RouterOS实例分享

Yu Song

http://www.irouteros.com
http://blog.163.com/athlon_sds


学习
交流
分享

RouterOS

入门到精通

《RouterOS入门到精通》PDF

关于

- 从2003年接触和使用RouterOS，多年的学习和工作积累，并把这些过程记录和整理为笔记，在2006年把笔记转化为RouterOS教程。

- 2015年，元旦在淘宝推出《RouterOS入门到精通》v6.2 PDF电子版

- 已经更新14个版本，电子版将持续更新内容

《RouterOS入门到精通》

YuS

案例分享 1

RouterOS BRAS应用

RouterOS PPPoE认证（BRAS）

1 测试RouterOS 基于大型运营商PPPoE认证的低成本解决方案；

2 测试RouterOS基于大型运营商PPPoE认证运行的对接和稳定性；

3 测试RouterOS基于大型运营商PPPoE认证的业务承载能力；

RouterOS 测试平台

RouterOS x86：
Dell R620（Intel E5-2609×2 2.4GHz 共8核心），Intel X520-DA2网卡（Intel 82599芯片，PCI-E 8X，SFP+ ×2），RouterOS版本6.33.2

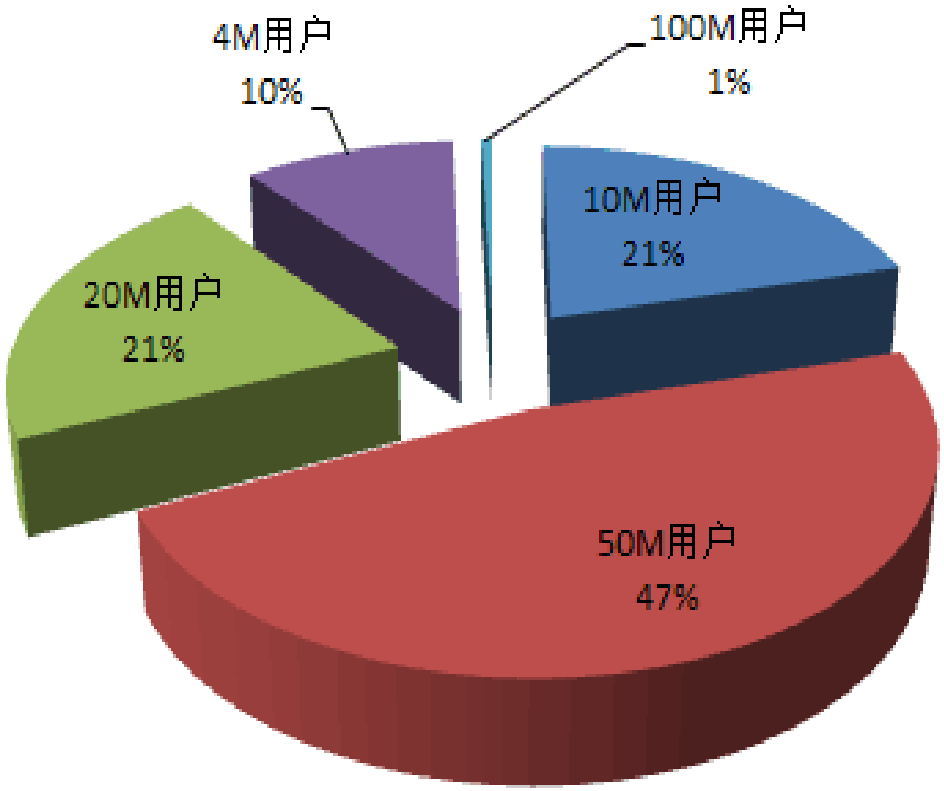
CCR1036-8G-2S+:
Tilera 1.2G 36核心，2个SFP+和8个1G电口，RouterOS版本6.33.3

CCR1072-1G-8S+：
Tilera 1G 72核心，8个SFP+和8个1G电口，RouterOS版本6.33.3

运营商网络情况

50M带宽用户为主

其次是20M和10M用户



基本配置情况

1 二层网络

运营商用户接入二层网络采用QinQ，预先配置5000条QinQ VLAN条目和5000条PPPoE Server条目

2 三、四层网络

建立OSPF路由，Connection tracking设置为auto，tcp-established-timeout=3h

3 账号

对接FreeRADIUS，新增Mikrotik-Address-List字段

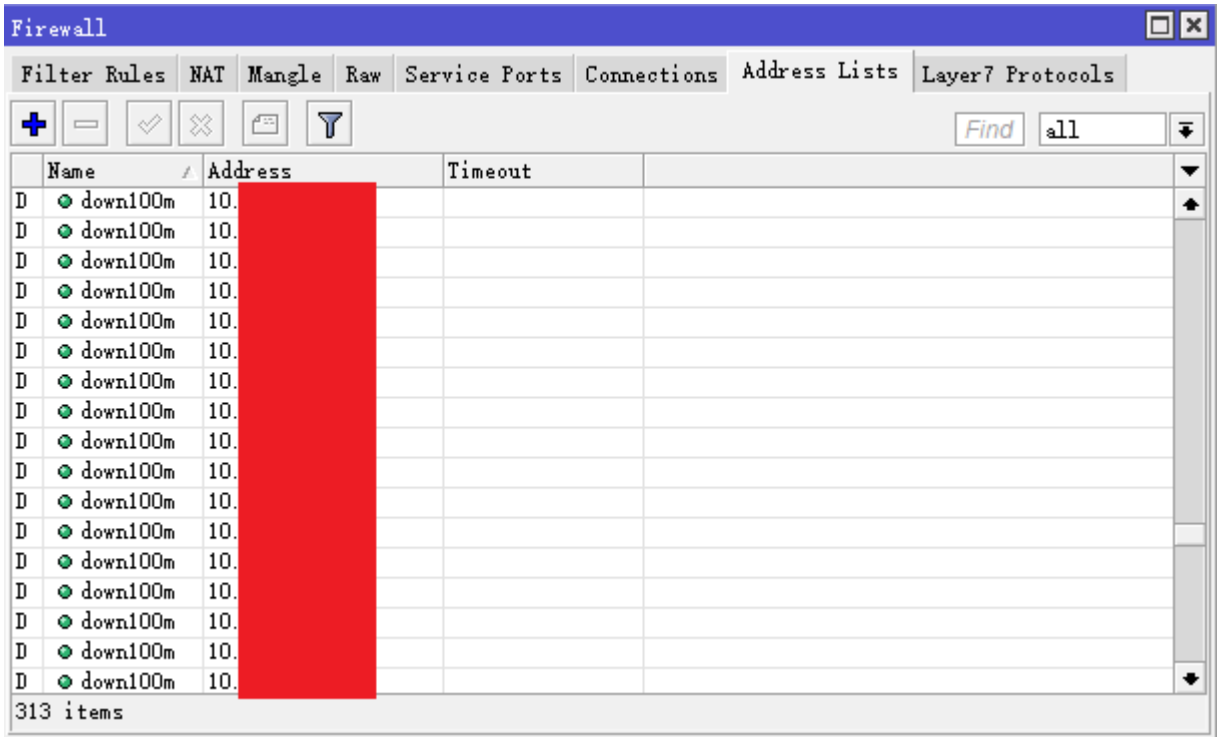
4 QoS

QoS策略采用address-list + Mangle + Simple Queue+PCQ，不采用传统simple queue

QoS 策略 Address-list

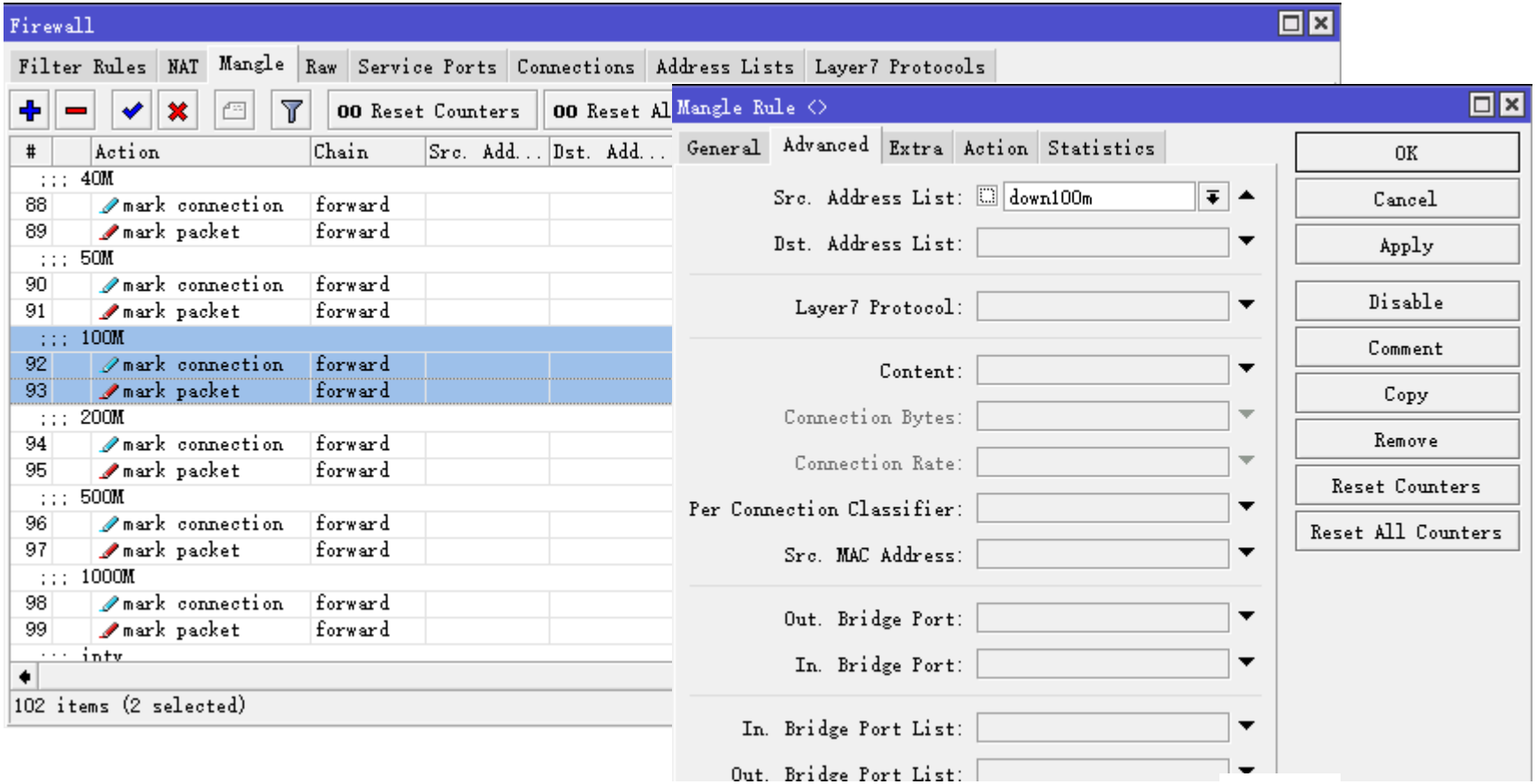
- Freeradius字典加入Mikrotik-Address-List字段，作为用户带宽分组地址列表

- 在当用户上线，在firewall address-list可以看到down100m的用户分类



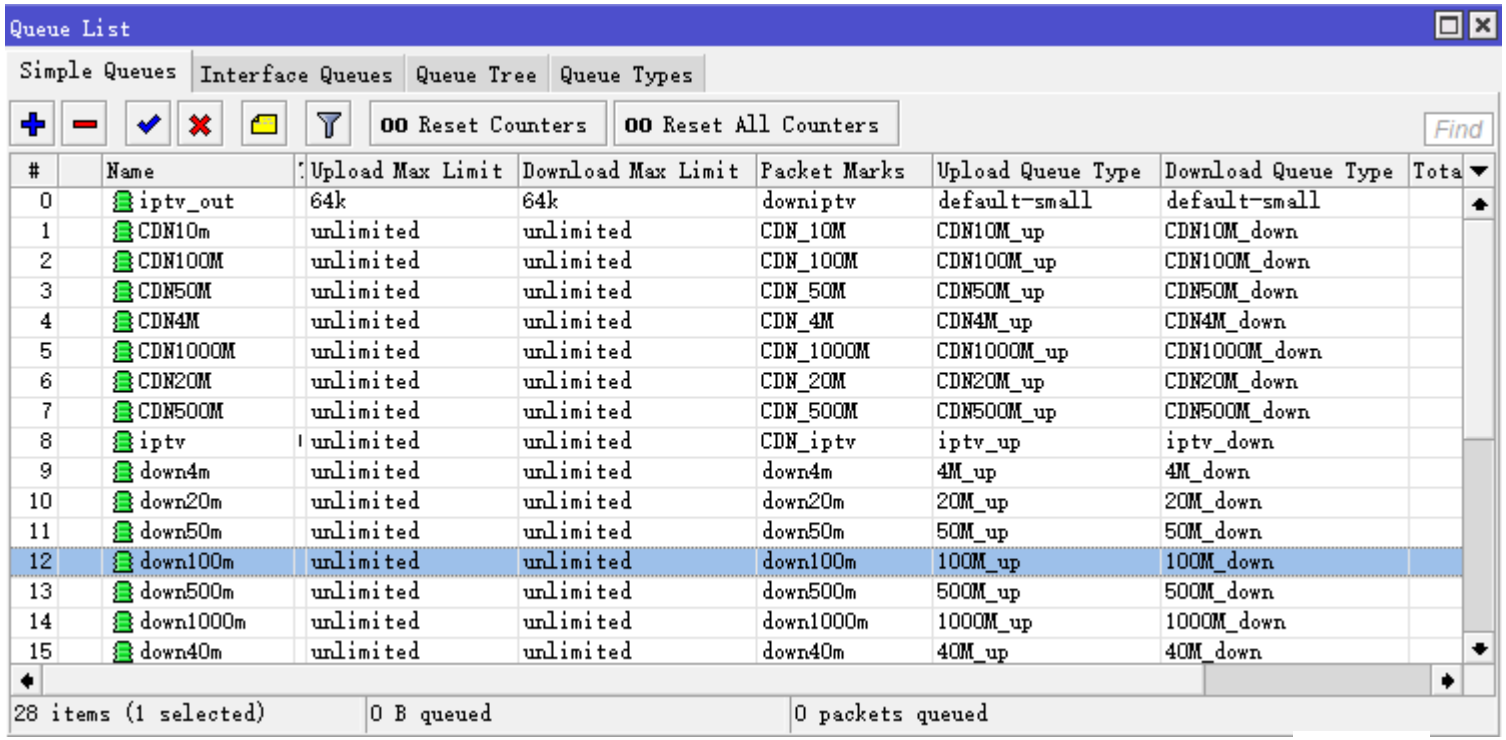
QoS 策略 Mangle

- Mangle中创建用户类型的packet标记



QoS 策略 Queue

- Queue type定义不同用户带宽的PCQ规则
- Simple queue配置对应的用户带宽PCQ规则，并利用Simple queue的FIFO算法，让到内网CDN的IP的流量优先处理



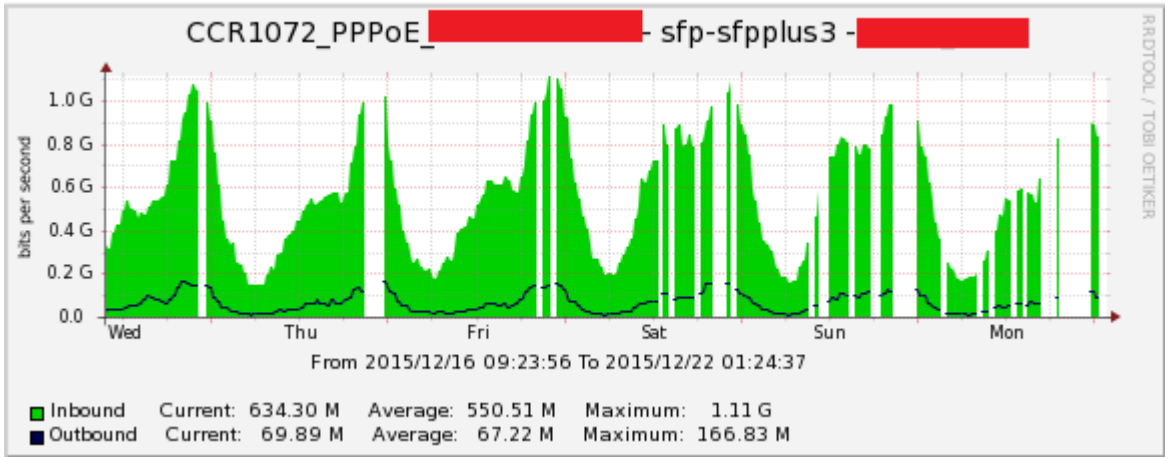
#	Name	Upload Max Limit	Download Max Limit	Packet Marks	Upload Queue Type	Download Queue Type	Tota
0	iptv_out	64k	64k	downiptv	default-small	default-small	
1	CDN10m	unlimited	unlimited	CDN_10M	CDN10M_up	CDN10M_down	
2	CDN100M	unlimited	unlimited	CDN_100M	CDN100M_up	CDN100M_down	
3	CDN50M	unlimited	unlimited	CDN_50M	CDN50M_up	CDN50M_down	
4	CDN4M	unlimited	unlimited	CDN_4M	CDN4M_up	CDN4M_down	
5	CDN1000M	unlimited	unlimited	CDN_1000M	CDN1000M_up	CDN1000M_down	
6	CDN20M	unlimited	unlimited	CDN_20M	CDN20M_up	CDN20M_down	
7	CDN500M	unlimited	unlimited	CDN_500M	CDN500M_up	CDN500M_down	
8	iptv	unlimited	unlimited	CDN_iptv	iptv_up	iptv_down	
9	down4m	unlimited	unlimited	down4m	4M_up	4M_down	
10	down20m	unlimited	unlimited	down20m	20M_up	20M_down	
11	down50m	unlimited	unlimited	down50m	50M_up	50M_down	
12	down100m	unlimited	unlimited	down100m	100M_up	100M_down	
13	down500m	unlimited	unlimited	down500m	500M_up	500M_down	
14	down1000m	unlimited	unlimited	down1000m	1000M_up	1000M_down	
15	down40m	unlimited	unlimited	down40m	40M_up	40M_down	

	CCR1036-8G-2S+	CCR1072-1G-8S+	RouterOS x86
硬件配置	2个SFP+和8个1G电口	8个SFP+和1个1G电口	4个1G电口，2个SFP+网卡
RouterOS	6.33.3	6.33.3	6.33.2
CPU	Tilera 1.2G 36核心	Tilera 1G 72核心	Dell620 Intel E5-2609×2 2.4G 8核
路由协议	OSPF	OSPF	OSPF
SNMP	开启	开启，高峰期负载高时snmp响应延迟，甚至无响应	开启
RADIUS	账号验证	账号验证	账号验证
流控策略	通过address-list分类，账号带宽采用PCQ	通过address-list分类，账号带宽采用PCQ	通过address-list分类，账号带宽采用PCQ
运用环境	PPPoE server和QinQ 5000条	PPPoE server和QinQ 5000条	PPPoE server和QinQ 5000条
	流量285Mb，CPU平均15%，在线919人	流量288Mb，CPU平均9%，在线1380人	流量最高412Mb，CPU平均30%，在线463人
	流量448Mb，CPU平均18%，在线571人	流量1.15Gb，在线1740人，CPU平均40%（短时间90%）	
运行时长	> 72h 无重启，死机	> 72h 无重启，死机	> 72h 无重启，死机
冗余电源	不支持	支持	支持
最大功耗	78w	125w	>120w

流量与CPU情况

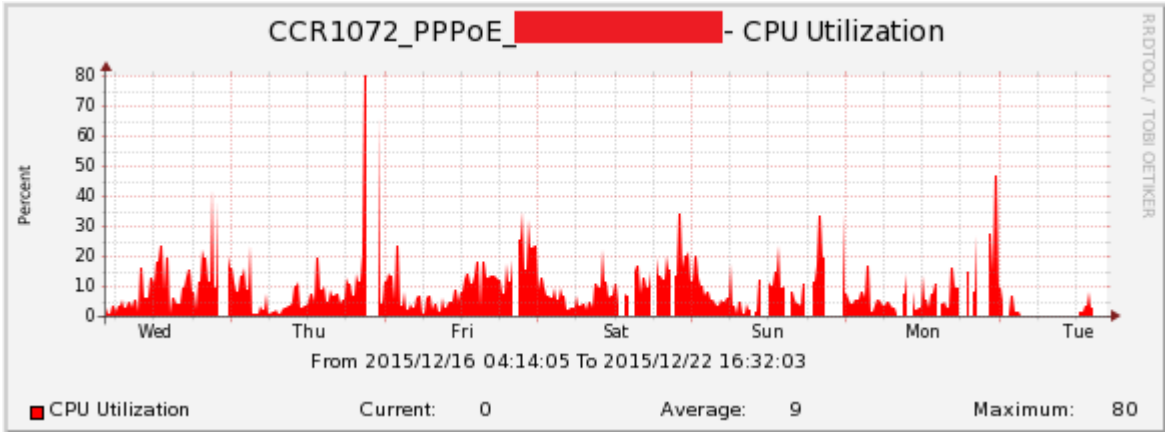
YuS

RouterOS SNMP监控在高负载情况下出现丢包



接口流量

CPU使用率



总结

1 QinQ与PPPoE

采用QinQ的运营商网络，配置条目过多，包括QinQ和PPPoE条目，导致配置复杂，配置加载时间过长，导致管理和配置问题。

2 网络情况

在线人数多少对CPU影响低，CPU消耗主要来至于会话和流量

3 QoS

通过address-list + Mangle + Simple Queue+PCQ，配合运营商的QoS策略，还可以进一步优化，例如关闭掉connection-tracking

4 其他

与专业BRAS厂商对比，不支持免认证功能，不支持主备引擎冗余，高负载情况下小问题较多，优势在于性价比，对于RouterOS来说也有自己的定位。

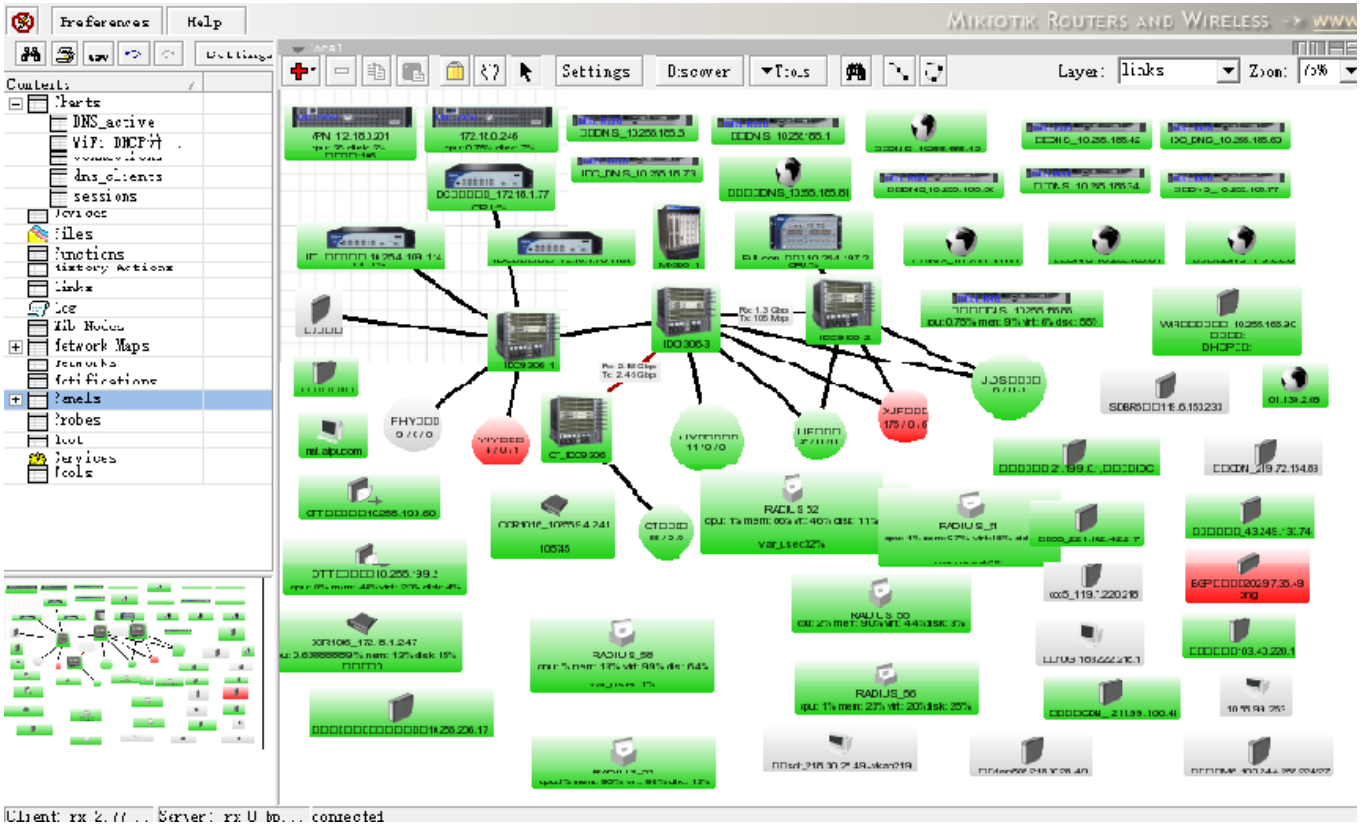
YuS

案例分享 2

RouterOS 配套应用

The Dude

提供ICMP和SNMP的网络监控，我在网络管理了785台网络设备，针对主要设备做snmp网络监控



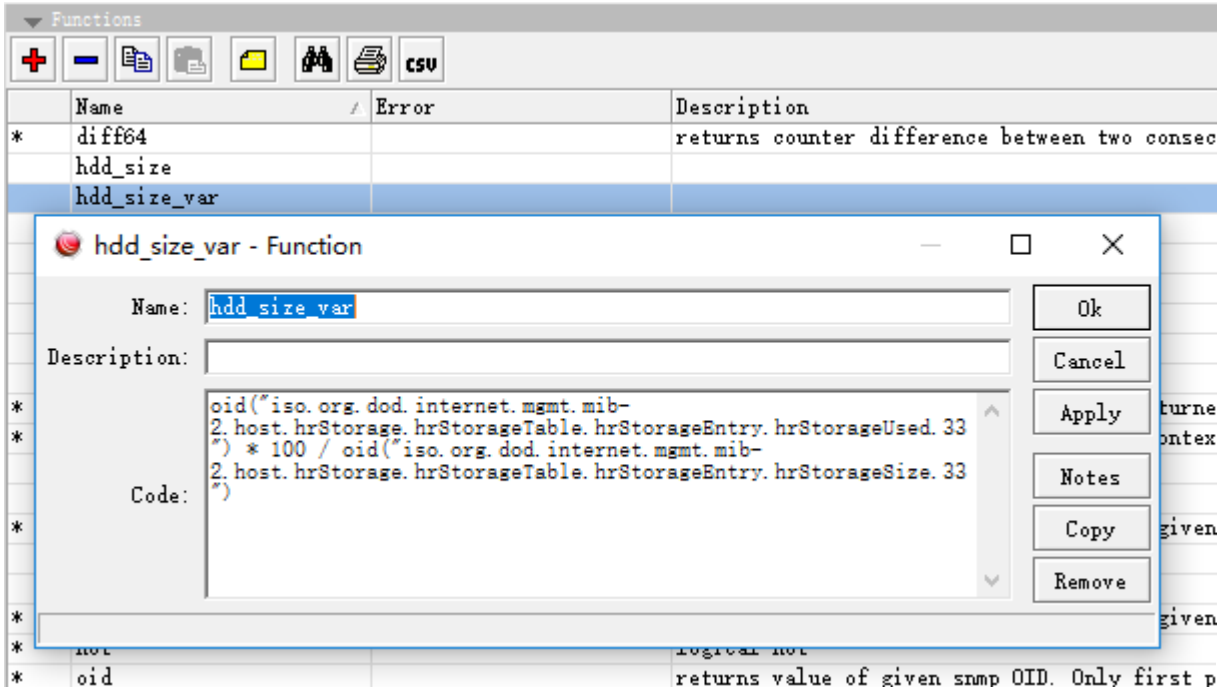
The Dude 监控磁盘使用率 1

- Linux服务器启用SNMP服务
- 对/var分区监控，获取var分区的两个oid值，分区空间和分区使用空间
- 在Dude中创建的一个函数，计算分区的使用率
- 通过监控使用率，超过90%就报警

The Dude 监控磁盘使用率 2

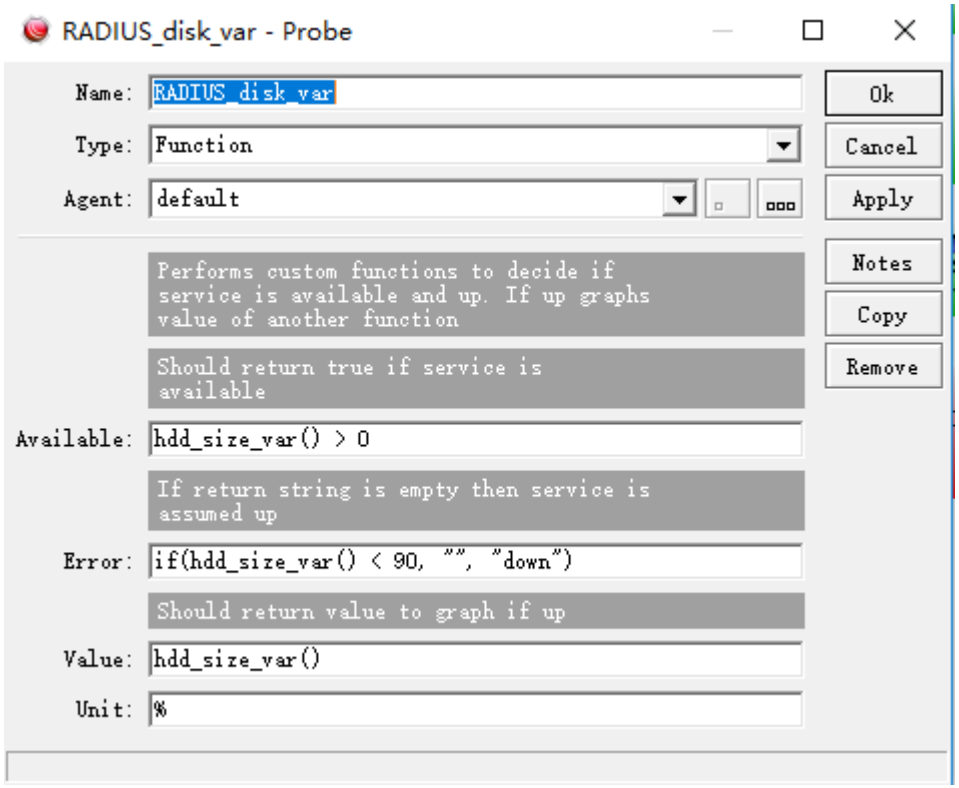
创建var分区使用率函数

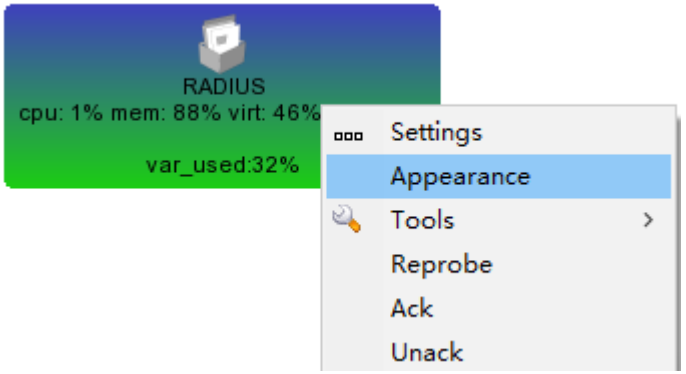
oid("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageUsed.33") * 100 / oid("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageSize.33")



The Dude 监控磁盘使用率 3

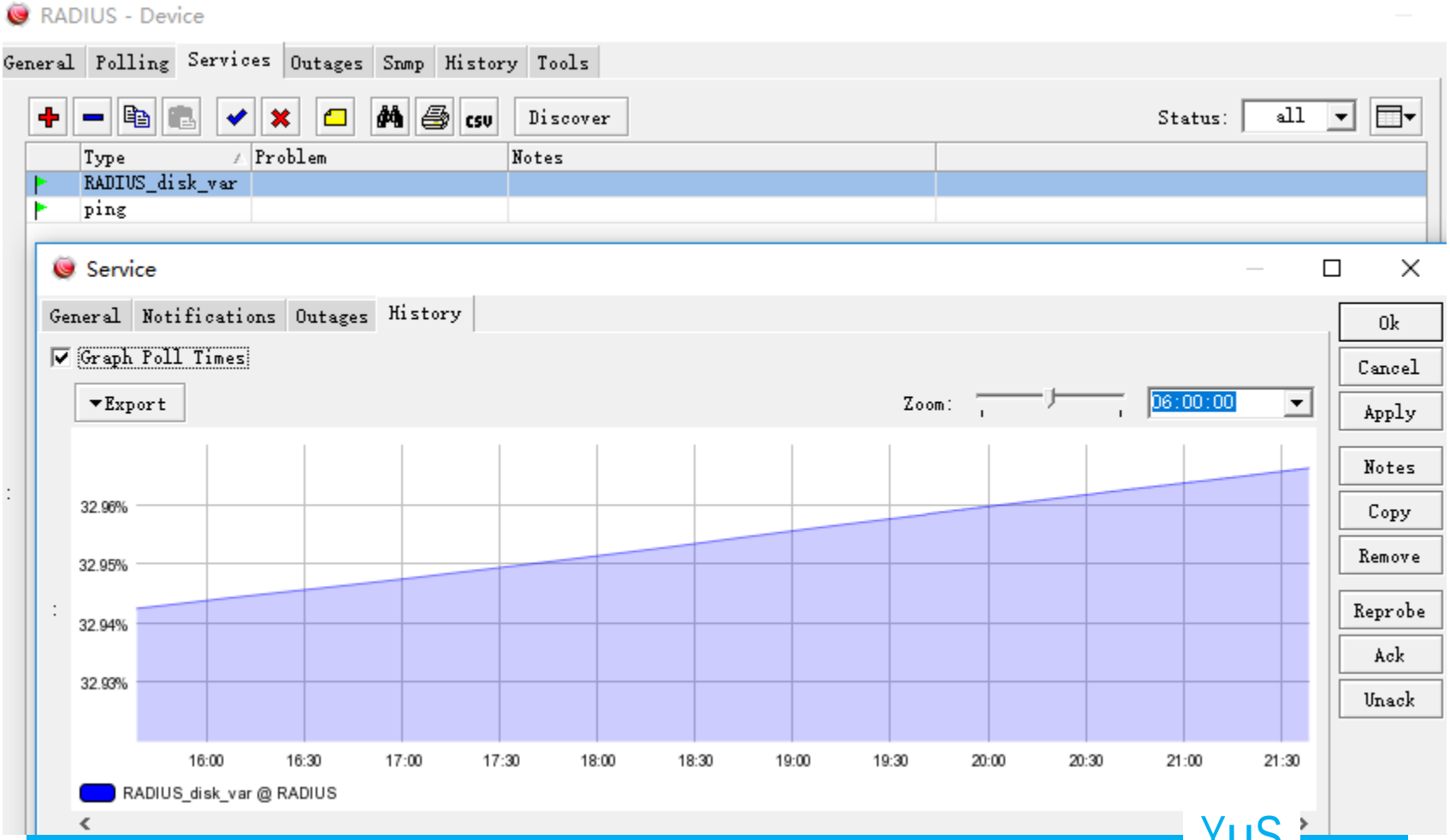
创建探针（probe），使用率超过90%，触发报警





The Dude 监控磁盘使用率 4

将创建的Probe应用到设备的service服务监控中



YuS

日志（Linux + Rsyslog + Mysql）

使用Rsyslog 接收RouterOS日志，可以针对不同日志分类，做到有效的管理和查询

国内网监要求用户访问日志保存半年，通过下面配置实现全nat日志保存

```
/ip firewall  filter
add action=log chain=forward connection-nat-state=srcnat log=yes log-prefix=srcnat protocol=!icmp src-address-list=in
```

Dell R510 Xeon双路CPU ， 24G内存 ， RAID卡， 10*2T SATA硬盘，配置RAID 0，存储20T

每天日志约100G，能保存半年的日志

RouterOS + Raspberry3 + Bind

1、通过树莓派搭建BIND DNS服务，处理DNS请求

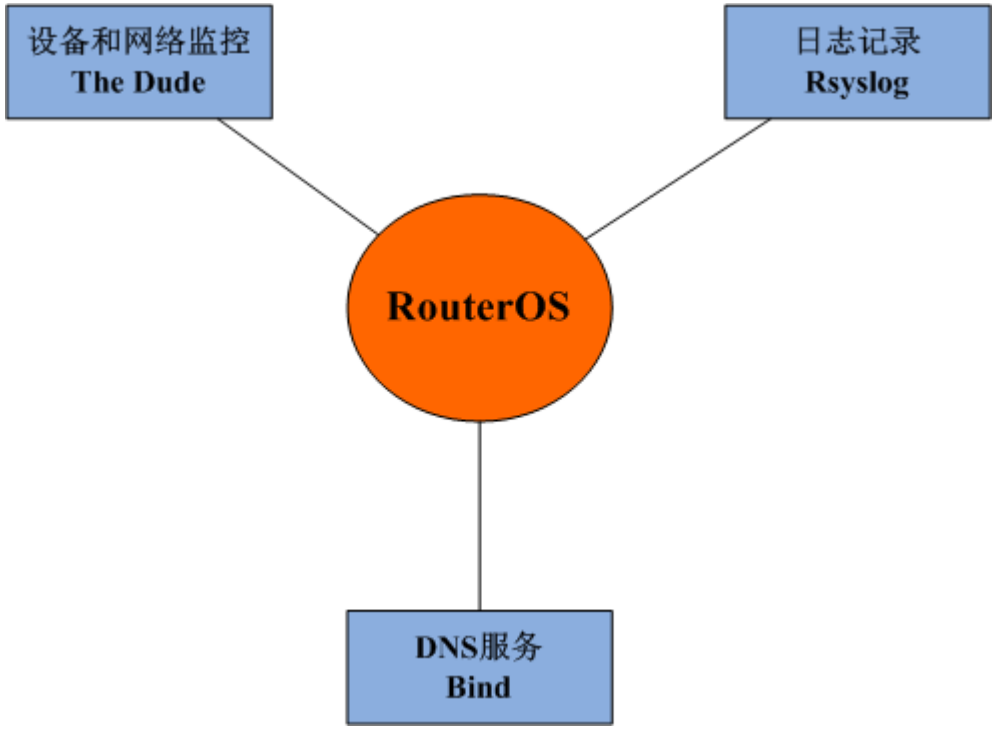
2、BIND DNS服务，实现A记录和forward转发域名到不同运营商DNS，优化出口。

3、一台树莓派3B，在实际运营网络环境能处理10,000+ 用户的请求

4、功耗5w，压力测试能处理 7370qps，每瓦处理1474qps/w，作为对比 Xeon X5680 双路，频率3.33GHz，功耗120w，54503qps，每瓦处理：454.2qps/w

RouterOS配套

系统化的网络运维，使用到了Rsyslog服务器，Bind的DNS服务和The Dude监控（其他还涉及到用户认证RADIUS服务器，以及内网的Cache缓存等）



Thanks!

http://www.irouteros.com
http://blog.163.com/athlon_sds