doi:10.3969/j.issn.1000-436x.2014.z1.017

使用集中式 802.1x 构建校园网认证系统

柳斌，贺聿志，章勇
（华中科技大学 网络与计算中心，湖北 武汉 430074）

摘 要：802.1x 认证通常采用分布式方式部署，随着校园网规模的不断扩大，分布式部署给设备管理和认证系统管理带来了许多不便；另一方面，传统 802.1x 集中部署无法对用户终端进行定位。结合（NAS IP，Port，Vlan）三元组定位，Super Vlan 和 Port+Vlan 的地址管理 3 种技术解决了 802.1x 集中部署模式下用户终端定位的问题，并在华中科技大学校园网中进行了部署实验，取得了良好的效果。
关键词：802.1x；Super Vlan；接入认证
中图分类号：TP393.1 **文献标识码**：A **文章编号**：1000-436X(2014)Z1-0087-04

Bulid campus network authentication system based on centralized 802.1x

LIU Bin, HE Yu-zhi, ZHANG Yong
(Network Center, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: 802.1x authentication was usually distributed deployment. However, With the expansion of the campus network and increasement of the number of control devices, the management of equipment and authentication system become so inconvenience. On the other hand, centralized 802.1x could not locate the terminal. The problem of terminal location under centralized 802.1x was solved by using （NAS IP, Port, Vlan）three tuple, Super Vlan and dynamic address allocation technology. Centralized 802.1x authentication system was tested in the of Huazhong Science and Technology University campus network, and achieved good results.
Key words: 802.1x authentication; Super Vlan; access authentication

1 引言

802.1x 认证是目前校园网常用的一种接入认证方式。802.1x 认证通常进行分布式部署，接入交换机作为 NAS（network access server）设备。随着校园网规模的不断扩大与更新，接入交换机经常发生变化，NAS 设备的频繁变化给设备和认证系统管理带来诸多不便。另一方面，传统的 802.1x 集中部署无法解决用户终端定位的问题。本文在 802.1x 集中部署模式下，结合(NAS IP, Port, Vlan)三元组用户位置标识，Super Vlan 以及 Port+Vlan 的地址分配 3 种技术解决了 802.1x 用户终端定位问题。

2 802.1x 的基本原理

2.1 802.1x 认证体系结构

802.1x 协议的体系结构如图 1 所示，包括 3 个重要部分：客户端（supplicant system）、认证系统（authenticator system）、认证服务器（authentication server system）。

1) 客户端。 一般为一个用户终端系统，该终端系统通常要安装一个客户端软件，用户通过启动这个客户端软件发起 IEEE 802.1x 协议的认证过程。客户端系统需支持 EAPOL（extensible authentication protocol over LAN）协议。

2) 认证系统。通常为支持 IEEE 802.1x 协议的网络设备，它为客户端提供接入局域网的端口，该端口可以是物理端口，也可以是用户设备的 MAC 地址、VLAN、IP 等逻辑端口。

3) 认证服务器。通常为 Radius 服务器，该服务器可以存储有关用户的信息，比如用户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等。当用户通过认证后，认证服务器会把用户的相

收稿日期：2014-10-15

关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量就将接受上述参数的监管。

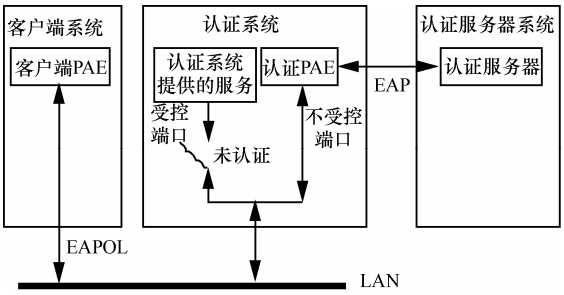


图 1　802.1x 协议的体系结构

2.2　802.1x 认证部署方式

1) 分布式部署

在接入层设备上进行 802.1x 认证即分布式部署。这种方案的优点是可以对用户进行精细化的管理和控制。随着校园网规模的扩大，接入设备会不断增多和更新，大量的接入层设备作为 NAS 设备给网络管理和认证管理带来不便。另一方面，接入交换机作为 NAS 设备与后台的认证系统联系比较密切，这导致数量众多的接入交换机在购置，更新选型时受制于认证系统。

2) 集中式部署

将 802.1x 认证部署在汇聚交换机，或者核心交换机上即集中式部署。集中式部署中只有汇聚交换机或者核心交换机是 NAS 设备， NAS 设备数大幅减少，这有利于管理，但是集中式部署无法对用户终端进行定位。所有认证用户都从一个 NAS IP（一台交换机），一个 NAS port（一个端口）上来，用户终端位置无法区分，而用户终端位置对于网络维护是十分重要的。

3　集中式 802.1x 模式下终端定位

集中式 802.1x 认证带来一个主要问题是无法进行用户终端位置定位，解决的思路是采用 NAS IP+NAS Port+Vlan 的方式进行用户终端位置的定位。为每个用户分配一个单独的 VLAN，后台计费系统根据用户认证时传上来的交换机 IP 信息、Port 信息和用户 Vlan 信息实现对用户终端的物理定位。

3.1　用户位置标识

按照 802.1q 标准，一台交换机最多支持 4 096 个 Vlan，一个 Vlan 一个用户，一台交换机最多连接 4 096 个用户，显然仅靠 Vlan 标识用户位置，Vlan 数量是不够的。因此，采用了（NAS IP，port，Vlan）三元组对用户终端位置进行标识，NAS port 之间进行端口隔离。

端口隔离后，每一个 port 下有 4 096 个 Vlan，假设一台接入交换机接 20 个用户，需要 20 个 Vlan，一个核心交换机端口下接入 200 台接入交换机，即 4 000 个 Vlan，可接 4 000 个用户。如果核心交换机有 24 个端口，那么一台核心交换机可接入 96 000 个用户，足够满足校园网用户位置标识需要。

3.2　Super Vlan

通常一个 2 层的 VLAN 对应于一个 3 层的 IP 子网。为了进行位置定位，为每一个用户划分了一个 VLAN，如果相应为每一个用户划分一个 IP 子网，则 IP 地址浪费严重，因为分配一个子网，有子网的网络号、广播地址和缺省网关 3 个 IP 地址被额外占用。一个 C 类地址不分子网时最多可连接 253 个用户，如果按照每用户一个子网方式最多只能接 64 个用户。

采用了 Super VLAN 方法进行 VLAN 聚合，有效地解决这个问题。Super Vlan 将一个网段的 IP 分给多个不同的 VLAN(称为 SubVlan)，这些 SubVlan 同属于一个 Super Vlan。每个 SubVlan 都是一个独立的广播域，不同 SubVlan 之间 2 层相互隔离。这样只需为 Super Vlan 分配一个 IP 子网，并为每个用户建立一个 SubVlan。所有 SubVlan 可以使用 Super Vlan 子网中的 IP 地址，当 SubVlan 内的用户需要进行 3 层通信时，使用 Super Vlan 的虚接口的 IP 地址作为缺省网关，这样多个 Sub VLAN 共享一个 IP 网关地址，从而节省了 IP 地址资源。

3.3　基于 Port+Vlan 的 IP 地址管理

使用（NAS IP，Port，Vlan）三元组解决了用户终端位置标识问题，使用 Super Vlan 解决了 IP 地址浪费的问题。但是，由于传统的 DHCP Server 只能基于 Vlan 或者三层路由端口进行 IP 地址分配，仍然存在 IP 地址段混乱的问题。

对于来自不同 Port 但是 SubVlan 相同的用户，它们是在一个 IP 子网里的，如（NAS IP1，port1，vlan1），（NAS IP1，port2，vlan1）2 个用户，尽管来自不同的 port，但 SubVlan 相同，那么 Super VLAN 就是一样的，这样 DHCP Server 会分配同一个子网的 IP 地址，也就是说来自不同楼栋的用户可能属于同一个 IP 子网，同一个楼栋的用户可能在不同的 IP 子网中，这十分不利于 IP 地址段的管理以及一些应用的部署。采用了一种基于 Port+Vlan 的

IP 地址管理方法，根据 Port 和 Vlan 信息进行 IP 地址的分配。

Port 若不同，规则如下。

规则 1：match ip IP 范围 port1 Vlan 范围。

规则 2：match ip IP 范围 port2 Vlan 范围。

其中，规则 1 与规则 2 的 VLAN 范围可以交叉重叠。

Port 若相同，规则如下。

规则 1：match ip IP 范围 port Vlan 范围 1。

规则 2：match ip IP 范围 port Vlan 范围 2。

规则 1 与规则 2 的 VLAN 范围不可以交叉重叠。

配置规则后，实现了对应规则的控制面（ARP 报文、IP 报文等）访问限制。若用户终端位置信息在 Port、Vlan 范围内，使用的 IP 地址不在规则 IP 范围内，用户终端发送的 ARP 报文、IP 报文都被过滤，从控制面上有效防止用户随意设置 IP 地址。根据规则进行控制面访问限制，保证每栋楼用户只能使用该楼栋分配的 IP 地址段，避免在同一个 SuperVlan 下，用户随意设置不同网段的 IP 地址。

4　集中式 802.1x 在校园网中的部署

在华中科技大学校园网进行了集中式 802.1x 部署测试，采用了锐捷 N18010 核心交换机作为集中 802.1x 认证交换机，网关和认证全部集中在 N18010 上，接入交换机不作为 NAS，后台认证为锐捷的 SAM 系统。组网示意如图 2 所示。

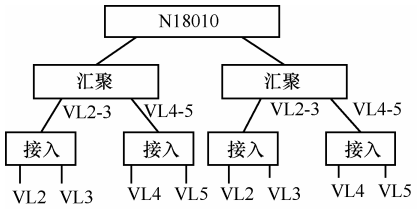


图 2　组网示意

4.1　部署方式

1) 接入设备部署

对于有线部分，每个与终端相连的端口都配置成 Access 口，并且每个端口都属于一个 VLAN，上联汇聚的端口配置成属于这些 VLAN 的 Trunk 口。对于无线部分，每个 AP 或者同一区域的多个 AP 都属于一个 VLAN。AP 内终端之间通信隔离。AC 上配置不允许同一个 VLAN 的 AP 之间通信。

2) 核心设备部署

通过 Super Vlan 作为网关，Super Vlan 配置多个 IP 网段，每个接入的终端属于一个 SubVlan，核心是不同端口下的终端允许在同一个 SubVlan 内，这样每个端口都要配置成属于所有 SubVlan 的 trunk 口，为了确保这些终端之间二层通信隔离，开启这些端口的二层端口保护功能。

3) 汇聚设备部署

和核心相连的上联口配置成属于所有 Sub VLAN 的 trunk 口，而下联接入的端口也配置成 Trunk 口，并根据接入设备所分配的 VLAN 范围进行裁剪。

4) 关键配置

Super Vlan 配置

```
vlan 4094 （用户 VLAN）
  supervlan
subvlan 1000-3000
interface vlan 4094
  ip address 222.20.1.254 255.255.254.0
  ip address 222.20.3.254 255.255.254.0 secondary
vlan 4093 （管理 VLAN）
  supervlan
  subvlan
interface vlan 4093
ip address 172.20.1.254 255.255.255.0
 ip address 172.20.2.254 255.255.255.0 secondary
```

设置 2 个 Super Vlan，一个作为管理 Super Vlan，一个作为用户 Super Vlan。

IP 地址管理配置

```
match ip 222.20.0.0 255.255.254.0 Gi1/1 Vlan 1000-3000
match ip 222.20.2.0 255.255.254.0 Gi 1/2 Vlan 1000-3000
```

来自 Gi1/1 分配 222.20.0.0/23 这段地址，来自 Gi1/2 分配 222.20.2.0/23 这段地址。

802.1x 认证配置

```
aaa new-model
aaa authentication web-auth default group radius
interface xxx
  dot1x port-control auto
```

4.2　运行情况

对 29 栋学生宿舍楼进行了集中 802.1x 认证部署。高峰期同时认证在线人数达到 7 800 人，ARP

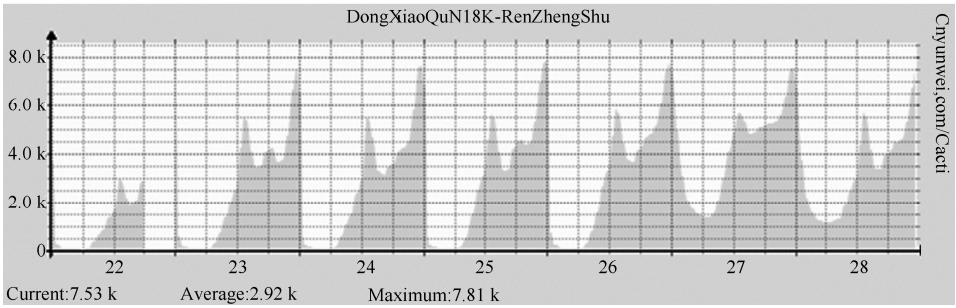


图 3　在线人数

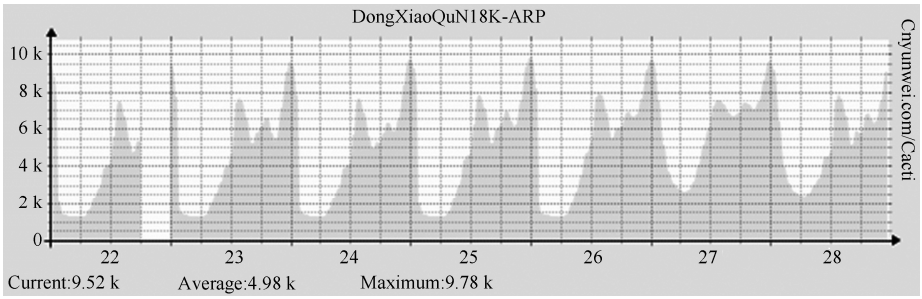


图 4　ARP 条目数

在线用户			
用户名	1999178	用户IPv4	218.199.87.133
用户MAC	0247E0E05A5	用户组	办公区用户组
网关地址		认证域	
子网掩码		DNS	
IPv6地址数	0	用户IPv6地址	
用户IPv6地址（本地链路）		VLAN	315
NAS IPv4	192.168.255.141	网关IPv6地址	
读写Community	rui jie	NAS Port	169
NAS IPv6			
具体型号	N18K	设备类型	锐捷交换机
设备位置		设备名称	
接入设备IP	192.168.58.11	接入设备型号	S2628G
接入设备Interface	Fa 0/3	接入设备Port	3
接入位置描述	韵苑5号楼3楼		

图 5　用户在线信息

条目数 9.78K 条，ND 条目数 17.13K 条，流量超过 4.96 Gbit/s。结果如图 3 和图 4 所示。

采用三元组标识用户的位置，在认证系统上可以通过 Port、Vlan 看到对应接入设备 IP 地址与接入设备端口，进行位置定位。结果如图 5 所示。

5　结束语

随着核心设备性能的不断提高，集中式认证将是校园网接入认证发展的趋势。本文通过结合 NAS IP+Port+Vlan 标识，Super Vlan 以及基于 Port+Vlan 的地址管理等技术解决了集中式的 802.1x 用户终端定位问题，通过在华中科技大学校园网中实际部署测试表明集中式 802.1x 是可行的。

参考文献：

[1]　吕才军. 基于 IEEE802.1x 的网络准入控制系统设计与实现，信息安全与技术, 2013, 6: 72-76.
LV C J. Network admission control based on IEEE 802.1x systems design and implementation[J]. Information Security and Technology 2013, (6):72-76.

[2]　林琳, 任礼. 802.1x、动态 VLAN 和 DHCP 技术在校园网中的应用[J]. 数字技术与应用, 2012,(11): 97-99.

（下转第 97 页）

参考文献：

[1] 黄荣怀，张进宝，胡永斌．智慧校园：数字校园发展的必然趋势[J].开放教育研究，2012,18(4):12-17.
HUANG R H, ZHANG J B, HU Y B.Smart campus: the developing trends of digital campus[J]. Open Education Research, 2012, 18(4): 12-17.

[2] 严岳林，李立，江南．IP 城域网接入层建设与发展[J].计算机与数字工程，2008,36(6):188-191.
YAN Y L, LI L, JIANG N. Programming and establishment of IP-MAN access layer based on MSTP[J].Computer & Digital Engineering, 2008, 36(6):188-191.

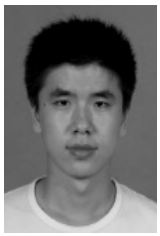
[3] 邵兵，李越鹏，赵保华．OSPF 协议性能测试的研究与实践[J].计算机应用, 2003, 23(10):62-64,66.
SHAO B , LI Y P , ZHAO B H. Research and practice of OSPF protocol performance test[J].Computer Applications, 2003,23(10): 62-64, 66.

[4] 李梅，梁岸兵．端口隔离在校园网中的实施和分析[J].电脑知识与技术,2010,6(6):1307-1308,1311.
Li M, LIANG A B. The measure and significance of port isolation in campus network[J].Computer Knowledge and Technology, 2010，6(6), 1307-1308, 1311.

[5] 潘顺军．代理 ARP 服务功能的应用[J].中国金融电脑,2012,5:66-68.
HUANG J, SHI Z T. Research on hidden node problem in WLAN[J].Shandong Communication Technology, 2012,32(1):36-39.

[6] 黄磊，石志同．WLAN 隐藏节点问题研究[J].山东通信技术, 2012, 32(1):36-39.
LI K, ZHANG Z F. Channel assignment algorithm in centralized WLAN[J]. Computer Engineer and Design, 2014,35(6):1888-1891.

作者简介：



付中南（1987-），男，山西应县人，北京大学工程师，主要研究方向为网络建设与管理。

尚群（1972-），男，北京人，北京大学计算中心高级工程师，网络室副主任，主要研究方向为无线网、网络管理、数据库等。

公绪晓（1982-），女，山东临沂人，北京大学工程师，主要研究方向为网络技术与应用。

（上接第 90 页）

LIN L, REN L. 802.1x, dynamic VLAN and DHCP technology used in campus network[J]. Digital Technology and Application 2012, 11:97-99.

[3] 李金方, 汪鸿伟, 郭国平. SuperVlan 技术的网络组网方法[J]. 网络安全技术与应用, 2013, (4): 46-48.
LI J F, WANG H W, GUO G P. Constructing network method of using super vlan technique[J]. Network Security Technology & Application, 2013, (4):46-48.

贺聿志（1960-），男，湖北武汉人，华中科技大学高级工程师，主要研究方向为网络管理。

作者简介：

柳斌（1971-），男，湖南长沙人，华中科技大学副教授，主要研究方向为网络管理、网络安全等。

章勇（1979-），男，湖北武汉人，华中科技大学工程师，主要研究方向为网络管理、网络安全等。