农大校园网802.1x实施体会

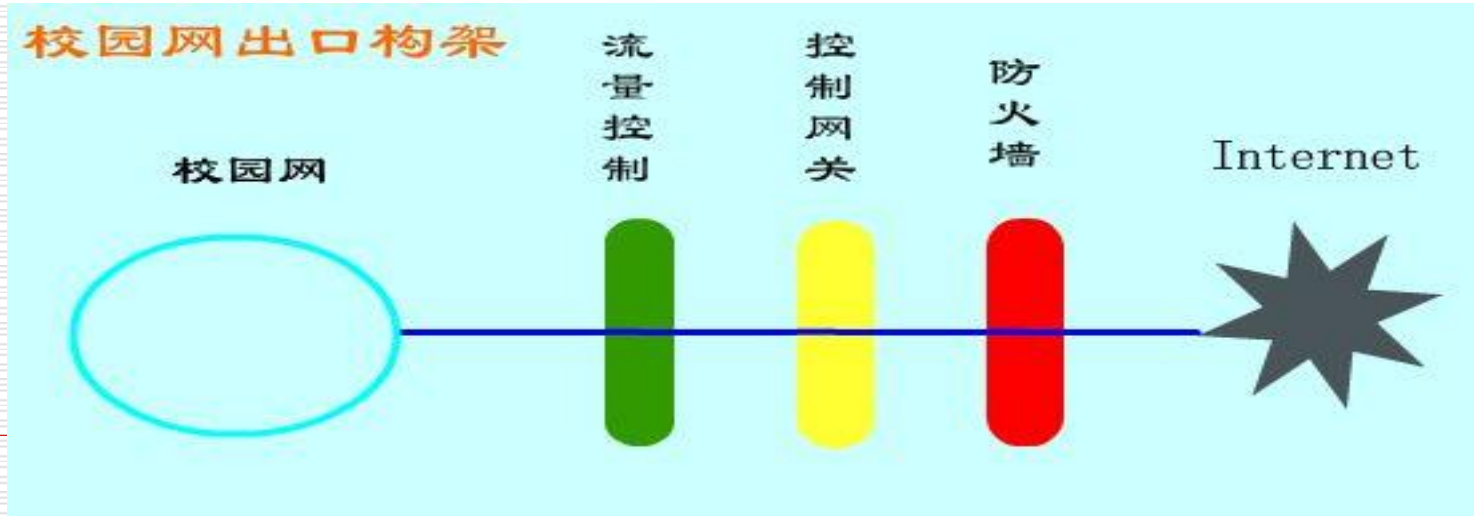
中国农业大学网络中心 邹仁明
zrm@cau.edu.cn

主要内容

- 为何要布署802.1x——需求分析
  - 传统入网控制方式存在的问题
- 我校802.1x接入控制实施方案
  - 主要功能
- 布署802.1x接入控制的优缺点
- 今后我校802.1x布署策略

为何要布署802.1x

- 传统的用户上网控制方式
  - 我校校园网接入控制方法为：出口网关控制方式。即：接入校园网时不受控制，只有在用户访问校外资源时，出口网关设备才控制用户的访问权限，并采取相应的策略进行上网计费。



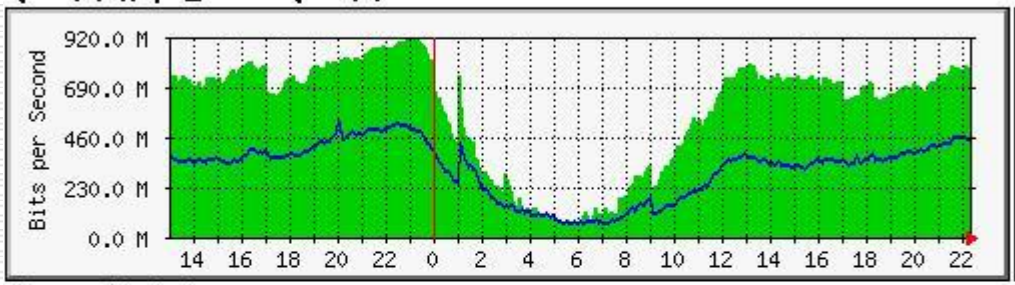
传统上网控制方式存在的问题

- 对校园网出口的影响：
  - 对用户的控制管理措施集中放在校园网出口来实施，对网络访问障碍较大，增加出口断网的风险概率。随着出口网速增大，出口网关将成为网络访问的瓶颈。
- 安全问题：
  - 不易确认用户的上网身份、不易定位上网主机
  - 主机接入校园网不受控制，主机上网没有记录
  - 用户可自由更改主机MAC地址、IP地址，当出现安全事件时，网管难以定位造事者。
- 计费问题
  - 上网帐户可以被合用、转让，可以采用网络共享、宽带路由器、代理服务器等方式来实现一个帐户大家共用。盗用帐户现象也时有发生。
- 难以了解用户主机上网的攻击行为、中毒情况
- 用户不能入网时，难以判断故障原因

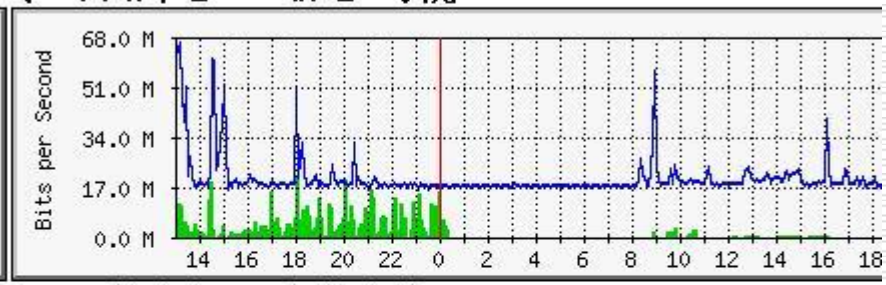
中国农业大学校园网流量图

校园网流量明细图：东区、西区；网络气象图 SCE2000

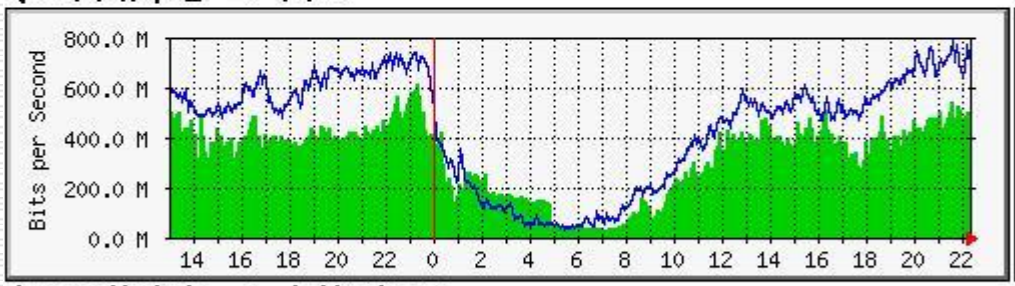
东区网络中心 => 东区出口



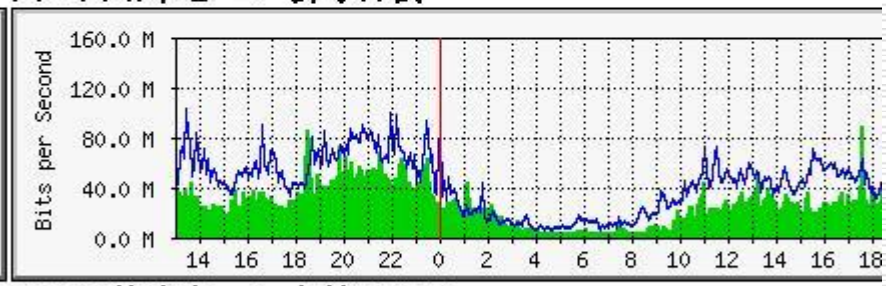
东区网络中心 => 信电工学院



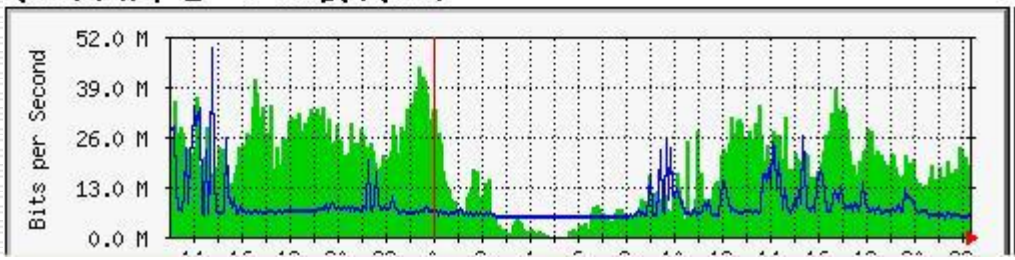
东区网络中心 => 西区



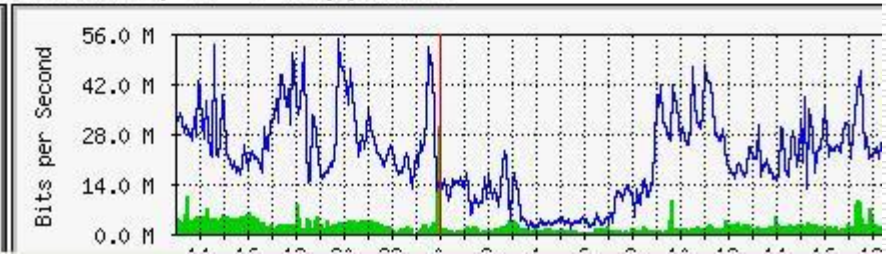
西区网络中心 => 新综合楼

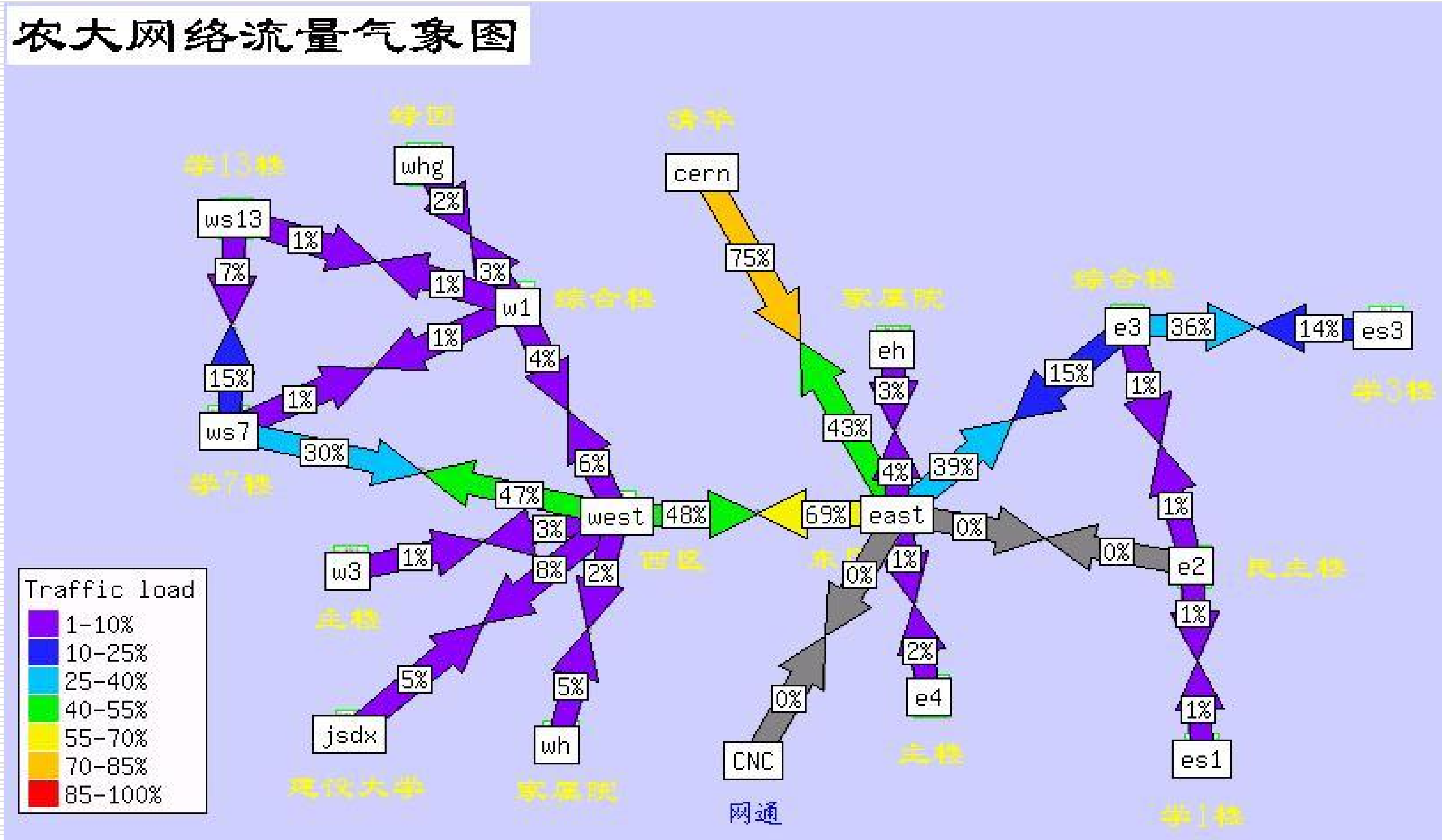


东区网络中心 => 主楼(东区)



西区网络中心 => 主楼(西区)




农大网络流量气象图
学13楼
清华
综合楼
家属院
学3楼
学7楼
西区
主楼
民主楼
学1楼
网通
whg
ws13
cern
w1
eh
e3
es3
ws7
west
east
w3
e2
e4
jsdx
wh
CNC
es1
Traffic load
1-10%
10-25%
25-40%
40-55%
55-70%
70-85%
85-100%

我校802.1x实施方案

- 采用锐捷SAM计费管理系统，有三块：
  - 认证服务器：radius认证服务器 + sql数据库 + jboss WWW服务器
  - radius接入设备：接入交换机(S2126G/S2150G)，接入端口启用802.1x认证
  - 用户安装锐捷SAM客户端软件，通过802.1x认证后方可访问校园网。
- 校园网出口网关不对用户进行访问控制，由锐捷SAM计费系统实施计费：包月方式。

锐捷SAM计费管理系统

计费策略


系统管理
安全管理
帐号模板
服务管理
计费策略管理
接入控制管理
接入时段管理
帐号模板管理
配置生效
用户组管理
用户管理
用户卡管理
充值卡管理
在线用户管理
帐务管理
营帐管理
统计信息
日志管理
添加计费策略
修改计费策略
删除计费策略
查询计费策略
计费策略管理简介
添加计费策略：
可以添加包月，计天，计时长和计流量等类型的计费策略。
修改计费策略：
修改计费策略的类型以及各项细节。
删除计费策略：
删除用户选择的计费策略。
查询计费策略：
查看计费策略的详细信息。

目前使用802.1x的主要功能

- 计费策略：包月
- 用户上网认证后，帐户、主机MAC自动与交换机端口绑定，帐户不能混用、共享使用
- 记录用户上网记录，明确用户的上网身份。


系统管理
安全管理
帐号模板
用户组管理
用户管理
用户审核
用户开户
设备管理员
用户BACL
用户付费
资料变更
用户暂停
用户恢复
用户销户
用户查询
用户卡管理
充值卡管理
在线用户管理
帐务管理
营帐管理
统计信息
日志管理
用户查询
共1999条记录 第1页 共100页 第 页 Go 下一页 刷新
用户列表
用户登录名 姓名 状态 用户IP 用户MAC NAS IP NAS PORT 余额(元)
bbb bbb 用户开户 0090F54A3DB1 202.112.162.99 1 0.00
c503105022 罗桂芬 暂停 0000E812D131 10.100.106.34 55 0.00
jd000012 杨启 暂停 0013D3ACDAEE 10.100.106.33 136 0.00
jd004101 王伟 暂停 00030D1C3E65 10.100.106.36 32 0.00
jd004102 冯光 暂停 000AEB64AA7B 10.100.106.36 32 0.00
jd004103 申国 暂停 000E06097B04 10.100.106.36 32 0.00
jd004111 吴天 正常 00E04C190349 10.100.106.32 12 20.00
jd004112 王硕 暂停 001A92597775 10.100.106.36 18 0.00
jd004113 李浩 暂停 00055DE2E783 10.100.106.36 18 0.00
jd004121 王可 暂停 00055D5DC1D2 10.100.106.36 34 0.00
jd004122 刘真 暂停 00E0E5000B17 10.100.106.36 34 0.00
jd004123 吴力 暂停 0004750A6F79 10.100.106.36 34 0.00
jd004131 张伟 暂停 00E0E2008A66 10.100.106.36 16 0.00
jd004131c 刘洋 正常 169.254.14.209 00E04C82D688 10.100.106.35 73 0.00
jd004132 张玥 暂停 00E0E2008B57 10.100.106.36 16 0.00
jd004133 王明 暂停 0016172408C9 10.100.106.36 16 0.00
jd004141 刘飞 暂停 00104B08F1ED 10.100.106.36 36 0.00


系统管理
安全管理
帐号模板
用户组管理
用户管理
用户卡管理
充值卡管理
在线用户管理
查询在线用户
清除在线用户
强制下线
帐务管理
营帐管理
统计信息
日志管理
查询在线用户
共337条记录 第1页 共17页 第 页 Go 下一页 刷新
在线用户列表
用户登录名 服务 用户IP 用户MAC NAS IP NAS Port 上线时间 子网掩码 网关
jd266079 internet 169.254.184.241 00115BA0762C 10.100.106.35 64 12-06 11:52:12 255.255.0.0 0.0.0.0
jd090036 internet 10.3.24.21 001BFCB9BC5C 10.100.106.35 45 12-08 11:22:28 255.255.255.0 10.3.24.254 202.
jd304512 internet 10.3.21.237 001636369C2E 10.100.106.33 68 12-30 13:04:55 255.255.255.0 10.3.21.254 202.
jd4835 internet 10.3.28.146 0013D4CAA2AD 10.100.106.37 2 01-07 19:43:18 255.255.255.0 10.3.28.254 202.
jd243936 internet 10.3.21.133 000AEB6A87F2 10.100.106.33 24 01-08 05:32:45 255.255.255.0 10.3.21.254 202.
jd230019c internet 10.3.31.177 001D92308FE4 10.100.106.40 24 01-08 06:08:18 255.255.255.0 10.3.31.254 202.
jd104133 internet 10.3.21.191 001636369C2E 10.100.106.33 68 01-08 06:11:29 255.255.255.0 10.3.21.254 202.
jd020003 internet 10.3.24.201 000C6EA9F48D 10.100.106.35 40 01-08 06:12:38 255.255.255.0 10.3.24.254 202.
jd113316 internet 10.3.24.78 001A4D98C253 10.100.106.35 50 01-08 06:14:08 255.255.255.0 10.3.24.254 202.
jd076037 internet 10.3.26.226 0016EC0E3210 10.100.106.36 63 01-08 06:20:52 255.255.255.0 10.3.26.254 202.

用户分布情况统计(按照用户组分类)

用户总数:1999人

用户组名称	人数(人)
教工组	45
设备管理员组	1
学生组	1953

在线用户统计(按照用户组分类)

在线用户总数:341人

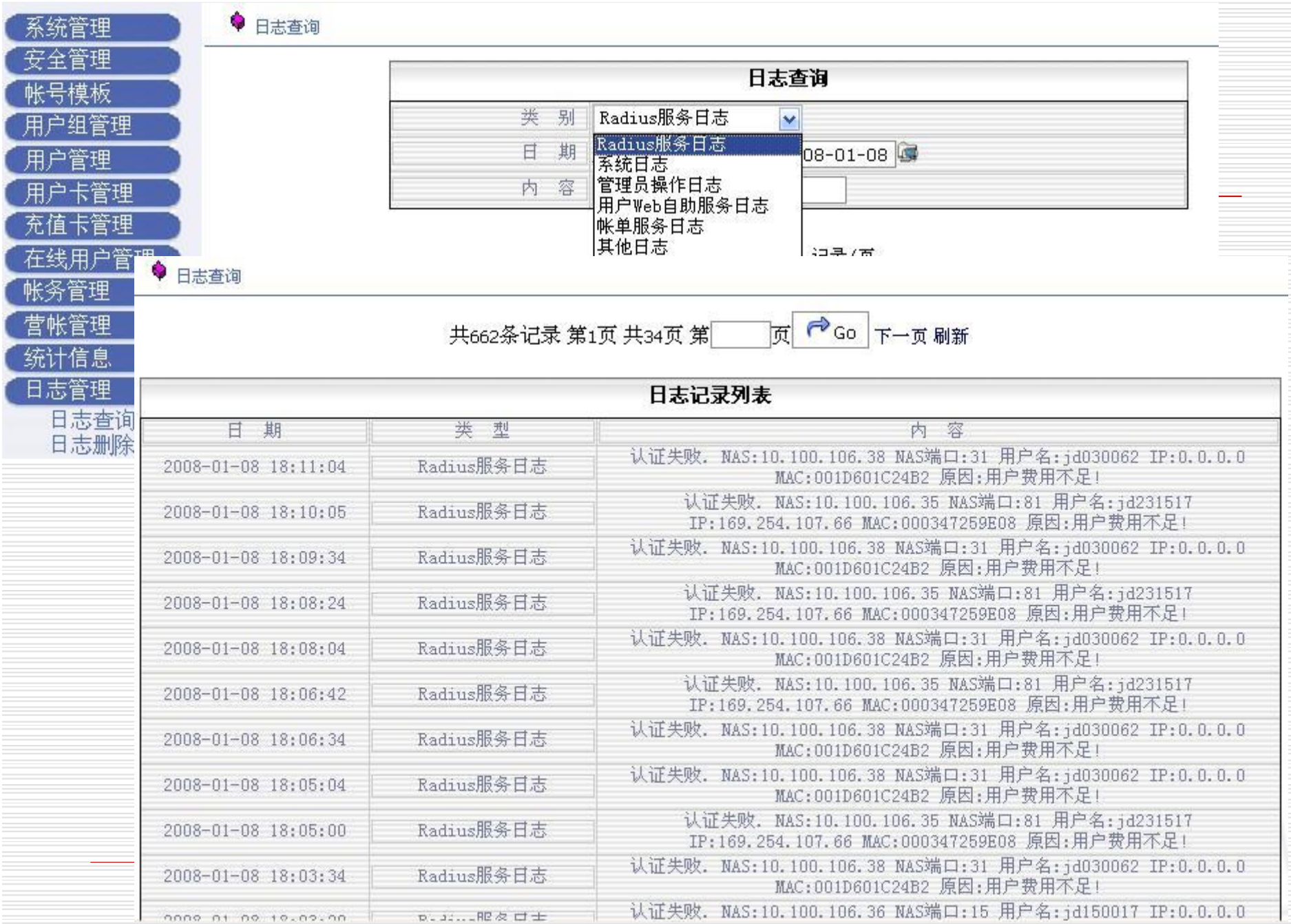
用户组名称	人数(人)
ROOT	0人
教工组	14人
设备管理员组	0人
学生组	327人

上网明细查询

用户登录名		精确匹配	模糊匹配
用户IP		精确匹配	模糊匹配
用户MAC		精确匹配	模糊匹配
NAS IP		精确匹配	模糊匹配
NAS Port		精确匹配	模糊匹配
使用服务			
开始时间	从 2008-01-08 年月日 时 分 秒		
	到 年月日 时 分 秒		

上网明细列表

用户登录名	用户IP	用户MAC	NAS IP	NAS Port	开始时间	结束时间	时长	流入流量(MB)	流出流量(MB)
jd201712	10.3.25.157	001A4DD0F111	10.100.106.35	101	01-08 09:42:59	01-08 18:22:26	8小时39分27秒	253.3	869.4
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:22:10	01-08 18:22:21	0小时0分11秒	1.2	2.9
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:21:58	01-08 18:22:09	0小时0分11秒	1.9	1.5
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:21:46	01-08 18:21:57	0小时0分11秒	1.5	1.4
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:21:34	01-08 18:21:45	0小时0分11秒	1.5	2.8
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:21:22	01-08 18:21:33	0小时0分11秒	2.3	2.6
jd251718	10.3.23.214	001D7D9DC468	10.100.106.34	27	01-08 16:12:14	01-08 18:21:24	2小时9分10秒	2.5	12.5
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:21:10	01-08 18:21:21	0小时0分11秒	1.6	1.8
jd091022	10.3.29.51	0016365E9529	10.100.106.38	29	01-08 18:20:34	01-08 18:21:11	0小时0分37秒	0.0	0.0
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:20:58	01-08 18:21:09	0小时0分11秒	1.5	2.1
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:20:46	01-08 18:20:56	0小时0分10秒	1.5	3.2
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:20:34	01-08 18:20:44	0小时0分10秒	1.3	1.5
jd118212	10.3.26.221	000AE4C7D276	10.100.106.36	55	01-08 15:15:10	01-08 18:20:35	3小时5分25秒	22.0	25.0
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:20:21	01-08 18:20:32	0小时0分11秒	2.2	2.5
jd250014	10.3.25.112	044B80302187	10.100.106.35	113	01-08 18:20:13	01-08 18:20:26	0小时0分13秒	0.0	0.0
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:20:09	01-08 18:20:20	0小时0分11秒	1.4	2.6
jd018004	10.3.23.241	0013A9A77237	10.100.106.34	29	01-08 18:19:57	01-08 18:20:08	0小时0分11秒	1.8	2.8
jd250014	192.168.1.100	044B80302187	10.100.106.35	113	01-08 17:53:44	01-08 18:20:07	0小时26分23秒	1.4	6.2
jd091022	0.0.0.0	0016365E9529	10.100.106.38	29	01-08 16:27:54	01-08 18:20:01	1小时52分7秒	6.9	43.0


系统管理
安全管理
帐号模板
用户组管理
用户管理
用户卡管理
充值卡管理
在线用户管理
帐务管理
营帐管理
统计信息
日志管理
日志查询
日志删除
日志查询
日志查询
类 别
Radius服务日志
日 期
08-01-08
内 容
Radius服务日志
系统日志
管理员操作日志
用户Web自助服务日志
帐单服务日志
其他日志
日志查询
共662条记录 第1页 共34页 第 页 Go 下一页 刷新
日志记录列表
日 期
类 型
内 容
2008-01-08 18:11:04 Radius服务日志 认证失败. NAS:10.100.106.38 NAS端口:31 用户名:jd030062 IP:0.0.0.0 MAC:001D601C24B2 原因:用户费用不足!
2008-01-08 18:10:05 Radius服务日志 认证失败. NAS:10.100.106.35 NAS端口:81 用户名:jd231517 IP:169.254.107.66 MAC:000347259E08 原因:用户费用不足!
2008-01-08 18:09:34 Radius服务日志 认证失败. NAS:10.100.106.38 NAS端口:31 用户名:jd030062 IP:0.0.0.0 MAC:001D601C24B2 原因:用户费用不足!
2008-01-08 18:08:24 Radius服务日志 认证失败. NAS:10.100.106.35 NAS端口:81 用户名:jd231517 IP:169.254.107.66 MAC:000347259E08 原因:用户费用不足!
2008-01-08 18:08:04 Radius服务日志 认证失败. NAS:10.100.106.38 NAS端口:31 用户名:jd030062 IP:0.0.0.0 MAC:001D601C24B2 原因:用户费用不足!
2008-01-08 18:06:42 Radius服务日志 认证失败. NAS:10.100.106.35 NAS端口:81 用户名:jd231517 IP:169.254.107.66 MAC:000347259E08 原因:用户费用不足!
2008-01-08 18:06:34 Radius服务日志 认证失败. NAS:10.100.106.38 NAS端口:31 用户名:jd030062 IP:0.0.0.0 MAC:001D601C24B2 原因:用户费用不足!
2008-01-08 18:05:04 Radius服务日志 认证失败. NAS:10.100.106.38 NAS端口:31 用户名:jd030062 IP:0.0.0.0 MAC:001D601C24B2 原因:用户费用不足!
2008-01-08 18:05:00 Radius服务日志 认证失败. NAS:10.100.106.35 NAS端口:81 用户名:jd231517 IP:169.254.107.66 MAC:000347259E08 原因:用户费用不足!
2008-01-08 18:03:34 Radius服务日志 认证失败. NAS:10.100.106.38 NAS端口:31 用户名:jd030062 IP:0.0.0.0 MAC:001D601C24B2 原因:用户费用不足!
认证失败. NAS:10.100.106.36 NAS端口:15 用户名:jd150017 IP:0.0.0.0

实施802.1x的好处

- 采用入网认证措施，增强了内网的安全性
- 帐户不能多机共享使用
- 帐户与上网端口自动绑定，帐户不能借用
- 用户上网日志详细、查询方便

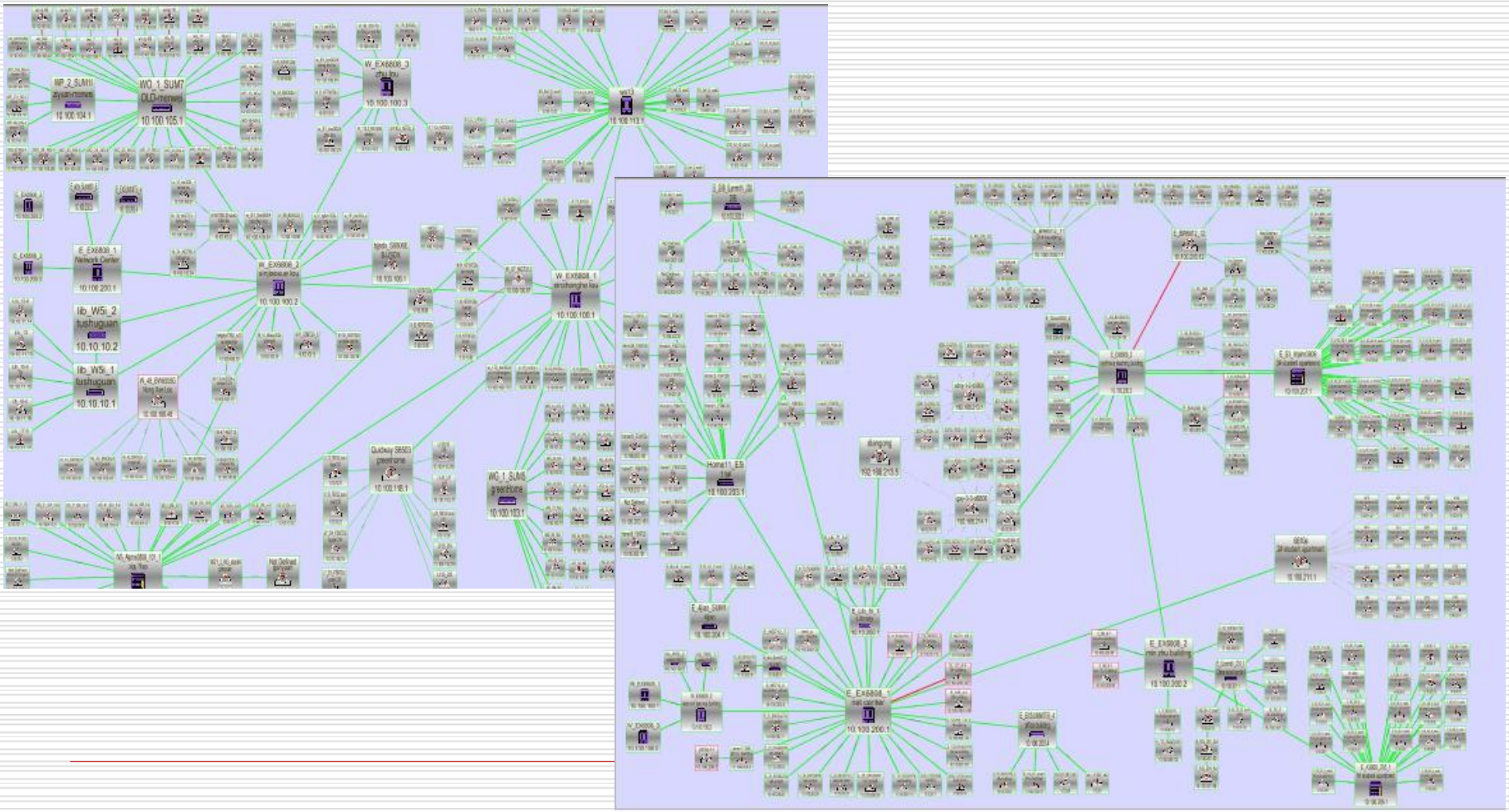
实施802.1x后存在的问题

- 帐户解绑问题
  - 帐户绑定与用户入网点变动的矛盾，要求管理员进行解绑定，增加了管理工作量。
- 计费方式比较单一：计时、包月
  - 对用户上网的上传下传量不可控制。我校是在出口安装了流量控制设备，控制BT等点到点应用。
- 全校范围内推广实施802.1x接入控制有一定的难度
  - 校园网交换机品牌较多，有点交换机支持802.1x、有的交换机不支持。
  - 802.1x分基本功能与扩展功能两部分，许多802.1x控制功能由其私有的扩展功能来实现的。不同厂家交换机802.1x扩展部分的功能不一样，给全校实施802.1x控制措施带来困难。
  - 如果希望在全校实施802.1x，一般需要选用同一家的产品，对不同家的二层网络设备需要更换或改造，给实施带来难度。

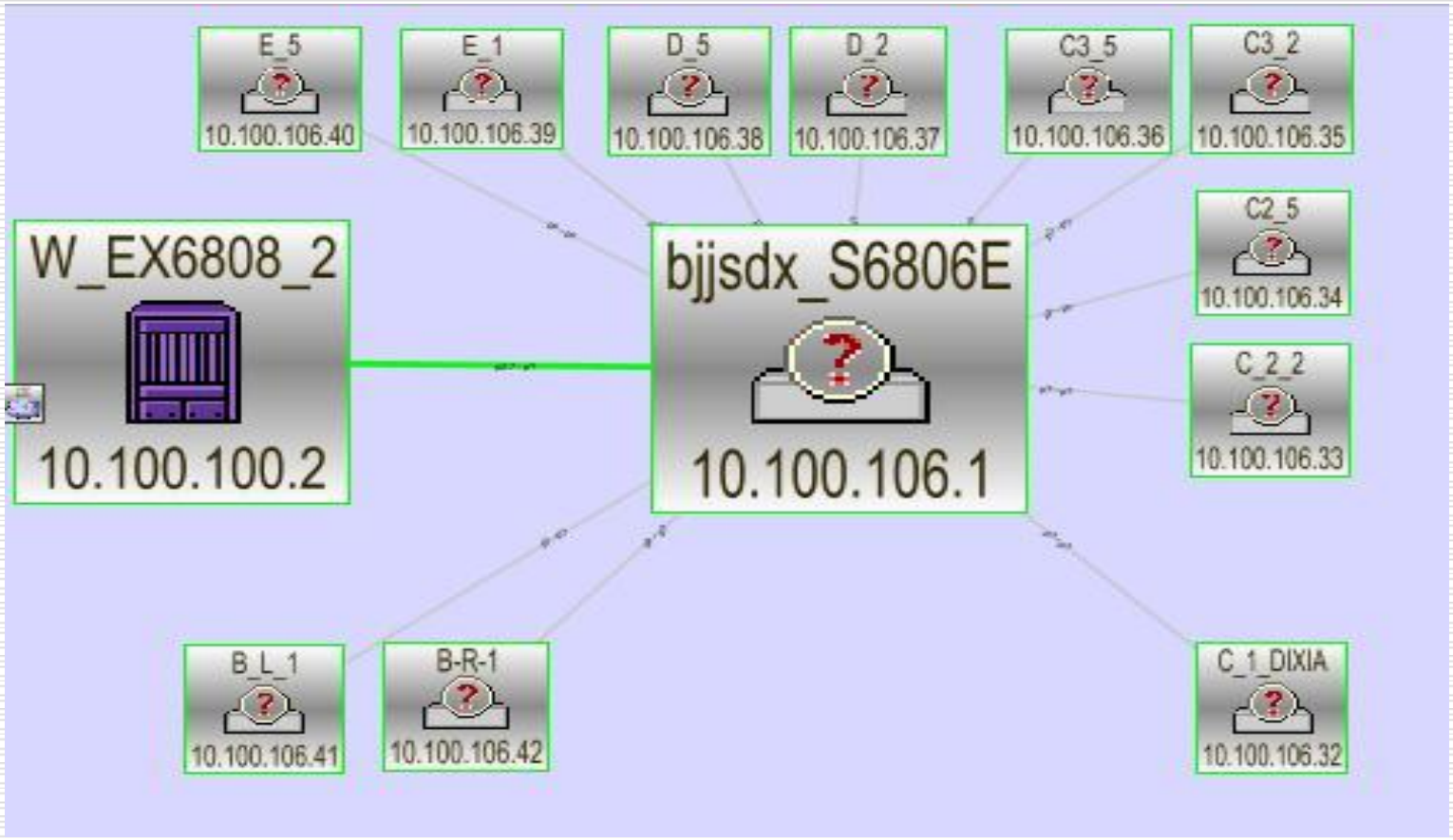
我校802.1x布署策略

- 在有条件的区域实施802.1X认证，如：新校区或新建楼宇。
- 在老的网络环境下仍采用网关方式，逐步过渡。
- 今后方向：
  - 计费、身份认证、防毒、安全审计一体化

我校网络拓扑结构



新校区网络拓扑结构—实施802.1x



谢谢！