping(网关 ping 监测)如图:

28. Bridge	
E PPP ARP	
The Switch Accounting	
*C Mesh Addresses Route List	
Routes Nexthops Rules VRF	
$ IP_{V6} $ DHCP Relay $(+) - \checkmark \times \Box \qquad Find all $	∓
System DHCP Server Dst. Address / Gateway	-
Queues DNS AS >0.0.0.0/0 10.0.0.1 reachable ether1-wan	
Files DAC 10.0.0.0/24 etherl-wan reachable Firewall DAC 192.168.0.0/24 ether2-lan unreachable	
Log Hotspot Route <0.0.0/0>	
A Radius Neighbors General Attributes	
Tools Packing Det Address: 0.0.0.0/0	
Mew Terminal Pool	
E MetaROUTER Routes Gateway: 10.0.0.1 ∓ reachable ether1-wan	₹
Bartition SMB Check Gateway: ping	₹ ▲
Make Supout.rif SNMP	
Manual Services	•
Exit Distance: 1	
Socks Scope: 30	
TFTP Target Scope: 10	
Traffic Flow Routing Mark:	•

第四步,NAT 地址转换

在/ip firewall nat 里点击 "+" 添加伪装规则:

🔚 Interfaces		
😹 Bridge		
🚅 PPP	ARP	[
🕎 Switch	Accounting	
°C Mesh	Addresses	Firewall
255 IP 🗅	DHCP Client	Filter Rules MAI Mangle Service Ports
👳 IPv6 🛛 🗅	DHCP Relay	+ ▼ = _ Reset Co
🎲 System 💦	DHCP Server	# Action Chain Src. Add Ds
룢 Queues	DNS	
📄 Files	Firewall	
📄 Log	Hotspot	

在 NAT 里添加新的规则,在 chain 里选择 srcnat 链表:

Firewall
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols
🛨 📼 🖉 🖾 🖀 Reset Counters OO Reset All Counters
Artion Chain Src. Add Dst. Add Pro Src. Port Dst. Port In Out Byt
New NAT Rule
General Advanced Extra Action Statistics
Chain: srenat 두
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
0 Tn_Interface:

在选择 action 里的 action=masquerade 规则:

New NAT Rule	
General Advar	nced Extra Action Statistics
Action:	accept accept add dst to address list add src to address list dst-nat jump log masquerade netmap passthrough redirect return same src-nat
	STC 180

添加完成后:

Firewal	1																	
Filter	Rules	NAT	Mangl	.e Se	rvic	e Por	ts C	onne	eti	ions	Ad	ldress	Lists	Lay	er7 H	rotoc	ols	
+ -	🛉 📼 🧭 🖾 🍸 🚝 Reset Counters 🛛 00 Reset All Count							ers		Fin	d	a						
#	Action	ı	C	hain		Src.	Add.	Ds	st.	Add.		Pro	Src.	Port	Dst.	Port	In.	
0	≓∥ mas	quera	.de s	rcnat														

第五步,DNS 配置

在/ip dns 的 settings 中添加多个 DNS 服务器地址,根据需要启用 DNS 缓存(allow remote requests),并能通过 Cache size 修改 DNS 缓存大小:

🕎 Switch			
°L ^e Mesh	ARP		
IP N	Accounting		
VE IPv6	Addresses		
💮 System 🗈	DHCP Client	DNS Settings	
🗬 Queues	DHCP Relay	Servers 61, 139, 2, 69	OK
Files	DHCP Server	202 98 96 68	Concol
Log	DNS	202. 30. 50. 00 ▼	Cancel
A Radius	Firewall	Dynamic Servers:	Apply
🗶 Tools 🗈 🗅	Hotspot	✔ Allow Remote Requests	Static
New Terminal	Neighbors	Max UDP Packet Size: 512	Cache
 MetaROVTER	Packing	Cache Size: 2048 KiB	
🔔 Partition	Pool	Cache Used: 13	
-	Routes		

到此,上述的单线上网事例就已经配置完成!

10、如何修改我的 telnet 或者 HTTP 服务的 TCP 端口?

你能通过/ip service 找到你需要修改协议的对应规则,并对这些规则进行操作,例如修改 http 和 telnet 服务端口的 CLI 如下:

/ip servcie set www port=8080 /ip service set telnet port=2323

18、如何备份或导入 RouterOS 配置

RouterOS 可以通过 backup 下的 save 命令将系统备份为二进制文件,采用 FTP 访问或在 winbox 中的 file 列表中下载备份文件,并可以通过备份文件恢复路由器设置。

Save 指令是保存当前配置到一个备份文件中,显示文件在/file 目录中。如需要回复指定的备份文件,可通过 /system backup 中的 load 指令载入配置,还原当前备份文件的配置。

例如:将当前的配置保存到文件 test:

[admin@MikroTik] system backup> save name=test
Saving system configuration
Configuration backup saved
[admin@MikroTik] system backup>

在路由器中查看保存的文件:

[admin@MikroTik] > file print				
# NAME	TYPE	SIZE	CREATION-TIME	
0 test.backup	backup	12567	aug/12/2002 21:07:50	
[admin@MikroTik] >				

导入备份文件 test:

[admin@MikroTik] system backup> load name=test Restore and reboot? [y/N]: y ...

Winbox 下配置直接在 files 菜单下,通过 backup 和 restore 操作

Tile Neme (Type Size Creation Time)									
	Type	2447 D	Ureation 11me						
	script	J441 D	may/10/2010 14.21.5						
= 55. rsc	script	16.9 KiB	Jan/25/2010 16:40:1						
🗏 J4W5-PG2G. key	.key file	204 B	May/11/2010_08:53:0						
📄 MikroTik-31052010-1355. backup	backup	383.6 KiB	May/31/2010 13:55:2						
🖹 adsl. rsc	script	390 B	Jan/02/1970_08:01:2						
🖹 games510. rsc	script	8.0 KiB	May/10/2010 23:10:1						
🖨 ipv6-5. Obeta2-mipsbe. npk	package	295.1 KiB	May/17/2010 16:22:3						
🖹 17-protos. rsc	script	24.0 KiB	Jan/28/2010 11:53:3						
🖹 mangle.rsc	script	1218 B	Jan/02/1970_08:01:2						
🖹 um-before-migration. tar	.tar file	15.5 KiB	Jan/02/1970_08:00:4						

YuS

2、如何设置端口映射?

根据以上网络拓扑,需要将内网的 http 服务器发布到外网,内网的 http 服务器 IP 地址 192.168.0.88,这里 需要做端口映射规则,进入 ip firewall nat 里,选择 chain=dstnat,我们的外网 IP 地址是 10.0.0.217 配置 到 dst-address, dst-port 为 tcp 协议 80 端口,如下图

Firewall	
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols	
🗣 🖃 🖉 🚝 🐨 Reset Counters 00 Reset All Counters 🛛 🛛 🖬 🖬	
# Action Chain Src. Add Dst. Add Pro Src. Port Dst. Port In 0	ut.
New NAT Rule	
General Advanced Extra Action Statistics	
Chain: dstnat	3
Src. Address:	•
Dst. Address: 10.0.0.217	
Protocol: 6 (tep)	
Src. Port:	•
Dst. Port: 80	.
Any. Port:	-
In. Interface:	
Out. Interface:	•

在 action 选择 dst-nat 操作, to-address 设置内网 http 服务器 IP 地址, 和端口 80

YuS

New NAT Rule	
General Advan	ced Extra Action Statistics
Action:	dst-nat 두
To Addresses:	192. 168. 0. 88
To Ports:	80

lirewa	11										
Filter	r Rules NAT Ma	ngle Servi	ce Ports	Connect	ions A	ddress Li	sts Lay	ver7 Pro	otocols		
+	- 🖉 🗶 🖻	7	Reset Co	ounters	OO Res	set All C	ounters		Find	all	Ŧ
#	Action	Chain	Src. Ad	d Dst.	Add	Protocol	Src. Po	rt Dst.	Port I	n	0u •
0	≓∥ masquerade	srcnat									
1	+ dst-nat	dstnat		10.0	.0.217	6 (tcp)		80			

3、如何设置单机带宽控制?

进入 Queue 添加带宽控制规则,选择 simple queue,添加主机 IP 是 192.168.0.3,并取名为 IP03, 设置带宽为上行(upload)1m,下行(download)2m,以下截图操作以 RouterOS v6 版本参考

°C Mesh	Queue List
IP 🗅	Simple Queues Interface Queues Queue Tree Queue Types
👳 IPv6 🛛 🗅	
🌐 System 🗈 🗈	Y Keset Counters OO Reset All C
🙊 Queues	# Name Target Rx Max L Tx Max L Pack
📄 Files	New Simple Queue
Log	General Advanced Statistics Traffic Total
🥵 Radius	Name: IPO3
🎇 Tools 🛛 🗅	Target: 192.168.0.3 ∓ 🜩
🔚 New Terminal	
🔜 MetaROVTER	
修 Partition	Target Upload Target Download
] Make Supout.rif	Max Limit: 1M ∓ 2M ∓ bits/s
🚱 Manual	-A- Burst
Exit	Burst Limit: unlimited ∓ unlimited ∓ bits/s
_	Burst Threshold: unlimited ∓ unlimited ∓ bits/s
	0 items Burst Time: 0 0 s
	- - Time

添加后,显示如下:

Queu	e List					
Simp	le Queues	Interface Queue	s Queue Tree	Queue Types	:	
÷		× 🖻 🍸 (🚝 Reset Coun	ters 00 Res	set All Counter	s Find
#	Name	Target	Rx Max L	Tx Max L	Pack	-
0	🔒 IP03	192.168.0.3	1M	2M		

4、如何设置 ADSL/PPPoE 拨号配置?
ADSL 拨号需要建立 PPPoE-client,进入 ppp 里点加号创建一个 PPPoE-client:

YuS

ю	🖓 🛛 Safe Mode							
	🔏 Quick Set							
	🔚 Interfaces							
	🤶 Wireless	PPP						
	📲 Bridge	Inte	rface	PPPoE Servers	Secrets	Profile	s Act	ive
	🚅 PPP	(+)	-		T PP	P Scanner	· PI	PTP :
	🕎 Switch		PPP S	12	2 MTV	Tx		
	°C <mark>8</mark> Mesh		PPP (
	255 IP 🗅		рртр	Server Binding				
	🍪 System 🛛 🗅							
	룢 Queues		SSTP	Server Binding				
	📄 Files		SSTP	Client				
	📄 Log		12TP	Server Binding				
~	🥵 Radius		1270	Client				
Ĩ	🄀 Tools 🛛 🗅		OVP	V Server Binding				
in	🔚 New Terminal	OVPN Server binding						
\geq	🔜 MetaROUTER							
S	🔔 Partition		DDD-	E Client	1			
5	Make Supout.rif		PPPO			-		
Ч	0							

PPPoE-client 创建后取名 pppoe-out1,选择拨号的 interface 为 ether1

New Interfac	2					
General Dia	1 Out	Status	Traffic		_	ОК
Name:	pppoe	-out1				Cancel
Type:	PPPoE		Apply			
L2 MTU:						Disable
Max MIU: Max MRII:	1480					Comment
MRRU:	1600					Сору
						Remove
Interfaces:	ether	1		₹		Torch
						PPPoE Scan

点击 Dial-out 里配置拨号参数, 用户名 user 为 yusong, 密码 password 为 123456, 将 use-peer-dns 和 add-default-route 选择上

YUS	
New Interface	
General Dial Out Status Traffic	OK
Service: 📃 🔻	Cancel
AC Name: 🗸 🗸 🗸	Apply
User: yusong	Disable
Password: *****	Comment
Profile: default 두	Сору
Keepalive Timeout: 60	Remove
Dial On Demand	Torch
✓ Use Peer DNS ✓ Add Default Route	PPPoE Scan
Default Route Distance: 1	
- Allow V pap V mschap1 V mschap2	

17.0

网线连接后 pppoe-out1 会自动拨号,连接成功后 pppoe-out1 会显示 R,代表拨号成功,可以进入/ip address 下查看自动获取的 ip 地址,网关也会自动添加到/ip route 中,会自己配置 DNS 到/ip dns 下

5、如何配置 DHCP 客户端

进入 winbox 后,进入 ip dhcp-client,新增添加选择 interface 为获取 DHCP 客户端的接口,其他参数默认,如下图:

DHCP Client		83
+ - 🖉	Rolocco Ronow New DHCP Client	Find.
🛓 ether1	DHCP Status Interface: ether1 Hostname: Client ID: Use Peer DNS Use Peer NTP	OK Cancel Apply Disable Copy
1 item	✓ Add Default Route Default Route Distance: 0 disabled stopped	Release Release

6、如何配置 DHCP 服务器

步骤一、进入/ip dhcp-server, 点击 DHCP-setup,在弹出的对放框中 DHCP server interface 选择对应网卡, 然后点击 next:

DHCP Server							
DHCP Networ	rks Leases O	ptions	Option Sets	Alerts			
+ - <) 💥 🍸 🗍	DHCP Cor	afig DHCP	Setup			
Name	🔺 Interf	ace	Relay	Lease Time	Address		
	Select inter	face to	run DHCP se	rver on			
	DHCP Server Interface: ether1						
			Back	Next	Cancel		

步骤二、选择 DHCP 地址段,即提供 DHCP 的 IP 地址段,这里配置 192.168.88.0/24, RouterOS 会自动 判断地址长度

DHCP Server									
DHCP Netwo	rks Leases Options	Option Sets	Alerts						
+ - «	🖄 🍸 DHCP Co	nfig DHCP	Setup						
Name	🛆 Interface	Relay	Lease Time	Address F					
	DHCP Setup								
	Select network for 1	DHCP address	92						
	DHCP Address Space: 192.168.88.0/24								
		Back	Next	Cancel					

步骤三、点击 next,设置 gateway-for-DHCP-Network,根据之前填写的 IP 地址段,RouterOS 自动判断 192.168.88.1 为分配给用户的网关:

DHCP S	erver							
DHCP	Networ	rks	Leases	Options	Option S	ets Ale	erts	
+ =	- 🗸	2		DHCP Co	nfig D	HCP Setu	Ф	
Nam	e	🛆 Interface			Relay	Lea	se Time	Address
		DHC Sel Ga	P Setup lect gat teway fo	eway for r DHCP Ne	given net twork: 🚺 Bac	work 92.168.8 k N	8.1 [[] ext	Cancel

点 next 后,会出现 DHCP-relay 的配置,可以忽略不管,直接通过点 next

DHCP Networ	ks Leases Options Option Sets Alerts							
+ - 🖉	🔀 🍸 DHCP Config DHCP Setup							
Name	🔺 Interface Relay Lease Time Addres							
DHCP Setup								
	If this is remote network, enter address of DHCP relay							
	DHCP Relay: 192.168.88.1							
	Back Next Cancel							
	There is no such IP network on selected interface							

YuS

步骤三、现在进入 Address-to-Give-Out,分配给内网可用的 IP 地址范围),RouterOS 会自动生成,排除 网关地址 192.168.88.1

DHCP S	erver									
DHCP	Networks	Leases	Options	Option	. Sets	Alert	z			
+	- 🖉 💈	8	DHCP Co	onfig	DHCP	Setup]			
Nam	e	🛆 Inte	rface	Rel	ay	Lease	Time	Addres	ss Pool	
	DHCP Setup									
	Se	lect poo	l of ip a	ıddresse	s give	en out l	y DHCP	server		
	Ad	Addresses to Give Out: 192.168.88.2-192.168.88.254								
		Back Next Cancel								

图 4

步骤四、设置 DNS-server(内网 DNS),如图 12。

- T I								
DHCP Server								
DHCP Networ	ks Leases Options Option Sets Alerts							
+ - 🖉	🔀 🍸 DHCP Config DHCP Setup							
Name	🛆 Interface 🛛 Relay 🔹 Lease Time	Address Poo						
	DHCP Setup							
	Select DNS servers							
	DNS Servers: 61.139.2.69							
	Back Next Cancel							

步骤五、点击 next 设置 Lease-Time(内网地址的租约时间),如图 13。

YuS

DHCP S	erver									
DHCP	Network	ks Lea	ses	Options	Optio	on Sets	Alert	s		
+	- 🖉	\otimes	T	DHCP Ca	nfig	DHCP	Setup			
Nam	e	A	Inter	face	Re	lay	Lease	Time		Address Pool
	DHCP Setup									
		Select	t lea	se time						
	Lease Time: 00:10:00									
	Back Next Cancel									Cancel

配置完成后,提示设置成功

DHCP Setup						
Setup has	completed	successfully				
		OK				

7、如何设置 ARP 绑定?

虽然主机在 IP 网络中是通过 IP 地址通话,但实际上硬件地址(MAC 地址)被用于主机到其他主机的数据传输。地址解析 协议 Address resolution protocol (ARP) 是提供硬件地址与 IP 地址之间的解析。每个路由器都一个 ARP 列表,记录 ARP 信息,由 IP 地址和相符合的 MAC 地址构成,一般 ARP 提供动态的 IP 与 MAC 地址对于关系,自动在 ARP 列表中产生。路 由器通过 ARP 列表的记录来回应各个主机的数据。我们也可通过静态的 ARP 记录,要求路由器只对静态的 ARP 做回应。这样就可以避免出现如有用户擅自修改 IP 地址或者通过 ARP 病毒影响路由路由器工作。如通过下面的设置:

6 CH Interfaces × ARP List Wireless + |-|Bridge MAC Address IP Address Interface A PPP D **192.168.0.2** 00:0C:42:02:0A:0B ether1 IP Addresses Ports Routes New ARP Entry × Queues Pool IP Address: 10.10.10.10 оĸ Drivers ARP MAC Address: :21:00:56:00:12 Cancel System VRRP Interface: ether2 -Apply: Files Firewall Log Socks Disable SNMP UPnP. Comment Users Traffic Flow Сору Radius Accounting Remove Tools Services New Terminal Packing

1. 在 WinBox 中添加一个静态主机的 ARP 记录。

或者通过命令操作:

```
YuS
```

```
[admin@RB450] ip arp> add address=10.10.10.10 interface=ether2
mac-address=00:21:00:56:00:12
同样的我们可以使用:
```

将所有的的 ARP 记录修改为静态的。

2. 设置 ether2 interface 仅回应静态 ARP 的请求:



命令操作如下:

[admin@RB450] > interface ethernet set ether2 arp=reply-only

19、RouterOS 策略路由方式有那些?

策略路由支持源地址、目标地址、地址列表、端口策略和负载均衡等,RouterOS 常见的负载均衡包括 Nth 和 PCC(3.24 后支持),大多策略路由是在 ip firewall mangle 中标记完成的,多采用 Prerouting 链表执行,普通的源和目标地址策略路由可以在 ip route 或者 ip route rules 里完成。具体可以参考《RouterOS 入门到精通》

8、如何做端口策略路由:

我们定义访问网页的端口,访问网页的端口是 TCP 80 端口,我们进入/ip firewall mangle 中做数据标记,从标记中提取路由标记,命名为"web",因为我们在前面的连接标记中做过了 passthrough 的设置,在这里就不用在重复设置。

E Firewall		
Filter Rules	NAT Mangle Service Ports Conn	ections Address Lists Layer7 Protocols
(+)- 🗸	New Mangle Rule	New Mangle Rule
# Acti		
;;; small	General Advanced Extra Action	General Advanced Extra Action Stat:
0 🥒 m.	Chain: prerouting	Action: mark routing
;;; big	Sun Addunati	New Provide a Harder and
1 🥒 m.	Src. Address.	New Louting mark: web
	Dst. Address:	Passthrough
	Protocol: 🗌 6 (tep)	
	Src. Port:	
	Dst. Port: 80	
	Anv. Port:	
	P2P:	

YuS

然后我们进入/ip route, 配置路由我们让标记好的 80 端口通过 pppoe-out1 出去:

Route List	
Routes Nexthops Rules VRF	
+ × = 7	
Dst. Address \land Gateway \lor Distance Rout:	ing Mark
AS \$0.0.0.0/0 pppoe-out1 reachable 1 web	
Route <0.0.0/0>	
General Attributes	OK
Dst. Address: 0.0.0/0	Cancel
Gateway: pppoe-out1 🔻 reachable 🗢	Apply
Check Gateway:	Disable
Type: unicast	Comment
Distance: 1	Copy
Scope: 30	Remove
Target Scope: 10	
Routing Mark: web	
Pref. Source:	

在这里,如果在 ip route rule 里有其他的策略规则出现,我们最好是在/ip route rule 里再次定义 80 端口的规则:

YuS		
Route List		
Routes Nexthops Rules VRF		
+- ** - 7		
# Src. Address Routing Int Action	Table	
0 🕨 web lookup	web	
■ Policy Routing Rule <web> Src. Address:</web>		
Dst. Address:	Cancel	
Routing Mark: web 🐺 🔺	Apply	
Interface:	Disable	
Action: lookup 🔻	Comment	
Table: web 🔻	Copy	
	Remove	
3 disabled		

在 ip route rules 定义的 web 标记在 web 路由表中去查找路由。

9、如何配置网关断线处理?

在多线路情况下,我们可以通过配置备份线路,避免默认网关异常断开后,其他线路进行备份,即配置默认网关和备份网关,我们通过定义 **distance(路由距离)**对多个网关进行备份,根据 **distance** 来判断 1 为最优先, 2 其次,依次类推。

如下图:默认网关的 **distance** 设置为 1,并设置 check-gateway=ping,通过 ping 监测网关状态:

Route <0.0.0/0	>		
General Attributes	5		
Destination:	0.0.0.0/0		
Gateway:	10.200.15.1		\$
Gateway Interface:] ‡
Interface:	wanl		
Check Gateway:	ping	₹	
Type:	unicast		₹
Distance:	1		•
Scope:	30		
Target Scope:	10		
Routing Mark:			•
Pref. Source:] -
disabled		active	stati

备份网关的 **distance** 设置为 2,并设置 check-gateway=ping,通过 ping 监测网关状态:

Route <0.0.0/0	>
General Attributes	5
Destination:	0.0.0/0
Gateway:	10. 200. 100. 2
Gateway Interface:	
Interface:	wan2
Check Gateway:	ping Ŧ ▲
Type:	uni cast 🔻
Distance:	2
Scope:	30
Target Scope:	10
Routing Mark:	▼
Pref. Source:	▼
disabled	active stat:

配置完成后的路由标如下图:

R	oute List						•
Rou	tes Rules						
÷	- * *					Find	all Ŧ
	Destination 🦷 /	Gateway	Gatewa	Interface	Distance	Routing Mark	Pref. S 🔻
: :	: 默认网关						
AS	0.0.0/0	10.200.15.1		wan1	1		
: :	: 备用默认网关						
S	0.0.0/0	10.200.100.2		wan2	2		
::	: 负载均衡标记器	各由1					
AS	0.0.0/0	10.200.15.1		wan1	1	1st_route	
::	: 负载均衡标记器	各由2					
AS	0.0.0/0	10.200.100.2		wan2	1	2nd_route	
DAC	▶ 10.200.15			wan1	0		10.200.15.99
DAC	▶ 10.200.100			wan2	0		10.200.10
DAC	▶ 192, 168, 10,			lan	0		192.168.1

23、firewall filter 里如何理解 input、foreword 和 ouput 的过滤规则?

下面是三条预先设置好了的 chains, 他们是不被能删除的:

- **input** 用于处理进入路由器的数据报,即数据报目标 IP 地址是到达路由器一个接口的 IP 地址,经过 路由器的数据报不会在 input-chains 处理。
- forward 用于处理通过路由器的数据报
- **output** 用于处理源于路由器并从其中一个接口出去的数据报。

他们具体的区别如下:

IP 数据报进入 input 链表的数据工作流程, 阴影部分代表经过的处理部件:

YuS



IP 数据报进入 output 链表的流程, 阴影部分代表经过的处理部件:



IP 数据进入 forward 链表的流程, 阴影部分代表经过的处理部件



当处理一条 chain (数据链),策略是从 chain 列表的顶部从上而下执行的。如果一个数据报满足策略的条件,这时会执行该操作。

16、如何使用防火墙过滤指定的端口?

添加一条 firewall 规则,将所有通过路由器到目标协议为 TCP,端口为 445 和 135 的数据包丢弃掉:

```
/ip firewall filter add chain=forward dst-port=135 protocol=tcp action=drop
/ip firewall filter add chain=forward dst-port=445 protocol=tcp action=drop
```

拒绝通过 Telnet 访问路由器(协议 TCP, 端口 23):

/ip firewall filter add chain=input protocol=tcp dst-port=23 action=drop

15、如何禁止 192.168.0.11 的 IP 地址上网?

进入 ip firewall filter 中,选择 chain=forward 链表,设置源地址为 192.168.0.11, action=drop

[admin@cdnat] > ip firewall filter [admin@cdnat] /ip firewall filter> add chain=forward src-address=192.168.0.11 action=drop

17、我如何导出防火墙配置,并用到其他 RouterOS 上?

首先打开 RouterOS 的终端控制台(CLI 命令行)进入/ip firewall filter, 输入命令 export file="文件名"

[admin@cdnat] > ip firewall filter [admin@cdnat] /ip firewall filter> export file=firewall

导出后,可以在 files 中找到,然后拷贝下传到另外一台 RouterOS 上,并通过/import file="文件名"导入到

16、如何使用 L7 脚本

7 层协议过滤操作是在/ip firewall 中 Layer7 Protocols 中,这里我们可以手动编辑 Regexp 表达式,具体操 作可以查看正则表达式,配置 sniffer 抓包工具分析相关网络程序的数据规律,下面的图中看到添加一个新的 qq2009 过滤操作:

E Firewall
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols
Name 🔨 Regexp 🗸 🗸
💷 New Firewall L7 Protocol 🛛 💌
Name: 292009 OK
Regexp: Cancel ^. ?. ?\x02. +\x03\$
Apply
Comment
Сору
Remove
0 items

7 层协议通过 Regexp 脚本编写相应应用程序的过滤代码, Regexp 可以通过网上搜索相关资料了解。在这里我们已经提供了一些常用程序的 7 层协议脚本:

通过在 http://www.mikrotik.com.cn 的"软件下载"里下载到 MikroTik RouterOS 3.07 层协议过滤脚本。 然后我们可以通过 FTP 上传或者直接拖放到 Files 对话框中。

		X					
re		Find					
Туре	Size	Creation Time 🔹 🔻					
script	14.4 KiB	Jan/02/1970_00:03:38					
script	24.0 KiB	Jan/03/1970 19:40:48					
script	11.9 KiB	Jan/02/1970 00:03:58					
30.2 MB	of 61.4 MB	50% free					
	re Type script script script 30.2 MB	re Type Size script 14.4 KiB script 24.0 KiB script 11.9 KiB 30.2 MB of 61.4 MB					

之后我们在命令行(Terminal)中导入7层协议脚本:

用 import 17-protos.rsc 命令来导入脚本

Terminal X MMM KKK MMM TTTTTTTTTTT KKK MMMM MMMM KKK TTTTTTTTTTT KKK MMM MMMM MMM III KKK KKK RRRRR 000000 III KKK TTT MMM MM MMM III KKKKK RRR RRR 000 000 TTT III KKKKK MMM III KKK KKK RRRRR MMM 000 000 TTT III KKK K MMM MMM III KKK KKK RRR RRR 000000 TTT III KKK MikroTik RouterOS 4.5 (c) 1999-2010 http://www.mikrotik.com/ jan/02/1970 04:21:38 system,error,critical login failure for user cdnat 0.200.100.2 via telnet Ξ jan/02/1970 04:22:23 system, error, critical login failure for user cdnat 0.200.100.2 via telnet [admin@MikroTik] > import 1 17-protos.rsc file-name [admin@MikroTik] > import 17-protos.rsc Opening script file 17-protos.rsc Script file loaded successfully

当系统提示 Script file loaded and executed successfully,说明脚本成功导入。

导入脚本后,我们可以在 Layer7 Protocols 中看到

II Firewall	
Filter Rules NA	T Mangle Service Ports Connections Address Lists Layer7 Protocols
+ - 2 1	Find
Name 🗡	Regexp 🗸
● 100bao	^
● aim	^ (*[].* ¹ % * .?.?.?.) flapon toc_signon.*0x
	user-agent:aim/
● applej	^ajprot
🛛 ares	^ L[]Z].?.? \$
● armage	YCLC_E CYEL
⊘battle	^ 4 <u></u>
⊘battle	^(◀?◀ .?.?.?.?.?(¶ -)) []].?battlefi
obgp	^? [U]
biff	^[a-z][a-z0-9]+@[1-9][0-9]+\$
Dittor	^(!!bittorrent protocol azver \$ get /scrape\?info_hash=)
O chikka	^CTPv1. [123] Kamusta. *\$
🔍 cimd	ר [0−4][0−9]: [0−9]+. * ^L \$
eiscovpn	^ ?
o citrix	28. K X
ounte	^ .*cstrikeCounter-Strike
106 items	

导入后,我们就可以在 ip firewall 中通过 Layer7 Protocols 参数调用,并做相应的规则处理,下面是一个在 防火墙得 Filter Rules 里面调用 L7 脚本

在这里我们通过禁止登陆 QQ 为例,在这里我们禁止所有用户无法登陆 QQ。我们进入 ip firewall filter 添加一 条规则选择 chain=forward,进入 Advanced 中的 Layer7 Protocols 选项选择 qq,然后在 Action 中设置为 drop 丢弃。

YuS

New Firewall Rule
General Advanced Extra Action Statistics
Src. Address List:
Dst. Address List:
Layer7 Protocol: 🗌 qq 🗾 두

因为要禁止登陆 QQ,所以选择 action=drop 掉数据

New Firewall Rule							
General Advanced Extra	Action Statistics						
Action: drop							

11、如何配置 PPTP 和 L2TP 服务器

配置版本基于 RouteroS v6.32 后,首先我看一下 PPTP 和 L2TP 的建立,同样是在 PPP 的目录下,interface 菜单中,选择 PPTP-Server 和 L2TP-Server 并启用服务:

PPP													
Interface	PPPoE Ser	vers 3	Secrets	Pro	files	Activ	e Connec	ctions					
+ -	< X	<u></u>	T PP	P Se	anner	PPTP	' Server	SST	P Server	L2TP Se	rver	OVPN	Se
Name	A	Type		_	- 12-	MTU T:	х		Rx			Tx Pac	ke
PPTP Serve	er.					×							
		🗸 Ens	bled		L2TP S	Server							
	Max MTU:	1450						🗸 Ena	bled)	0	к	
	Max MRU:	1450				Ma	ax MTU:	1450			L Con		
	MRRU:	1600	•			M	ax MRU:	1450					
Keepalive	Timeout:	30	•				MRRU:			•	App	jiy	
Default	Profile:	defau	lt-∓		Keepa	live T:	imeout:	30		•			
- Authent:	ication —				Def	ault Pr	rofile:	defaul	lt-encrypt:	ion Ŧ			
🗸 pap	~	chap			- Aut	henti c	ation —						
🗸 🗸 mschaj	p1 🔽	mschap	2		🗹 p	ар			chap				
					🗹 m	schap1		v 1	nschap2				
Uitems					-								
								V Use	IPsec				
					L	IPsec S	Secret:	***					

在 L2TP 服务器配置下多了 Use IPsec 选项,这是在 RouterOS 6.16 后加入的 IPsec 选项,方便 windows 客户端的连接, Default-Profile 类型选择 default-encryption, Autentication 认证方式也可以选择相同方式。

这里我们举一个实例,我们建立了一个主机的 VPN 服务,同时启用 PPTP 和 L2TP 方式,分配远程 IP 为 192.168.89.2-192.168.89.254 的地址池,我用 192.168.89.1 做为 VPN 隧道的本地 IP。

首先我进入 ip pool 中配置地址池:

IP Pool						٦×
Pools U	sed Addre	esses				
+ -	T				F	ind
Name	Δ	Addre	esses	Next	Pool	-
🕆 eth		192.1	68.20.10-192.168.20.100	none		
🕆 offic	e	192.1	68, 70, 10-192, 168, 70, 100	none		
🕆 out		192.1	68. 10. 10-192. 168. 10. 100	none		
🕆 vpn		192.1	.68, 89, 2-192, 168, 89, 254	none		
	IP Pool New Address Next Po	<pre><vpn) <="" [="" es:="" me:="" ol:="" pre=""></vpn)></pre>	> <mark>7pn</mark> 192. 168. 89. 2-192. 168. 89. 254 none ₹] ‡] ▲	OK Cancel Apply Copy Remove	
4 items	(1 select	ed)				

配置好地址池后,在 PPP Profiles 中使用默认的 default-encryption 组规则,配合本地 IP 地址 192.168.89.1, 在远程 remote-address 种配置之前添加号的地址池 VPN,设置 DNS 为 119.6.6.6,其他配置参数如下:

PPP						
Interfac	e PPPoE Servers	Secrets	Profiles	Active Co	nnections	
+ -						
Name	🔺 Local Add	ress Rem	note Addres	s Bridge	Rate L.	Onl
e i i i i i i i i i i i i i i i i i i i	ult ult- 192-168-8	9 1 1 1001	<u>,</u>			def def
a dere	PPP Profile <defa< td=""><td>ult-encry</td><td>vption≻</td><td></td><td></td><td>der</td></defa<>	ult-encry	vption≻			der
	General Protoco	ls Limit	ts Queue			
		Name:	default-e	ncryption		
	Local	Address:	192, 168, 8	9. 1	Ŧ	
	Remote	Address:	vpn		₹	•
	Remote IPv6 Pref	ix Pool:				-
	DHCPv6	PD Pool:				•
		Bridge:				-
2 items	Bridge Port P	riority:				•
	Bridge Pa	th Cost:				•
	Incoming	Filter:				-
	Outgoing	Filter:				•
	Addre	ss List:				\$
	DNS	Server:	119.6.6.6			\$

在 limits 选项中,配置相应的 Idle-timeout (空闲超时时间)为10分钟、Rate-limit (带宽)为1M 上行和 2M 下行,配置 Only-one (账号是否唯一性):

PPP Profile <default-encryption></default-encryption>	
General Protocols Limits Queue	OK
Session Timeout:	Cancel
Idle Timeout: 00:10:00	Apply
Rate Limit (rx/tx): 1m/2m	Comment
- Only One	Copy
C default C no 📀 yes	Remove

在 PPP secret 中配置用户,账号 yus,密码 yus, service 参数用于选择 VPN 类型,这里设置为默认 any 这 样支持 L2TP 和 PPTP 登陆方式, profile 为 default-encryption,

PPP					
Interface	PPPoE Server:	s Secrets	Profiles	Active Connec	tions
+ - •	×	T PPF	Authentic	ation & Accoun	ting
Name	A Password	Service	Caller ID	Profile	Local Address
😯 vpn	1233	any		default	
🕜 yus	yus	any		default	
	PPP Secre	t <yus></yus>			
		Name:	yus		OK
		Password	yus	^	Cancel
		Service	any	₹	Apply
		Caller ID:	:	•	Disable
		Profile	default-e	encryption 🔻	Current
					Comment
	Locs	l Address:	:	•	Copy
•	Remot	e Address:		•	Remove
2 itoms (1)	COL PLANE TR	.e pe:			

配置完成后,我们便可以通过 PPTP 或者 L2TP 连接 RouterOS 的 VPN 服务,在 windows 下可以通过 PPTP 的方式直接连接 RouterOS 的 VPN 服务,由于 windows 要求 L2TP 进行 IPsec 的加密方式连接,所以需要在 L2TP 配置 IPsec 密钥,如果不考虑使用 IPsec 的 L2TP 连接,可以修改 windows 注册表。

YuS

L2TP Server		
	✓ Enabled	OK
Max MTU:	1450	Cancel
Max MRU:	1450	
MRRU:	•	Apply
Keepalive Timeout:	30	
Default Profile:	default-encryption Ŧ	
- Authentication -		
🖌 рар	🖌 chap	
🖌 mschap1	🖌 mschap2	
	🗸 Use IPsec	
IPsec Secret:	123	

Windows 配置在 VPN 属性中,选择"安全", VPN 类型选择"使用 IPsec 的第 2 层隧道协议(L2TP/IPsec)", 点击"高级设置",设置"使用预共享的密钥作为身份验证"

测试VPN 连接 属性	23
常规 选项 安全 网络 共享 VPN 类型(T):	
(使用 IFsec 的第 2 层隧道协议 (121F/IFsec) 高级设 数据加密 ⑪):	▼ 置(S)
a 高级属性	
 ● 使用预共亭的密钼作身份验证 (P) 密钥 (K): 123 	
 ○ 将证书用于身份验证 (C) ✓ 验证服务器证书的 " 名称" 和 " 用法" 	犀 性 (V)
	, 12 III (17)
	III III IIII IIII IIII IIIII IIIII IIIII

12、创建 PPPoE Server

通过 Winbox 配置 PPPoE 服务器,这里我们首先通过进入 PPP 目录下的 PPPoE Server, 配置 Service Name 为 MikroTik,用于 PPPoE 服务器名,并把 PPPoE 服务指向 ether2 的网卡上,其他参数如图所示:

PPP							
Interface PPPoE	Servers Se	crets Pr	ofiles A	ctive Com	nections		
+ - × ×	T						
Servic 🛆 In	nterface	Max MTV	Max MRU	MRRU	Default	Auth	entics
😗 servicel et	her2-1an	1480	1480		default	pap	chap m
	PPPoE Serv	ice Kserv	ice1>				×
	Serv	ice Name:	servi cel			OK	
	I	nterface:	ether2-1	an	Ŧ	Cancel	
		Max MTU:	1480			Apply	
		Max MRU:	1480				
		MRRU:			-	Disable	-
	Keepalive	Timeout:			-	Copy	
	Default	Profile:	default		₹	Remove	
			🖌 One Se	ession Per	Host		
1	Max S	Sessions:			-		
I item (I selected	- Authent:	ication —					
	🗸 pap		🗸 cha	ъ			
	🗸 mschaj	p1	🗸 msc	hap2			
	enabled						

这里我们选择的是 default-encryption 的 profile 规则,所有我们需要进入 profiles 中配置该规则的参数, loacl-address 为本地路由器网关 IP, remote-address 则是远程客户端 IP 地址。这里我们设置 local-address 为 192.168.10.1, remote-address 添加在 ip pool 中设置好的地址池 pppoe,然后配置 DNS 参数,其他 配置如图:

PPP		1		
Interface PPPoE Servers	Secrets Profile	Active Connec	ctions	
+ 7				
Name 🛆 Local	Address Remote A	ddress Bridge	Rate L	Only One
* 🕜 default				default
* 😭 default				default
	PPP Profile <def:< th=""><th>ault-encryption></th><th></th><th></th></def:<>	ault-encryption>		
	General Protoco	ls Limits		ОК
	Name:	default-encryp	tion	Cancel
	Local Address:	192, 168, 10, 1	₹ ▲	Apply
	Remote Address:	pppoe	₹ ▲	Comment
	Bridge:		•	Copy
	Incoming Filter:		•	Remove
	Outgoing Filter:		•	
2 items (1 selected)	Address List:		•	
	DNS Server:	61.139.2.69	\$	
	WINS Server:		\$	
	- Change TCP MSS	·		I
	• default	C no	O yes	
	1			

在 5.0 后增加了 IPv6 的支持,这里我们可以选择关闭 IPv6 的支持:

YuS



下面配置 Limits 参数, Idle-timeout 设置为 20 分钟, 即当用户在 20 分钟内没有任何数据流量就注销该用户, 每个用户带宽我们设置 512k 上行, 1M 下行, only-one 参数只该 profile 下的账号只允许一个用户登陆:



这样用户的组规则配置完成,根据需要也可以增加其他的组规则到 profile 中。接下来配置每个用户信息,进入 ppp secrets 添加用户帐号:

YuS

PPP			
Interface 3	PPPoE Serve	rs Secrets Profiles Active Connections	
+ - •	' 🗙 🗖	PPP Authentication & Accounting	
Name	A Passwor	d Service Caller ID Profile Local Add	hress Remote A
(? 123	123	pppag defeult	
🖓 yus	yus	PPP Secret (yus)	
		Name: yus	OK
		Password: yus	Cancel
		Service: pppoe 🗸	Apply
		Caller ID:	Disable
		Profile: default-encryption 🐺	Comment
		Local Address: 📃 🔻	Copy
		Remote Address: 📃 🔻	Remove
		Remote IPv6 Prefix:	
2 items (1 s	elected)	Routes:	
		Limit Bytes In:	
		Limit Bytes Out: 📃 🔻 🔻	
		enabled	

这里 Name 为用户帐号名, Password 为用户密码。Profile 选择刚才设置好的 default-encryption,根据情况也可以调用其它相应的 profile 规则。配置完用户的帐号和密码后, PPPoE 服务就可以启动。

13、如何配置 Hotspot 认证

一个网关路由器的网络参数如下:

```
WAN 口对应外网 IP 为 10.200.15.119/24,网关为 10.200.15.1
LAN 口对应内网 IP 为 192.168.10.1/24
DNS: 61.139.2.69
```

在根据这些参数我们需要先配置好 IP 地址、网关和 DNS,并打开 DNS 缓存等。

进入 ip address 配置 IP 地址:

Address List		
+- < = =	T	Find
Address 🔿	Network	Interface 🔻
🕂 10. 200. 15. 119/24	10.200.15.0	ether1-wan
🕆 🕆 192, 168, 10, 1/24	192.168.10.0	ether2-lan

进入 ip route 配置网关

Rout	te Li	st					
Rou	ites	Nexthops	Rule	es VRF			
÷		* X		T	Fi	nd all	₹
	Dst.	Address		Gateway	Distance	Routing	Ma ▼
AS -	⊳ 0	.0.0.0/0		10.200.15.1 reachable ether1-wan	1		
DAC	▶ 1	0.200.15.0	0/24	ether1-wan reachable	0		
DAC	▶1	92.168.10.	0/24	ether2-lan reachable	0		

进入 ip firewall nat 设置好 NAT 伪装:

Firewall
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols
🕂 🗕 🖌 🗶 🔽 🍸 OO Reset Counters OO Reset All Counters Find all
Action Chain Src. Add Dst. Add Pro Src. Port Dst. Port In Out Bytes Pa
0 ≓∥m srenat 60 B
NAT Rule \diamondsuit
General Advanced Extra Action Statistics
Action: masquerade

进入 ip dns 配置 DNS 缓存, DNS 和启用缓存对于 Hotspot 非常重要,如果 DNS 错误将导致用户认证跳转或 无法浏览网页:

DNS			
Static	Cache		
+ -	/ × × T	Settings	Find
#	Name	Address TTL (s)	-
	DNS Settings		
	S	ervers: 61.139.2.69	
		✓ Allow Remote Requests	
	Max UDP Packe	t Size: 512 Apply	
	Cach	e Size: 2048 KiB	
	Cach	e Vsed: 8	
			1

现在我们的基本参数已经配置完成,现在我们需要配置的 Hotspot 参数,配置 Hotspot 参数的基本流程是:

1	、先进入 ip hotspot user profile 设置用户分组规则
2	、然后在 ip hotspot user 添加用户的帐号
3	、进入 ip hotspot server profile 配置服务器规则
4	、在 ip pool 中分配 IP 地址段,根据需要启用 DHCP 服务
- 59	9- 编写:余松

5、在 ip hotspot server 添加并启用 hotspot 服务

现在我们进入 ip hotspot, 并配置 ip hotspot use profile

Hotspot						
Users User Profiles	Active Hosts I	[P Binding	s Service	Ports W	alled Garden	Walled Gar
+ - 7	Hotspot User F	rofile <d< th=""><th>efault></th><th></th><th></th><th>٢.</th></d<>	efault>			٢.
Name A Ses	General Adve	rtise Sc	ripts		OK]├───
* 🚷 default		Name:	default		Cancel	1
	Addre	ss Pool:	none	Ŧ	Apply	j
	Session	Timeout:		•	Copy]
	Idle	Timeout:	00:30:00	₹ ▲	Remove	
	Keepalive	Timeout:		•		
	Status Auto	refresh:	00:01:00			
	Share	d Vsers:	1	^		
	Rate Limit	(rx/tx):	1m/2m			
1 item (1 selected)	Addre	ss List:		₹ ▲		
	Incoming	Filter:		₹ ▲		
	Outgoing	Filter:		₹ ▲		
	Incoming Pack	et Mark:		T		
	Outgoing Pack	et Mark:		₹ ▲		
	Open Stat	us Page:	always	₹]	
			Transpar	ent Proxy	7	
	default					-

在 user profile 里面一般配置如下几个参数:

```
Idle-Timeout:用户在一定时间内没有任何流量发出后自动注销连接,这里我们设置 30 分
Keepalive-Timeout:路由器主动通过 ICMP 探测主机是否在线,如果在一定时间为探测到自动注销连接(如果用户机开
启防火墙,路由器无法探测到)
Shared-users:帐号的分享用户多少,默认为1,即仅一个用户使用该帐号。
Rate-Limit:分配每个帐号带宽,格式为"上行 / 下行",单位为 bit,只能使用整型,设置为1m/2m
Transparent-proxy:透明代理功能是否开启,如果你启用了/ip proxy透明代理,可以将该规则组的用户经过 proxy,并
能作 web 缓存的功能
其他参数请参考具体 Hotspot 手册。
```

Address pool 这个是 DHCP 的地址池,给用户分配 IP,我们可以在 ip pool 中分配地址段,具体操作请参考 RouterOS 的 DHCP 操作。

在 user 配置用户登录帐号和密码,以及所属的 profile 类型,这里默认 server 服务器为 all:

- 60 -

Server Profil	es Users User Profiles Active Ho	sts IP Bindings Service Ports Wal
+ - 🖉	🙁 🖅 🔽 OO Reset All Counte	rs
Server	New Hotspot User	🗆 🗙 e Uptin
	General Limits Statistics	OK
	Server: all Ŧ	Cancel
	Name: yusong	Apply
	Password: yus	Disable
	Address: 📃 🔻	Comment
	MAC Address:	Conv
	Profile: default 🐺	Bemore
	Routes:	Itemove
	Email:	Reset All Counters
O items	enabled	

1	
Deceword	家田生い
rasswuru:	名旧ハ VUS

Profile:用户组规则,这里选择我们之前设置的 default 规则

在 Hotspot 我们可以对本地 User 做时间和流量的限制,我们可以选择 user 下的 limits 进行设置,例如我限制 yusong 的账号只能使用 48 小时

Hotspot		
Server Profile	es Users User Profiles Active Hos	ts IP Bindings Service Ports
+ - 🗸	🗶 📋 🍸 00 Reset All Counter	2
Server	Hotspot User <yusong></yusong>	ΟΧ. υ
🤗 થી	General Limits Statistics	OK
	Limit Uptime: 48:00:00	Cancel
	Limit Bytes In:	Apply
	Limit Bytes Out:	Disable
	Limit Bytes Total:	Comment
		Сору
		Remove
		Reset All Counters
l item (1 sele	enabled	

配置完用户规则后,进入 ip hotspot server profile,配置服务器器规则。

YuS

Hotspot		
Servers Server Profiles	Users User Profiles Active Hosts I	P Bindings Service Ports
+ - 7		
Name 🛆 DNS 1	Hotspot Server Profile <default></default>	
* 🕜 default	General Login RADIUS	OK
	Name: default	Cancel
	Hotspot Address:	Apply
	DNS Name:	Copy
	HTML Directory: hotspot	▼ Remove
	Rate Limit (rx/tx):	
	HTTP Proxy:	
	HTTP Proxy Port: 0	
	SMTP Server:	
1 item (1 selected)		
	default	

这里有几个参数我们需要说明:

- **Hotspot address**: 认证服务器的 IP 地址,如果你只有一个 hotspot 认证接口,这个参数可以默认不设置,但当你有多个接口的 hotspot 接口,且每个接口不同 IP 地址段,为了用户能都能同时访问一个 IP 地址认证,我们可以设置一个静态的地址,这样可以便于网络的管理。
- **HTML Directory**: 该参数是指定 Hotspot 的认证也路径(在 Files 目录下可以找到),当你拥有多个 hotspot 认证接口时,你对不同接口的用户选择不同的认证页面,我们仅需要建立多个 server Profiles 规则。
- Rate Limit: 该 hotspot 服务器规则下的总带宽,一般建议不用设置,由我们自定义用户的带宽。

配置 login 登录方式,即用户提交账号密码时采用的传输加密方式,一般默认启用 HTTP CHAP 即可,

Hotspot		
Servers Server Profiles	Users User Profiles Active Hosts IP Bindi	ngs Service Por
+ - 7		
Name 🛆 DNS 1	Hotspot Server Profile <default></default>	
* Wyustaurt	General Login RADIUS - Login By	OK Cancel
	MAC ☐ Cookie ✓ HTTP CHAP ☐ HTTPS	Apply
	MAC Auth. Password:	Copy Remove
	HTTP Cookie Lifetime: 3d 00:00:00 SSL Certificate: none	
	🗌 Split User Domain	
1 item (1 selected)	Trial Uptime Limit: 00:30:00	
	Trial User Profile: default	
	default	

Cooke 等值一般不用选择,这里选择 HTTP CHAP 加密方式提交账号密码,HTTP PAP 是明文的账号密码提交。

至于 RADIUS 根据需要开启,如果你有对应的 RADIUS 服务器,并要使用 RADIUS 计费,这里的 Use RADIUS 必须选择

Hotspot		
Servers Server Profiles	Users User Profiles Active Hosts IP Binds	ings Service Por
+ - 7		
Name 🛆 DNS	Hotspot Server Profile <default></default>	
* 🚱 default	General Login RADIUS	ок
	Vse RADIUS	Cancel
	Default Domain:	Apply
	Location ID:	Copy
	Location Name: 📃 🔻	Remove
	MAC Format: XX:XX:XX:XX:XX:XX	
	Accounting	
	Interim Update: 📃 🗸 🗸	
	NAS Port Type: 19 (wireless-802.11) 🔻	
1 item (1 selected)		
	default	

- 63 -

配置完成以上参数后,最后我们启用 Hotspot 服务器,并选择 interface 为我们的 lan 接口:

Hotspot							
Servers Server Profiles	Vsers Vser P	rofiles	Active	Hosts	IP E	Bindings	Service Ports
+ - × × 7 I	Reset HTML	Hotspot	Setup				
Name 🛆 Int	erface	Address	Pool Pr	ofile	¢	Address	
🕜 server1 eth	er2-lan	none	de	fault			
	Hotspot Serv	ver Kserv	ver1>				×
		Name:	server1			OK	
	Int	erface:	ether2-1	lan Ŧ		Cancel	
	Addres	s Pool:	none	Ŧ		Apply	
	P:	rofile:	default	Ŧ		Disable	
	Idle T	imeout:		•		Сору	
	Keepalive T	imeout:		•		Remove	
	Addresses P	er MAC:		-	R	leset HTMI	
1 item (1 selected)	IP of DN	S Name:	0.0.0.0				
	Proxy	Status:	running				
	enabled			Н	ITTPS		

YuS

当启用完成后,所有对路由器或者外网访问都需要通过 web 认证,当用户随便输入一个网站都会跳转到认证页面,用户访问到的认证页面如下图:

	YuS					
🏉 internet hotspot >	login - Windows Internet Expl	orer		-		
🕤 🕞 🗢 🙋 http	o:// 192.168.10.1 /login		-	•		×
х 📆 🗸						
🖕 收藏夹 🛛 🏫	🥙 建议网站 🔻 💋 网页快讯库	▼ 🔛 百度				
🏉 internet hotspot	> login			- 🔊	× 🖃	e.
	Latviski					
	Please log on to use the internet	: hotspot service				
	login					
	login					
	password					
	0	K				
	Hotspot gat	EWAY				
	powered by Mikro	Tik				

我们输入账号和密码认证通过后,我们将跳转到以下页面:

🏉 mikrotik hotspot > statu	us - Windows Intern	et Explorer	4.1		
🕞 🔾 🗢 🙋 http://192	2.168.10.1/status			▼ 🗟 49	×
x 🔁 🗸					
🚖 收藏夹 🔗 🙆 建	议网站 🔻 🤌 网页的	快讯库 🔻 <mark></mark> 百度			
🏉 mikrotik hotspot > sta	atus		🏠 📼	N - 🖃	-
Ĩ		· · · ·			
	Welcom	e vusona!			
		, , , , , , , , , , , , , , , , , , , ,	1		
	IP address:	192.168.10.2			
	bytes up/down:	984 B / 1395 B			
	connected / left:	2s / 1d23h59m58s			
	status refresh:	1m			
	ю	g off			

这时我们可以在 ip hotspot active 中看到用户登录的在线情况:

Hosts IP	Bindings	Servi	ce Ports	Wall	ed (Garden	Walled	Garden	IP	List		
Domain	Address		Uptime	Ιċ	lle	Time	Session	ι T	Rx	Rate	Тx	Rate
	192.168.10	. 2	00:02:4	48	0	00:00:00	1d 23	:57:12	188	33	ОЪ	ps
	Hosts IP Domain	Hosts IP Bindings Domain Address 192.168.10	Hosts IP Bindings Servi Domain Address 192.168.10.2	Hosts IP Bindings Service Ports Domain Address Uptime 192.168.10.2 00:02:	Hosts IP Bindings Service Ports Wall Domain Address Uptime Id 192.168.10.2 00:02:48	Hosts IP Bindings Service Ports Walled Domain Address Uptime Idle 192.168.10.2 00:02:48 0	Hosts IP Bindings Service Ports Walled Garden Domain Address Uptime Idle Time 192.168.10.2 00:02:48 00:00:00	Hosts IP Bindings Service Ports Walled Garden Walled Domain Address Uptime Idle Time Session 192.168.10.2 00:02:48 00:00:00 1d 23	Hosts IP Bindings Service Ports Walled Garden Walled Garden Domain Address Uptime Idle Time Session T 192.168.10.2 00:02:48 00:00:00 1d 23:57:12	Hosts IP Bindings Service Ports Walled Garden Walled Garden IP Domain Address Uptime Idle Time Session T Rx 192.168.10.2 00:02:48 00:00:00 1d 23:57:12 188	Hosts IP Bindings Service Ports Walled Garden Walled Garden IP List Domain Address Uptime Idle Time Session T Rx Rate 192.168.10.2 00:02:48 00:00:00 1d 23:57:12 1883	Hosts IP Bindings Service Ports Walled Garden Walled Garden IP List Domain Address Uptime Idle Time Session T Rx Rate Tx 192.168.10.2 00:02:48 00:00:00 1d 23:57:12 1883 0 b

获取现时用户列表:

[admi	[admin@MikroTik] ip hotspot active> print								
Flags: R - RADIUS, B - blocked									
#	USER	ADDRESS	UPTIME	SESSION-TIMEOUT IDLE-TIMEOUT					
0	yusong	192.168.10.2	4m17s	55m43s					
[admin@MikroTik] ip hotspot active>									

用户如果需要注销,通过在浏览器里输入 192.168.10.1 进入 Hotspot 认证网关,点击 log off 退出登录页面

14、如何使用 Log Downloader 下载并记录访问日志

首先打开 Log Downloader 程序,如图所示,添加需要记录 RouterOS 的日志的 IP 地址,并配置相应的参数:

YuS

Routers		Configuration 下载日志间期
IP Address	Status	Download logs every: 15 sec
Add ip	×	Start new file every a
10 20	载的路由器IP地址	✓ Timestamps enabled
OK	Cancel	Save logs in: 保存日志的路径
		E:\log

然后在 RotuerOS 打开,并启用日志的远程记录,在 ip accounting 中设置:

Interfaces			
Bridge		IP Traffic Accounting	\mathbf{X}
PPP		Settings) W (Teb Access) 🖾 Take Snapshot	
IP	Addresses	Syc. Address / Dst. Address Packets Bytes	~
Routing	Routes		
Ports	Pool	13 624	
Queues	ARP	✓ Enable Accounting OK 2 144	
Drivers	VRRP	Account Local Iratic Cancel	
System	Firewall	Threshold: 256	leb A
Files	Socks	Accessible via We	в ок
Log	UPnP	10.200.11.100 192.168.11.254 Address: 0.0.0.0/0	-
SNMP	Troffin Blow	10, 200, 11, 100 219, 133, 48, 90	Cance
11	Traine row	10.200.11.100 222.45.101.22	Appl
USERS	Accounting	10, 200, 11, 100 210, 22, 23, 182	
Radius	Services		
Tools	Packing	50. 00, 9. 03 192, 100, 13, 56 14 4(52	<u> </u>

注意:该软件只能通过 RouterOS 的 web 端口记录,即 web 端口默认必须是 80。

15、如何配置 Web 代理

步骤一、启用 web-proxy,路径: ip/web-proxy,打开 web-proxy 后点 web-proxy-settings,选择 Enabled, 开启代理功能,图1所示。

Port: 代理端口, 默认为 8080; Max-Cache-Size: 设最大缓存的值; Cache-On-Disk: 缓存的数据保存在硬盘; 其它选项保持默认。

	YuS		
Web Proxy Access Cache Direct Com	nections Reset Counters 54 Reset A	111 Counters 🕅	eb Proxy Settings
Web Proxy Settings	· · ·	×	thod A Redi Hit
General Status Lookups	Inserts	OK	
(Enabled	Cancel	
Src. Address:	•	Apply	
Port:	8080 🗘	Clear Cache	
Parent Proxy:			
Parent Proxy Port:			
Cache Administrator:	webmaster		
Max. Cache Size:	none Ŧ KiB		
	Cache On Disk		
Max. Client Connections:	600		
Max. Server Connections:	600		
Max Fresh Time:	3d 00:00:00		
	□ Serialize Connections		
	Always From Cache		
Cache Hit DSCP (TOS):	4		
Cache Drive:	system		
	图 1		

步骤二、在防火墙中设置将 80 端口的数据重定向到 8080 端口,路径: /ip firewall nat chain=dstnat protocol=tcp dst-port=80 action=redirect to-ports=8080。图 2、图 3 所示。

General Advanced	Extra Action Statistics	
Chain:	dstnat	4
Src. Address:		
Dst. Address:		
Protocol:	□ <mark>6 (tcp)</mark>	.
Src. Port:		
Dst. Port:	80	
Any. Port:		
In. Interface:		
Out. Interface:		
Packet Mark:		
Connection Mark:		
Routing Mark:		
Connection Type:		

图 2

eneral	Advan	ed Extra	Action	Statistics	
Ac	tion:	redirect			
To Ports:		8080			

YuS

注意 web-proxy 对 CPU 要求非常高,所以当你要使用 web-proxy 缓存网页时,请选择高性能的硬件

24、如果理解 mangle 标记,什么是 prerouting,有什么作用?

Mangle 的作用是一个标记器,修改和标记经过数据流的数据包信息,可以用于路由规则、流量控制规则和 防火墙规则的调用,也可以修改 TTL 值和 TCP MSS 值等

Prerouting 通常意义是路由之前的规则标记,即进入路由器的数据,大部分策略路由规则都在次配置,进入路由器的流控规则也可以在此标记

17、如何配置 PCC 的 mangle 路由标记

我们可以通过选择 in-interface=lan 代替源地址为内网范围(如固定 IP 上网的办公室和网吧),如果内网 采 用 的 是 PPPoE 拨 号 上 网 , 我 们 需 要 通 过 源 地 址 src-address 来 定 义 内 网 范 围 , 如 src-address=192.168.100.0/24 规定需要做 PCC 地址范围,下面是普通局域网上的脚本如下:

```
/ip firewall mangle
add action=mark-connection chain=prerouting comment="" disabled=no \
    in-interface=lan new-connection-mark=1st_conn passthrough=yes \
    per-connection-classifier=both-addresses:2/0
add action=mark-routing chain=prerouting comment="" connection-mark=1st_conn \
    disabled=no in-interface=lan new-routing-mark=1st_route passthrough=yes
```

提取走第二条线路的连接标记取名位 **2nd_conn**,并从连接里提取路由标记名位 **2nd_route**,设置: per-connection-classifier=both-addresses:2/1,设置 in-interface=lan:

/ip firewall mangle
add action=mark-connection chain=prerouting comment="" disabled=no \
 in-interface=lan new-connection-mark=2nd_conn passthrough=yes \
 per-connection-classifier=both-addresses:2/1
add action=mark-routing chain=prerouting comment="" connection-mark=2nd_conn \
 disabled=no in-interface=lan new-routing-mark=2nd_route passthrough=yes

在 winbox 在 mangle 中设置完成后如下:

Fil	ter Rules NAT Ma	ngle Servia	ce Ports Conne	ctions Address Lists	Layer7 Protocols	
💠 🗕 🖌 🗶 🔽 🍸 OO Reset Counters OO Reset All Counters Find prerouting ∓						
# 3	Action	Chain	In. Interface	Per Connection Clas	New Connection Mark	B 🔻
:	;; pccl					
0	🖉 mark connection	prerouting	lan	both addresses:2/0	1st_conn	0 B
1	🖉 mark routing 👘	prerouting	lan			ΟB
:	;; pcc2					
2	🖉 mark connection	prerouting	lan	both addresses:2/1	2nd_conn	0 B
3	🖉 mark routing 👘	prerouting	lan			OB

以上配置完成后,我们可以在 ip route 配置路由规则

20、Nth 和 PCC 有什么区别?

Nth 第 N 次的排列是基于连接的负载均衡,是重新排列连接分组,将每次新建立连接的数据进行负载 均衡。PCC 每次连接分类是通过哈希算法计算连接关联的负载均衡,将相关链接的 IP 地址进行负载均衡。 在实际使用时 PCC 稳定性比 Nth 高,但负载流量 Nth 比 PCC 相对较均衡,但建议使用 PCC 负载均衡, 避免因 Nth 出现的网银和论坛后台无法登陆的问题。具体可以参考《RouterOS 入门到精通》

21、什么是 PCQ 动态流控?

PCQ 是 Pre Connection Queue,每次连接队列,是通过下面主机连接进行分类的一种流量控制方式,通 过源和目标 IP 地址来判断当前网络使用情况,通过 PCQ 算法对带宽进行动态分配,最好的 PCQ 设置方式 是先在 ip firewall mangle 里的 prerouting 和 forward 链表标记对应数据包,在 queue tree 对标记好的数据 包进行动态流控。原理如图所示:



10、如何设置 simple queue 里的 PCQ 限速

这里我们按照 RouterOS 6.0 版本来做配置,首先进入 Queue Type 中配置 PCQ 的上行和下行分别为 512k 和 1m,设置 pcq-download-default 为 1M,在线用户数 100 人,我们增加 total-limit,因此是 50× 100=5000,下行分类为 dst-address

首先进入 queue type,选择 pcq-download-default 和 pcq-upload-default 规则

YuS

	YuS	
Queue Type <pcq-down< th=""><th>load-default></th><th></th></pcq-down<>	load-default>	
Type Name:	cq-download-default	OK
Kind:	pcq Ŧ	Cancel
Rate:	1M	Apply
Limit:	50	Copy
Total Limit:	5000	Remove
Burst Rate:	▼	
Burst Threshold:	▼	
Burst Time:	00:00:10	
- Classifier Src. Address Src. Port	✓ Dst. Address □ Dst. Port	
Src. Address Mask:	32	
Dst. Address Mask:	32	
Src. Address6 Mask:	128	
Dst. Address6 Mask:	128	
default		

上行分类选择 src-address,并配置 512k 的上行流量配置如下:

Queue Type <pcq-uplo< th=""><th>ad-default></th><th></th></pcq-uplo<>	ad-default>	
Type Name:	pcq-upload-default	OK
Kind:	pcq Ŧ	Cancel
Rate:	512k	Apply
Limit:	50	Copy
Total Limit:	5000	Remove
Burst Rate:		
Burst Threshold:	•	
Burst Time:	00:00:10	
- Classifier		
🗸 Src. Address	Dst. Address	
Src. Port	🗌 Dst. Port	
Src. Address Mask:	32	
Dst. Address Mask:	32	
Src. Address6 Mask:	128	
Dst. Address6 Mask:	128	
default		

在配置好 Queue Type 后,进入 Simple Queue 中配置流量控制规则,这里在 General 中配置总下行带宽为 10M,总上行带宽为 5M,内网地址段为 192.168.10.0/24:

Simple Qu	ieue (PCQ)	,						
General	Advanced	Statistics	Traffic	Total	Tot	al Statistics		
	Name:	PCQ						
	Target:	192.168.10.0,	/24					₹ \$
	Dst.:					•		
		Target Upload				Target Download		
Ma	x Limit:	5m			Ŧ	10m	Ŧ	bits/s
-A- Burs	st							
Burs	t Limit:	unlimited			Ŧ	unlimited	₹	bits/s
Burst Th	reshold:	unlimited			Ŧ	unlimited	₹	bits/s
Bur	st Time:	0				0		s
-▼- Time	e							

进入 advanced 菜单, 配置 Queue-type 类型,选择上行和下行为 PCQ 类型 pcq-download-default 和 pcq-upload-default:

Simple Queue 付	cq>					
General Advan	ced Statistics Traffic Total Total Statistics					
Packet Marks:	\$					
Target Upload Target Download						
Limit At:	unlimited ∓ unlimited ∓ bits/s					
Priority:	8 8					
Queue Type:	pcq-upload-default 🗧 pcq-download-default 🗧					
Parent:	none					

这样 PCQ 配置就完成,只需要在 simple queue 中配置一条规则,就可以控制所有 192.168.10.0/24 用户的流量。

22、什么是 HTB?

HTB (Hierarchical Token Bucket)算法的流量管理功能,可有效提高带宽利用率和限制各种网络流量等。对于正常上网的内网主机,系统将允许它偶然突破最大限速;相反,对于长期下载的内网主机,系统将会减小它的带宽,使其对其他主机的影响降到最低。

支持根据 IP 地址、协议、端口等信息对数据流进行优先级设置,然后针对不同类别的数据流进行带宽控制。 指定主机或服务预留带宽、限制最高带宽,也能实现平均分配带宽,并进行优先级管理,特别适合语音视频和数 据混合的网络。

HTB 等级令牌桶允许创建一个等级队列结构,并确定队列之间的关系,就像"父亲与儿子"或"兄弟之间"。

一旦队列添加了一个 Child (子队列) 将会变为 inner(内部队列),所有向下没有 Children (子队列) 称为 Leaf 队列 (叶队列),内部队列仅负责传输的分配,所有 Leaf 队列对符合的数据进行处理。在 RouterOS 必须指定 Parent(父级)选项并指定一个队列为子队列。

- 72 - 编写:余松


如何配置两张网卡的二层桥接?

把接□ ether1 和 ether2 放在一个桥里:

添加一个桥接口,命名为 MyBridge:

/interface bridge add name="MyBridge" disabled=no

把 ether1 和 ether2 添加到 MyBridge 界面:

/interface bridge port add interface=ether1 bridge=MyBridge /interface bridge port add interface=ether2 bridge=MyBridge

Wlan 无线应用 FAQ

1、应该把中心 AP 放在那里?

中心 AP 应该被放在一个地区的制高点,使得周围的用户都在视距范围内,例如高层建筑的屋顶,铁塔等

2、构建一个中心基站需要什么?

中心基站设备组成包括 MikroTik 无线路由器,全向天线或者扇区天线与设备连接的馈线、电源等, MikroTik 路由器连接有线网络,路由器配置为桥接模式,用于连接无线和有线网络,通过全向天线将信号发送到周边的客户。

3、一个中心基站能连接多少个客户端?

支持 2007 个客户端, 然而实际情况并不是如此, 需要根据系统的性能和承载能力。实际环境中终端 PC 的数量, 带宽情况和信号连接状态都会影响, 802.11a 下支持 20-30 个左右客户比较合适, 802.11bg 下接入 端最好在 10-20 个客户端, 如果你通过流量控制和数据过滤就能更好的对他们进行管理。

4、我需要连接一个客户端的网络,应该怎么做?

你需要一个客户端设备(CPE),例如一个 MikroTik 无线路由设备、以太网接口、定向天线、低损耗馈线。 MikroTik 无线路由器可以为本地客户端的网络提供需多功能,如防火墙、NAT、流量控制、DHCP 服务等。 定向天线应该安装在可以看见中心基站的位置。

5、每个系统的传输速度如何?

RouterOS 支持 802.11abgn 无线传输协议, 2.4GHz 在 802.11b 模式下,数据传输是 11Mbps。然而实际吞吐 量在 5-6Mbps。5GHz 在 802.11a 模式和 2.4GHz 的 802.11g 模式下,数据传输为 54Mbps。

5GHz 的 802.11a 模式下,为得到理想的带宽,在中心基站和客户端最好使用 800MHz 的 CPU。同样 RouterBOARD 系列建议使用 400 系列和 600 系列。所有用户都可以分配到相同的带宽。

6、能否限制每个用户的带宽?

是的,可以限制每一个用户的带宽速度,通过 RouterOS 的 queue 选项,如果你是 bridge 桥接无线网卡和有 线网卡,请将 bridge setting 里的 use-ip-firewall 选项开启。

7、中心基站与客户端之间无线传输最大距离能达到多少?

最大距离和天线、馈线、传输功率和信号接收的灵敏度、周围环境和天线安放的位置等有关系。

在 2.4GHz, 中心基站和客户端通常不会超过 10-12km.

在 5GHz,我们已测试中心基站使用 17dBi 平板天线,客户端使用 30dBi 圆盘抛物面天线连接距离在 25 公里, 实际传输速率 10Mbps

8、我能否从设备使用更长的馈线连接到天线?

可以,但无线传输距离和信号会受到影响。

9、我是否使用功率放大器增加距离?

可以,功率放大器有增强功率的作用,增加传输距离。同样他也可以连接馈线,增加馈线的传输距离。

10、无线连接是否要求在视线范围内?

是的,视距范围内总是被需要的,直接能看到对方,即两个连接点中间不能存在障碍物。

11、什么是 Fresnel 区?

Fresnel 区是一个视线区域的无线电波分布范围,这个区域必须无障碍,否则信号强度会被削减。例如 在一个 16 公里使用 5.8G 连接的无线,60%的 fresnel 区是一个 8.7 米的圆球区,在 2.4GHz 同样的距离是 13.6 米。

-74- 编写:余松



12、我是否可以将两个无线网络桥接?

是的,能使用 MikroTik 无线路由器建立透明桥接在两个设备间,具体可查看 RouterOS 技术文档。

13、安装一个 Wlan 无线系统需要多长时间?

一个基本的无线系统,如包含 3-5 个客户端的系统,在人员足够的情况下需大概 1-2 天时间

14、Wlan 运行在 Station 模式下是否能做桥接?

不能, station 模式不支持桥接功能, station 应用于三层的 IP 通信连接。

15、Wlan 桥接模式一般使用哪种?

一般 RouterOS 的桥接模式选择 ap-bridge 对 station-wds, 需要开启 WDS 选项, 并设置默认的桥接参数。

16、802.11n 或 ac 能使用 wds 模式吗?

在 5.0 前 RouterOS 对 802.11n 仅支持 EoIP 隧道的传输模式,在 5.0 后启用 Nv2 协议后支持高带宽传输 的 WDS 模式。802.11ac 在 RouterOS 6.0 出现,也是通过 Nv2 协议完成配置

17、RouterOS 最大的 5G 传输带宽能达到多少

我们所测试到的单网卡,最大单向带宽在 5G-Turbo 模式下,可以达到 75Mbps,双向带宽在 40Mbps 左右,使用 802.11n 的 5G 传输,可以获得更高的带宽,合适的环境和设备下可以得到近 200Mbps 的带宽。

18、mode=bridge 模式支持那种连接方式

采用 bridge 模式只能支持与 ap-bridge、station-wds 和 bridge 连接的通信,即只支持点对点无线连接,如果你采用 RB411 无线设备 RouterOS 是 L3 级,那么 2 个 RB411 点对点通信只能使用使用 bridge 模式。在 5.0 版本后出现的 station-bridge 模式也是可以和 bridge 通信

19、什么是 Nstreme

Nstreme 是 MikroTik 独立开发的一套无线传输协议,是将多个帧进行重组,即将数据量较小的帧重新 组合成大的帧进行转发,提高数据传输的效率,有助于 Wlan 无线传输带宽的提升,5.0 后 Nstreme 改进版 本 Nv2(Nstreme version2)采用 TDMA 技术有效的支持了 11n 的高带宽传输。

20、什么是 Nstreme Dual

- 75 - 编写:余松

MikroTik 开发的双向传输协议,即每个设备采用两个无线模块,一个无线模块做 tx (发送),一个无线模块做 rx (接收)把数据接收发送分离成两个无线传输的方式,有助于提高无线传输的带宽和效率。

21、什么是 Nv2 协议

Nv2 是 MikroTik 为 802.11n 优化的私有无线协议,基于 TDMA 技术(Time Division Mulitple Access 时分 多址), Nv2 基于 TDMA 好处在具有更大的吞吐量、低延迟、适用于点对多点网络连接。

TDMA 是一个频段访问共享网络,允许多个用户在同频率下通过在不同时间段信号间隔访问方式,在属于 他自己的时间间隔内,每一次用户传输一连串的数据。这个允许多个网站共享相同的传输介质,在一段时间内使 用一部分的频率信道

工作在 Atheros 芯片上,支持 802.11n 系列芯片包括 R52n、R52Hn、AR9220 和 AR9300 系列芯片等,从 RouterOS v5.0beta5 版本开始支持 nv2 协议,你可在 wireless 菜单下配置 Nv2。

21、WLAN 与 WiFi 区别

WLAN 是 Wireless Local Area Network 的缩写,指应用无线通信技术将计算机设备互联起来,构成可以互相通信和实现资源共享的网络体系。无线局域网本质的特点是不再使用通信电缆将计算机与网络连接起来,而是通过无线的方式连接,从而使网络的构建和终端的移动更加灵活。Wi-Fi(WirelessFidelity),无线保真技术与蓝牙技术一样,同属于在办公室和家庭中使用的短距离无线技术。WI-FI是 WLAN 的一个标准 WLAN 是无线局域网,无线局域网是由无线设备构成的,包括无线路由器或其他发射装置以及各种例如笔记本、平板电脑、手机等网络终端,设备之间是通过 WiFi 无线技术连接的。

22、RB751U 天线选择问题

RB751U 集成一个 2GHz 802.11bgn 无线网卡,并内置了 PIF 2.5dBi 天线。同时提供一个外接天线的 MMCX 接头。由于该设备提供内置和外置天线,所以需要特别说明天线在 wireless 选项中的配置如下:

Chain0
o one antenna for TX
o one antenna for RX
Chain1
o one antenna for TX/RX
o MMCX 外接天线接口

如果启用 MMCX 接口,需设置天线模式为 antenna-b,在 wireless HT 菜单下禁用内置的 Chain1 天线

802.11 无线配置

1、如何配置无线点对点

设置在 ap-bridge 和 station-wds 模式的我们分以下步骤:

- 1、 在 ap-bridge 和 station-wds 中添加 bridge, 定义 bridge 的接口,并分配管理的 IP 地址
- 2、 配置 ap-bridge 和 station-wds 的无线参数
- 3、 检查桥接连接情况

步骤 1: 进入 bridge 添加 bridge1 的桥接,通常情况下我会开启 rstp 协议,启用生成树协议:

Bridge Ports Filters NAT Hosts Ports Filters NAT Hosts Find Name Type Tx Rx Tx P Rx F MAC Address Find Name Type Tx Rx Tx P Rx F MAC Address Find Name Type Tx Rx Tx P Rx F MAC Address Find Name Type Tx Rx Tx P Rx F MAC Address Find Name Type Tx Rx Tx P Rx F MAC Address Find Name Find Find Find	💷 Bridge						23
Name / Type Tx Rx Tx P Rx P MAC Address R 4thbridge1 Bridge 40.0 kbps 7.7 kbps 13 12 00:00:42:16:FF:6B Image: String and the	Bridge Ports Filter	rs NAT Hosts	5				Find
K 12 bridge 40.0 kbps 7.7 kbps 13 12 00.00.42216.FF.65 Image 40.0 kbps 7.7 kbps 13 12 00.00.42216.FF.65 Image Image 40.0 kbps 7.7 kbps 13 12 00.00.42216.FF.65 Image Image Image 00.0000000000000000000000000000000000	Name A	Type	Tx	Rx	Tx P R	x P MAC Ad	dress 🔻
		Interface < br General STP S Protocol Prio Max Message Forward D Transmit Hold C Ageing	ridge1> tatus Traff Mode: C nor rity: 8000 Age: 00:00 ealy: 00:00 ount: 6 Time: 00:05	fic te C stp :20 :15	• rstp hex	OK Cancel Apply Disable Comment Copy Remove	

YuS

添加 ether1 和 wlan1 到 brdige1 桥接中,这里在 interface 中分别添加 ether1 和 wlan1 进入 bridge1 中。这 样 ether1 和 wlan1 就实现了桥接功能,能实现数据二层的透明传输:

<u>.</u>	Bridge						(×
В	ridge Ports	Filters NAT Hos	sts					
4	F — 🖌 🕽	K 🗖 🍸					F	ind
	Interface	∧ Bridge	Priori	Path Cost	Hor	Role	Root P	-
	4 thether1	bridge1	80) 10		designated port		
I	1 ⊐1wlan1	bridge1	80) 10		disabled port		
			Bridge Port <e< th=""><th>ther1></th><th></th><th></th><th>×</th><th></th></e<>	ther1>			×	
		Ger	neral Status				OK	
			Interface:	ether1			Cancel	
			Bridge:	bridge1			Apply	
			Priority:	80		hex	Disable	
			Path Cost:	10			Comment	
			Horizon:			▼ [Сору	
2	itome (1 malas	tod)	Edge:	auto		.	Remove	
2	rtems (r sered	Poi	int To Point: [auto		₹		
		1	External FDB:	auto		Ŧ		

注: 在 RouterOS3.0 的 bridge 中增加了一个设置选项,是否选择 ip firewall 过滤,如果不使用 ip firewall 过滤路由器的桥接转发速度将提升性能,但如果你要求对无线传输过程中的 IP 数据进行过滤处理,那就需要开 启 use-ip-firewall 功能:



注: 以上配置操作适用于 ap-bridge 和 station-wds 设备

设置完桥接后我们进入 ip address 给 **ap-bridge**和 station-wds 的 bridge 配置一个 IP 地址 192.168.10.1/24 和 192.168.10.2/24,用于管理设备和监测用。这样 wlan1 口和 ether1 都能分配到这个地址。命令如下:

ap-bridge 设备 /ip address add address=192.168.10.1/24 interface=bridge1 station-wds 设备 /ip address add address=192.168.10.2/24 interface=bridge1

步骤 2:桥接和 IP 地址设置好后,现在配置 ap-bridge 和 station-wds 的无线参数。

设置 ap-bridge 的无线,这里 mode=ap-bridge, band=5G, frequency=5200, SSID=CDNAT

III Wireless Tables	X
Interfaces Nstreme Dual Access List Registration Connec	t List Security Profiles
	Find
Name 🛆 Type Tx Rx Tx R MAC Add	ress ARP Mode 🔻
<pre></pre>	2:2B:7 enabled ap bridge
Interface <wlan1></wlan1>	
General Wireless WDS Nstreme Status	OK
Mode: ap bridge 두	Cancel
Band: 5GHz Ŧ	Apply
Frequency: 5200 7 MHz	Dirahla
SSID: CDNAT	
Scan List: 📃 🔻	Comment
Security Profile: default ∓	Torch
Antenna Mode: antenna a 두	Scan
	Freq. Usage
Default Al IX Nate.	Align
berault cilent ix hate.	Sniff
✓ Default Authenticate	Snooper
✓ Default Forward Hide SSID	Report Configuration
Compression	neset configuration
F	Advanced Mode

配置 ap-bridge 的 WDS 模式, 配置参数 wds-mode=dynamic-mesh(动态方式), wds-default Bridge=bridge1 (将连接无线添加到 bridge 中)

💷 Interfa	ce <v< th=""><th>vlan1></th><th></th><th></th><th></th><th>—</th></v<>	vlan1>				—
Wireless	WDS	Nstreme	Status	Compression Status		ОК
	WDS	₹	Cancel			
WDS Defau	ilt Br	idge: br	dge1		₹	Apply
			WDS Igno	re SSID		Disable
						Comment

配置 station-wds 端的设置只需要将 Mode=station-wds band=5G, SSID=CDNAT, 不需要设置 Frequency 参数, station-wds 在匹配 Band 和 SSID 后会自动搜索:

Interface <wlan1></wlan1>	
General Wireless WDS Nstreme Status	ОК
Mode: station wds	₹ Cancel
Band: 5GHz	▼ Apply
Frequency: 5200 Ŧ	MHz Dischla
SSID: CDNAT	

在 station-wds 模式下与 ap-bridge 的 WDS 参数配置相同

💷 Interfac	e <wlan1></wlan1>				.
Wireless	WDS Nstrem	e Status	Compression Status		ОК
	WDS Mode:	lynamic me	sh	Ŧ	Cancel
WDS Defaul	t Bridge:	ridgel 👘		₹	Apply
		WDS Igno	ore SSID		Disable
					Comment

步骤 3: 当配置完成后,我们可以通过在 ap-brdige 端的设备查看是否连接,如果正常连接后 ap-bridge 端 的 Wireless Tables 下会在 wlan1 前现时 "R",并增加一个 wds1 的无线接口。

	💵 Wireless Tables										
Int	Interfaces Nstreme Dual Access List Registration Connect List Security Profiles										
+											
	Name 🛛 🕹	Туре	Tx	Rx	Tx H	R	MAC Address	ARP	Mode	Band	-
R	«🐎 wlani	Wireles	O bps	424 bps	0	1	00:00:42:2	enabled	ap bridge	5GHz	
DRA	≪-≫wds1	WDS	O bps	424 bps	0	1	00:00:42:2	enabled			

在 ap-bridge 下的 Bridge 中可以看到, WDS 模式自动将 wds1 接口添加到 Port 中:

	Bridge								1	×
Bri	dge Ports	Filte	ers NAT	Hosts						
÷		× 6	- 7						F	ind
	Interface	A	Bridge		Priori	Path Cost	Hor	Role	Root P	•
	⊈ tether1		bridge1		80	10		designated port		
D	⊈t wds1		bridge1		80	100		root port	100	
	⊈t wlan1		bridge1		80	10		designated port		

我们可以通过在无线注册信息列表中查看信号强度:

	/ir	eless	Tables												×
Inte	rf	aces	Nstreme Du	ıal	Access	List	Regi	strat	ion	Connect	Lis	t Secu	ty Pr	ofiles	
	5	T	🚝 Reset												Find
	E.	MAC A	ddress		Inte	Uptim	e	AP	WDS	Last A.	Si	gnal	Tx/Rx	Rate	-
(D.	00:00	:42:23:D2:4	46	wlani	00:1	1:16	no	yes	0.4	30	-63	54Mbps	/54Mbps	

这里显示的是-63,信号能连接使用的最低值在 "-88 到-90",数字越接近正数 "1"信号越强。Station-wds 端在连接后会自动适用 ap-bridge 的参数,并正常通信。

2、如何设置 RouterOS 无线 AP 覆盖上网

假设我们有一个校园的广场区域需要进行 WiFi 的覆盖,采用 802.11bg 的无线协议,对周围 100 米范围的用户 进行无线上网覆盖,并对无线进行加密,这里我们采用 12dBi 的全向 2.4G 天线

进入 RouterOS 打开 wireless 菜单,可以看到无线网卡(要求无线网卡是 Atheros 芯片),如果是新安装到 RouterOS 上的无线网卡,默认是灰色被禁用,所有首先要启用网卡

Interfaces	
Wireless	💷 Wireless Tables 🛛 💌
Bridge	Interfaces Nstreme Dual Access List Registration Connect List Security Profiles
PPP	
Mesh	
IP D	Name / lype L2 M10 lx Kx lx r Kx r. ▼ R ∰wlani Wireless (Athero 2290 75.3 kbps 9.1 kbps 25 13
IPv6 🗅	
System 🗅	
Queues	
Files	
Log	
Radius	
Tools D	
New Terminal	
Make Supout.rif	
Manual	
Exit	▲ I item out of 8 (1 selected)

当我们启用网卡后,我们双击网卡打开配置菜单,普通设置仅需要配置一下几个参数:

- 1、 mode 无线配置模式,选择 ap-bridge
- 2、 band 无线频段,选择 2.4GHz-B/G
- 3、 Frequency 无线发射频率,选择 2417MHz,也可以根据实际环境选择其他频率
- 4、 SSID 身份验证,自己定义 AP 的身份名,这里设置为 cdnat
- 5、 Security-profile 安全策略,设置无线加密方式,避免其他人非法接入

Interface <wlan1></wlan1>	
General Wireless WDS Nstreme Status	
Mode: ap bridge 🖉 🗸	
Band: 2.4GHz-B/G	
Frequency: 2417 🐺 MH:	z
SSID: cdnst	
Scan List:	,
Security Profile: profile1	
Antenna Mode: antenna a 🛛 🐺	
Default AP Tx Rate:	5
Default Client Tx Rate: 📃 🔻 bp:	5
✓ Default Authenticate	
Default Forward	
Hide SSID	
Compression	

这里我们设置 AP 方式为无线网桥,即桥接模式,我们需要在 bridge 里设置 ether1 与 wlan1 进行桥接,首先我 们添加一个 bridge

Interfaces		
Wireless		
Bridge		
PPP	🔳 Bridge	
Mesh	Bridge Ports Filters	
IP D	General STP Status Traffic	OK
IPv6 D	Name: bridgel	Cancel
System 🗅	R 17pp R 17pp: Bridge	Apply
Queues	MTV: 1500	
Files	L2 MTU: 1600	Disable
Log	MAC Address: 00:0C:42:2B:75:58	Comment
Radius	ARP: enabled	Сору
Tools D	Admin _ NAC Address: 00:00:42:28:75:58	Remove
New Terminal	Auniti. mac Auress. 00.00.42.20.13.30	
Make Supout.rif		Torch
Manual		
Exit		
	▲ 1 item out of 8 (1 selec	
	disabled running slave	

之后在 port 里将 ether1 和 wlan1 依次添加入 port 里,并指定 bridge 为 bridge1

💷 Bridge				
Bridge Ports Filters	💷 Bridge Port <	ether3-lan>		×
+ - × A	General Status			OK
Interface / Bri ⊈tether3-lan bri	Interface:	e theri	₹	Cancel
	Bridge:	bridgel	₹	Apply
	Priority:	80	hex	Disable
	Path Cost:	10		Comment
	Horizon:		•	Сору
	Edge.	anto	I	Remove
	Point To Point:	auto	╶╴	
	External FDB:	auto	.	
2 items (1 selected)				

配置无线传输加密

我们进入 wireless 菜单,里打开 security-profile,添加一条 profiles1 的加密策略

- 82 - 编写:余松

💷 Wireless Tab	les				— ×		
Interfaces Nst	reme Dual A	ccess List	Registration	Connect List	Security Profiles		
+ - T							
Name A	Mode	Authentic	Unicast C.	Group Cip.	WPA Pre-Share 🔻		
default	none				*****		
profile1	dynamic key	rs WPA PSK	tkip	tkip	*****		

我们添加 profile1 规则,选择 mode 为动态 key(dynamic keys),验证方式用 WPA PSK, tkip 方式, 密钥设 置为 abcabc123456

Security Profile <profile1></profile1>	×
General RADIUS EAP Static Keys	OK
Name: profile1	Cancel
Mode: dynamic keys 🐺	Apply
- Authentication Types	
V WPA PSK WPA2 PSK	Copy
WPA EAP WPA2 EAP	Remove
- Unicast Ciphers	
✓ tkip aes ccm	
Course Circle and	
- Group Cipners	
✓ tkipaes ccm	
WPA Pre-Shared Key: abcabc123456	
WPA2 Fre-Shared Key:	
Supplicant Identity:	
Group Key Update: 00:05:00	
Management Protection: allowed	
Management Protection Key:	

设置完成后,我们在 wlan1 配置上可以选择 security profile

Mode:	ap bridge 두
Band:	2.4GHz−B/G
Frequency:	2417 🐺 MHz
SSID:	cdnat 🔺
Scan List:	▼
Security Profile:	profile1 Ŧ
Antenna Mode:	antenna a 🐺

我们可以在 Registration 里可以看到客户端的链接情况,和信号强度 signal

💷 Wireless	Tables											×
Interfaces	Nstreme Dual	Access I	List	Registratio	n (Connec	t List	Sec	urity Pro	files		
Find												
Radio A	MAC Address	Inte	rface	Uptime	AP	WDS	Last A.	. S	ignal	Tx/Rx	Rate	-
<\>	00:21:00:5F:C4	:AO wlan	.1	05:48:42	no	no	0.0	00	-64	11Mbps	s-SP/54Mł	bps
*	00:1C:B3:BC:83	:82 wlan	1	00:03:30	no	no	2.9	50	-83	48МЪрз	s/36Mbps	

RouterOS 如何隐藏 SSID

3、如何隐藏 WLAN 的 SSID

打开 wlan1 无线网卡配置,勾选 Hide SSID,即隐藏无线 SSID

Interface <wlan1></wlan1>	
General Wireless HT }	CT MCS WDS Nstreme
Mode:	ap bridge 🔻
Band:	2GHz−B/G/N ∓
Channel Width:	20MHz Ŧ
Frequency:	2422 T MHz
SSID:	yusong
Scan List:	default 7
Wireless Protocol:	802.11
Security Profile:	default F
Bridge Mode:	enabled Ŧ
Default AP Tx Rate:	▼ bps
Default Client Tx Rate:	▼ bps
	✓ Default Authenticate
	✔ Default Forward
	✔ Hide SSID

4、如何使用 Access-list 控制客户端

要让 access-list 中的规则生效,我们需要将 wireless 菜单下的 default-authenticate 参数选择为 no,即默认 连接情况下客户端不允许自动验证通过

Interface <wlan2></wlan2>
General Wireless HT HT MCS WDS Nstreme NV2
Mode: ap bridge 두
Band: 2GHz-B/G/N
Channel Width: 20/40MHz HT Above
Frequency: 2412 F MHz
SSID: YuS1
Scan List: default
Wireless Protocol: 802.11
Security Profile: profile1 두
Bridge Mode: disabled 두
Defeult àP Ty Rete:
berault A IX nate.
Default Client Tx Rate: ▼ bps
Defenit Anthenticate
Default Retword
Vil. CCTD
Lide 27D

当我们关闭掉 default-authenticate,所有连接 AP 的客户端或者 station 要会进入 access-list 进行匹配,如果没有匹配的设备将无法连接到 AP。这样的操作类似于我们有线网络中通过 MAC 地址绑定计算机一样

假如我们有这样一个客户端要对其进行连接控制

- MAC 地址为: 00:bc:32:1a:dd:09
- 连接无线网卡 wlan1

Wireless Tables	
Interfaces Nstreme Dual Access List Registration Connect Li	st Security Profile
+ - 🖌 🗶 🗖 🍸	
# MAC Address / Interface ∇ Signal Authentic	ation Forwarding
0 ♦00:BC:32:1A: wlan1 -120120 yes	yes
AP Access Rule <00:BC:32:1A:DD:09>	
MAC Address: D0:BC:32:1A:DD:09	_ ▲ ОК
Interface: wlani	
Signal Strength Range: -120120	Apply
AP Tx Limit:	▼ Disable
Client Tx Limit:	▼ Comment
Authentication	Copy
✓ Forwarding	Remove
1 ite Private Key: none 🐺 Ox	
Private Pre Shared Key:	
Management Protection Key:	
- - Time	
enabled	

在 access-list 规则中的 authenticate 参数,当我们在规则中关闭后,表示对该用户拒绝连接到 AP,例如我 们要禁止 MAC: 00:AC:3A:1A:CD:02 的连接

AP Access Rule <00:AC:3A:1A	:CD:02>	
MAC Address:	00:AC:3A:1A:CD:02	OK
Interface:	wlani 🔻	Cancel
Signal Strength Range:	-120 120	Apply
AP Tx Limit:	▼	Disable
Client Tx Limit:	▼	Comment
	Authentication	Сору
-	✓ Forwarding	Remove
Private Key:	none 🔻 Ox	
Private Pre Shared Key:		
Management Protection Key:		
-▼- Time		
enabled		

当远端设备是 RouterOS 的 station,我们可以通过 ap-tx-limit 和 client-tx-limit 限制 station 的连接速率

AP Access	s Rule <00:BC:32:1A	:DD:09>		
	MAC Address:	00:BC:32:1A:DD:09	•	OK
	Interface:	wlani	;	Cancel
Sign	al Strength Range:	-120120		Apply
	AP Tx Limit:	5M		Disable
	Client Tx Limit:	1M 🗸	•	Comment
		✓ Authentication		Сору
		✓ Forwarding		Remove
	Private Key:	none 🛛 🕶 Ox		
Priva	te Pre Shared Key:			
Manageme	nt Protection Key:			
- ▼ - Tim	e		_	
enabled				

如上图,我们限制了 00:BC:32:1A:DD:09 的 station 的速率,AP 发向 station 的带宽为 5Mbps, station 发向 AP 的带宽为 1M,即对于 station 而言下载为 5Mbps,上传为 1Mbps。

5、如何创建虚拟 AP(VAP)

当我们想通过一台 AP 在一个区域内建立多个 SSID,并对不同的 SSID 下的用户进行管理,例如:办公区 域里,可以区分为员工、经理和老板的 WiFi 上网,在家庭中可以用来区分父母和子女的 WiFi 上网

虚拟 AP 的好处在与通过一个物理网卡,模拟出多个 AP 信号,在一个区域内广播多个 SSID,让不同的用 户选择对应的 SSID。当然虚拟 AP 也支持加密的安全策略,有助于你对 WiFi 网络的区域划分和管理。

建立一个虚拟 AP,可以进入 wireless 目录下,点加号可以找到 VirtualAP

Wireless Tab	les									
Interfaces	Nstreme Dual	Access List	Registrat	Connect List			Security Profiles			
+-	~ X 🖻	🝸 Scanne	r Freq.	Usag	e A	lignme	nt	Wirele	ss Sniff	er
Virtual	AP		L2 MTV	Tx		Rx		Tx P	Rx P]
14/20		s (Athero	. 2290		O bps	0	bps	0	0	T
WDS		s (Athero	. 2290		O bps	0	bps	0	0	J
Nstren	ne Dual									

打开后,我们新建一个名为 wlan3 的虚拟 AP,可以看到 type 为 VirtualAP

Wireless Tabl	les									
Interfaces	Nstreme	Dus	al Access Li	st Re;	gistratio	Conne	ect List	Securi	ty Profiles	
∳ ▼	/ 🙁	C	New Interfac	e						
Name		Тy	General Wi:	reless	WDS Sta	tus Tr	affic		OK	
Wani V Wanian?		Wi Wi	Name	wlan	3				Cancel	
A Aburanc			Туре	Virt	ualAP				Apply	
			MTU	1500						
			L2 MTV	:					Disable	•
			1 10 111	00.0	0.00.00.0	2.00			Comment	t I
			MAL Address	00:0	0:00:00:0	00:00			Сору	
			ARP	enab	led				Remove	
									Torch	
									Advanced	Node
•										
2 items out	of 4									

打开虚拟 AP 的 wireless 菜单,可以到基本和物理网卡相同的配置参数,主机 Master-interface 是选择虚拟 AP 从属于那个物理网卡

Wireless Tables		
Interfaces Nstreme Dual Access Li	st Registration Connect List Security Profiles	
+ - < ≈ 🖻 🍸 Scs	New Interface	
Name / Type	General Wireless WDS Status Traffic	ОК
Image: White Amage:	SSID: V_wifi	Cancel
	Master Interface: #/an/ #/an/	Apply
	Security Profile: #Jan2	Disable
	Default AP Tx Rate: 📃 🔻 bps	Comment
	Default Client Tx Rate: 📃 🔻 bps	Сору
	✓ Default Authenticate	Remove
	✓ Default Forward Hide SSID	Torch
		Advanced Mode
•		
2 items out of 4		

我们定义了 SSID 为 V_wifi,从属于 wlan1 物理网卡,且我们选择加密的 security-profile=vip

YuS

Interface <wlan3></wlan3>		
General Wireless W	DS Status Traffic	ОК
SS	ID: V_wifi	Cancel
Master Interfa	ce: #lani 🔻	Apply
Ar	ea:▼	Disable
Security Profi	le: default ∓ default	Comment
Max Station Cou	nt: vip	Сору
Proprietary Extensio	ns: post-2.9.25 ∓	Remove
WMM Suppo	rt: disabled ₹	Torch
Default AP Tx Ra	te: ▼ bps	Simple Mode
Default Client Tx Ra	te: 📉 🔻 bps	
	✔ Default Authenticate	
	✓ Default Forward	
	Hide SSID	

添加完成后,我们可以看到 wlan3 从属于 wlan1 网卡下:

Wi	reless Tabl	les										
I	nterfaces	Nstreme Dual	Access List	Re	gistrati	on	Cor	nec	t List	Se	curity Pr	ofiles
4	┝ ▼ ━	/ X 🗂	🝸 Scanne	r	Freq. l	[sage	e	Al	i gnmen	t	Wireless	Sniffer
	Name	🛆 Туре			L2 MTV	Тx			Rx		Tx P	Rx P
	🖇 wlani	Wireless (Atheros 11N)		2290		0	bps	0	bps	0	0
	≪-≫wlan3	VirtualAP			2290		0	bps	0	bps	0	0
Х	🖇 wlanZ	Wireless V	Atheros AK521	27	2290		0	bps	0	bps	0	0

这时你可以在终端设备上搜索到 V_wifi 的信号。

6、802.11ac 双频共享 SSID

近期 MikroTik 推出的 hAP ac lite 和 hAP ac 两款基于 802.11ac 的家用办公无线路由器,支持 2.4G 和 5G 双频,也就是 802.11bgn 和 802.11ac 两个协议同时工作。由于 802.11ac 采用 5G 频率覆盖范围有限,一般仅 能在视距内传输,但能提供更高的带宽,如果 3×3 80MHz 的 MIMO 可以获得 1.3G 的带宽,如果非视距内只能 通过 802.11bgn 来弥补。下面是关于 802.11n 和 802.11ac 的技术参数,以及 hAP ac 和 hAP ac lite 在无线 MIMO 的区别

下面是关于 802.11n 和 802.11ac 的技术参数,以及 hAP ac 和 hAP ac lite 在无线 MIMO 的区别

技术规格	802.11n	802.11ac		
频率	2.4G, 5G	5G		
调制方案	OFDM	OFDM		
信道带宽	20, 40MHz	20,40,80MHz		
单流额定传输率	150Mbps (1×1 40MHz)	433Mbps (1×1 80MHz)		
多流额度传输率 450Mbps (3×3 40M		1.3Gbps (3×3 80MHz)		

	YuS		
hAP ac MIMO	3×3 支持 450Mbps	3×3 支持1.3Gbps	
hAP ac lite MIMO	2×2 支持 300Mbps	1×1 支持 433Mbps	

不过作为客户端同时只能连接一个频率,要么 2.4G 的 802.11bgn 或者 5G 的 802.11ac,一般 802.11ac 的 路由器会提供 2.4G 和 5G 两个配置,即两个无线网络一个 2.4G 或一个 5G,配置不同两个不同的 SSID。也可 以配置所谓的双频合一,即使采用双频合一相同的 SSID,客户端也只会连接到一个频率上,只是会在两个频率 上根据信号强弱做切换。很多厂商的无线路由器提供了双频合一的设置,这样的设置客户端也只是在 5G 信号好 的时候连接 802.11ac,当 5G 信号变弱后,切换到 2.4G 的 802.11bgn。

在 RouterOS 里可以看到两个无线网卡, 一个 wlan1 是 802.11bgn, 一个 wlan2 是 802.11ac

	eress labres								
In	terfaces Nstreme	e Dual Aco	ess List	Registra	tion	Conne	et Lis	st :	Secu
÷	• - 🖉 🚿		CAP	Scann	.er	Freq.	Usage		Ali
	Name	∧ Type			Tx				Rx
S	♦♦ wlani	Wireless	: (Atheros	AR9300)			0	bps	
S	∜ wlan2	Wireless	: (Atheros	AR9888)			0	bps	

两张无线网卡负责不同的协议, 那该如何设置双频合一, AR9300 负责 802.11bgn, AR9888 负责 802.11ac, 我的思路是把两个无线网卡做 WDS 漫游方式, 即通过桥接创建 rstp 协议的 WDS 无线漫游。

具体配置如下:

进入 bridge 创建 bridge1

```
/interface bridge
add name=bridge1 protocol-mode=rstp
```

进入 bridge port 将 wlan1 和 wlan2 加入 bridge1

```
/interface bridge port
add bridge=bridge1 interface=wlan1
add bridge=bridge1 interface=wlan2
```

配置路由器 bridge1 的 IP 地址,即分给用户的 IP 地址段

/ip address
add address=192.168.88.1/24 interface=bridge1

创建 DHCP 服务, 配置地址池:

```
/ip pool
add name=pool1 ranges=192.168.88.2-192.168.88.100
```

配置 DHCP 服务的接口和地址池

```
/ip dhcp-server
add address-pool=pool1 disabled=no interface=bridge1 name=server1
```

配置 DHCP 服务分配给用户的网关和 DNS 服务器

```
YuS
```

/ip dhcp-server network

```
add dns-server=192.168.88.1 gateway=192.168.88.1 netmask=24
```

配置 DNS 服务器 IP 地址和开启 DNS 本地解析

/ip dns

set servers=61.139.2.69 allow-remote-requests=yes

启用 nat 转换

/ip firewall nat

add action=masquerade chain=srcnat

无线网络配置

配置无线安全密码,创建 wpa/wpa2 的无线密码,设置为 1234567890

/interface wireless security-profiles add mode=dynamic-keys authentication-types=wpa-psk,wpa2-psk group-ciphers=tkip,aes-ccm name=yus unicast-ciphers=tkip,aes-ccm wpa-pre-shared-key=1234567890 wpa2-pre-shared-key=1234567890

配置无线网卡,设置两个无线网卡 SSID 相同取名 yus,设置 wds 模式为 dynamic-mesh, wed-default-bridge 为 bridge1

/interface wireless

set [find default-name=wlan1] ssid=yus band=2ghz-b/g/n disabled=no frequency=2422 mode=ap-bridge security-profile=yus wds-default-bridge=bridge1 wds-mode=dynamic-mesh

set [find default-name=wlan2] ssid=yus band=5ghz-a/n/ac channel-width=20/40/80mhz-Ceee disabled=no frequency=5745 mode=ap-bridge security-profile=yus wds-default-bridge=bridge1 wds-mode=dynamic-mesh

以上配置完成后,终端设备会自动连接信号最强的频率,例如首先当连接上 5G 的 802.11ac,当你移动 5G 信号变弱后,终端设备会自动连接到 2.4G 的 802.11bgn,但如果你要从 802.11bgn 切换到 802.11ac,需要你终端设备去完成,而非路由器决定。无线漫游的切换都是由终端设备决定的。