RG-ASME防代理产品及解决方案介绍

目录 Contents

客户端防代理技术的困境

客户端维护工作量大

- 需经常升级，才能屏蔽破解软件
- 由于学生终端环境复杂，客户端升级易出现兼容性问题，管理员工作量大，切换周期长

破解、共享工具泛滥，更新快

- 破解工具：如锐捷助手、mentohust、RP-link
- 共享软件：各类Wi-Fi助手(360/猎豹/百度)、Wi-Fi共享精灵、connectify等
- 特点：破解版本更新快，靠SAM客户端升级也防不住

不支持无线、PPPoE等场景

- 客户端防代理，只对802.1x有线接入有效，不支持无线接入、PPPoE接入防代理
- 部分学校为防止无线接入逃费，只能暂不建无线校园网

误判限制多，满意度低

- 用户双网卡、VPN应用均会被误判为代理，报障/投诉多

学校/学生/运营商 多方抱怨

传统方案已不可行，**基于DPI的应用层防代理**成为必然趋势

学校

- 逃费占比可达25，影响校园网收入
- 实名审计有名无实

运营商

- ICT校园网PPPoE认证居多，无法防代理，带来大量运营损失

学生

- 终端共享受限、私设代理导致网络不稳定，学生大量抱怨和投诉

China unicom 中国联通

中国移动通信 CHINA MOBILE

中国电信 CHINA TELECOM

Ruijie Networks

目录 Contents

产品介绍

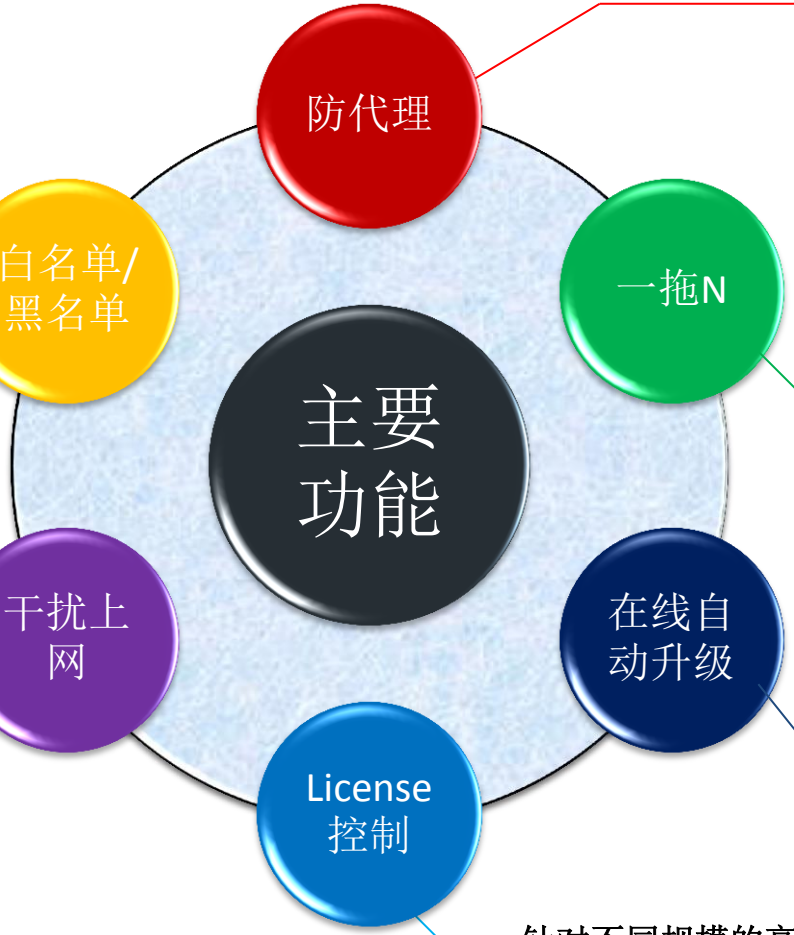
RG-ASME：接入共享管理引擎（Access Sharing Management Engine）

通过嗅探用户数据流进行行为特征分析，锁定接入共享用户及共享设备数量，实现防代理。

型号		RG-ASME1000
硬件规格	形态	2U，盒式设备
	业务口	8个千兆光/电Combo口 2个万兆口+2个复用万兆口
	管理口	2个USB、1个千兆MGMT口、1个串口
功能	支持的认证方式	有线 / 无线 802.1x / Web / PPPoE
	升级方式	特征库支持远程静默升级
有效检测	破解软件	锐捷助手，mentohust
	代理方式	360随身Wi-Fi，猎豹Wi-Fi系列，小度随身Wi-Fi connectfy NAT代理(RP-link)，Wi-Fi共享精灵 等
性能	支持用户规模	最大6万并发用户数（需license授权）
	误判率	低于1%
	吞吐率(上行流量)	＞5Gbps

RG-ASME1000

产品概述



基于DPI检测，能够防住各种破解及代理软件

特权用户白名单（老师/访客）
违例用户黑名单

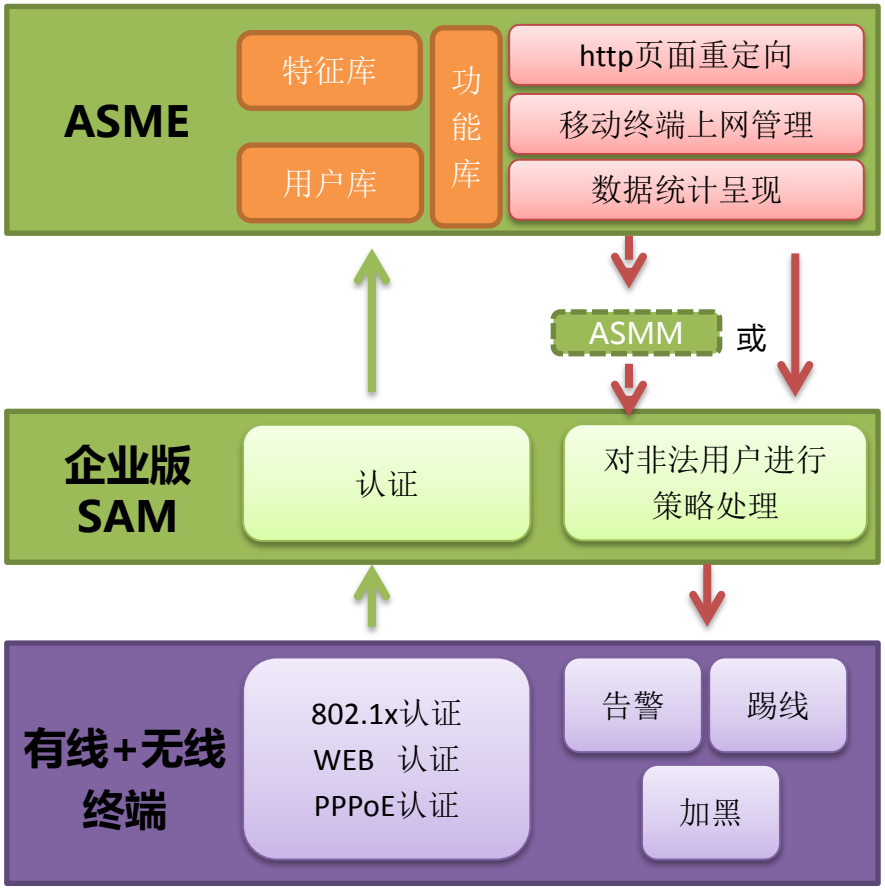
解决移动终端上网刚需，可设置允许移动终端上网

针对违例用户，实现http重定向干扰

支持在线自动升级，启用在线自动升级后，能够自动获取新版本完成升级

针对不同规模的高校，采用license控制

基础方案、组件功能介绍（校园网纯SAM认证场景）



ASME核心功能

特征库： 用于检测用户是否存在代理，可在线更新

用户库： 从SAM或ASMM获取账号信息，并向SAM反馈非法用户信息，提供账号老化机制

功能库： 提供故障自检，允许拖带移动终端数量设置及http重定向等功能

可选组件

ASMM： 将SAM的账号获取、策略处理等模块抽离为独立插件。

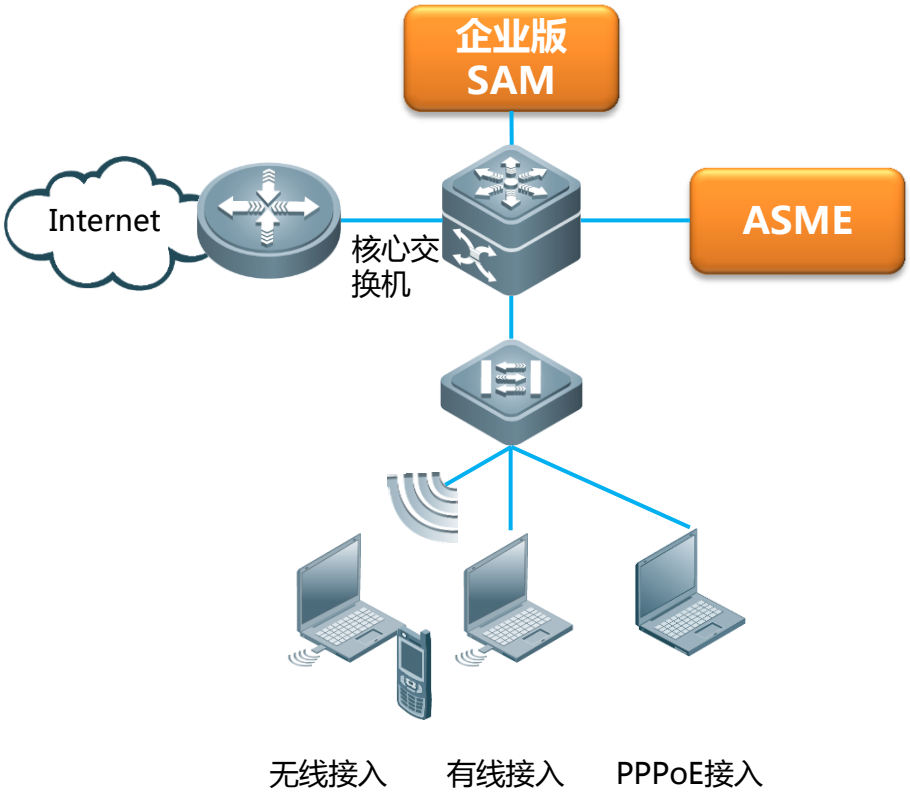
作用：

1）提升ASME与SAM无关性，避免ASME方案升级导致SAM需升级；

2）实现按模板部署处理策略/白名单等功能。

注：使用web及PPPoE认证时，告警信息通过重定向网页推送；使用客户端认证时，告警通过客户端展示。

基础方案部署模式（校园网纯SAM认证场景）



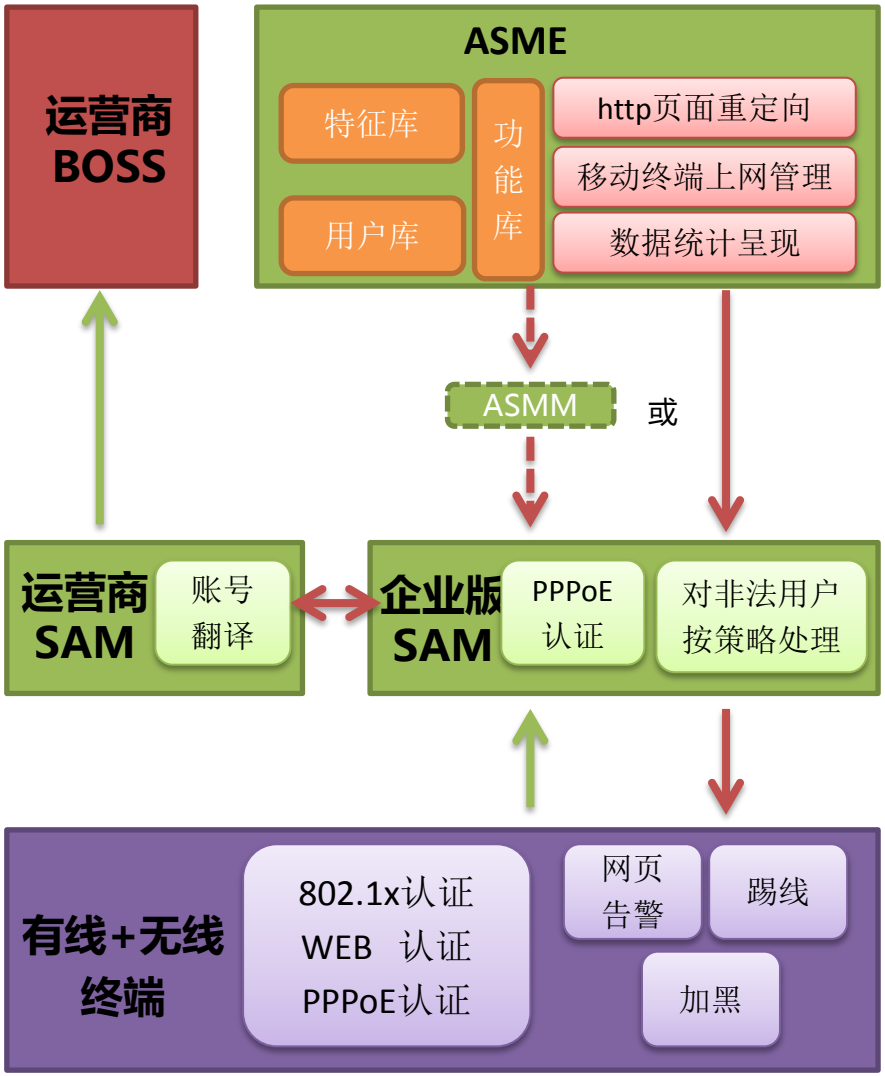
部署位置： ASME旁挂到核心或出口设备，将用户出口流量镜像至ASME

必备组件： ASME+企业版SAM(3.95版本)

工作流程：

1. ASME从SAM获取用户动态信息，同时对出口镜像流量做嗅探分析，锁定共享用户。
2. ASME将共享上网用户信息传回SAM
3. SAM向管理员展示代理用户信息、出具统计报告。并根据策略对共享用户实施干预。

运营商版方案、组件介绍（BOSS+PPPoE认证场景）



ASME核心功能

特征库： 用于检测用户是否存在代理，可在线更新

用户库： 从SAM或ASMM获取账号信息，并向SAM反馈非法用户信息，提供账号老化机制

功能库： 提供故障自检，允许拖带移动终端数量设置及http重定向等功能

配套组件

企业版SAM： 1.实现用户认证，将账户信息同步至ASME/ASMM；2.配置防代理策略；3、根据ASME结果调用接口执行策略。

运营商SAM： 1. BOSS系统与企业版SAM间的桥梁，实现radius报文翻译，将SAM账户上下线等信息同步给BOSS系统。

可选组件

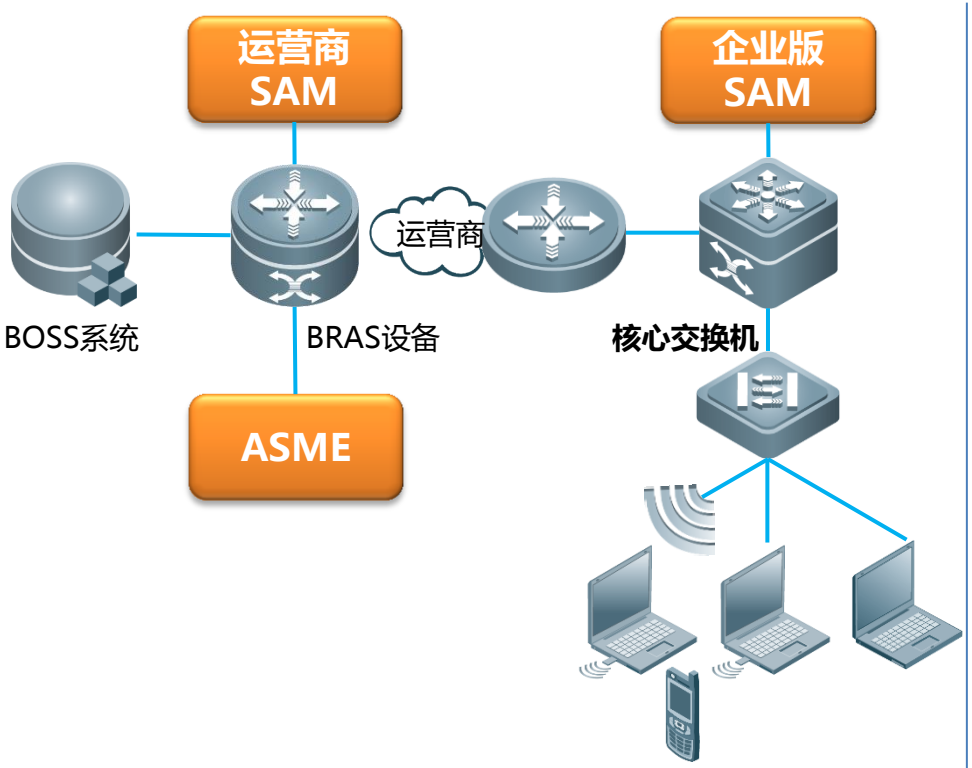
ASMM： 将SAM的账号获取、策略处理等模块抽离为独立插件。

作用：

1）提升ASME与SAM无关性，避免ASME方案升级导致SAM需升级；

2）实现按模板部署处理策略/白名单等功能。

运营商部署模式一（ BOSS+PPPoE认证场景 ）



部署位置： **ASME(必须)旁挂到BRAS**，镜像上联口TX方向流量

必备组件： ASME*n套+企业版SAM*n套+运营商SAM*1

工作流程：

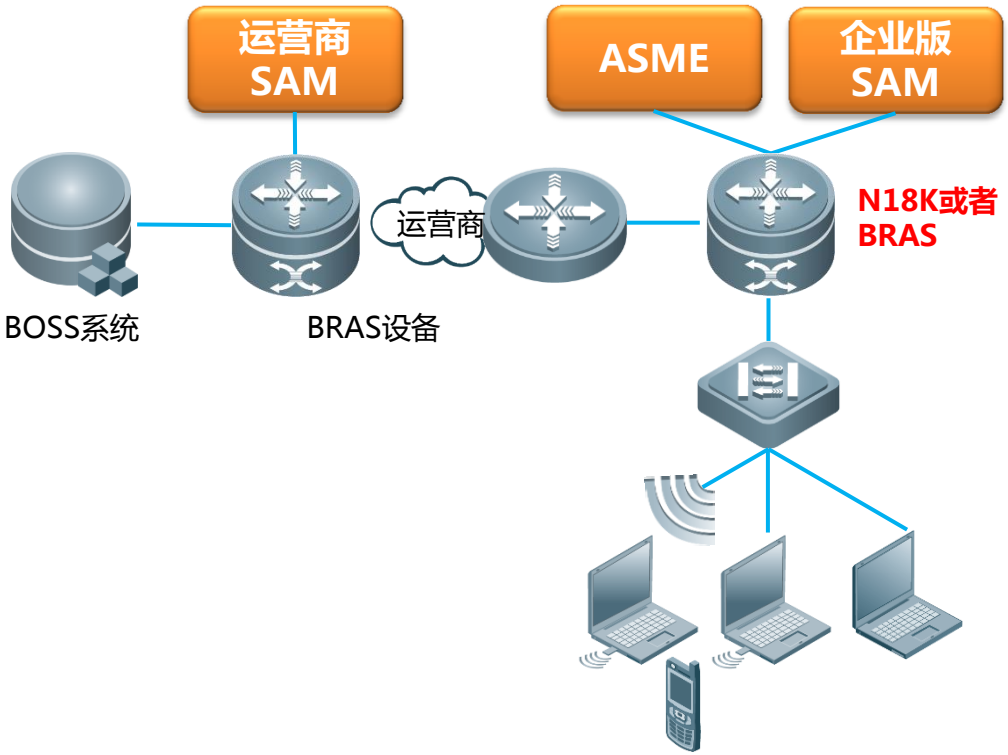
1. ASME从企业版SAM获取用户动态信息，同时对BRAS上联口镜像流量做嗅探分析，锁定共享用户。
2. ASME将共享上网用户信息传回企业版SAM。
3. 企业版SAM根据策略对共享用户实施干预，并将账户状态经由运营商SAM，同步至运营商BOSS系统。

注：

1、ASME在此场景中**必须部署在BRAS设备下**。因为ASME只能分析PPPoE报文解封装后的镜像流量。

2、如果是运营商同时投资多个学校（即有多套企业版SAM）的情况下，每一个学校需对应一套ASME。

运营商部署模式二（ BOSS+PPPoE / 802.1x /web认证场景 ）



部署位置： ASME旁挂到核心或出口位置，镜像出口流量

必备组件： ASME*n套+企业版SAM*套+运营商SAM*1

工作流程：

1. 所有认证在核心交换机（或BRAS）上进行，
2. ASME从企业版SAM获取用户动态信息，同时对出口镜像流量做嗅探分析，锁定共享用户。
3. ASME将共享上网用户信息传回企业版SAM。
4. 企业版SAM根据策略对共享用户实施干预，并将账户状态经由运营商SAM，同步至运营商BOSS系统。

注：

1、ASME在此场景中必须部署在BRAS设备下。因为ASME只能分析PPPoE报文解封装后的镜像流量。

2、如果是运营商同时投资多个学校（即有多套企业版SAM）的情况下，每一个学校需对应一套ASME。

方案原理

关于防代理检测机制：为防恶意破解，具体机制保密

- 使用DPI技术，基于用户流量的应用层特征进行检测，识别接入共享行为
- 能精确的计算拖带的设备数量
- 对于移动终端，可以进一步检测出设备类型（iPhone、安卓）

方案特点

1、彻底杜绝互联网破解工具

- 无客户端，传统破解方式无效
- 纯嗅探方案，无外出报文，防止漏洞
- 可实时更新特征库，快速封杀新工具

2、业界最“聪明”识别算法，误判率＜1%

- 创新的多维度、应用层交叉匹配检测，像人一样思考，解决多网卡、VPN等常见误判
- 已经过10万用户规模验证。特征库持续更新，提升准确率

3、部署方便，适用广泛

- 旁路部署，即插即用，不改变用户原有拓扑
- 支持有线、无线、web、802.1x、PPPoE等各种认证方案
- 未来还将兼容其他厂商radius，杜绝厂商捆绑（通过兼容组件）

4、关注用户体验

- 提供警告、重定向、下线、黑/白名单等多种策略，柔性控制
- 实时展示代理用户统计，效果直观可见
- 升级期间不断流，不影响现有业务

目录 Contents

- ❑ 防代理的困境
- ❑ RG-ASME解决方案
- ❑ 同类产品对比
- ❑ 案例介绍

同类产品对比

维度	对比项		ASME	某SXF行为审计设备
使用者	认证方式	802.1x	支持	支持
		web认证	支持	支持
		pppoe认证	支持	支持
	代理方式	NAT代理场景	支持	支持
		随身Wi-Fi代理场景	支持	支持
		软件代理场景	支持	支持
		检测机制	多维度、应用层交叉匹配检测，并定期升级特征库，避免破解	仅检测移动终端代理，易被破解
	处理策略	告警	支持（客户端+HTTP重定向）	支持（HTTP重定向）
		上网阻断	支持	支持（HTTP阻断）
		踢线+黑名单	支持	支持
运维者	升级管理	在线自动升级	支持	不支持，升级需要收费
		设置自动升级时间	支持	不支持
	信息管理	代理明细	支持	支持
		代理排行榜、代理报表	支持	不支持
	策略管理	白名单	支持	未知
	部署方式		旁挂	只支持串行
	性能	吞吐率	5Gbps	未知
	容量		最大6万并发用户	未知
	证据显示		支持	未知
	误判率		低于1%	据客户反馈较高，放弃使用

目录 Contents

- ❑ 防代理的困境
- ❑ RG-ASME解决方案
- ❑ 同类产品对比
- ❑ 案例介绍

案例1：郑州某大学

背景：

- 学校采用SAM认证计费系统，基于802.1x客户端防代理。但发现客户端被猎豹Wi-Fi破解了，营收大幅减少。
- 购买了一批无线AP，准备部署无线网络，却发现无线网没有防代理方案；

效果：

- 4月21号，部署ASME后，**每天**抓到**代理用户数500~600**；
- 5月4号，部署无线并启用自动踢线+黑名单策略，代理用户不断减少，每天抓到的**代理用户数＜10个**；
- **半个月后，增加开户数1000**

郑州经贸：代理用户统计

位置:运维管理 > 并机用户统计

开始日期 * 2014-05-01 结束日期 * 2014-05-29 并机用户数报表 并机用户曲线变化图

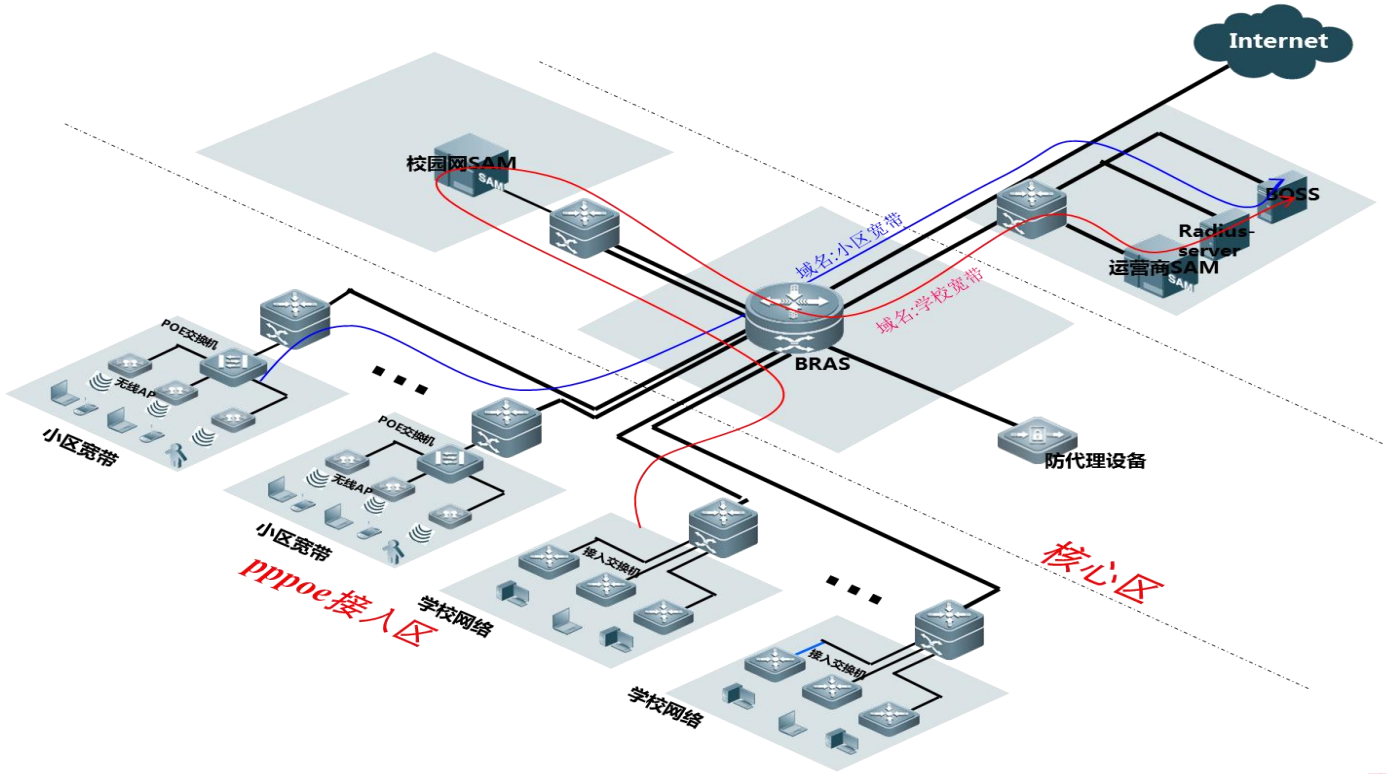
2014-05-11	3741	34	0.91%	3.79
2014-05-12	4139	27	0.65%	3.41
2014-05-13	4490	41		
2014-05-14	4478	43		
2014-05-15	4452	39		
2014-05-16	4361	23	0.53%	3.65
2014-05-17	3871	29	0.75%	3.66
2014-05-18	4032	26	0.64%	3.81
2014-05-19	4425	48	1.08%	3.67
2014-05-20	4590	37	0.81%	3.43
2014-05-21	4573	46	1.01%	3.67
2014-05-22	4230	17	0.4%	3.06
2014-05-23	4284	12	0.28%	2.83
2014-05-24	3859	5	0.13%	4.0
2014-05-25	3718	8	0.22%	4.13
2014-05-26	3830	9	0.23%	3.89
2014-05-27	4327	10	0.23%	4.0
2014-05-28	4343	9	0.21%	3.67
2014-05-29	3983	9	0.23%	5.11

并机用户数不断减少，新增开户数1000，每年增收30万

案例2：佛山某*ICT*项目

背景：

- 广州某技术学院是佛山运营商宽带的学校（采用PPPoE认证），由于运营商的宽带账号没有限制账号共享功能，导致很多宿舍出现几个学生共享一个账号，而目前联通宽带系统也不具备限制账号共享功能。
- 经过深入调研及测试后，最终选择锐捷运营商SAM+ASME防代理解决方案。



广州某学院：代理用户统计

位置：运维管理 > 并机用户统计

开始日期 * 2014-08-30 结束日期 * 2014-09-16 并机用户数报表 并机用户曲线变化图

并机用户数报表

日期	上线人数	并机用户数	并机用户比例	平均终端数量	平均可疑度
2014-08-30	37			1.52	59.33
2014-08-31	42			1.45	54.55
2014-09-01	103			1.82	67.55
2014-09-02	268			2.08	74.66
2014-09-03	547			1.92	67.18
2014-09-04	927			2.0	69.79
2014-09-05	1091	145	13.29%	1.91	65.04
2014-09-06	959	119	12.41%	1.93	65.58
2014-09-07	978	104	10.63%	1.85	65.0
2014-09-08	1145	117	10.22%	1.94	67.21
2014-09-09	1321	114	8.63%	2.02	63.98
2014-09-10	1629	150	9.21%	1.95	63.77
2014-09-11	1720	179	10.41%	2.05	66.85
2014-09-12	1851	164	8.86%	2.08	68.87
2014-09-13	1822	214	11.75%	2.2	69.38
2014-09-14	2012	198	9.84%	2.24	71.64
2014-09-15	2134	215	10.07%	2.17	69.09
2014-09-16	1790	159	8.88%	2.31	70.3

刚开始，用户只有2000左右，代理用户比例高达20%~30%。而学校老师预期的开户数在2300人左右。

并机用户数报表

日期	上线人数	并机用户数	并机用户比例
2014-10-08	4344	334	7.69%
2014-10-09	4464	384	8.6%
2014-10-10	4516	312	6.91%
2014-10-11	4726	236	4.99%
2014-10-12	5208	474	9.1%
2014-10-13			7.4%
2014-10-14			7.15%
2014-10-15			7.65%
2014-10-16			7.33%
2014-10-17			6.32%
2014-10-18	4683	370	7.9%
2014-10-19	5049	273	5.41%
2014-10-20	5599	304	5.43%
2014-10-21	5692	344	6.04%
2014-10-22	5626	348	6.19%
2014-10-23	5690	374	6.57%
2014-10-24	5625	329	5.85%
2014-10-25	5220	341	6.53%
2014-10-26	5609	393	7.01%

在线高峰期稳定在5500左右，并机率减少到5%左右

THANKS

星网锐捷网络有限公司

地址：北京海淀区复兴路29号中意鹏奥大厦东塔A座11层　邮编：100036

Office Tel: 010-51715999　　Fax: 010-51413399

www.ruijie.com.cn