校园网数字终端的智能化管理

柳 斌

华中科技大学 网络与计算中心

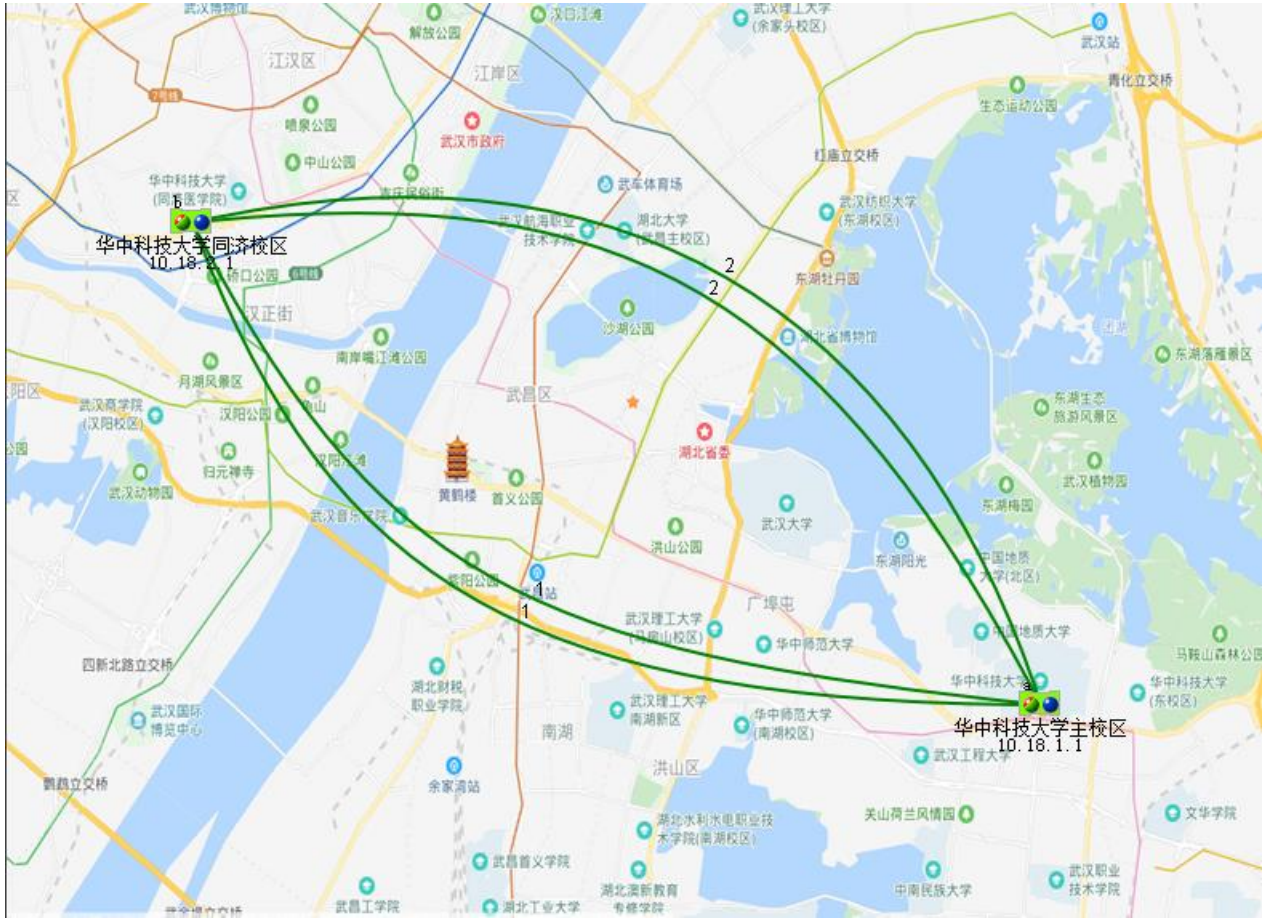
2019.11.13

提纲

- 校园网概况
- 认证终端管理
- 特殊设备管理
- 物联专网管理
- 小结

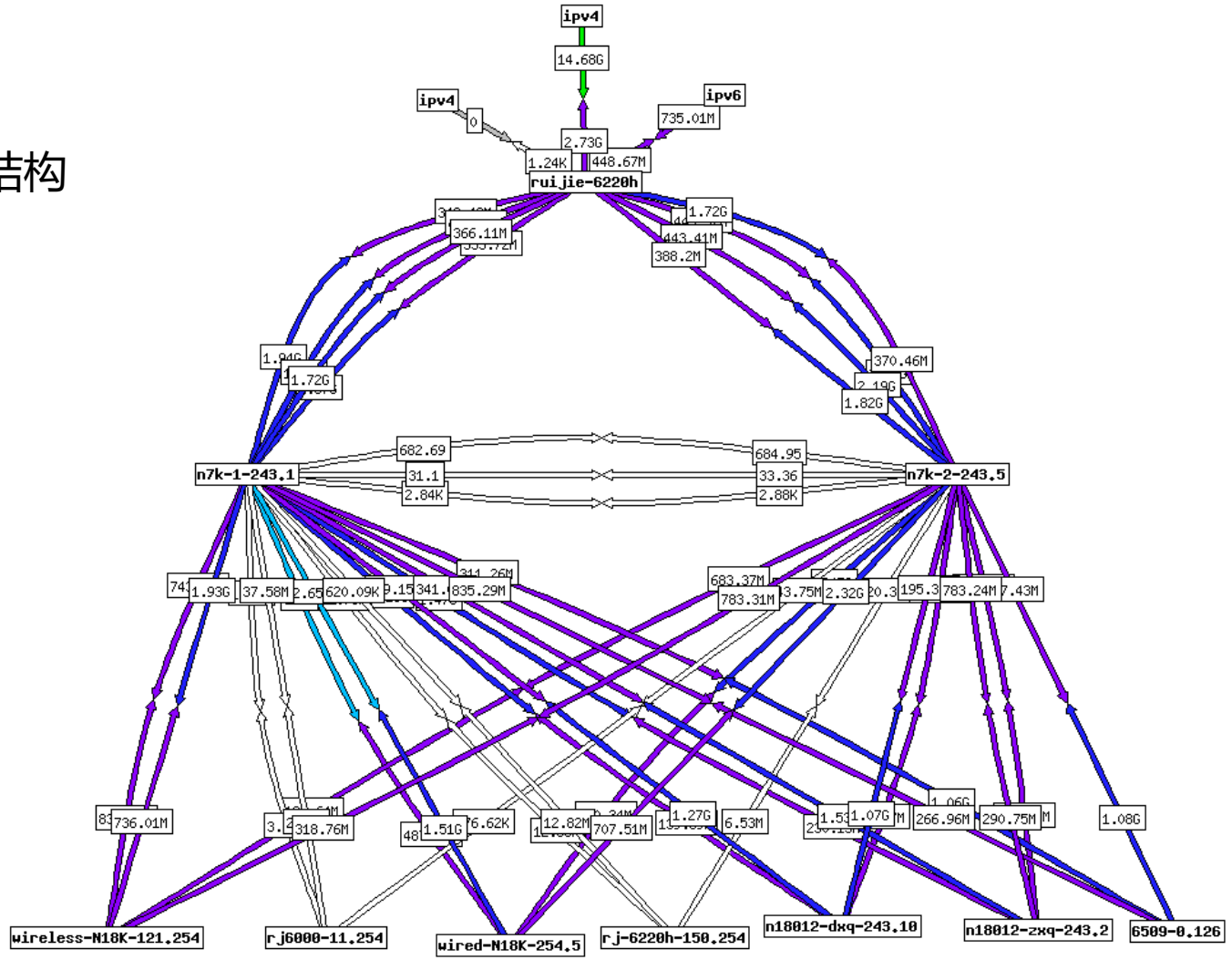
校园网概况

- 两个校区
- 校园网覆盖办公区、学生宿舍区260栋楼，10多万接入点，服务约8万师生用户，每日活跃约6万用户数
- 校园网出口带宽共有33G，包括10G移动、20G教育网、1G电信、2G IPV6，每日高峰期流量可达32G
- 校园网7300芯公里



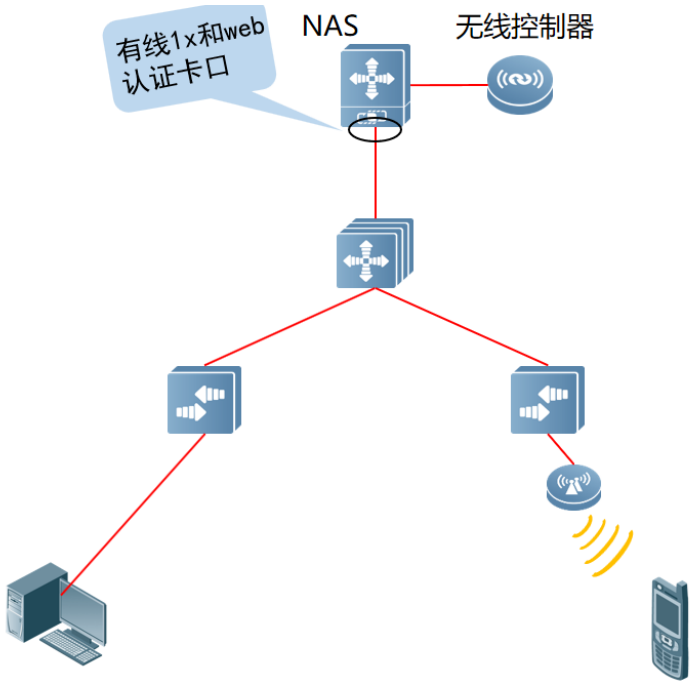
校园网拓扑架构

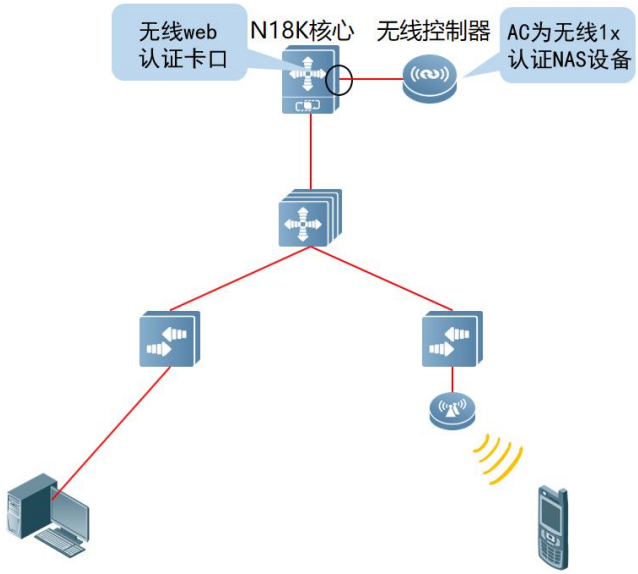
- 各单位光缆直连到网络中心
- 三层设备集中在网络中心，大二层结构
- 采用路由+VPC+VRRP结构



认证终端

- 采用准入认证方式
- 扁平化的认证结构
  - 6台NAS交换机，15台AC NAS
- 认证系统
  - 有线、无线认证
  - 计费、充值
  - 自助网站
  - Portal系统
  - 容灾





认证方式

- 有线网：

  802.1x认证（客户端）

  Portal 认证

  无感认证

- 无线网

  802.1x认证

  Portal 认证

  无感认证

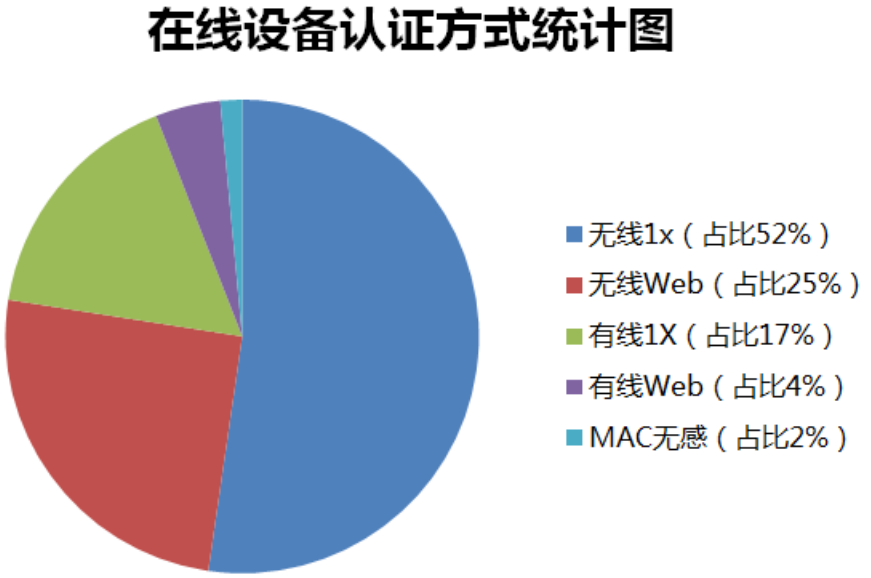
计费策略

- 开户数约8万，包括6万学生用户和2万教工用户，最高同时在线设备数7万。
- 计费管理：使用包时段策略，不限制时段内流量的使用。
  - 教工用户实行免费上网
  - 学生用户在办公区有线免费上网
  - 宿舍区设置了5种套餐供选择
  - 时间、区域、终端数、上网形式

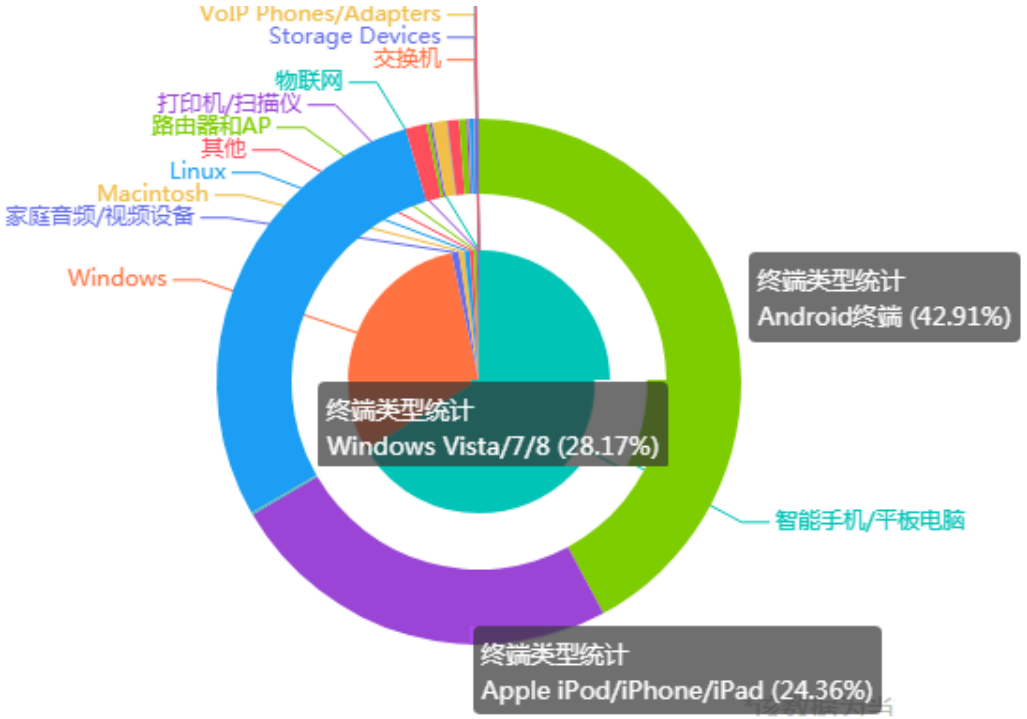
用户类型	终端数	上网时段	上网区域		套餐				
			办公区	宿舍区	1元/天	5元/周	20元/月	60元/4个月	100元/半年
大一新生	1	6：00-24：00	免费	收费	√	√	√	√	√
本科生	2	6：00-24：00	免费	收费	√	√	√	X	√
研究生	2	全天	免费	收费	√	√	√	X	√
教工	4	全天	免费	不可用	免费				

上网统计

用户最常选择使用的是无线1x认证方式，占到在线设备数的52%。无线1x认证上下线频繁，在每天240万条上网明细中93%的日志来自于无线1x用户。



移动设备占比67%，其中用户偏爱Android终端，使用率达到43%。



认证逃生机制

- 在认证服务器宕机或无法连通的情况下NAS交换机上的用户自动放通认证。

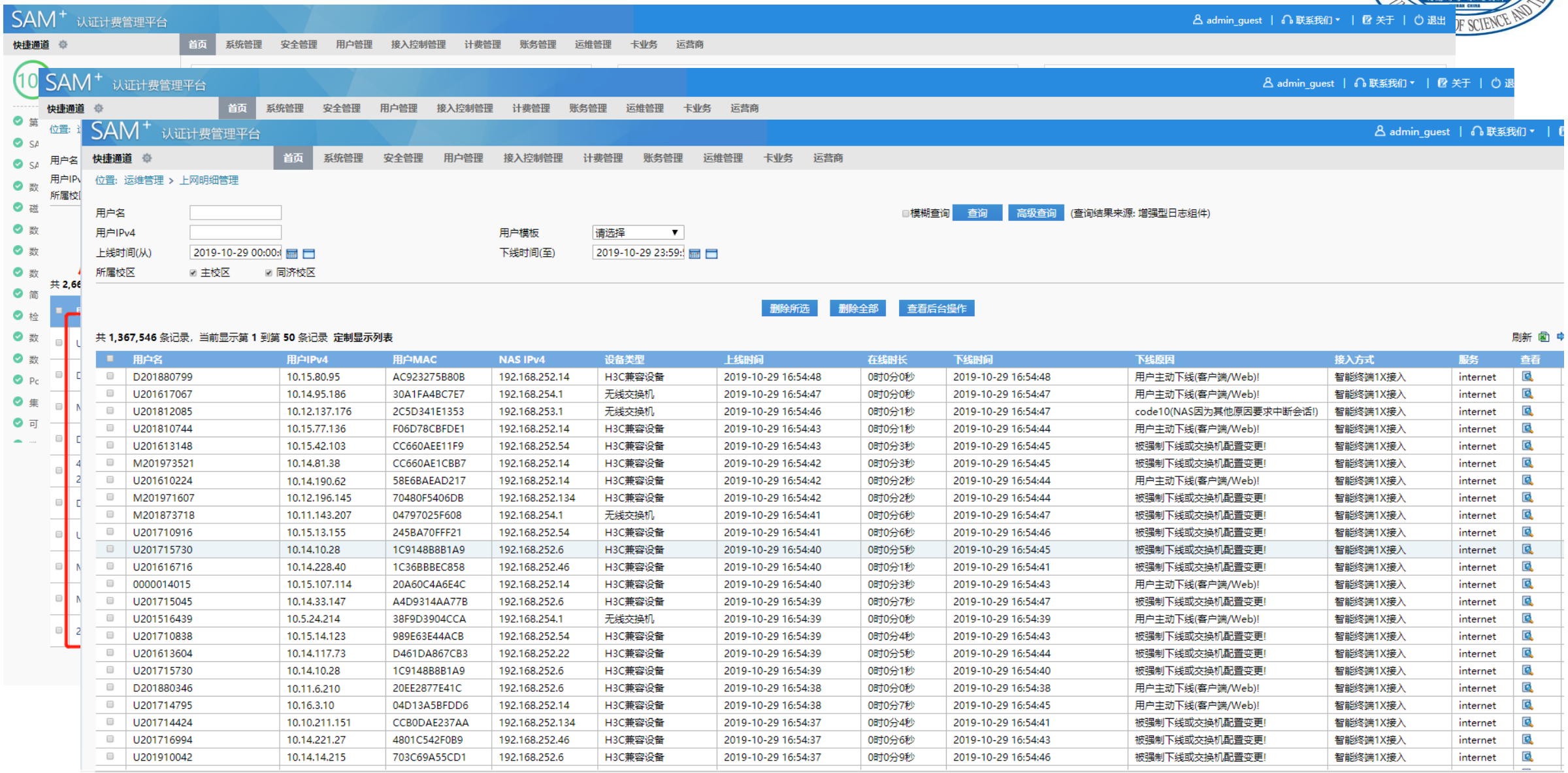
- 每隔2分钟使用逃生账号向认证系统判断服务器是否正常。
  radius-server dead-criteria time 120 tries 12 在120秒内重传12次判断逃生，防止逃生检测过于敏感造成认证抖动。

- 网络中一旦出现了Radius服务器不可用的情况，用户在访问外网的时候会弹出认证页面，此时，用户使用任何账户/密码信息均可认证通过，无条件放行。

- 有线用户的802.1X客户端模拟正常认证过程，实际不校验用户信息直接放通。

	用户名	用户姓名	用户IPv4	用户MAC
	taosheng	Radius逃生检测	10.4.[redacted]	00D[redacted]

认证终端管理



用户名	用户IPv4	用户MAC	NAS IPv4	设备类型	上线时间	在线时长	下线时间	下线原因	接入方式	服务	查看
D201880799	10.15.80.95	AC923275B80B	192.168.252.14	H3C兼容设备	2019-10-29 16:54:48	0时0分0秒	2019-10-29 16:54:48	用户主动下线(客户端/Web)!	智能终端1X接入	internet	
U201617067	10.14.95.186	30A1FA4BC7E7	192.168.254.1	无线交换机	2019-10-29 16:54:47	0时0分0秒	2019-10-29 16:54:47	用户主动下线(客户端/Web)!	智能终端1X接入	internet	
U201812085	10.12.137.176	2C5D341E1353	192.168.253.1	无线交换机	2019-10-29 16:54:46	0时0分1秒	2019-10-29 16:54:47	code10(NAS因为其他原因要求中断会话!)	智能终端1X接入	internet	
U201810744	10.15.77.136	F06D78CBFDE1	192.168.252.14	H3C兼容设备	2019-10-29 16:54:43	0时0分1秒	2019-10-29 16:54:44	用户主动下线(客户端/Web)!	智能终端1X接入	internet	
U201613148	10.15.42.103	CC660AEE11F9	192.168.252.54	H3C兼容设备	2019-10-29 16:54:43	0时0分3秒	2019-10-29 16:54:45	被强制下线或交换机配置变更!	智能终端1X接入	internet	
M201973521	10.14.81.38	CC660AE1CBB7	192.168.252.14	H3C兼容设备	2019-10-29 16:54:42	0时0分3秒	2019-10-29 16:54:45	被强制下线或交换机配置变更!	智能终端1X接入	internet	
U201610224	10.14.190.62	58E6BAEAD217	192.168.252.14	H3C兼容设备	2019-10-29 16:54:42	0时0分2秒	2019-10-29 16:54:44	用户主动下线(客户端/Web)!	智能终端1X接入	internet	
M201971607	10.12.196.145	70480F5406DB	192.168.252.134	H3C兼容设备	2019-10-29 16:54:42	0时0分2秒	2019-10-29 16:54:44	被强制下线或交换机配置变更!	智能终端1X接入	internet	
M201873718	10.11.143.207	04797025F608	192.168.254.1	无线交换机	2019-10-29 16:54:41	0时0分6秒	2019-10-29 16:54:47	被强制下线或交换机配置变更!	智能终端1X接入	internet	
U201710916	10.15.13.155	245BA70FFF21	192.168.252.54	H3C兼容设备	2019-10-29 16:54:41	0时0分6秒	2019-10-29 16:54:46	被强制下线或交换机配置变更!	智能终端1X接入	internet	
U201715730	10.14.10.28	1C9148B8B1A9	192.168.252.6	H3C兼容设备	2019-10-29 16:54:40	0时0分5秒	2019-10-29 16:54:45	被强制下线或交换机配置变更!	智能终端1X接入	internet	
U201616716	10.14.228.40	1C36BBBEC858	192.168.252.46	H3C兼容设备	2019-10-29 16:54:40	0时0分1秒	2019-10-29 16:54:41	被强制下线或交换机配置变更!	智能终端1X接入	internet	
0000014015	10.15.107.114	20A60C4A6E4C	192.168.252.14	H3C兼容设备	2019-10-29 16:54:40	0时0分3秒	2019-10-29 16:54:43	用户主动下线(客户端/Web)!	智能终端1X接入	internet	
U201715045	10.14.33.147	A4D9314AA77B	192.168.252.6	H3C兼容设备	2019-10-29 16:54:39	0时0分7秒	2019-10-29 16:54:47	被强制下线或交换机配置变更!	智能终端1X接入	internet	
U201516439	10.5.24.214	38F9D3904CCA	192.168.254.1	无线交换机	2019-10-29 16:54:39	0时0分0秒	2019-10-29 16:54:39	用户主动下线(客户端/Web)!	智能终端1X接入	internet	
U201710838	10.15.14.123	989E63E44ACB	192.168.252.54	H3C兼容设备	2019-10-29 16:54:39	0时0分4秒	2019-10-29 16:54:43	被强制下线或交换机配置变更!	智能终端1X接入	internet	
U201613604	10.14.117.73	D461DA867CB3	192.168.252.22	H3C兼容设备	2019-10-29 16:54:39	0时0分5秒	2019-10-29 16:54:44	被强制下线或交换机配置变更!	智能终端1X接入	internet	
U201715730	10.14.10.28	1C9148B8B1A9	192.168.252.6	H3C兼容设备	2019-10-29 16:54:39	0时0分1秒	2019-10-29 16:54:40	被强制下线或交换机配置变更!	智能终端1X接入	internet	
D201880346	10.11.6.210	20EE2877E41C	192.168.252.6	H3C兼容设备	2019-10-29 16:54:38	0时0分0秒	2019-10-29 16:54:38	用户主动下线(客户端/Web)!	智能终端1X接入	internet	
U201714795	10.16.3.10	04D13A5BFDD6	192.168.252.14	H3C兼容设备	2019-10-29 16:54:38	0时0分7秒	2019-10-29 16:54:45	用户主动下线(客户端/Web)!	智能终端1X接入	internet	
U201714424	10.10.211.151	CCB0DAE237AA	192.168.252.134	H3C兼容设备	2019-10-29 16:54:37	0时0分4秒	2019-10-29 16:54:41	被强制下线或交换机配置变更!	智能终端1X接入	internet	
U201716994	10.14.221.27	4801C542F0B9	192.168.252.46	H3C兼容设备	2019-10-29 16:54:37	0时0分6秒	2019-10-29 16:54:43	被强制下线或交换机配置变更!	智能终端1X接入	internet	
U201910042	10.14.14.215	703C69A55CD1	192.168.252.6	H3C兼容设备	2019-10-29 16:54:37	0时0分9秒	2019-10-29 16:54:46	被强制下线或交换机配置变更!	智能终端1X接入	internet	

非认证终端

- 除了认证终端外，校园网中还有不少非认证的终端。
- 非认证终端包括特殊设备，物联网终端，网络设备、机房等，我们需要知道终端在哪里？啥设备，责任人是谁？

```
HUST-wire-N18K#sh arp counter
ARP Limit:                    85000
Count of static entries:      10050
Count of dynamic entries:     20068 (complete: 19695  incomplete: 373)
Total:                        30118 (overlayer: 0  underlayer: 30118)

HUST-wireless-N18K#sh arp counter
ARP Limit:                    85000
Count of static entries:      4556
Count of dynamic entries:     22991 (complete: 22748  incomplete: 243)
Total:                        27547 (overlayer: 0  underlayer: 27547)

N18012-dongxiaoqu#sh arp counter
ARP Limit:                    170000
Count of static entries:      5891
Count of dynamic entries:     23434 (complete: 23198  incomplete: 236)
Total:                        29325 (overlayer: 0  underlayer: 29325)

N18012-zhuxiaoqu#sh arp counter
ARP Limit:                    170000
Count of static entries:      5271
Count of dynamic entries:     8692 (complete: 8626  incomplete: 66)
Total:                        13963 (overlayer: 0  underlayer: 13963)

TJMU-RG-N18K#sh arp counter
ARP Limit:                    85000
Count of static entries:      1162
Count of dynamic entries:     9736 (complete: 9686  incomplete: 50)
Total:                        10898 (overlayer: 0  underlayer: 10898)

TJMU-N18010-BanGong#sh arp counter
ARP Limit:                    85000
Count of static entries:      700
Count of dynamic entries:     3216 (complete: 3207  incomplete: 9)
Total:                        3916 (overlayer: 0  underlayer: 3916)
```

特殊设备管理

- 校园网中存在不少因各种原因无法认证的终端，我们称之为特殊设备，没有纳入到认证系统进行统一管理。
- 特殊设备种类众多，且类型复杂，存在不少安全隐患。
- 特殊设备IP放置在用户本地，地理位置分散，和用户在同一个网段。

华中科技大学校园网特殊设备申请表

设备信息				
负责人姓名	楼栋	房号	联系电话	人员编号
设备名称		MAC地址		操作系统
-请选择-		格式为：XX-XX-XX-X...		
上传设备照片				
点击此处上传附件（建议使用谷歌（chrome）、火狐浏览器，360浏览器、搜狗浏览器请切换成极速模式，ie浏览器需要升级至ie10以上）				
请点击此处，添加设备信息!				
单位名称	网络与计算中心		联系电话	18627038206
申请日期	2019-11-04	申请年限（申请年限不超过1年，1年后请重新申请）		1年

特殊设备入网是指不能安装认证程序的网络设备，下框内应说明入网设备的名称、用途、功能等。
本人承诺所申请特殊设备符合《校信息化〔2018〕1号 校园计算机网络管理办法》文件要求，并承担所申请设备安全责任。
已阅读《校信息化〔2018〕1号 校园计算机网络管理办法》

单位信息化联络员审核		审核人		审核时间
单位负责人审批		审批人		审批时间
网络与计算中心用户服务部预审核		审核人		审核时间
网络与计算中心分管信息化负责人审批		审批人		审批时间
网络与计算中心网络运行部审核		审核人		审核时间

特殊设备入网

步骤一：准确查找用户所在网段（最好先联系一下用户认证一下）；

步骤二：查找空闲IP；

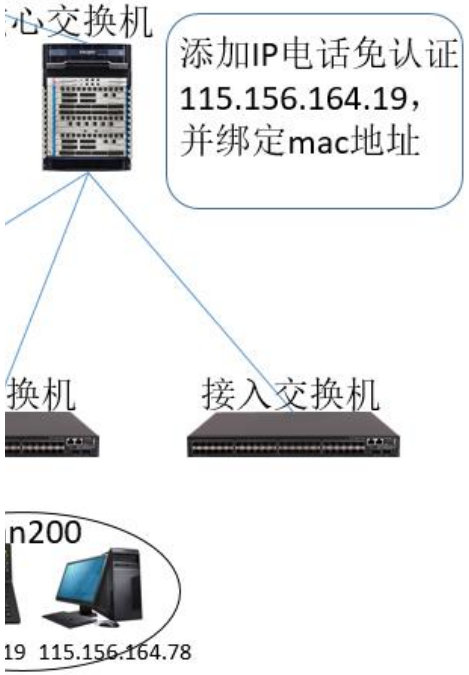
步骤三；在dhcp中排除掉IP地址；

步骤四：在核心交换机上做安全通道放通，IP地址和mac绑定；

步骤五：记录表格。

步骤六：通知用户。

```
660 permit ip host 211.67.23.245 host 2047.4780.6f82 any any
680 permit ip host 122.205.1.249 host 0025.90e8.279c any any
710 permit ip host 122.205.1.248 host 001a.640a.b610 any any
720 permit ip host 202.114.2.38 host 60eb.69d2.5880 any any
730 permit ip host 202.114.2.7 host 0015.178f.8f74 any any
740 permit ip host 202.114.3.250 host a036.9f99.d221 any any
760 permit ip host 211.67.23.244 host 54c4.15dd.9c63 any any
810 permit ip host 211.67.19.248 host 0080.91ab.5166 any any
840 permit ip host 211.67.19.246 host 408d.5c9c.dd66 any any
850 permit ip host 211.67.19.247 host b8ca.3aa5.b423 any any
860 permit ip host 122.205.1.247 host 00e0.db31.342a any any
870 permit ip 192.168.0.0 0.0.255.255 any any any
880 permit ip host 211.67.19.245 host 00e0.b453.ac77 any any
890 permit ip host 210.42.111.253 host 0cc4.7a6b.0a30 any any
900 permit ip host 210.42.111.252 host 0cc4.7a41.21d2 any any
910 permit ip host 210.42.111.251 host 0cc4.7a02.ef3a any any
920 permit ip host 210.42.111.250 host 0cc4.7a31.e33a any any
930 permit ip host 210.42.111.249 host fcaa.141d.36e8 any any
950 permit ip host 210.42.111.247 host 0007.e949.2037 any any
980 permit ip host 211.67.19.243 host 704d.7b6c.efbe any any
990 permit ip host 115.156.245.253 host 2880.23a1.3918 any any
1000 permit ip host 115.156.245.252 host 0cc4.7ae5.55b0 any any
1010 permit ip host 115.156.245.251 host 00e8.4c68.5952 any any
1020 permit ip host 115.156.245.250 host 00e8.4c68.5928 any any
1030 permit ip host 115.156.245.249 host c860.0062.8452 any any
1040 permit ip host 115.156.245.248 host ac22.0b85.1af3 any any
1050 permit ip host 211.67.19.242 host 001e.8fda.e56c any any
1060 permit ip host 211.67.19.241 host 0026.737b.99d0 any any
1070 permit ip host 115.156.161.252 host 1866.daf9.1eec any any
1080 permit ip host 211.67.19.240 host 0026.7350.4df7 any any
1090 permit ip host 211.67.19.239 host 40a8.f0b5.dc04 any any
1100 permit ip host 210.42.111.244 host 68f7.28c8.e223 any any
1110 permit ip host 115.156.245.247 host b05a.dac2.2018 any any
1180 permit ip host 211.67.23.243 host 5046.5d66.f376 any any
1190 permit ip host 202.114.21.250 host b8ae.edf0.d23a any any
1200 permit ip host 202.114.21.243 host 000c.4330.5277 any any
1210 permit ip host 202.114.21.224 host 0080.9171.d025 any any
1220 permit ip host 202.114.21.223 host 009c.0205.b9cb any any
1230 permit ip host 202.114.21.221 host 80c1.6e94.8a80 any any
1240 permit ip host 202.114.21.219 host 0080.9177.b1e4 any any
1250 permit ip host 202.114.21.218 host 0080.91b2.6e34 any any
1280 permit ip host 202.114.21.249 host 001f.d01f.dd09 any any
1290 permit ip host 202.114.21.247 host 00e0.4c67.f401 any any
1300 permit ip host 202.114.21.246 host 2089.84ed.93b8 any any
1310 permit ip host 202.114.21.245 host 2089.84f7.5cf7 any any
1320 permit ip host 202.114.21.242 host 001e.679d.5dd9 any any
1330 permit ip host 202.114.21.229 host 0023.ae5a.dc20 any any
1340 permit ip host 202.114.21.227 host 0080.9177.b1e4 any any
1350 permit ip host 202.114.21.226 host 001e.0bff.4404 any any
```



特殊设备入网

（1）IP地址分配不便

（2）交换机上配置步骤多，易出错，工作量大

（3）消耗大量核心交换机ACL资源

（4） 需要维护一张复杂且没有规律的表

（5）后期IP地址难以变动

（6）IP地址缺乏有效监控，很难回收，实现“年审制度”

首页 > IP管理系统 > 特殊设备入网

查询信息　总记录数：1605条

序号	负责人	联系电话	设备名称	MAC地址	IP地址	操作
121			大屏	60-a4-4c-34-b3-63	202.114.5.129	详情
122			大屏	78-2c-29-85-fb-cb	122.205.22.110	详情
123			hp M712 A3黑白打印机	84-a9-3e-53-3d-89	202.114.21.190	详情
124			摄像头	98-8b-0a-ad-d6-9a	115.156.245.244	详情
125			摄像头	98-8b-0a-ad-d7-c6	115.156.245.243	详情
126			摄像头	98-8b-0a-ad-d6-f5	115.156.245.242	详情
127			服务器	d8-9e-f3-35-cf-4b	115.156.215.221	详情
128			服务器	1c-1b-0d-9b-81-6d	115.156.217.240	详情
129			服务器	6c-92-bf-16-5d-a7	115.156.222.253	详情
130			服务器	04-d4-c4-8f-4d-64	202.114.8.123	详情

页13/161 总页　首页 上一页 下一页 末页

特殊设备管理-基于SDN控制器

三大部分：

- 拓扑架构

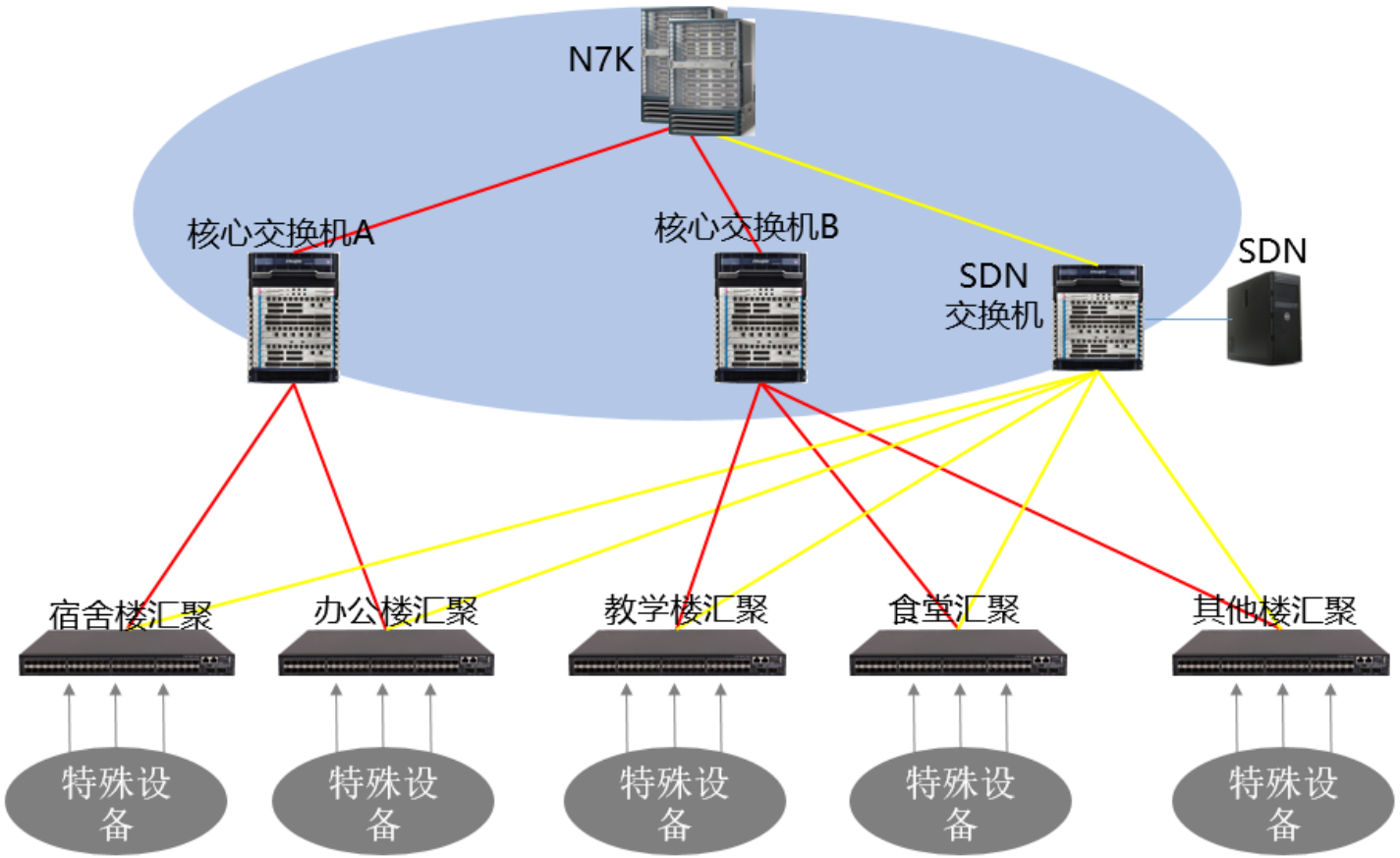
  网关分离，链路共用，多网融合；

- SDN交换机

  采用openflow、netconf、snmp协议联动SDN控制器，执行控制器策略；

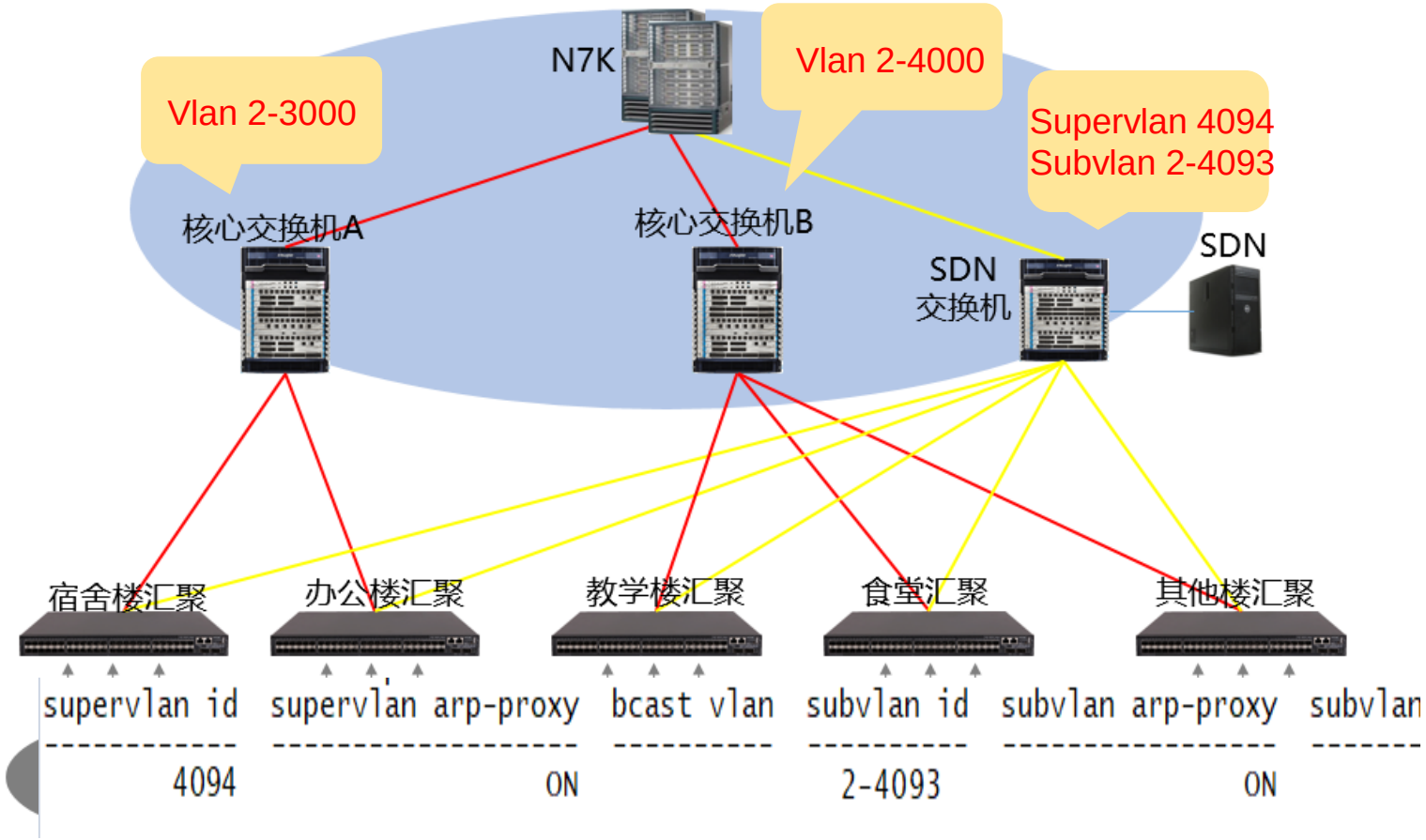
- SDN控制器

  给终端入网加上一把锁，控制终端入网，精细化安全策略控制，可视化管理；



特殊设备管理-拓扑架构

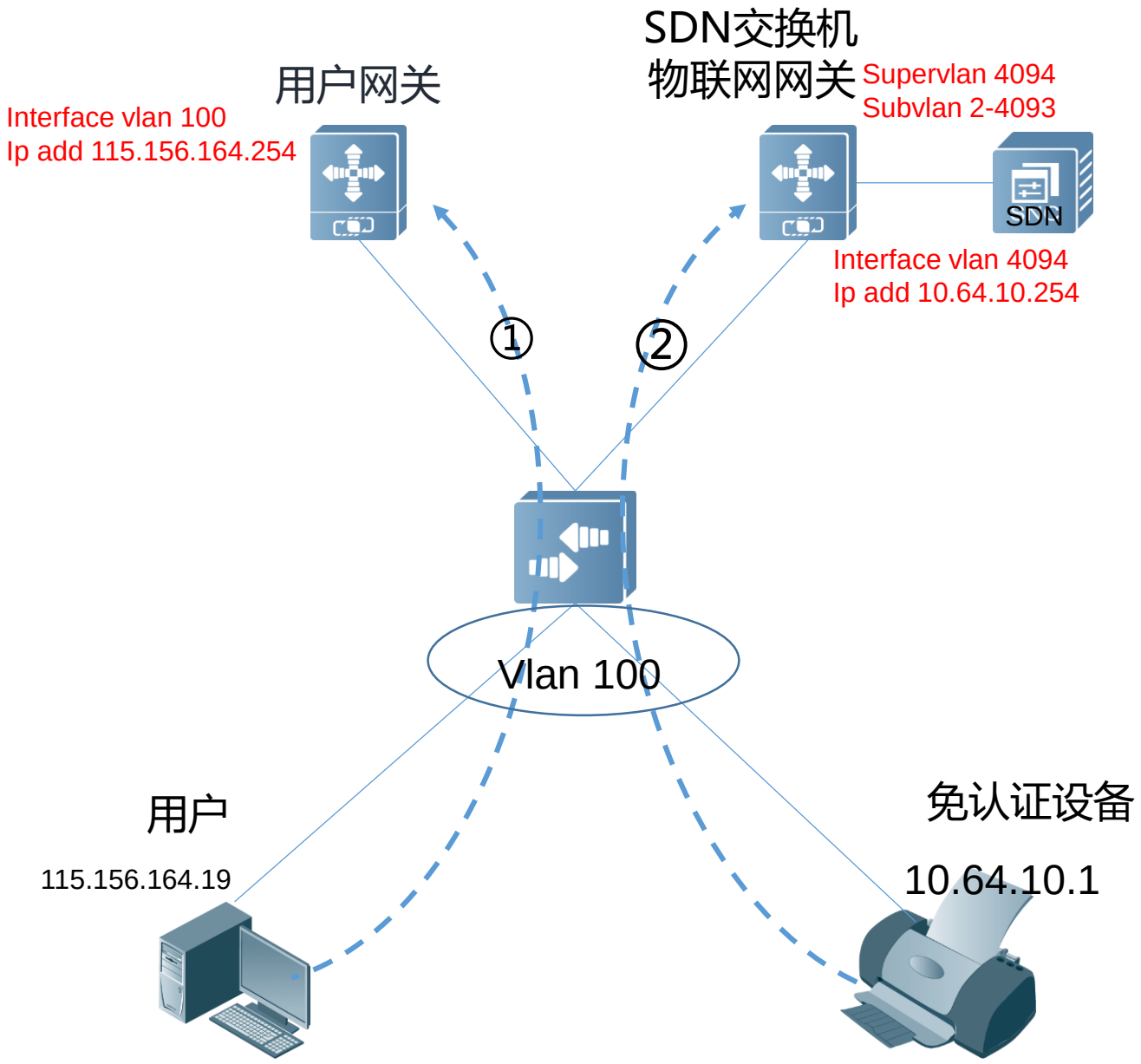
- 实现机制
  - 从每台汇聚上新增一条链路到SDN核心交换机。
  - 在核心上起一个supervlan，用户vlan作为这个supervlan的subvlan。
  - 在不改动原有网络结构的情况下实现网关分离和链路复用。在汇聚和接入交换机上，设备、链路和vlan复用，实现在一套网络中承载多种业务。
  - 实现了终端的即插即用。



特殊设备管理-分离网关

①用户流量走向

②特殊设备流量走向

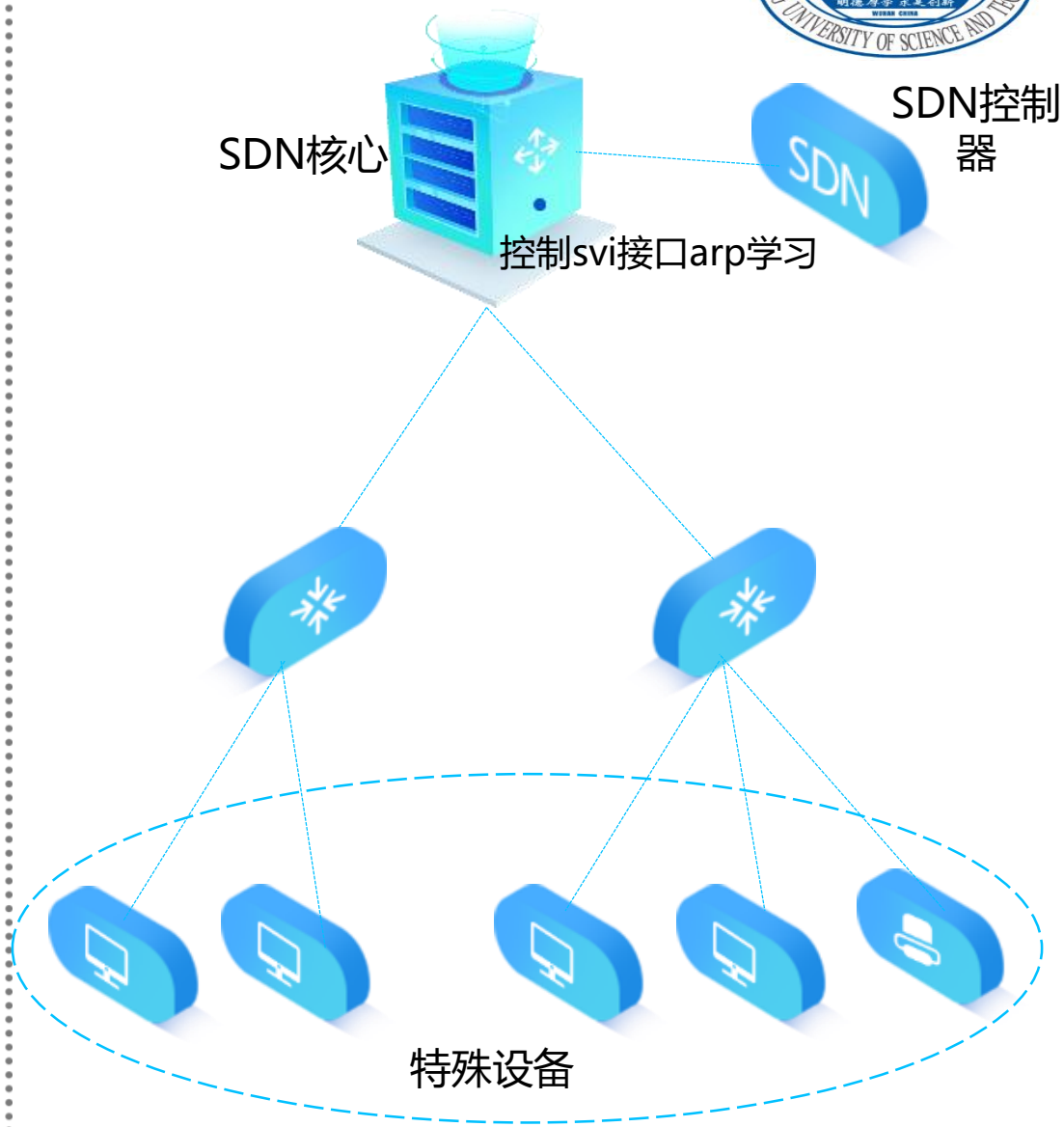


特殊设备管理-SDN交换机/控制器

准入控制：利用SDN控制器/交换机实现终端ARP表项的自动控制

“关闭ARP学习“+”将ARP上送控制器”+“控制器下发静态ARP绑定”

- 控制器开启管控，SVI口关闭ARP学习功能
- 用户接入网络，发起ARP请求
- 网关将ARP上送报文至控制器
- 控制器发现用户
- 控制器审批通过，下发ARP静态绑定
- 网关回复用户ARP
- 用户流量转发



特殊设备管理-设备联动

- 准入管控相当于给终端入网上了一把锁，开启准入管控后，控制器会通过netconf协议下发关闭ARP学习的命令，通过openflow协议下发流表，流表上传控制器产生审批表项，通过审批的终端允许入网

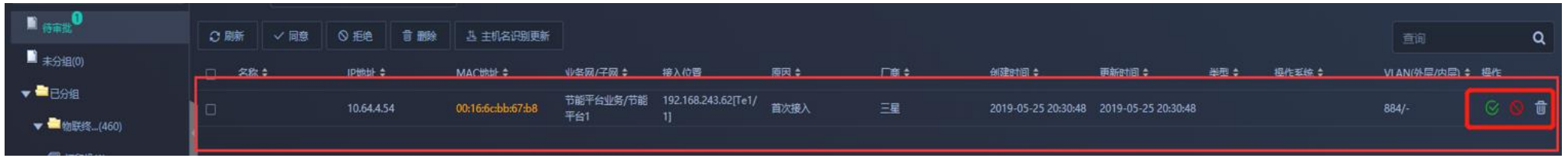
```
interface VLAN 4094
 description Free_Device
 ip address 222.20.95.254 255.255.254.0
 ip address 10.64.15.254 255.255.255.0 secondary
 ip address 192.168.163.254 255.255.252.0 secondary
 arp disable-learning 192.168.160.0 255.255.252.0
 arp disable-learning 222.20.94.0 255.255.254.0
```

关闭arp学习

```
/****************** openflow flow table[0]---flow number[22] ******************/

{table="0", duration_sec="16894049", priority="500", flags ="0x0",idle_timeout="0", hard_timeout="0", cookie="0xf8ea95b378000", packet_count="71928374", by
te_count="4891129932". match=oxm{eth_type="0x806", arp_spa="10.64.4.0", arp_sha_mask="255.255.255.0"} instructions=[apply{acts=[output{port="controller", m
ax_len="65535"}, output{port="normal"}]}]}
xid=281, sync_flag=0x0, ss_index=0x1

{table="0", duration_sec="16893902", priority="500", flags ="0x0",idle_timeout="0", hard_timeout="0", cookie="0xf8ea9ebc68000", packet_count="594146", byte
_count="40401928". match=oxm{eth_type="0x806", arp_spa="10.64.5.0", arp_sha_mask="255.255.255.0"} instructions=[apply{acts=[output{port="controller", max_l
en="65535"}, output{port="normal"}]}]}
xid=401, sync_flag=0x0, ss_index=0x4

{table="0", duration_sec="16893884", priority="500", flags ="0x0",idle_timeout="0", hard_timeout="0", cookie="0xf8ea9fd0a4000", packet_count="5341382", byt
e_count="363213988". match=oxm{eth_type="0x806", arp_spa="10.64.6.0", arp_sha_mask="255.255.255.0"} instructions=[apply{acts=[output{port="controller", max
_len="65535"}, output{port="normal"}]}]}
xid=415, sync_flag=0x0, ss_index=0x5
```

匹配到arp

送控制器处理



特殊设备管理-设备联动

静态ARP生成

控制器审批通过之后，会下发静态ARP绑定给核心交换机，这样终端就可以和网关通信，然后入网。

```
arp 192.168.160.11 988b.0ace.ad2b arpa
arp 192.168.160.12 30b4.9e4c.2450 arpa
arp 192.168.160.13 bcba.c288.13fc arpa
arp 192.168.160.14 00a8.59e8.2c32 arpa
arp 192.168.160.15 8825.93fc.aa5f arpa
arp 192.168.160.16 b83a.08f1.e828 arpa
arp 192.168.160.17 0894.ef94.1188 arpa
arp 192.168.160.18 a08c.fd85.a3bb arpa
arp 192.168.160.19 0894.ef7e.d2a0 arpa
arp 192.168.160.20 9c7b.ef90.f16a arpa
arp 192.168.160.21 f80d.609b.32ac arpa
arp 192.168.160.22 6c4b.9073.2272 arpa
arp 192.168.160.23 7489.f374.9870 arpa
arp 192.168.160.24 7489.e28a.8070 arpa
arp 192.168.160.25 ac16.2dce.8baf arpa
arp 192.168.160.26 480e.ec5d.46c6 arpa
arp 222.20.94.1 2004.0fee.b8a0 arpa
arp 222.20.94.2 4cd9.8f74.de64 arpa
arp 222.20.94.3 6c92.bfdd.051f arpa
arp 222.20.94.4 0025.90e6.a13a arpa
arp 222.20.94.5 305a.3a75.d086 arpa
arp 222.20.94.6 78b9.6781.ed4a arpa
arp 222.20.94.7 b026.2855.c3fa arpa
arp 222.20.94.8 107b.447e.2d35 arpa
arp 222.20.94.10 ac1f.6ba1.0d52 arpa
arp 222.20.94.11 0015.17ea.5b04 arpa
arp 222.20.94.12 ac1f.6b6b.49d8 arpa
arp 222.20.94.13 d050.99d2.6634 arpa
arp 222.20.94.14 d050.99d2.66bb arpa
arp 222.20.94.15 d050.99d2.6897 arpa
arp 222.20.94.16 d050.99d2.6827 arpa
arp 222.20.94.17 305a.3a76.102a arpa
```

控制器下发静态arp绑定

```
HUST-SDN-N18007#sh arp
Protocol  Address          Age(min)  Hardware       Type   Interface
Internet  10.64.0.1        <static>  a0d3.c129.80f7 arpa   VLAN 895
Internet  10.64.0.2        <static>  3464.a90c.7f32 arpa   VLAN 895
Internet  10.64.0.3        <static>  1c1b.0d9e.4d15 arpa   VLAN 895
Internet  10.64.0.4        <static>  3464.a90c.7fee arpa   VLAN 895
Internet  10.64.0.100      <static>  0030.1807.f8ed arpa   VLAN 895
Internet  10.64.0.101      <static>  0030.1807.f99d arpa   VLAN 895
Internet  10.64.0.102      <static>  0030.1804.5986 arpa   VLAN 895
Internet  10.64.0.103      <static>  0030.1804.5990 arpa   VLAN 895
Internet  10.64.0.104      <static>  0030.1807.f487 arpa   VLAN 895
Internet  10.64.0.105      <static>  0030.1807.faf6 arpa   VLAN 895
Internet  10.64.0.106      <static>  0030.1807.f88b arpa   VLAN 895
Internet  10.64.0.200      <static>  0066.0cb3.ae23 arpa   VLAN 895
Internet  10.64.0.201      <static>  0066.0cb3.ae3e arpa   VLAN 895
Internet  10.64.0.202      <static>  0066.0cb3.adfd arpa   VLAN 895
Internet  10.64.0.203      <static>  0066.0cb3.ae10 arpa   VLAN 895
Internet  10.64.0.205      <static>  0066.0cb3.ae3c arpa   VLAN 895
Internet  10.64.0.206      <static>  0066.0cb3.ae06 arpa   VLAN 895
Internet  10.64.1.1        <static>  3464.a90c.6d9e arpa   VLAN 895
Internet  10.64.1.3        <static>  a0d3.c10f.054b arpa   VLAN 895
Internet  10.64.1.104      <static>  0030.1807.faee arpa   VLAN 895
Internet  10.64.1.105      <static>  0030.1807.f8c6 arpa   VLAN 895
Internet  10.64.1.107      <static>  0030.1807.fb00 arpa   VLAN 895
Internet  10.64.1.108      <static>  0030.1807.f923 arpa   VLAN 895
Internet  10.64.1.109      <static>  0030.1807.f92d arpa   VLAN 895
Internet  10.64.1.110      <static>  0030.1807.f95a arpa   VLAN 895
Internet  10.64.1.112      <static>  0030.1803.b42b arpa   VLAN 895
Internet  10.64.1.113      <static>  0030.1807.f899 arpa   VLAN 895
Internet  10.64.1.202      <static>  0066.0cb3.ae35 arpa   VLAN 895
Internet  10.64.1.203      <static>  0066.0cb3.ae3b arpa   VLAN 895
Internet  10.64.1.204      <static>  0066.0cb3.ae00 arpa   VLAN 895
Internet  10.64.1.205      <static>  0066.0cb3.ae15 arpa   VLAN 895
Internet  10.64.1.206      <static>  0066.0cb3.ae19 arpa   VLAN 895
Internet  10.64.1.207      <static>  0066.0cb3.adfe arpa   VLAN 895
Internet  10.64.2.7        <static>  3464.a90c.7f3a arpa   VLAN 895
Internet  10.64.2.8        <static>  3464.a90c.7ff4 arpa   VLAN 895
Internet  10.64.2.9        <static>  1c1b.0d9e.9f9c arpa   VLAN 895
Internet  10.64.2.100      <static>  0030.1807.f892 arpa   VLAN 895
Internet  10.64.2.101      <static>  0030.1807.f890 arpa   VLAN 895
Internet  10.64.2.104      <static>  0030.1807.f88f arpa   VLAN 895
Internet  10.64.2.106      <static>  0030.1807.f8e2 arpa   VLAN 895
Internet  10.64.2.107      <static>  0030.1807.f891 arpa   VLAN 895
```

特殊设备管理

特

地址

➢

➢

步骤

，在

定

步骤

设计 部署 策略 网络监控

admin

资源访问策略 子网互访策略 服务链编排

刷新 导入 导出 高级配置 终端位置更新

关联业务子网：免认证设备/校园免认证设备公网

刷新 新增 删除 重新准入 有效时间

查询

类型 IP 接入位置 自动识别类型 责任人

名称	终端MAC	业务网/子网	IPv4地址	IPv6地址	接入位置	厂商	入网状态	有效期	更新时间	类型	操作系统	VLAN(外层/内	责任人	操作
服务器	b0:26:28:55:c3:fa	免认证设备/校园免认证设备公网	222.20.94.7		172.19.77.253[Ten-GigabitEthernet1/0/26]	Broadcom Limi...	准入成功	无限期	2019-10-31 11:07:44	电脑	Windows	395/-	罗辉，15972160075	
监控设备需要上网	98:8b:0a:d7:21:3b	免认证设备/校园免认证设备公网	222.20.94.21		192.168.133.125[GigabitEthernet0/0/11]		准入成功	2020-10-08	2019-10-31 15:17:12	监控设备		1038/-	徐龙，13871326462	
服务器	18:66:da:42:a2:f6	免认证设备/校园免认证设备公网	222.20.94.22		192.168.130.29[Gi0/26]	戴尔	准入成功	2020-10-08	2019-10-31 15:39:50	电脑	Windows	447/-	艾小猛，13397103651	
VPN设备	00:1c:54:d0:91:76	免认证设备/校园免认证设备公网	222.20.94.23		172.19.6.31[Gi0/28]	Hillstone Net...	准入成功	无限期	2019-10-31 15:27:17	电脑	Linux	527/-	韩兰胜,18971274240	
服务器	ac:1f:6b:a0:82:7a	免认证设备/校园免认证设备公网	222.20.94.20		192.168.130.29[Gi0/26]	Super Micro C...	准入成功	2020-09-25	2019-10-31 15:43:10	电脑	Windows	1237/-	陶波，13437140569	
服务器	4c:d9:8f:74:de:64	免认证设备/校园免认证设备公网	222.20.94.2		192.168.133.125[GigabitEthernet0/0/24]		准入成功	无限期	2019-10-31 15:17:19	电脑	Linux	1144/-	刘德欢,15623739776	
服务器	10:7b:44:7e:2d:35	免认证设备/校园免认证设备公网	222.20.94.8		192.168.243.62[Te3/4]	华硕	准入成功	2020-10-30	2019-10-31 15:39:02	电脑	Windows	63/-	龚珣,13517245799	
服务器	00:15:17:ea:5b:04	免认证设备/校园免认证设备公网	222.20.94.11		192.168.243.62[Te3/4]	Intel Corpora...	准入成功	2020-09-17	2019-10-31 15:39:27	电脑	Windows	1116/-	杨钢，13607149138	
服务器	d0:50:99:d2:68:97	免认证设备/校园免认证设备公网	222.20.94.15		192.168.90.1[Gi0/28]	ASRock Incorp...	准入成功	2020-09-23	2019-10-31 15:44:25	电脑	Windows	368/-	邓磊敏，17740699908	
服务器	30:5a:3a:76:10:2a	免认证设备/校园免认证设备公网	222.20.94.17		192.168.243.62[Te3/4]	华硕	准入成功	2020-09-23	2019-10-31 15:36:40			368/-	邓磊敏，17740699908	
专用服务器	e4:54:e8:61:36:09	免认证设备/校园免认证设备公网	222.20.94.27		192.168.243.62[Te3/4]		准入成功	2020-10-30	2019-10-30 15:16:55	电脑	Windows	-/-	杨州军，13986027126	

显示: 50 条 共24条

优点

- IP地址分配便捷

  特殊设备IP地址连续，可根

进行排序，不需要维护一

于统计归类。

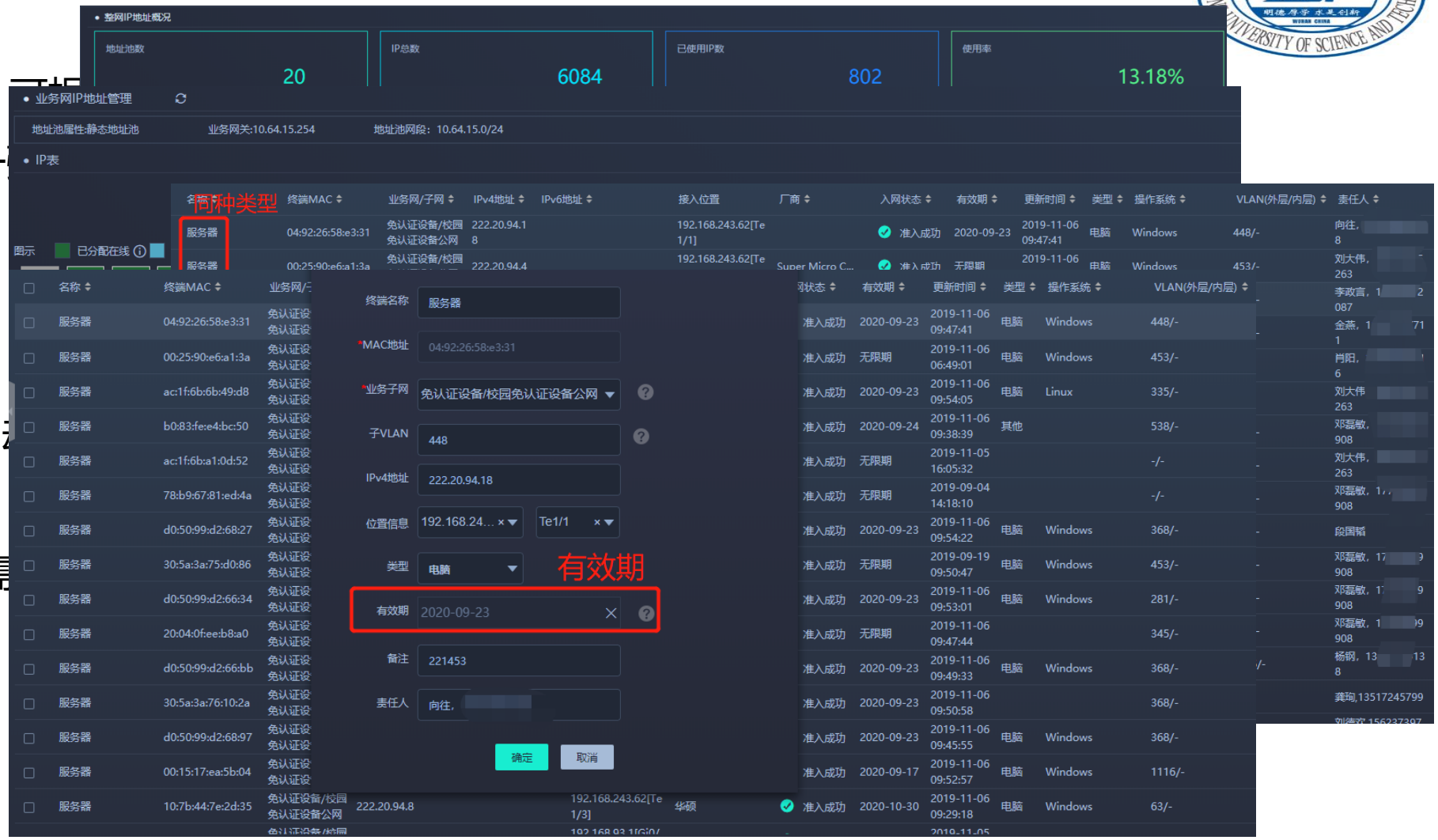
- 用户终端即插即用
- 易于实现终端年审

  设置有效期，到期后自

- 终端状态可视化管理
- 终端在各楼栋迁移无需

  受地理位置限制。

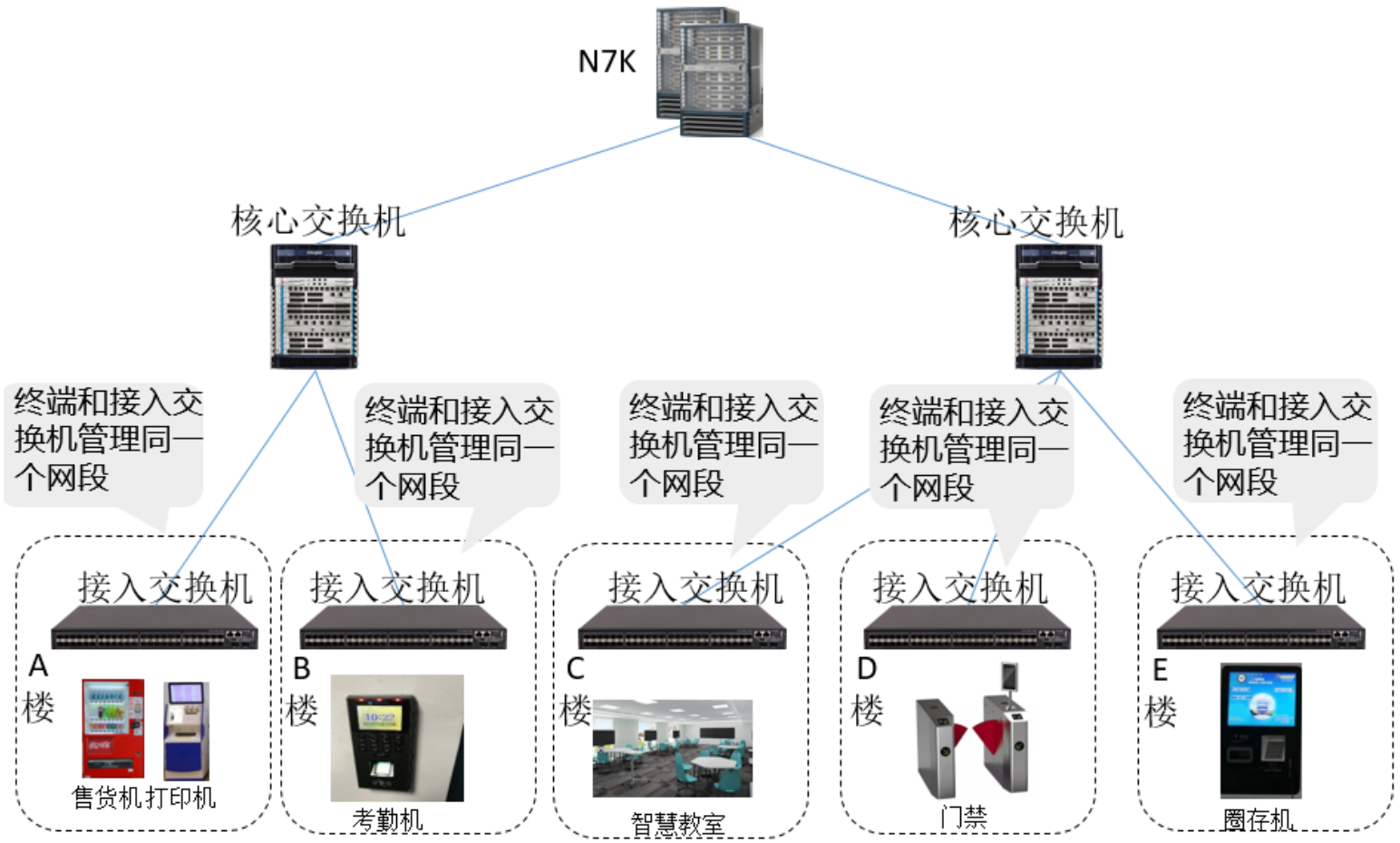
- 节省交换机ACL资源
- 图形化操作



物联专网的管理

- 校园网承载越来越多物联网专网的应用，如消防系统，节能平台，电表远程抄表，水表远程抄表，信息发布，体育课考勤。。。
- 专网特点：
    - 覆盖面广，所有的楼栋，需要借助校园网来承载
    - 每个楼终端数少，流量小。
    - 分属不同部门管理
    - 系统缺乏运维人员
    - 可靠性安全性要求越来越高

物联专网管理-传统方案



传统的做法：

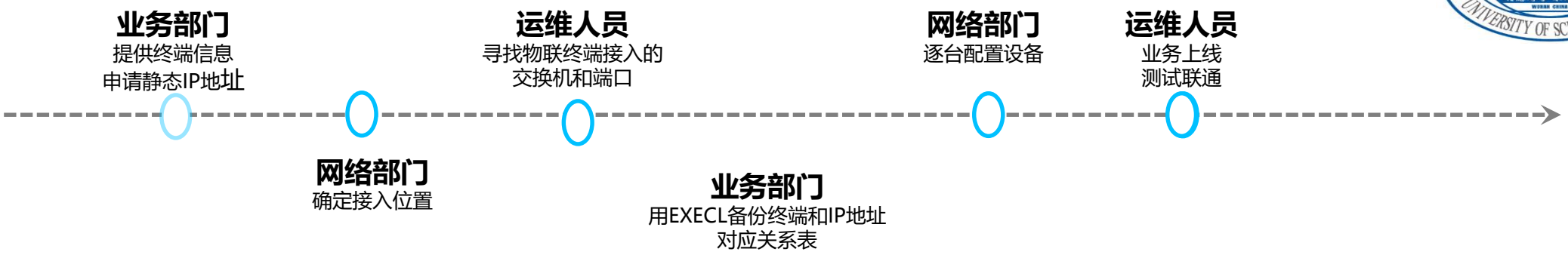
1.首先派人协助联到哪台交换机的哪个端口。

2.用户交端口对应表。

3.利用每栋楼交换机的管理网段，终端所在接口更改为交换机的管理vlan。

4.做好记录。

物联专网管理-传统方案



1. 专网开通时间长。
2. 不同应用网络混和在一起。
3. IP地址过于分散无法进行管控。
4. 安全性问题，访问权限过大，校内资源都能够访问，不少设备存在弱密码。
5. 缺乏系统监控，时间一长，管理员不清楚终端数量、位置和管理部门。

物联专网管理

N7K
Supervlan 4094
Subvlan 2-4093
消防业务一个网段
搜索已分组下分组
关联业务子网：自动售货机/自动售货机
刷新
新增
删除
重新准入
有效时间
查询
待审批
未分组(0)
已分组
物联终端(804)
打印机(1)
公网免认证设备(25)
节能平台(261)
室外无线(5)
私网免认证设备(26)
体育课部(53)
消防业务(248)
一卡通501(93)
一卡通门禁(8)
一卡通饮食中心(4)
自动售货机(80)
黑名单(0)
白名单(0)
名称 终端MAC 业务网/子网 IPv4地址 IPv6地址 接入位置 厂商 入网状态 有效期 更新时间 类型 操作系统 VLAN(外层/内层) 责任人 操作
YQ17072568205 00:e0:b4:19:3b:fd 自动售货机/自动售货机 10.64.12.23 192.168.243.62[Te1/5] TECHNO SCOPE ... 准入成功 无限期 2019-11-08 10:39:15 -/-
TCN111963403 00:e0:b4:18:1d:fa 自动售货机/自动售货机 10.64.12.37 172.19.76.253[GigabitEthernet1/0/10] TECHNO SCOPE ... 准入成功 无限期 2019-11-08 10:34:31 -/-
YQ17120868204 00:e0:b4:19:78:6d 自动售货机/自动售货机 10.64.12.17 172.18.31.252[GigabitEthernet1/0/6] TECHNO SCOPE ... 准入成功 无限期 2019-11-08 10:43:53 -/-
YQ17072568204 00:e0:b4:19:42:f0 自动售货机/自动售货机 10.64.12.57 192.168.243.62[Te1/5] TECHNO SCOPE ... 准入成功 无限期 2019-11-08 10:39:14 -/-
fc:c2:3d:18:d8:1b 自动售货机/自动售货机 10.64.12.61 192.168.243.62[Te3/4] Atmel Corpora... 准入成功 无限期 2019-11-08 10:53:15 -/-
YQ17120868203 00:e0:b4:19:78:83 自动售货机/自动售货机 10.64.12.41 172.19.66.253[GigabitEthernet1/0/10] TECHNO SCOPE ... 准入成功 无限期 2019-11-08 10:51:41 -/-
YQ17072568210 00:e0:b4:19:37:b8 自动售货机/自动售货机 10.64.12.9 172.20.74.253[GigabitEthernet1/0/21] TECHNO SCOPE ... 准入成功 无限期 2019-11-08 10:33:58 -/-
YQ17080168212 00:e0:b4:19:37:3e 自动售货机/自动售货机 10.64.12.45 172.18.30.253[GigabitEthernet1/0/6] TECHNO SCOPE ... 准入成功 无限期 2019-11-08 10:39:20 -/-
LZ17031413401 00:e0:b4:18:19:ea 自动售货机/自动售货机 10.64.12.2 172.20.67.253[GigabitEthernet1/0/21] TECHNO SCOPE ... 准入成功 无限期 2019-11-08 10:39:20 -/-
YQ17080168201 00:e0:b4:19:3e:c1 自动售货机/自动售货机 10.64.12.47 172.18.27.253[GigabitEthernet1/0/8] TECHNO SCOPE ... 准入成功 无限期 2019-11-08 10:39:17 -/-
LZ17031413401 00:e0:b4:14:64:0e 自动售货机/自动售货机 10.64.12.35 192.168.145.244[GigabitEthernet2/0/22] TECHNO SCOPE ... 准入成功 无限期 2019-11-08 10:39:19 -/-
fc:c2:3d:18:82:c5 自动售货机/自动售货机 10.64.12.71 192.168.243.62[Te3/1] Atmel Corpora... 准入成功 无限期 2019-11-08 10:44:47 -/-
YQ17080168214 00:e0:b4:19:3e:b6 自动售货机/自动售货机 10.64.12.14 172.20.78.253[GigabitEthernet1/0/21] TECHNO SCOPE ... 准入成功 无限期 2019-11-08 10:51:42 -/-
YQ17080168204 00:e0:b4:19:3e:b5 自动售货机/自动 172.18.21.252[Gig TECHNO SCOPE ... 准入成功 无限期 2019-11-08 -/-
紫崧一栋
楼栋汇
消防业务
消防业务
消防业务
消防业务

物联专网管理-免管控时段

- 物联专网业务的特点是终端数量多，位置分散，工程周期长。
- 设置免管控时段，控制器通过netconf下发网关开启arp的学习，业务内的终端配置了正确IP入网不受限制。

名称	终端MAC	业务网/子网	IPv4地址	IPv6地址	接入位置	厂商	入网状态	有效期	更新时间	类型
YQ17072568205	00:e0:b4:19:3b:fd	自动售货机/自动售货机	10.64.12.23		192.168.243.62[Te1/5]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:37:13	
TCN111963403	00:e0:b4:18:1d:fa	自动售货机/自动售货机	10.64.12.37		172.19.76.253[GigabitEthernet1/0/10]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:24:50	
YQ17120868204	00:e0:b4:19:78:6d	自动售货机/自动售货机	10.64.12.17		192.168.243.62[Te1/6]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:29:59	
YQ17072568204	00:e0:b4:19:42:f0	自动售货机/自动售货机	10.64.12.57		192.168.243.62[Te1/5]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:37:13	
	fc:c2:3d:18:d8:1b	自动售货机/自动售货机	10.64.12.[illegible]		192.168.243.62[Te3/4]	Atmel Corpora...	准入成功	无限期	2019-11-06 10:34:31	
YQ17120868203	00:e0:b4:19:78:83	自动售货机/自动售货机	10.64.12.41		172.19.66.253[GigabitEthernet1/0/10]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:29:32	
YQ17072568210	00:e0:b4:19:37:b8	自动售货机/自动售货机	10.64.12.9		192.168.243.62[Te1/5]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:03:32	
YQ17080168212	00:e0:b4:19:37:3e	自动售货机/自动售货机	10.64.12.45		192.168.243.62[Te1/6]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:37:13	
LZ17031413401	00:e0:b4:18:19:ea	自动售货机/自动售货机	10.64.12.2		192.168.243.62[Te1/5]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:29:35	
YQ17080168201	00:e0:b4:19:3e:c1	自动售货机/自动售货机	10.64.12.47		192.168.243.62[Te1/6]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:37:13	
LZ17031413401	00:e0:b4:14:64:0e	自动售货机/自动售货机	10.64.12.35		192.168.243.62[Te1/6]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:37:13	
	fc:c2:3d:18:82:c5	自动售货机/自动售货机	10.64.12.71		192.168.243.62[Te3/1]	Atmel Corpora...	准入成功	无限期	2019-11-06 10:31:16	
YQ17080168214	00:e0:b4:19:3e:b6	自动售货机/自动售货机	10.64.12.14		192.168.243.62[Te1/5]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:37:13	
YQ17080168204	00:e0:b4:19:3e:b5	自动售货机/自动售货机	10.64.12.49		192.168.243.62[Te1/6]	TECHNO SCOPE ...	准入成功	无限期	2019-11-06 10:37:15	
[illegible]	[illegible]	自动售货机/自动	[illegible]		192.168.243.62[Te	[illegible]	[illegible]	[illegible]	2019-11-06	

不用审批，直接入网

SDN控制器-审批入网

工程期后，终端入网需要管理人员审批，只有管理员审批通过后才能接入网络。审批入网后，会自动根据**业务IP加入**所在分组，并进行**IP+MAC+位置信息绑定。**后期设备位置变动，设备更换，都需要管理员审批入网。

物联专网管理-应用间的隔离

- 过去的物联网接入，没有对不同应用之间进行隔离控制，不同应用终端之间仍然能够互访，有很大的安全风险。
- 一种应用对应一个网段， 易于实现应用间隔离，实现了在一张物理网络中，承载多种逻辑专网。
- 通过SDN控制器实现图形化操作。

物联专网管理-自动化上线

- 目前的物联专网入网按应用分配好不同网段
- 设置免管控时段周期
- 各业务部门根据分配好的网段进行终端IP地址的配置，在免管控时段内即插即用，控制器自动完成终端信息记录。
- 相比传统的入网流程，不需要再到现场对接入交换机端口勘察分配、接口的vlan配置，以及繁琐的表格登记。各部门之间配合更加高效。

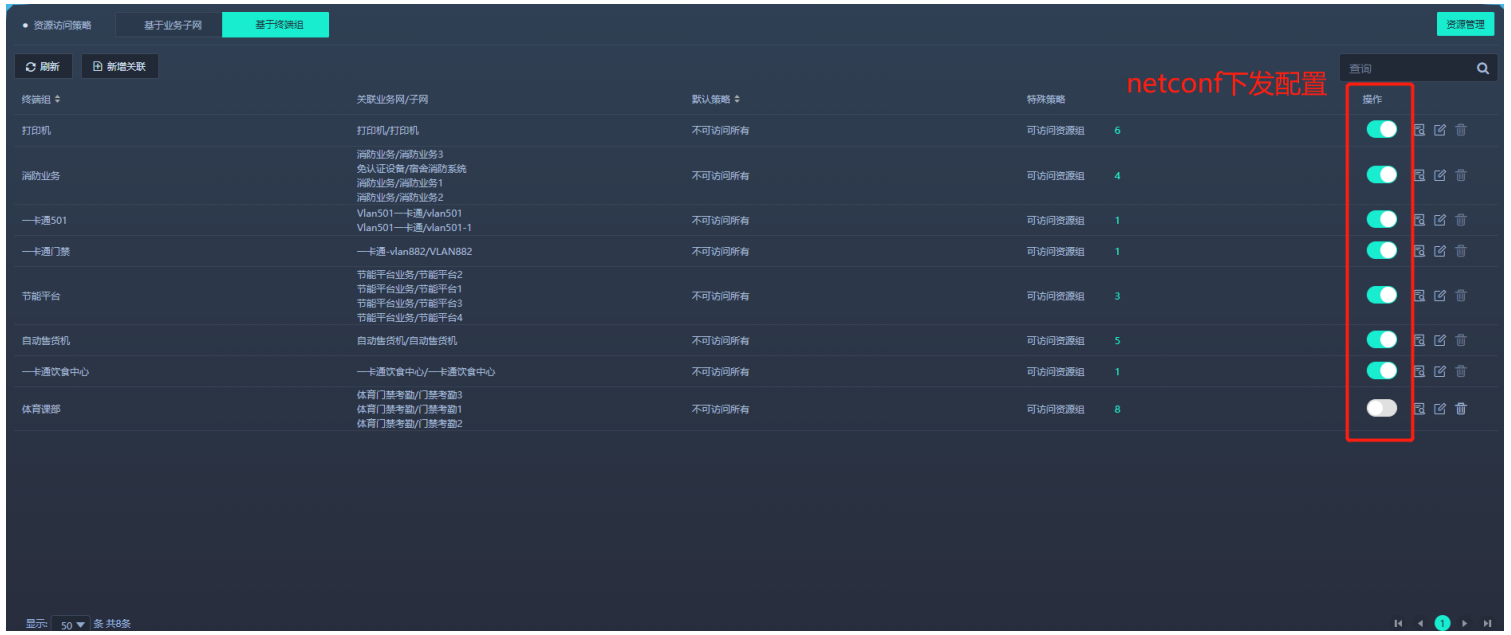
删除　重新准入　有效时间

自动识别终端位置，不再依附表格

终端MAC	业务网/子网	IPv4地址	IPv6地址	接入位置	厂商	入网状态	有效期	更新时间
00:30:18:07:f8:ed	体育门禁考勤/门禁考勤1	10.64.0.100		172.19.77.253[Ten-GigabitEthernet1/0/26]	Jetway Inform...	准入成功	无限期	2019-11-07 16:00:58
00:30:18:07:f8:99	体育门禁考勤/门禁考勤2	10.64.1.113		192.168.133.125[GigabitEthernet0/0/11]	Jetway Inform...	准入成功	无限期	2019-11-07 15:59:14
00:30:18:07:f9:23	体育门禁考勤/门禁考勤2	10.64.1.108		192.168.130.29[Gi0/26]	Jetway Inform...	准入成功	无限期	2019-08-31 09:18:00
00:66:0c:b3:ad:fd	体育门禁考勤/门禁考勤1	10.64.0.202		172.19.6.31[Gi0/28]		准入成功	无限期	2019-11-07 15:59:31
00:66:0c:b3:ad:fe	体育门禁考勤/门禁考勤2	10.64.1.207		192.168.130.29[Gi0/26]		准入成功	无限期	2019-11-07 16:00:22
00:66:0c:b3:ae:35	体育门禁考勤/门禁考勤2	10.64.1.202		192.168.133.125[GigabitEthernet0/0/24]		准入成功	无限期	2019-11-07 16:01:23
00:66:0c:b3:ae:36	体育门禁考勤/门禁考勤3	10.64.2.202		192.168.90.1[Gi0/28]		准入成功	无限期	2019-11-07 15:58:21
00:30:18:07:f8:90	体育门禁考勤/门禁考勤3	10.64.2.101		192.168.90.1[Gi0/28]	Jetway Inform...	准入成功	无限期	2019-11-07 16:00:22
00:30:18:07:f8:91	体育门禁考勤/门禁考勤3	10.64.2.107		192.168.90.1[Gi0/28]	Jetway Inform...	准入成功	无限期	2019-11-07 16:00:22
00:30:18:07:f8:92	体育门禁考勤/门禁考勤3	10.64.2.100		192.168.90.1[Gi0/28]	Jetway Inform...	准入成功	无限期	2019-11-07 15:59:09
DS 34:64:a9:0c:7f:f4	体育门禁考勤/门禁考勤3	10.64.2.8		192.168.80.65[Gi0/26]	惠普	准入成功	无限期	2019-11-07 16:00:23
34:64:a9:0c:7f:3a	体育门禁考勤/门禁考勤3	10.64.2.7		192.168.90.1[Gi0/12]	惠普	准入成功	无限期	2019-11-07 16:00:22
00:66:0c:b3:ae:1a	体育门禁考勤/门禁考勤3	10.64.2.207		172.18.2.202[Gi0/28]		准入成功	无限期	2019-11-07 16:03:08
00:30:18:07:f9:5a	体育门禁考勤/门禁考勤2	10.64.1.110		192.168.130.29[Gi0/26]	Jetway Inform...	准入成功	无限期	2019-11-05 05:37:47

控制器与设备对接-Netconf协议

控制业务只能访问固定服务器资源，开启后通过netconf下发acl配置




```
ip access-list extended RG-ONC-NETWORK
 8190 permit udp any any eq bootps
 8191 permit udp any any eq bootpc
 1581051 permit ip 10.100.14.0 0.0.0.255 10.100.14.0 0.0.0.
 1843200 deny ip 10.64.3.0 0.0.0.255 10.64.7.0 0.0.0.255
 1843201 deny ip 10.64.3.0 0.0.0.255 10.64.6.0 0.0.0.255
 1843202 deny ip 10.64.3.0 0.0.0.255 10.64.4.0 0.0.0.255
 1843203 deny ip 10.64.3.0 0.0.0.255 10.64.5.0 0.0.0.255
 1843204 deny ip 10.64.0.0 0.0.0.255 10.64.7.0 0.0.0.255
 1843205 deny ip 10.64.0.0 0.0.0.255 10.64.6.0 0.0.0.255
 1843206 deny ip 10.64.0.0 0.0.0.255 10.64.4.0 0.0.0.255
 1843207 deny ip 10.64.0.0 0.0.0.255 10.64.5.0 0.0.0.255
 1843208 deny ip 10.64.1.0 0.0.0.255 10.64.7.0 0.0.0.255
 1843209 deny ip 10.64.1.0 0.0.0.255 10.64.6.0 0.0.0.255
 1843210 deny ip 10.64.1.0 0.0.0.255 10.64.4.0 0.0.0.255
 1843211 deny ip 10.64.1.0 0.0.0.255 10.64.5.0 0.0.0.255
 1843212 deny ip 10.64.2.0 0.0.0.255 10.64.7.0 0.0.0.255
 1843213 deny ip 10.64.2.0 0.0.0.255 10.64.6.0 0.0.0.255
 1843214 deny ip 10.64.2.0 0.0.0.255 10.64.4.0 0.0.0.255
 1843215 deny ip 10.64.2.0 0.0.0.255 10.64.5.0 0.0.0.255
 1843216 deny ip 10.64.3.0 0.0.0.255 10.100.17.0 0.0.0.255
 1843217 deny ip 10.64.3.0 0.0.0.255 10.100.14.0 0.0.0.255
 1843218 deny ip 10.64.3.0 0.0.0.255 10.64.9.0 0.0.0.255
 1843219 deny ip 10.64.3.0 0.0.0.255 10.64.8.0 0.0.0.255
 1843220 deny ip 10.64.3.0 0.0.0.255 10.64.10.0 0.0.0.255
 1843221 deny ip 10.64.0.0 0.0.0.255 10.100.17.0 0.0.0.255
 1843222 deny ip 10.64.0.0 0.0.0.255 10.100.14.0 0.0.0.255
 1843223 deny ip 10.64.0.0 0.0.0.255 10.64.9.0 0.0.0.255
 1843224 deny ip 10.64.0.0 0.0.0.255 10.64.8.0 0.0.0.255
 1843225 deny ip 10.64.0.0 0.0.0.255 10.64.10.0 0.0.0.255
 1843226 deny ip 10.64.1.0 0.0.0.255 10.100.17.0 0.0.0.255
 1843227 deny ip 10.64.1.0 0.0.0.255 10.100.14.0 0.0.0.255
 1843228 deny ip 10.64.1.0 0.0.0.255 10.64.9.0 0.0.0.255
 1843229 deny ip 10.64.1.0 0.0.0.255 10.64.8.0 0.0.0.255
 1843230 deny ip 10.64.1.0 0.0.0.255 10.64.10.0 0.0.0.255
 1843231 deny ip 10.64.2.0 0.0.0.255 10.100.17.0 0.0.0.255
 1843232 deny ip 10.64.2.0 0.0.0.255 10.100.14.0 0.0.0.255
 1843233 deny ip 10.64.2.0 0.0.0.255 10.64.9.0 0.0.0.255
 1843234 deny ip 10.64.2.0 0.0.0.255 10.64.8.0 0.0.0.255
 1843235 deny ip 10.64.2.0 0.0.0.255 10.64.10.0 0.0.0.255
 1843236 deny ip 10.64.3.0 0.0.0.255 10.64.14.0 0.0.0.255
 1843237 deny ip 10.64.3.0 0.0.0.255 10.100.21.0 0.0.0.255
 1843238 deny ip 10.64.0.0 0.0.0.255 10.64.14.0 0.0.0.255
 1843239 deny ip 10.64.0.0 0.0.0.255 10.100.21.0 0.0.0.255
 1843240 deny ip 10.64.1.0 0.0.0.255 10.64.14.0 0.0.0.255
 1843241 deny ip 10.64.1.0 0.0.0.255 10.100.21.0 0.0.0.255
 1843242 deny ip 10.64.2.0 0.0.0.255 10.64.14.0 0.0.0.255
 1843243 deny ip 10.64.2.0 0.0.0.255 10.100.21.0 0.0.0.255
 1843244 deny ip 10.64.9.0 0.0.0.255 10.100.17.0 0.0.0.255
 1843245 deny ip 10.64.9.0 0.0.0.255 10.100.14.0 0.0.0.255
 1843246 deny ip 10.64.9.0 0.0.0.255 10.64.14.0 0.0.0.255
 1843247 deny ip 10.64.9.0 0.0.0.255 10.64.7.0 0.0.0.255
```

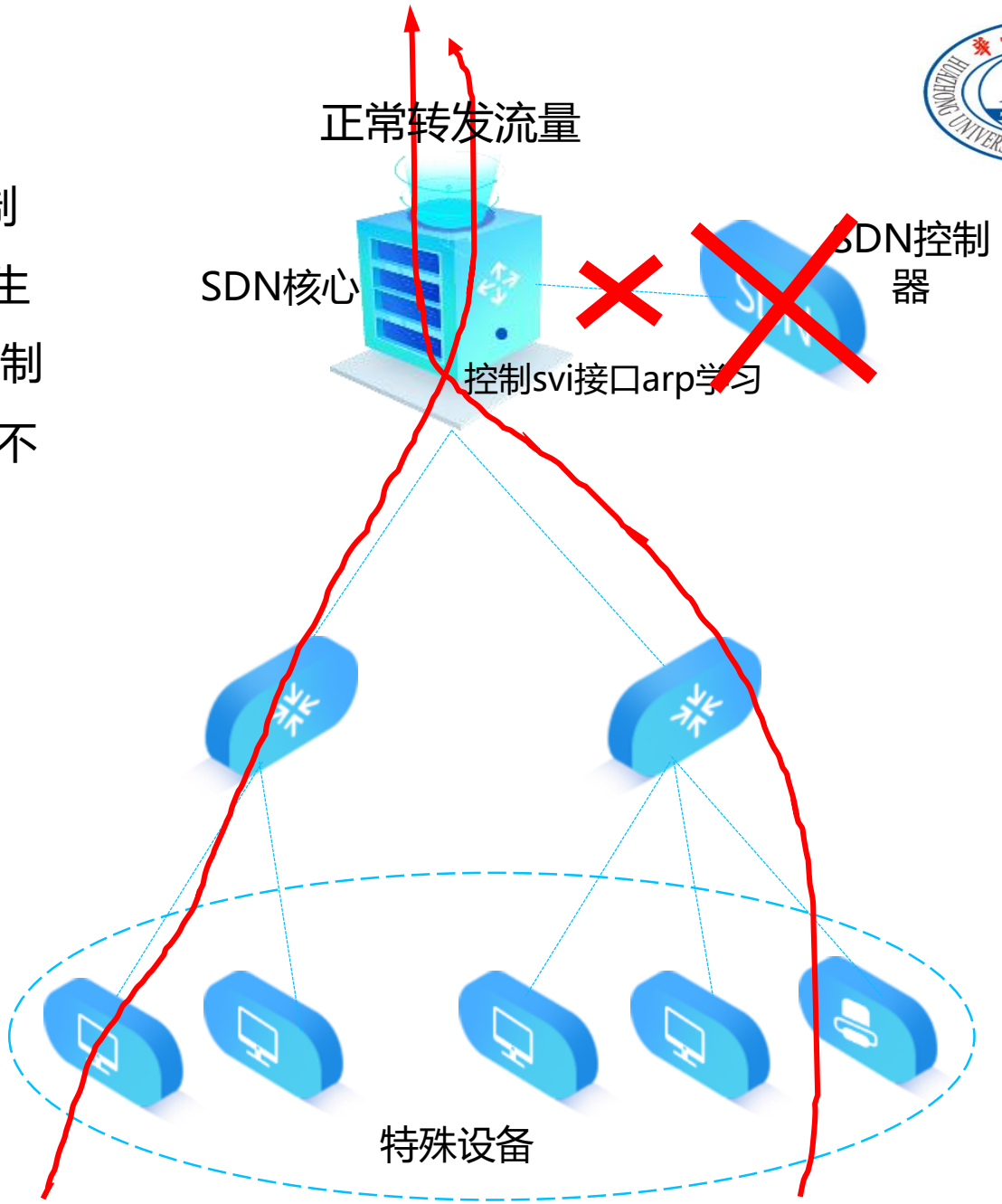
SDN控制器-IP地址管理

通过SDN控制器可图形化展示节能平台、消防、一卡通、门禁业务IP地址使用率。

直观显示已分配IP、可用IP、冲突IP信息。对终端上下线信息进行监控。

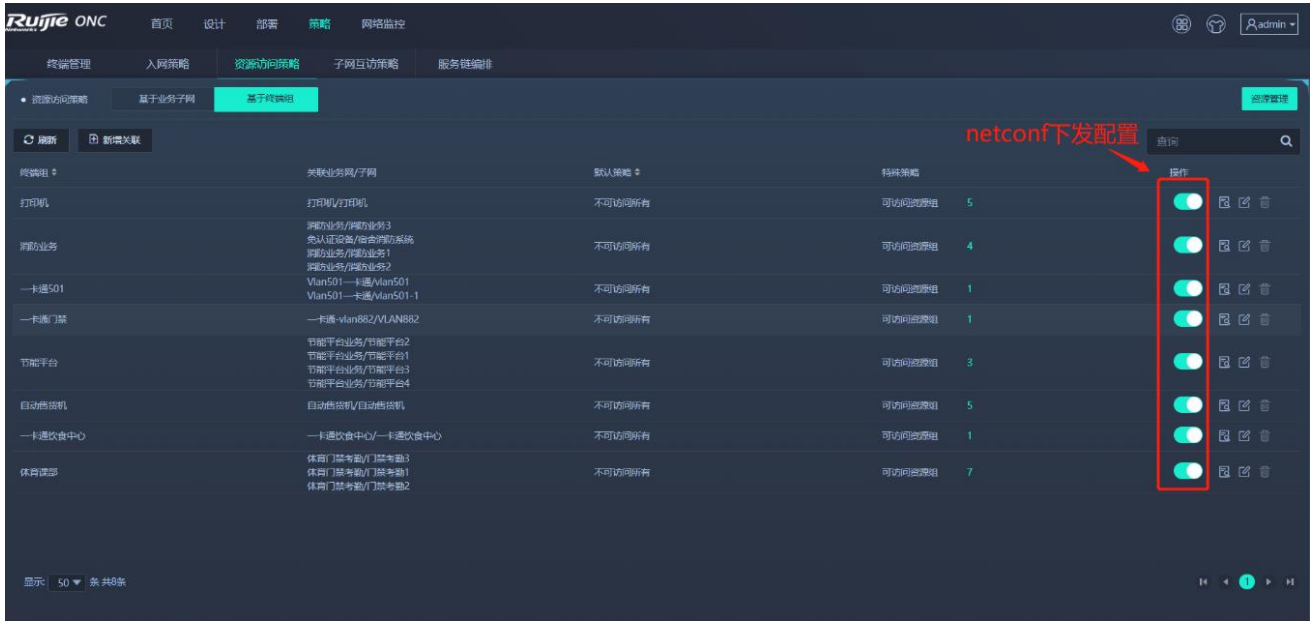
可靠性

SDN控制器是通过控制网关的arp学习，来控制是否允许终端入网，对于允许入网的终端自动生成静态arp表项，静态arp表项不会因为SDN控制器故障而消失，所以链路或SDN控制器故障都不会影响业务的正常运行



物联专网-上线业务

- 我校已在SDN上上线了9种物联专网，包括师生服务中心的打印机业务、水电科的节能平台业务、体育课部的体育考勤业务、保卫科的消防业务、后勤集团的自动售货机业务，物联网终端遍布校园每个区域。
- 各业务之间通过SDN给交换机下发ACL策略实现业务之间安全隔离，并控制各业务只允许访问必要的服务器资源。



物联专网管理

搜索已分组下分组
关联业务子网：
消防业务/消防业务3
免认证设备/宿舍消防系统
消防业务/消防业务1
消防业务/消防业务2
目地子网
源子网
节能平台1
节能平台2
节能平台3
节能平台4
门禁考勤1
门禁考勤2
门禁考勤3
室外AP
消防业务1
消防业务2
消防业务3
整网IP地址概况
地址池数
20
IP总数
6084
已使用IP数
803
使用率
13.19%
IP使用率Top5
使用率
100
80
60
40
20
0
免认证设备/宿舍消防系统
节能平台业务/节能平台1
自动售货机/自动售货机
节能平台业务/节能平台3
Vlan501—卡通/vlan501-1
业务网视图
终端组视图
IP地址使用情况
查询
业务网/业务子网
认证终端组
IP总数
已使用IP数
使用率
免认证设备/宿舍消防系统 253 197 77.86%
节能平台业务/节能平台1 253 173 68.37%
自动售货机/自动售货机 253 80 31.62%
节能平台业务/节能平台3 253 52 20.55%
Vlan501—卡通/vlan501-1 253 49 19.36%
Vlan501—卡通/vlan501 253 44 17.39%
消防业务/消防业务3 253 26 10.27%
消防业务/消防业务1 253 23 9.09%

小结

- 校园网中所有终端都应做到可管、可控和可追溯。
- 人物网关分离的拓扑架构清晰，终端即插即用，管理方便，共享物理链路，具有扩展性。
- SDN交换机/控制器通过对终端ARP控制，实现了物联网终端的准入，具有容量大，图形化操作的特点。
- ACL进行业务隔离，在一张物理网上实现多张逻辑网。提高了物联专网的稳定性和安全性。

谢 谢