上海交通大学
Shanghai Jiao Tong University

Web认证下的无线用户规模可扩展性研究

报告人：谢锐

2008年10月29日

上海交通大学网络信息中心

Agenda

- 问题的提出
- 支持无线用户规模可扩展性的系统的组成
- 系统主要功能介绍：
  - Web认证的基本过程
  - 支持大规模web用户接入的无线系统的功能实现
- 结束语

Knowledge Pre-requisites

- IEEE-802.11
- Radius (RFC2138/RFC2865)
- DHCP (RFC2131/RFC2132)

问题的提出

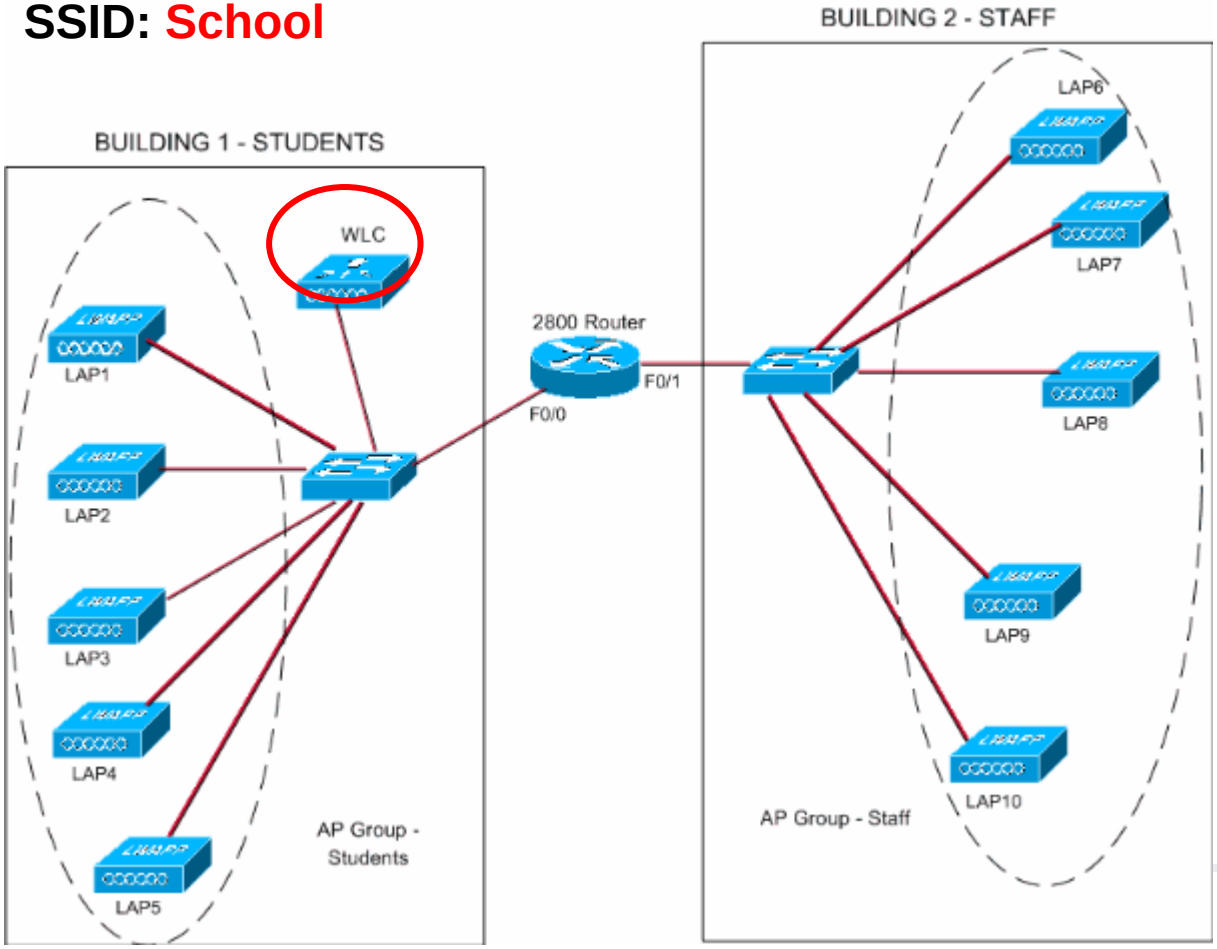
- 802.11网络身份认证Authentication方式
  - Web
    - Web是明文认证方式而缺乏安全性（也可通过https/ssl提高安全性）；
    - 浏览器是所有客户端操作系统都默认的配置，使用起来比较方便，因此是一种较常用的方法。
  - 802.1X
    - 如果802.1x使用简单的Dynamic WEP进行认证，已经证明可以通过很简单的方法进行密码破解；
    - 使用基于EAP-TLS/EAP-TTLS等的认证方法，客户端和服务器端上需要进行专门的配置，这对普通用户（特别是操作系统类型不一）而言又是无形中的一个技术门槛；
    - 认证消息交换是可加密的，用户数据还需另外的加密机制来保护。

问题的提出

- web认证较802.1X有着更广泛的实际用户群：
  - 在笔者所在的学校中，经过统计，80%以上的师生员工都在使用基于web的认证方式访问802.11网络。
- SSID-VLAN Mapping
  - 由于web认证时，传统的无线局域网厂商设备广播出的SSID在无线系统中只能做到一个SSID 对应一个VLAN，所以web认证下的用户通常只存在于一个vlan中；
  - 规模可扩展性问题；
  - 改进：
    - 某些厂家有所谓“AP Groups VLAN”概念；
    - 通过在中央控制器上配置，使得在同一个SSID下，某些AP只能属于VLANx，某些AP只能属于VLANy。

问题的提出

AP Group 1:
AP Group Name : Students
Dynamic Interface : Student-VLAN
SSID: School



AP Group 2:
AP Group Name : Staff
Dynamic Interface : Staff-VLAN
SSID: School

局限性！

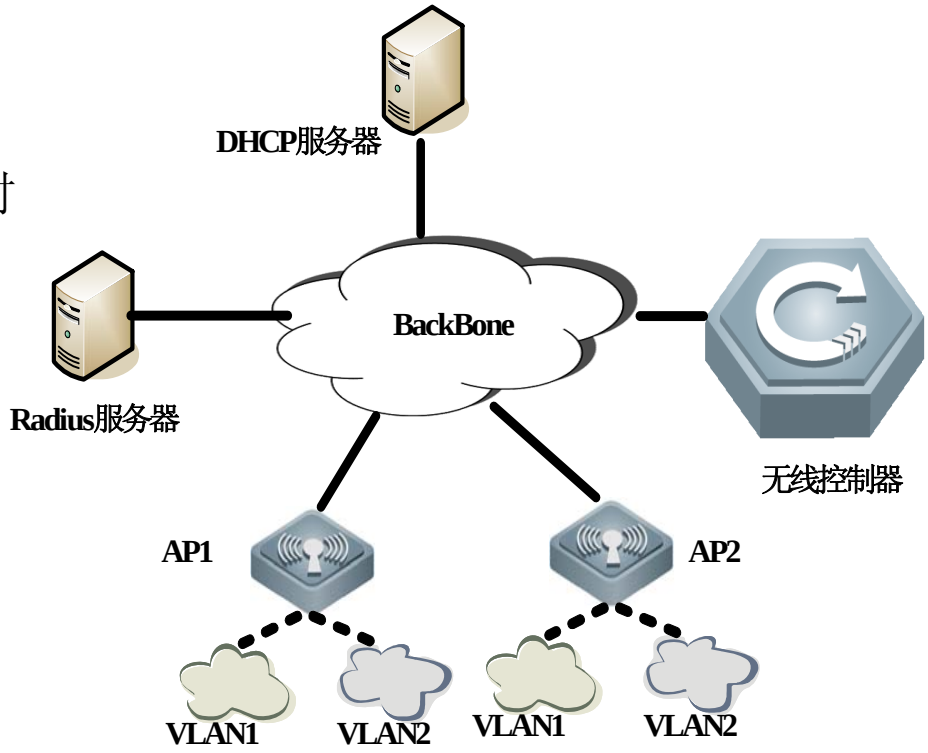
问题的提出

本文给出的解决方法：

- 提出了一个综合的无线系统解决方案，结合Radius和DHCP协议，实现无线网内一个SSID 可以映射多个VLAN，动态的决定用户的vlan membership。
- 用户在连接入网络中时，先临时分配一个vlan（称作Temporary VLAN），在此vlan内用户使用WEB 进行认证成功后，再由Radius服务器指派相应的Permanent VLAN。
- 可解决Web认证下的无线用户规模可扩展性的问题。

支持无线用户规模可扩展性的系统组成

- 为提高无线用户规模的可扩展性，基于web认证的无线系统架构(同时也可选支持802.1x认证方式) 应当包含右图所示组件：



- AP与有线网络互联，是无线流量的起始点，负责广播SSID，接受从空口上传来的用户流量，将流量从空口转发给无线用户；

- 无线控制器 (Access Controller, 简称AC) 与有线网络互联，是无线流量的终结点，具备丰富的二层与三层功能，如DHCP服务器、DHCP Snooping功能以及支持路由协议等；

- AP与无线控制器之间将使用隧道的方式来承载无线流量，隧道协议基于UDP来实现；Radius服务器完成身份认证和vlan成员关系的指派；DHCP服务器将完成无线用户IP地址的申请分配与强制释放。

系统主要功能介绍

- 基本的web认证过程：
  - 首先STA的802.11 MAC层使用Scanning功能来完成Discovery，选择合适的AP(采用被动侦听来自AP的Beacon帧或主动发Probe帧两种方式)。
  - STA的802.11MAC通过使用开放式系统或简单的SSID或MAC地址进行认证后建立与AP之间的Association关系(STA将只跟建立Association关系的AP交换数据)。
  - STA通过DHCP协议从无线系统中获得IP地址。
  - STA使用IP地址，进行基于Web方式的认证。
  - 一旦通过认证，无线控制器将根据从AAA服务器(如Radius)上获得的该用户的权限信息，对SAT的访问权限进行控制。此时STA就可以访问外部网络了。

系统主要功能介绍

- 支持大规模web用户接入的无线系统的功能实现：
  - 无线控制器AC主要功能包括：
    - 与AP之间建立隧道；
    - 作为内部DHCP服务器，为认证前的无线用户分配临时IP地址；
    - 将用户的认证信息转发给Radius服务器；
    - 根据DHCP Relay特性,作为ip-helper为无线用户从外部DHCP服务器上申请正式IP地址；
    - 根据DHCP Snooping的功能以及Radius返回的vlan ID信息，记录下无线用户MAC地址、vlan关系、隧道信息以及IP地址信息，作为未来报文转发的依据。

系统主要功能介绍

支持大规模web用户接入的无线系统的功能实现：

- Radius服务器 主要功能：
  - 除了完成基本的AAA功能之外，还将实现vlan pool的功能。该功能将根据每次AC转发的web认证请求，采用轮询调度算法round-robin，为用户的每次请求指定其所属的vlan membership。假设vlan pool中共有n个vlan，根据round-robin算法，为第m次认证用户分配的VLAN-ID 将是第m-[m/n]n个。
  - 一旦确定了vlan number关系后，Radius服务器在返还给AC的Access-Accept报文中将包含Tunnel attributes来指明vlan信息（当然，AC也可以在Access-Request报文中通过使用Tunnel attributes为无线用户来显示的要求一个vlan assigment）。
  - 为了完成上述VLAN assignment, Radius服务器将使用到下面的tunnel attributes参数用以构造UDP报文以返回给AC:

    Tunnel-Type=VLAN (13)

    Tunnel-Medium-Type=802

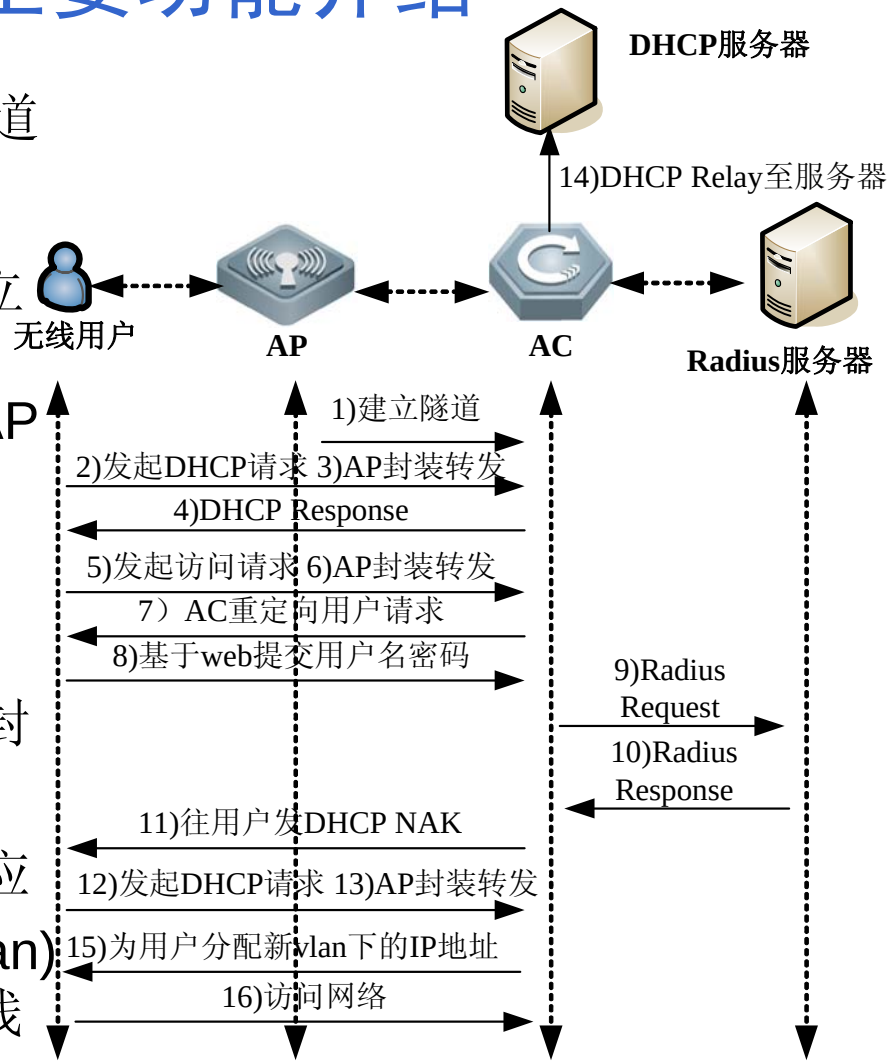
    Tunnel-Private-Group-ID=VLANID

注：1) 其中VLANID 为 12个bit,取值范围在1～4094,

2) 为了实现同一个AP可以支持多个vlan用户的数据，AP与有线网络相连的端口应当被配置成Access类型，AC与有线网络相连的端口则被配置成Trunk类型。

系统主要功能介绍

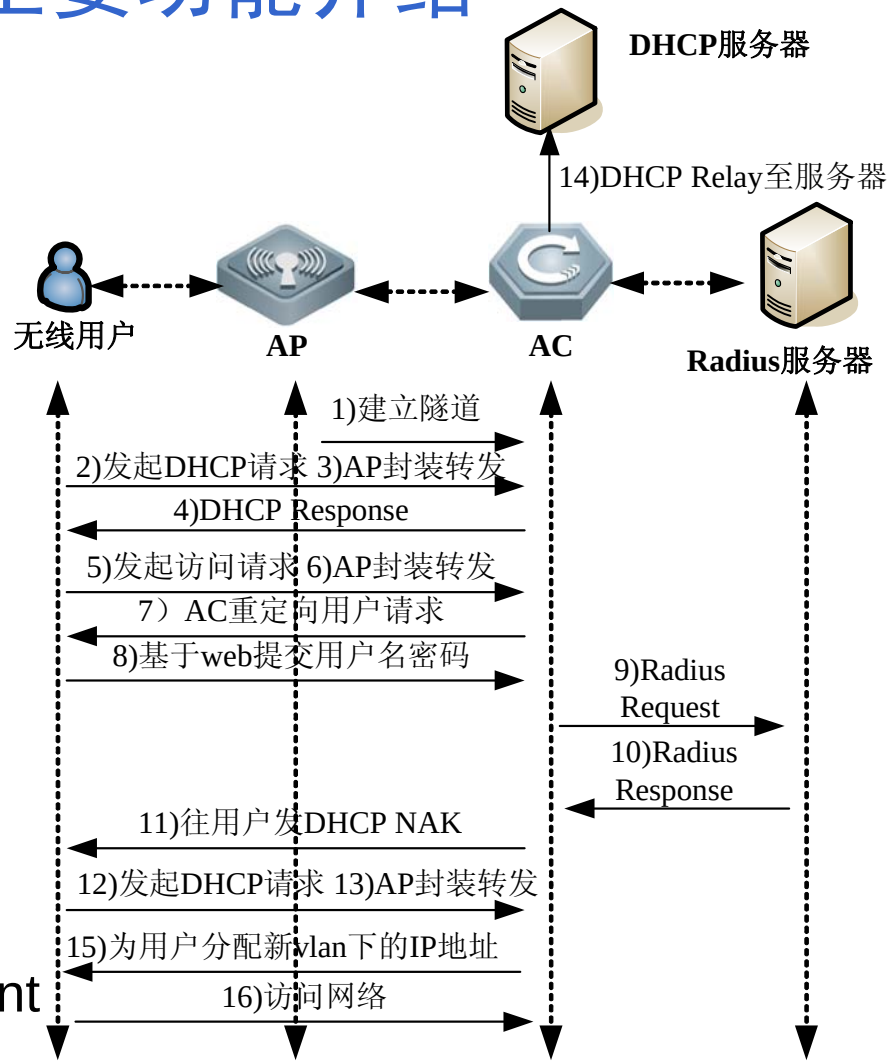
- 1) AP将通过无线系统，使用隧道的方式(如Aruba的GRE隧道或CISCO所使用的IETF草案LAWPP)，跨越2层/3层网络建立起与无线控制器的连接；
- 2) 一旦通过简单的认证关联到AP上后，用户操作系统将发起DHCP Discovey和DHCP Request，以获得无线端口上的IP地址；
- 3) AP将用户的DHCP请求报文封装在隧道内传送至无线控制器；
- 4) 在基于web认证的SSID所对应的Temporary vlan(如default vlan)内收到用户的IP地址申请后,无线控制器从内部DHCP服务器的DHCP pool中分配一个地址，以DHCP Offer/DHCP Ack报文形式通过隧道返回给用户；



系统的详细功能描述

系统主要功能介绍

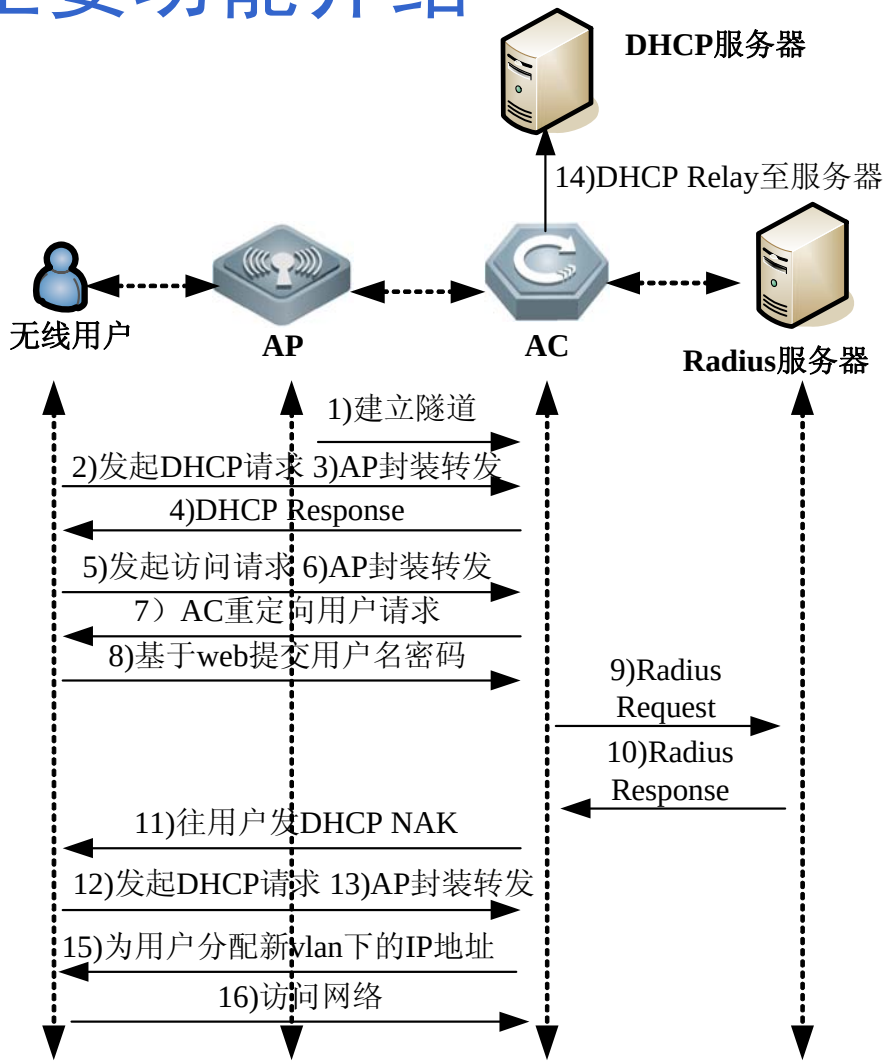
- 5) 用户收到由AC发来的临时IP地址后，使用本地的TCP/IP协议栈，进行基于web的访问；
- 6) AP将用户的报文封装在隧道中转发给AC；
- 7) AC收到后将劫持并重定向用户的web请求到一个认证界面(portal),并返回给用户；
- 8) 用户收到重定向报文后，依据页面，填写自己的用户名和密码，并将此信息提交给AC；
- 9) AC收到后，作为Radius Client将用户名和密码通过Radius协，以UDP报文转发给远端的Radius Server进行鉴别；



系统的详细功能描述

系统主要功能介绍

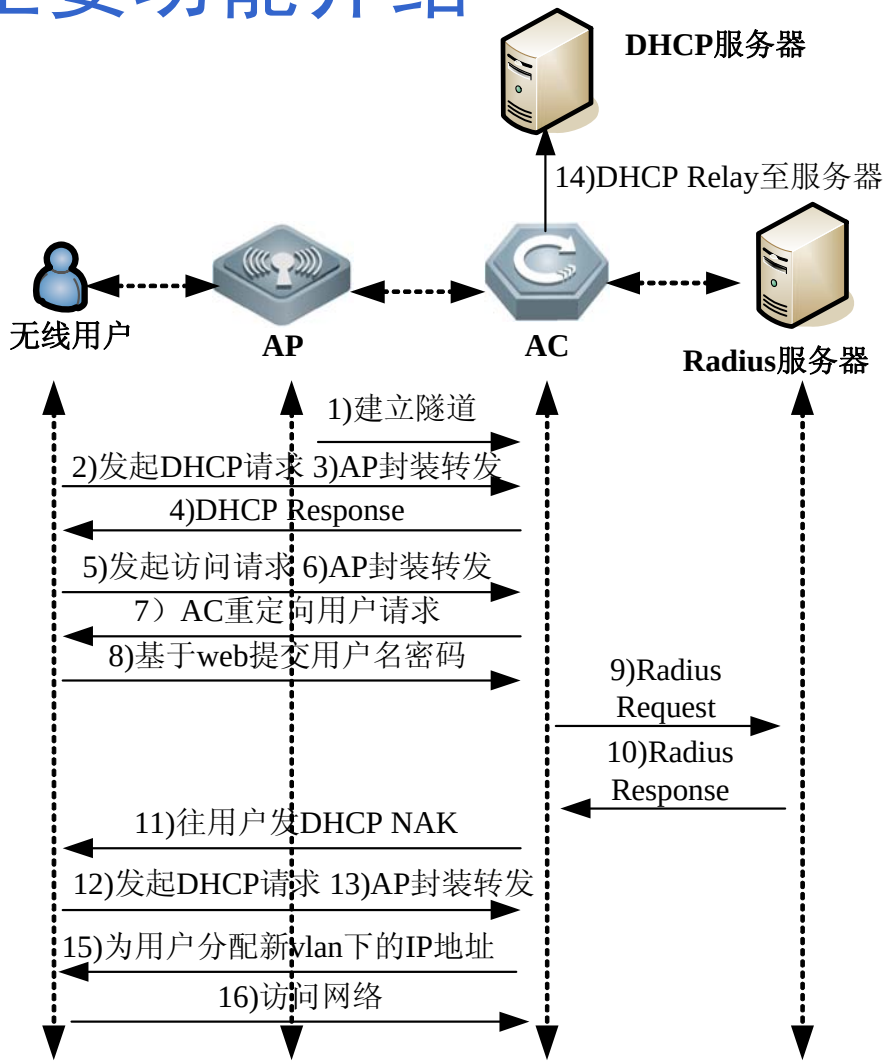
- 10) Radius Server收到用户名和密码信息后，一旦鉴别通过，则从本地的vlan pool中，通过round-robin的方式，决定当前用户应该所属的vlan number信息，并封装在自己的协议报文中，再以UDP报文的形式转发给AC；
- 11) AC收到Radius返回的信息后，立刻在本地建立用户**MAC-VLAN Number-隧道号的表项**，发DHCP NAK给用户，此时完成无线用户的vlan分配；
- 12) 用户收到AC发来的NAK信息后，被迫放弃当前的临时IP地址，并重新发起DHCP Request；
- 13) AP继续封装上述请求，转发给AC；



系统主要功能介绍

- 14) AC收到新的IP地址申请后，根据当前用户的MAC所属的Permanent VLAN信息，以该vlan的ip地址为ip-helper发起新的DHCP relay给远端的外部DHCP服务器；
- 15) 当AC从远端的DHCP服务器获得响应后，将把正式IP地址分配信息转发给用户，同时会在11）中产生的表项之后增加此IP地址信息，作为未来无线数据转发的依据；
- 16) 用户将获得新的IP地址，此时用户就可以使用新的IP地址访问互联网了。

通过这些步骤，利用Linux操作系统对IP协议的良好支持，可以很好实现web认证下同一个SSID用户可以被分配到不同vlan的功能。



系统的详细功能描述

结束语

- 本系统为解决web认证下无线用户规模可扩展性问题，利用十分成熟的协议，提出了一个简单高效的系统方案。由于AC在整个系统中扮演了非常重要的角色。因此未来上述功能可以考虑与专门的厂商合作，采用硬件如ASIC或TCAM来生成与维护有关的各种表项。
- 当然系统功能还有需要丰富的地方。例如没有考虑无线用户在非正常离线情况下，系统对vlan资源的回收情况。即有可能在某一个vlan ID上尽管没有很多实际用户，但是Radius也为其分配了vlan资源。这样就造成实际上某些ID对应大量实际用户，某些ID只对应了少量用户的资源不均衡现象。
- 这可以通过改进vlan分配算法来解决；或者利用AC来监视无线用户MAC地址的老化时间，一旦time out，AC告知Radius服务器，用户已经从无线系统中离开，可以立刻撤销目前的某个MAC-VLAN Number-隧道号-IP地址的表项，该vlan ID可以分配给后续申请的用户了。

路漫漫其修远兮。。。

Thank You!