基于无感知的校园网有线无线一体化认证

南开大学信息化建设与管理办公室

林初建

报告要点

- 研究背景
- 技术路线比较与选择
- 认证框架
- 认证机制与实现
- 一些问题与对策
- 总结

研究背景

- 移动终端的普及，用户通过多终端跨区域认证

  ——要求统一认证方式

- 用户要求流量可控，网络安全管理的需要

  ——要求提供二次认证

- 基于BRAS的校园网基础架构扁平化部署

  ——创造了在保证安全接入的前提下，简化并统一认证过程的可行性

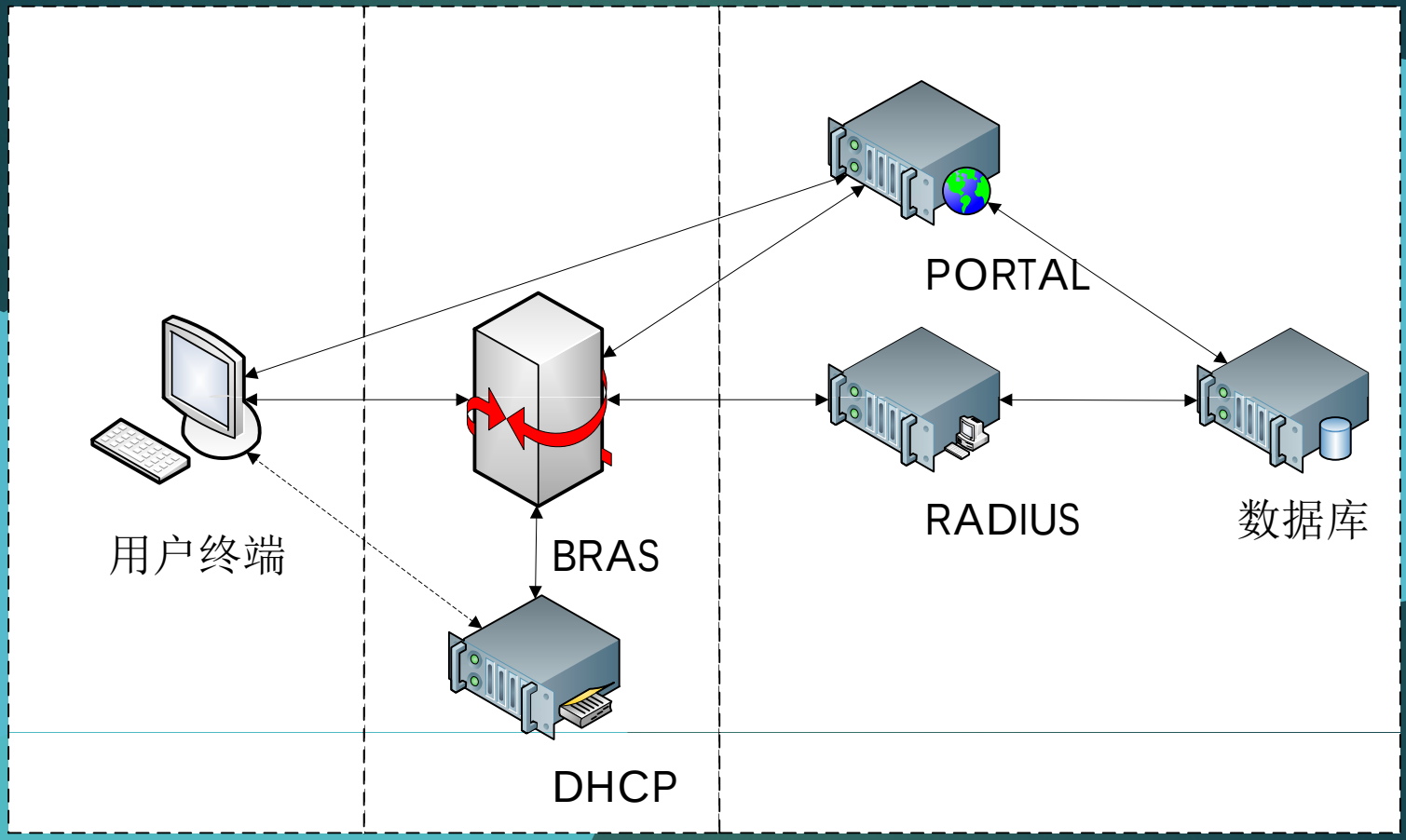
技术路线比较与选择

认证方式	网络场景		认证方式			客户端要求	无感知认证	可控性
	有线网络	无线网络	准入	准出	二次认证			
802.1X	适用	适用	适用	适用	不适用	需要	支持	高
PPPoE	适用	不适用	适用	适用	不适用	需要	不支持	高
IPoE	适用	不适用	适用	不适用	不适用	需要	支持	低
MAC	适用	适用	适用	不适用	不适用	不需要	支持	低
portal	适用	适用	适用	适用	适用	需要	不支持	高

技术路线比较与选择

- DHCP+MAC+Portal的技术路线
- 在用户进行首次准入认证和准出认证前由DHCP为用户终端分配IP地址
- 通过终端MAC地址进行准入认证，并根据认证结果把用户分配到不同的认证域，分别实现基于MAC的无感知准入和首次PORTAL准入过程中用户和MAC对应关系绑定。
- 以PORTAL方式实现用户准出认证

认证框架



客户端　　NAS子系统　　业务控制子系统

认证框架组成

- 客户端

  安装有可以运行HTTP、HTTPS的浏览器的终端；浏览器用于触发portal认证，通过portal向BRAS提交用户认证信息。

- NAS子系统：
  - BRAS：负责网络承载和业务控制，通过认证域(domain)对服务控制策略的引用，实现对用户的业务控制和管理。
  - DHCP服务器：通过为BRAS上的不同认证域绑定不同的地址池，实现不同接口下的用户终端IP地址的分配。
- 业务控制子系统
  - RADIUS服务器：与BRAS结合，负责用户认证（包括用户首次准入MAC绑定）、授权与记账，负责下发用户服务控制策略至BRAS。
  - portal服务器：即认证入口（portal），BRAS把用户访问请求重定向至portal认证页面，用户通过portal认证页面把认证信息提交给BRAS进行认证。
  - 用户数据库：包括用户和MAC对应关系表在内的用户认证计费数据的存放。

认证机制与实现

- 认证域的划分
  - 认证前域：用户通过MAC认证后所归属的域，引用的服务控制策略允许用户访问局域网资源以及准出认证portal页面、DNS和自服务系统等。
  - 重定向域：用户MAC认证失败后所归属的域，允许用户访问准入认证（MAC绑定）portal页面、DNS和自服务系统等。
  - 认证后域：用户通过准出认证后所归属的域，允许用户访问互联网，并根据用户服务控制策略实现有差别的计费。

认证机制与实现

- 认证流程
  - 无感知准入认证

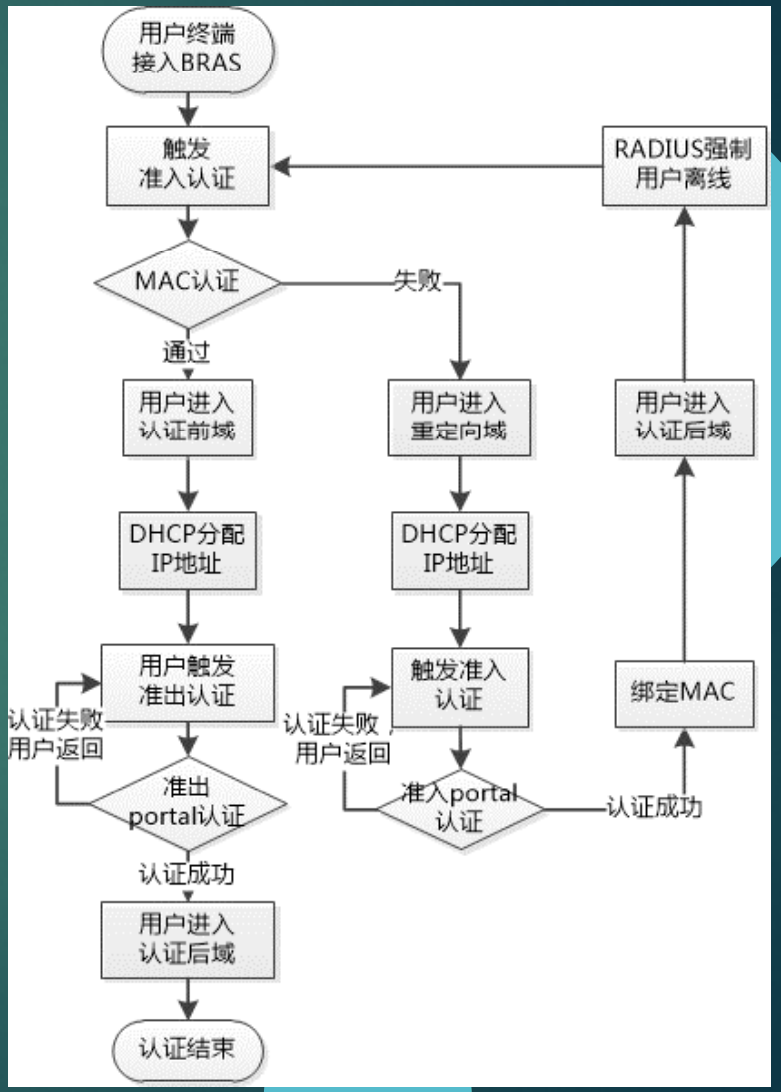
通过终端MAC对用户进行认证，认证通过则进入认证前域，失败进入重定向域进行首次准入portal认证

  - 首次准入portal认证

用户通过portal向BRAS提交认证信息，结合BRAS上的MAC地址，进行用户—MAC地址的对应关系绑定。绑定成功后进入认证后域，强制离线并触发无感知准入认证。

  - 准出portal认证

如果用户访问请求在认证前域允许的范围之外，则触发准出portal认证，认证成功后进入认证后域。



认证机制与实现

- MAC地址自学习

虽然用户仅在终端首次接入网络时需要通过portal页面进行一次MAC地址绑定，但在由其他准入方式转向无感知准入的整体部署过程中，会造成所有用户需要进行MAC绑定的情形。为确保平滑过渡，在部署实施的过程中，我们在RADIUS服务器上启用了MAC地址学习机制，提前把用户和MAC的对应关系写入后台数据库。

- 有线无线的一体化认证

在扁平化架构下，无线用户的流量通过本地转发方式，和有线同样通过二层接入至同一个BRAS，这与有线用户认证过程上没有本质的差异，因此不管用户接入的是固定信息终端盒还是WLAN，均可以通过无感知的方式实现准入，以portal的认证方式实现准出。

- 多终端关联

通常情况下，同一用户在不同终端登录网络，后接入的网络终端会造成前一个终端的强制下线。考虑用户同时拥有笔记本电脑、移动智能终端的情形，通过对业务控制系统的自定义开发，允许同一用户同时可以绑定多个终端的MAC地址，超过最大限制后自动覆盖最先绑定的MAC地址，做到了单用户多终端的无感知接入。

一些问题和对策

- 可能会出现重复的MAC地址，导致冲突

  ——发生几率较小，可接受

- 用户进行MAC认证后进入认证前域的机制，采用了强制离线再次认证方式，而不是直接由RADISU下发认证域，流程上还比较复杂，也缺乏规范

  ——进一步的定制开发简化

- DHCP采用BRAS内置方式，无法达到精细化的IP地址管理

  ——采用外置的专用DHCP服务器

总结

- 集成了MAC认证的良好用户体验和portal的易部署、兼容性好等特点
- “一次认证，多次使用”：用户绑定的终端MAC达到最大限制之前，只需要一次准入认证，即可永久的无感知准入
- 避免了多次输入用户名密码的弊端，提高终端接入网络的速度，提高用户的体验
- 实现了有线无线统一的认证，既简化了认证方式，也避免了多种认证方式所带来的用户认证计费信息同步与繁复的定制开发

谢谢

请各位专家指正！