* 1. 认证方案

无线网络中既有有线用户，也有无线用户，且同时需要对有线网络和无线网络都进行认证，保证接入网络的用户的合法性。华为有线无线一体化方案坚持“只有合法的用户才能接入网络”，只有认证通过后的用户，才能使用网络。

针对校园的特点，我们推荐建议在汇聚层设备上作Portal认证对有线用户进行认证，在AC上对无线用户作认证。这种认证方式与接入层设备无关，终端设备既可以安装代理客户端，也可以不安装（Web强推方式），适应各种终端接入（PC、手持设备等），方便灵活，管理维护方便。旧网改造中若需要增加安全接入控制功能，而又不希望改变原来网络结构，可以直接在汇聚层部署Portal认证。

**用户接入认证**

通过用户接入认证，可以对接入网络的用户身份进行合法性进行认证，只有合法用户才允许接入，并且不同的角色，不同的用户所能够访问的资源是不同。管理员可以为用户分组，或者定义不同的角色，配置不同的资源，使得特定的用户只能访问授权的特定资源，禁止访问未授权的网络资源。

WLAN网络根据用户的角色不同，建议采用三种认证方式。一是普通职工通过WEB PORTAL方式，每次上网要求进行用户名和密码认证；二是教师的手执终端只需输入第一用户名和密码，以后不用再次认证；三是临时访客用户由短期认证授权方式，账户和密码具有一定的时效性，即访客制度。园区访客制度需要解决以下安全性核心问题：

* 对访客申请的账号进行统一管理；
* 限制访客访问权限，保障园区信息安全；

对访客上网行为审计，以避免法律风险。

华为eSight Agile Controller支持园区内部员工和外部访客使用同一套系统访问，实现全网用户统一认证、授权，对访客访问网络的带宽、流量等进行限制，支持访客账号自助申请，并能进行有效管理。访客管理系统处理流程如下：

* 接待人员反馈信息，由管理员或接待人员申请临时账号；
* 管理员审批信息，批准临时账号，通过短信/邮件把发送临时账号给接待人员；
* 访客通过临时账号登录网络，TSM进行认证和记录；
* 定期清理园区临时账号信息，减轻管理难度。

**认证方式选择**

华为终端准入方案支持802.1x、MAC认证、Portal认证等多种网络访问控制方式，并可灵活部署在用户网络的接入交换机、汇聚交换机、无线控制器、AR等多种网络设备上，配合NAC的终端代理和服务器共同完成NAC控制，为校园网提供安全可靠的访问控制。

* 802.1x认证

标准的802.1x协议是一种基于端口的网络接入控制协议，用于在局域网接入设备的端口一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

802.1x认证使用EAP（Extensible Authentication Protocol）认证协议，实现客户端、设备端和认证服务器之间认证信息的交换。在客户端与设备端之间，EAP协议报文使用EAPoL（EAP over LAN）封装格式，直接承载于LAN环境中。

* Portal认证

Portal认证是一种三层认证方式。用户可以通过访问Portal服务器（Web服务器）上的Web认证页面，输入用户帐号信息，实现对终端用户身份的认证。采用Portal认证，用户可以无需安装客户端软件，用户访问Portal页面时，通过自动提示下载的ActiveX控件实现基本安全检查功能。

Portal认证支持Web认证且可以无需安装客户端软件，这两个特性使得Portal认证对于访客和出差用户具有很好的支持。

* MAC认证

对某些特殊情况，终端用户不想或不能通过输入用户帐号信息的方式完成认证。例如某些特权终端希望能“免认证”直接访问网络；对于某些特殊的PC终端，如打印机、IP电话等设备，无法安装客户端软件，也无法通过输入用户帐号信息的方式进行认证授权。此时，可以采用MAC认证的方式实现对终端的网络访问控制。

MAC认证就是以终端的MAC地址作为身份凭据到系统进行认证。启用MAC认证后，当终端接入网络时，网络准入设备提取终端MAC地址，并将该MAC地址作为用户名和密码进行认证。如果认证失败使用户下线，并保持一段时间内不再发起认证和探测，超时后重新开始探测过程；如果认证成功，交换机将增加该MAC地址进入MAC表，用户将可以正常访问网络。

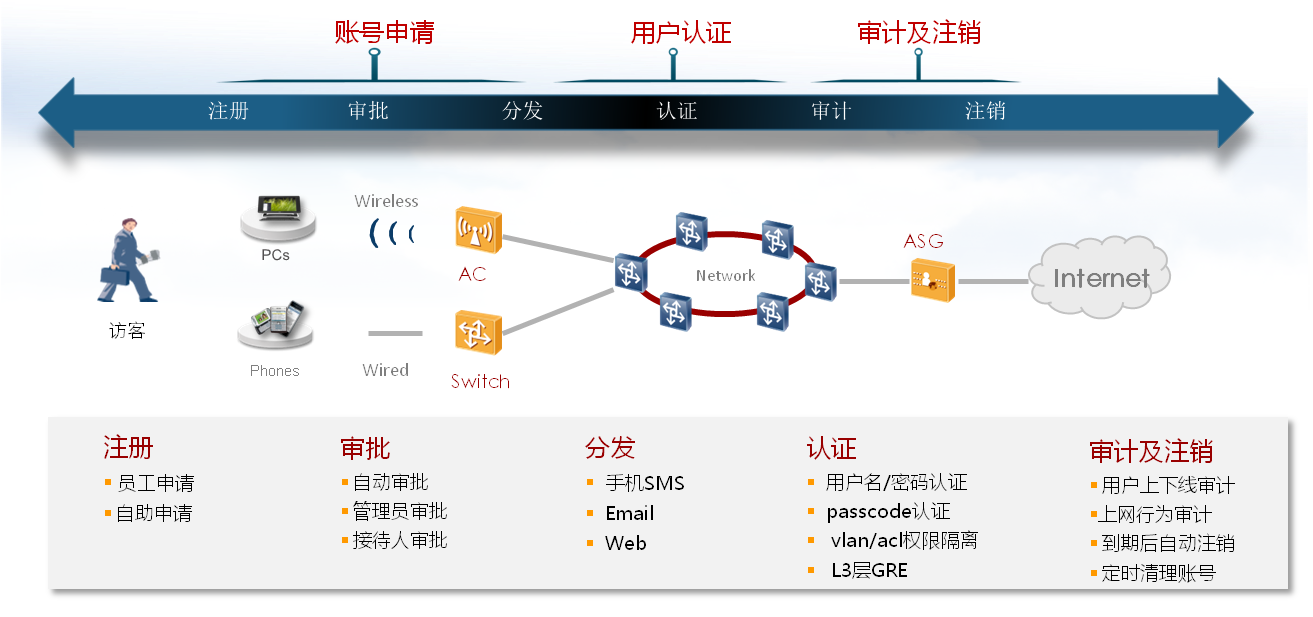
**访客管理**

随着园区与外界交往的增加，WLAN移动办公能够灵活满足客户沟通、交流、参观过程中对网络接入的诉求，访问园区公共资源或internet。园区提供一套访客管理系统，既能方便客户交流，提升园区形象，同时对访客的网络接入权限做到精细管控。园区访客系统需要解决以下安全性核心问题：

* 对访客申请的账号进行统一管理；
* 限制访客访问权限，保障园区信息安全；
* 对访客上网行为审计，以避免法律风险。

华为eSight Agile Controller支持园区内部员工和外部访客使用同一套系统访问，实现全网用户统一认证、授权， 对访客访问网络的带宽、流量等进行限制，支持访客账号自助申请，并能进行有效管理。访客管理系统处理流程如下：

* 接待人员反馈信息，由管理员或接待人员申请临时账号；
* 管理员审批信息，批准临时账号，通过短信/邮件把发送临时账号给接待人员；
* 访客通过临时账号登录网络，TSM进行认证和记录；
* 定期清理园区临时账号信息，减轻管理难度。



* 1. 身份认证方案
     1. 用户认证方案

Agile Controller系统建立了完善的接入用户身份认证机制，支持系统内置账号和外部数据源方式。系统内置账号包括普通账号、MAC账号，外部数据源账号支持从AD账号、LDAP账号和CA账号等第三方的用户系统中同步账号，实现终端的网络准入前的身份认证过程。

Agile Controller系统中，终端用户是以终端角色来进行安全策略和网络访问权限管理的，终端只有完成身份认证才能接入园区内网，因此本次实施方案需完成终端用户的认证账号配置。

Agile Controller系统参考现有园区的组织和管理结构，采用树状结构的多级管理方式，账号数据源支持系统内置账号和外部数据源方式。系统内置账号包括普通账号、MAC账号，外部数据源账号支持从AD账号、LDAP账号和CA账号等第三方用户系统中同步账号，完成Agile Controller系统的接入认证。

* + 1. 多模式授权管理

Agile Controller系统建立了完善的接入用户身份认证机制，可以根据业务的需要，根据用户的组织结构，区分用户所属的部门进行接入授权。也可以根据业务维度，根据用户所属的角色，区分用户角色进行接入授权。

在本方案中,可根据管理员、校长、老师等设置不同的部门信息，不同部门的用户不同的认证策略和权限策略。

* 1. 终端设备自动识别

Agile Controller系统提供设备识别功能，能够根据设备识别探针获取的设备特征数据，根据数据特征判断该设备的设备类型和操作系统类型。Agile Controller支持多种类型的设备识别探针。

Agile Controller系统，支持同时使用多种探针技术，通过多种探针获取的数据进行综合分析，能够比单一的方式更加准确的判断终端的设备类型。在BYOD应用环境中，Agile Controller的设备识别功能，可以与网络准入控制功能配合，对不同类型的终端实施不同的网络接入策略，提升IT运维的效率。

* 1. 教师上网管理方案
     1. 教师账号生成

教师终端用户的账号可由现有的人事系统、邮箱系统或者其他数据库中导出，然后通过Agile Controller系统提供的Excel模板统一批量导入到系统里，Agile Controller提供了批量导入功能，可根据每个教师的工号或者姓名，统一一个默认密码导入到系统中，要求教师上网第一次认证之后必须更改密码，即可实现教师账号的开户。

* + 1. 教师认证

教师通过无线登录认证的流程如下：

1. 教师在终端搜索无线SSID，与AP建立关联，获取IP地址。
2. 教师访问WEB站点，AC 将用户请求重定向到Portal认证页面。
3. 教师在认证页面输入用户名及密码或者PASSCODE,进行认证。
4. Portal服务器向AC发起Portal协议认证。
5. AC向AAA服务器发起Radius认证
6. 认证通过，向AC下发访客网络权限。
7. AC通知Portal服务器发送认证成功。
8. Portal服务器提示认证成功。
   1. Agile Controller可靠性介绍
      1. 操作安全性

Agile Controller系统采用基于管理角色的操作权限控制，并记录管理员的操作日志保证提高操作安全性和可追溯性。Agile Controller系统支持管理员、操作员、审计员权限分离。通过权限分离，实现系统管理的安全性，有效防止权限乱用。

* + 1. 数据安全性

Agile Controller系统提供完善的数据安全解决方案。

**数据传输方面：**

* Secospace Agile Controller系统服务器之间的数据传输采用华为私有协议进行加密；
* 代理程序与服务器之间的通讯通过SSL协议加密；
* 补丁和软件的分发均支持数据完整性检查和断点续传功能，充分保证数据传输的安全性；

**数据存储方面：**

* Agile Controller系统通过数据库保存终端的违规日志信息，支持数据镜像和增量备份功能；
* 系统管理员通过管理界面进行日志管理时无法删除任何的违规信息，保证存储数据的完整性和原始性；
  1. 方案特点及优势

整体方案实现了集中统一的认证、授权管理，管理员不在需要费尽脑汁去配置网络中的各个设备，去完成相应的访问控制机制，所有的安全策略都由Agile Controller服务器统一的进行配置和下发，无论对于安全策略的定义、执行还是故障排查，都提供了很大的方便性。

**1：统一的策略引擎/ 基于5W1H的情景感知**

基于场景的接入控制：在整个组织内实施统一访问策略（有线、无线，内网，外网一体化）,实现基于用户、设备类型、资产类型、接入时间、接入地点、接入方式的认证和授权，满足园区接入认证多层次、泛终端接入的需求，实现园区用户接入安全，保证合法的用户接入且合理、合法的使用园区网络

**2:个性化Portal定制 ，灵活的页面推送功能**

个性化定制Portal登录界面，提供所见即所得的定制功能，降低二次开发成本，提高公司品牌形象。灵活的页面推送，可基于终端IP范围、位置等推送个性化定制页面，满足园区自定义广告推送的增值服务需求

**3:随时随地的接入、无感知认证技术助力BYOD**

智能化终端识别，内置200多种设备类型模板：过识别终端的设备类型，为不同的设备设置不同的认证方式；或者在Web认证方式下推送适合某种终端类型的页面，并可以限制其网络访问策略。

智能终端无感知认证，提高用户体验：基于MAC地址优先的Portal认证，可配置一定时间内的智能终端一次认证后无感知上线，提高用户体验，降低BYOD实施难度