基于IP控制网关和802.1x的校园网认证记费解决方案

北京大学计算中心

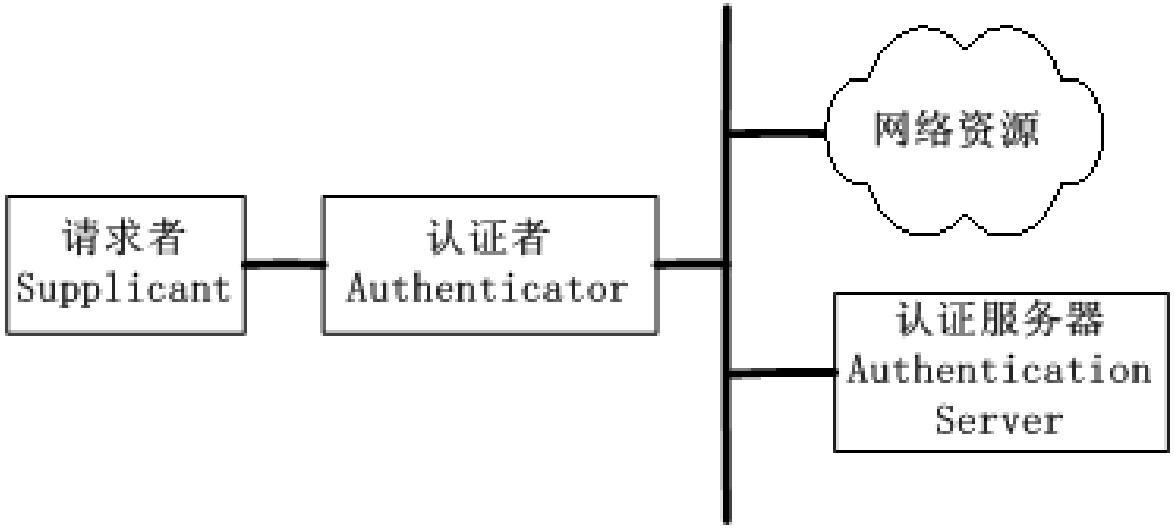
2008年1月9日

- 校园网用户的认证和记费，是校园网管理工作中的关键性任务。
- 授权目前主要针对具体应用系统，目前还不是校园网管理工作。
- 理想的校园网认证计费系统：
  （1）对网络用户进行有效的管理和控制，以确保网络的安全性，
  （2）适合校园网计费实际需要的计费方式。
- IP控制网关（ IP control Gateway ）
- 802.1x认证

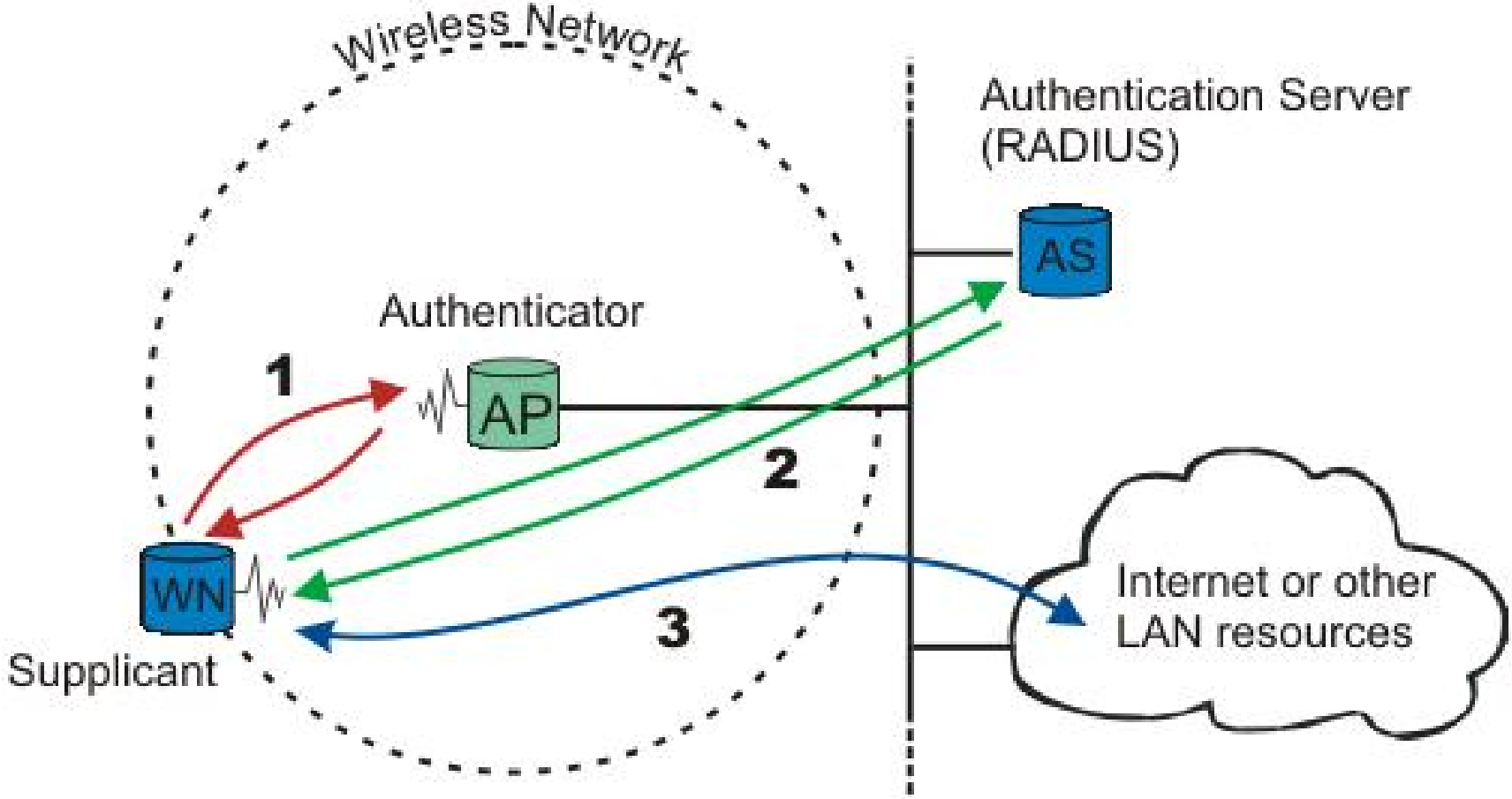
IEEE 802.1x协议

- 802.1x协议由IEEE于2001年提出，它是一种基于端口的网络访问控制协议。
- 802.1x协议起源于802.11协议，它的提出最初是为了解决无线局域网用户的接入认证问题。但是，802.1x协议不仅仅适用于无线局域网，它同样适用于有线局域网。

802.1x认证体系

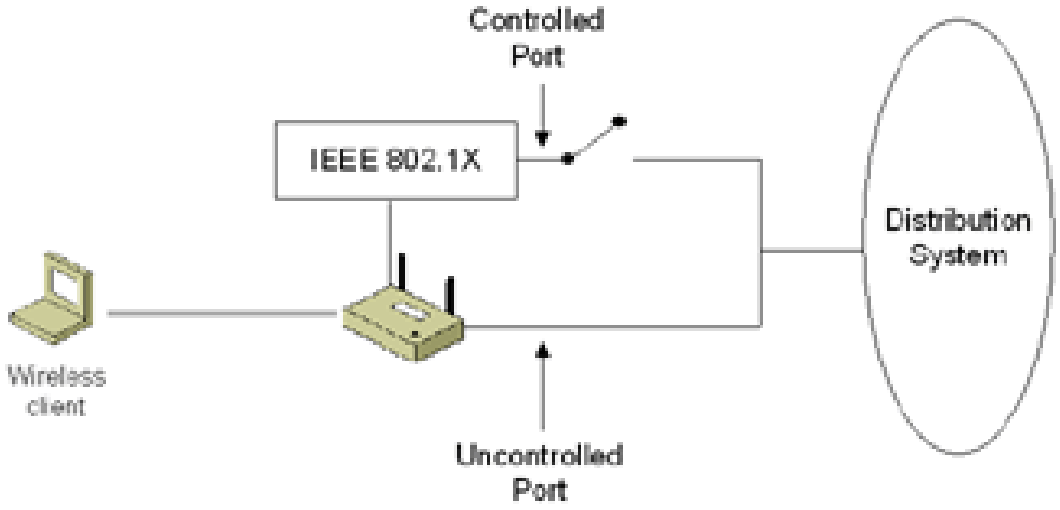


- 请求者是局域网中的一个结点，通常是局域网中支持802.1x的用户终端设备（客户端）。
- 认证者负责对请求者进行认证，它通常是支持802.1x协议的网络设备（例如交换机或AP）。
- 认证服务器负责提供认证服务，它通常是RADIUS服务器。


Wireless Network
Authentication Server
(RADIUS)
AS
Authenticator
1
AP
2
WN
3
Internet or other
LAN resources
Supplicant

- 802.1x使用可扩展认证协议（Extensible Authentication Protocol，简称为EAP）在请求者、认证者和认证服务器之间传递认证数据。EAP通常是工作在数据链路层。

可控端口和非可控端口



- 认证者与请求者连接的接入端口由可控端口和非可控端口组成。非可控端口始终处于打开状态，负责传递EAP报文。受控端口在认证前处于关闭状态，只在认证成功后打开。受控端口负责传递各种网络数据。因此，请求者必须通过认证才能访问网络资源。

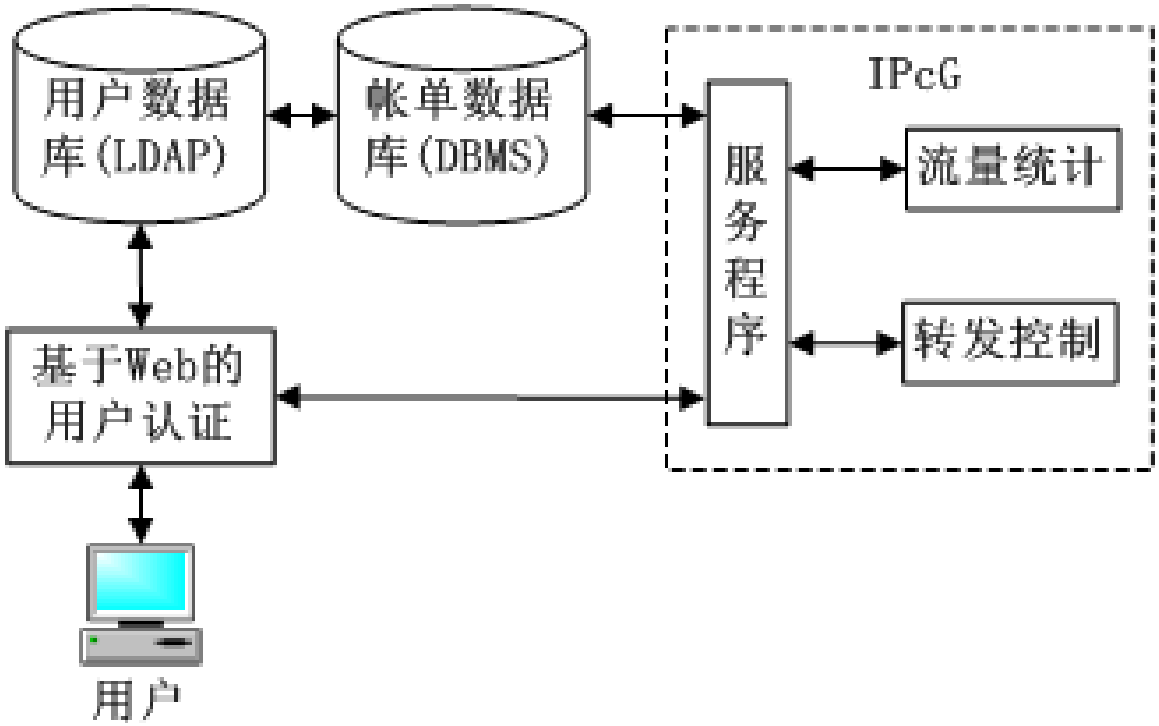
802.1x认证的特点

- **（1）安全性**：在接入层对用户进行认证和控制，比传统的认证方式（例如基于网关的认证方式）更安全。
- **（2）认证协议所在网络层**：数据链路层。因此，通过认证前，无需给请求者分配IP地址。
- **（3）对客户端的要求**：作为请求者的客户端必须要运行802.1x客户端软件。
- **（4）对网络设备的要求**：作为认证者的网络设备（如交换机或AP）必须支持802.1x协议。
- **（5）网络记费**：802.1x协议本身并没有给出计费方案。尽管作为认证服务器的RADIUS服务器能提供一定的记费功能，但802.1x认证体系中的RADIUS服务器不能按用户访问的IP地址来对用户进行计费（比如区分国际、国内流量进行记费）。而按用户访问的IP地址来对用户进行计费是校园网记费系统不可缺少的功能。

IP控制网关简介

- 基于透明网关的设计思想，北京大学计算中心自行设计开发了千兆IP控制网关（IP control Gateway，简称IPcG）。
- IPcG工作于千兆网络环境中，实时检查网络链路上通过的数据包的IP地址等信息，并根据计费策略控制数据包的转发，从而控制校内IP地址的对外访问。同时，IPcG能统计相关网络流量、访问记录等信息。
- IPcG通过软件实现，适应于通用开放平台（主流PC服务器、通用网卡、操作系统），易于维护和升级。

IP控制网关（IPcG）体系结构



注：用户也可使用专用的客户端进行认证

IPcG实际运行情况

- 2002年，IPcG在北大校园网正式部署和实施，架设于出口路由器和出口交换机之间的双IPcG系统共同承载着北京大学的出口流量。五年多时间的实际运行证明，IPcG很好地满足了校园网计费和管理的需要。
- 目前，IPcG系统已经在中国农业大学、北京地质大学等十多所高校中实际运行。

IPcG的特点

- **（1）安全性**：存在一定的安全隐患。主要表现在：不能在接入层对用户进行认证和控制。
- **（2）认证协议所在网络层**：IP层。在认证前，必须保证所有请求认证的用户（客户端）都能够获得（静态或动态获得）和使用有效的IP地址，无论这些用户是否合法。在这种认证体系下，不合法的用户也可以得到和使用有效的IP地址，这既增加了网络的不安全因素，也造成了IP资源的浪费。
- **（3）对客户端的要求**：用户可以使用IE等网络浏览器进行认证，不需使用专用的客户端软件。
- **（4）对网络设备的要求**：IPcG集中部署于校园网出口处，对网络设备无特殊要求。
- **（5）网络记费**：能够基于用户访问的IP地址进行计费（比如区分国际、国内流量），满足校园网记费的需要。

802.1x认证和IPcG的比较

（1）802.1x认证

(a)主要优势在于安全性，能在网络边缘对用户进行管理和控制。

(b)其主要的局限性:

*它要求相关的网络设备和客户端必须支持802.1x认证。

*由于802.1x认证本身不能完全解决校园网的计费问题，因此，802.1x的部署实施必须结合其它的计费体系进行部署实施。

（2）IPcG认证

(a)主要优势在于：

*其部署和实施的灵活性（对网络设备以及客户端无特殊要求）。

*较好实现了对校内IP地址对外访问的控制和记费。

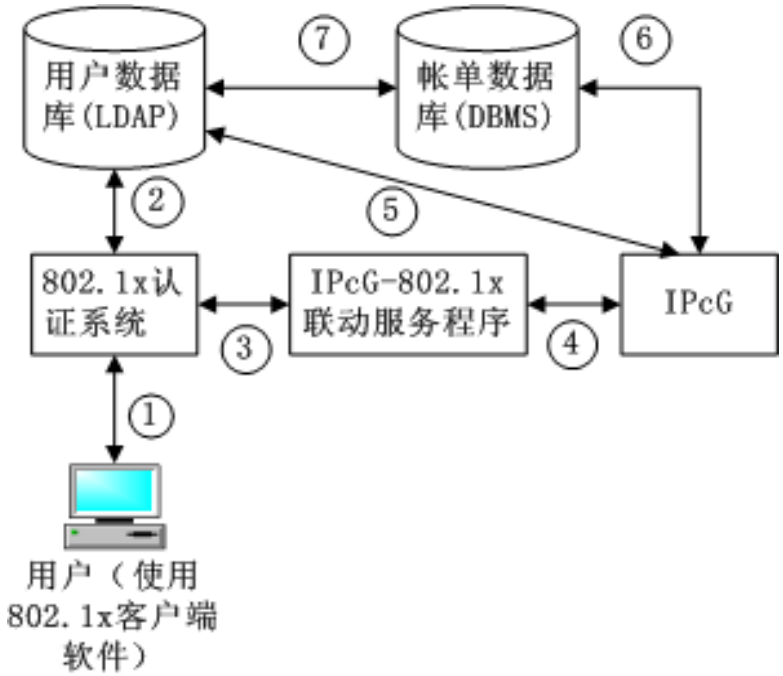
(b)其主要的局限性在于：

*安全性存在局限性，不能在网络边缘对用户进行管理和控制。

*在一定程序上造成IP资源的浪费。

IPcG-802.1x解决方案

- 综合考虑IPcG和802.1x认证的特点，我们提出了将两者相结合的校园网认证记费解决方案—IPcG-802.1x



IPcG-802.1x—基于IPcG和802.1x的校园网认证记费解决方案

- （1）实现了IPcG和802.1x认证的有效结合。

  （a）用户必须通过802.1x认证后方可获得和使用有效的IP地址，从而连入校园网和访问校内网络资源。这样做的目的是利用802.1x认证加强对用户的管理，提高网络的安全性，减少IP资源的浪费。

  （b）用户必须通过IPcG认证后才能访问校外网络资源（国际或国内网络资源）。由IPcG对用户的对处访问进行管理和记费，以发挥IPcG的优势。

- （2）用户只需“一次认证”即可进行802.1x认证以及IPcG认证。

  虽然访问校外网络资源的用户须经过802.1x认证以及IPcG认证两次认证过程，但用户只需输入一次用户身份（例如用户名和密码）及相关信息（例如网络访问范围）。因此，从用户的角度来看，只须经过一次认证即过访问相关的网络资源。

- （3）系统构架方面，IPcG和802.1x认证系统保持相对的独立性。

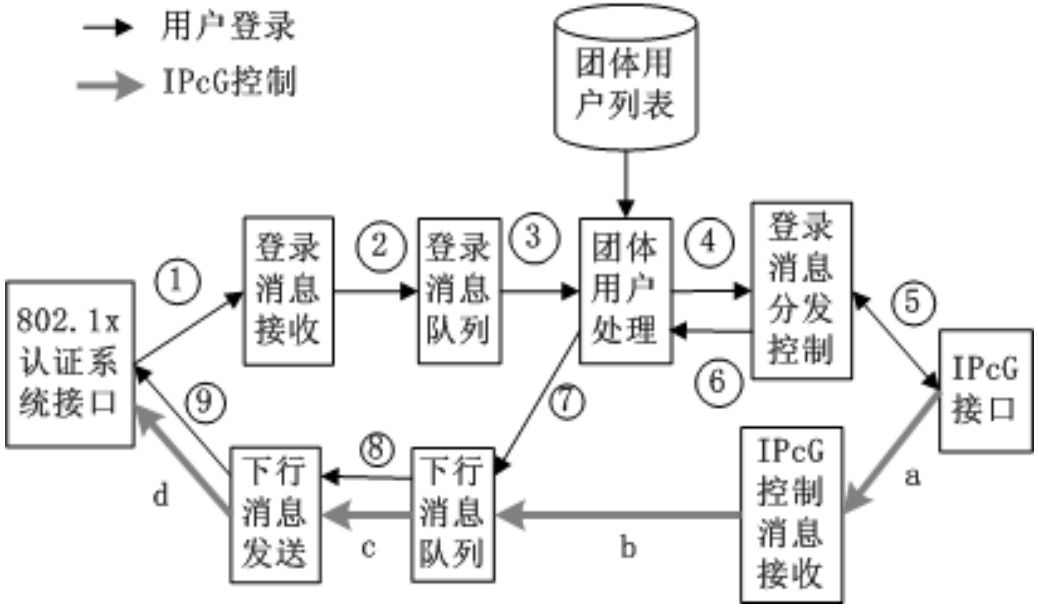
  双方的协同主要通过IPcG-802.1x联动服务程序来完成。这种系统构架尽可能地减少了802.1x认证系统和IPcG的耦合度，有利于提高IPcG-802.1x系统的研发效率和简化该系统的部署实施。
- （4）在遵循802.1x认证以及IPcG认证机制的前提下，实现了对团体用户的更安全的管理。

  (a)使用个人账户进行802.1x认证

  (b)使用公共账户登录IPcG，

  (c)个人账户与公共账户的转换由IPcG-802.1x联动服务程序自动完成，该过程对用户来说是完全透明。

IPcG-802.1x联动服务程序



- 用户登录:

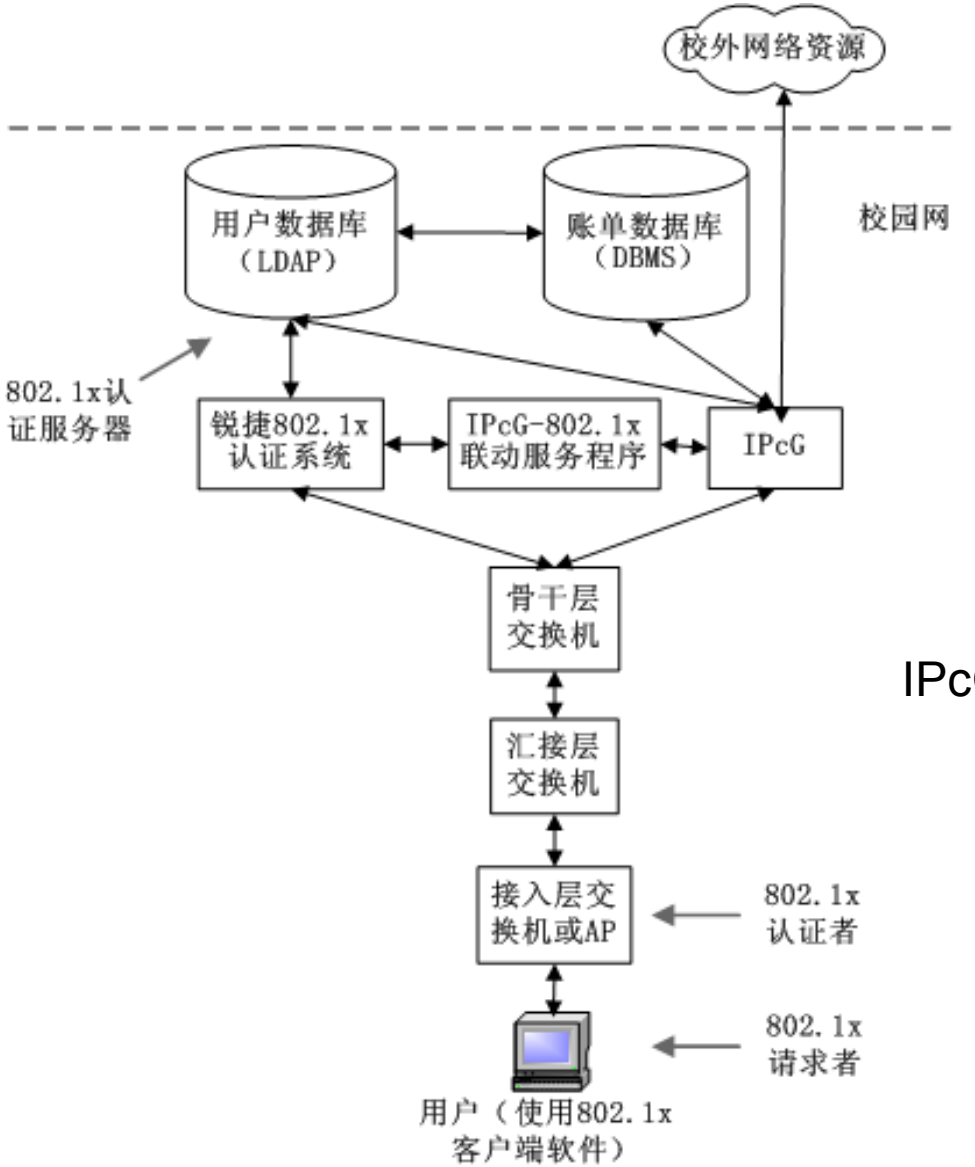
  用户登录程序把从802.1x认证系统发送来的用户登录请求发送到IPcG，并把IPcG的认证结果发送回802.1x认证系统。

- IPcG控制

  IPcG控制程序负责把IPcG下发的控制消息送到802.1x认证系统。这些控制消息的作用是：将用户账户情况(如余额等属性)以及IPcG对用户采取的措施(如强行断开用户与校园网外地址连接、封锁、注销用户账户)的信息发送给802.1x认证系统。

IPcG-802.1x系统的实现

- 主要的研发工作包括IPcG-802.1x联动服务程序的研发、IPcG与联动服务程序接口的研发工作。
- 锐捷公司对IPcG-802.1x项目给以积极的支持，根据我们提出的IPcG-802.1x方案，提供了符合联动服务程序接口规范的802.1x认证系统 。



IPcG- 802.1x校园网管理记费系统实例

总结

- 提出了基于IP控制网关(IPcG)和802.1x的校园网认证记费解决方案。
- 该方案能加强对校园网用户的管理，提高网络安全性，同时又较好地满足了校园网的记费需要。
- 在条件允许的情况下，将在在更大的区域部署和实施IPcG-802.1x系统，以在实际运行中不断完善IPcG-802.1x校园网认证记费解决方案。

大规模部署802.1x认证需解决的问题

- 技术层面：
  设备
  802.1x客户端的分发
  二次开发（如计费）
  处理短期用户以及团体用户

- 非技术层面：
  用户的需求以及行政推广的力度
  工作量的增加?

- 谢谢！