无线网络安全解决方案

1.WLAN的应用现状

1.1 Wi-Fi在全球范围迅速发展的趋势

无线局域网(WLAN)作为一种能够帮助移动人群保持网络连接的技术，在全球范围内受到来自多个领域用户的支持，目前已经获得迅猛发展。无线局域网(WLAN)的发展主要从公共热点(在公共场所部署的无线局域网环境)和企业组织机构内部架设两个方向铺开。世界范围内的公共无线局域网（WLAN）热点数量三年增加近60倍。预计将从2002年的14717个增长到2006年的30多万个，用户数量增加四倍。据IDC预测，到2004年全球的WLAN用户将达到2460万，比2002年增长近十倍；2002年销售的全部笔记本电脑中只有10%支持WLAN，目前是31%，预计到2005年，售出的笔记本电脑中将有80%具备无线支持能力。

在亚太区，这一发展势头同样强劲。市场调查公司Gartner Dataquest指出，公共无线局域网(WLAN)服务在亚太地区将保持强劲的发展势头。至少在澳大利亚、香港、日本、新加坡、韩国和台湾这六大市场，热点的数量在迅速增加。2002年亚太地区只有1，625个热点，预计到2007年，热点的数量将接近3.8万。

1.2

在企业、学校等组织机构内部，笔记本电脑的普及也带动了无线局域网(WLAN)的普及。

以英特尔公司为例，全球79，000名员工中有65%以上的人使用笔记本电脑，其中80%以上的办公室都部署了无线局域网(WLAN)，英特尔围绕具备无线能力的笔记本电脑如何改变其员工的生活习惯和工作效率进行了调查，结果表明，员工的工作效率平均每周提高了两小时以上，远远超过了所花费的升级成本，而且完成一般办公室任务的速度提高了37%。此外，无线移动性还迅速改变了员工的工作方式，使其能够更加灵活自主地安排自己的工作。

2. WLAN面临的安全问题

由于无线局域网采用公共的电磁波作为载体，电磁波能够穿过天花板、玻璃、楼层、砖、墙等物体，因此在一个无线局域网接入点(Access Point)所服务的区域中，任何一个无线客户端都可以接受到此接入点的电磁波信号，这样就可能包括一些恶意用户也能接收到其他无线数据信号。这样恶意用户在无线局域网中相对于在有线局域网当中，去窃听或干扰信息就来得容易得多。

WLAN所面临的安全威胁主要有以下几类：

2.1网络窃听

一般说来，大多数网络通信都是以明文（非加密）格式出现的，这就会使处于无线信号覆盖范围之内的攻击者可以乘机监视并破解（读取）通信。这类攻击是企业管理员面临的最大安全问题。如果没有基于加密的强有力的安全服务，数据就很容易在空气中传输时被他人读取并利用。

2.2 AP中间人欺骗

在没有足够的安全防范措施的情况下，是很容易受到利用非法AP进行的中间人欺骗攻击。解决这种攻击的通常做法是采用双向认证方法（即网络认证用户，同时用户也认证网络）和基于应用层的加密认证（如HTTPS＋WEB）。

2.3 WEP破解

现在互联网上存在一些程序，能够捕捉位于AP信号覆盖区域内的数据包，收集到足够的WEP弱密钥加密的包，并进行分析以恢复WEP密钥。根据监听无线通信的机器速度、WLAN内发射信号的无线主机数量，以及由于802.11帧冲突引起的IV重发数量，最快可以在两个小时内攻破WEP密钥。

2.4 MAC地址欺骗

即使AP起用了MAC地址过滤，使未授权的黑客的无线网卡不能连接AP，这并不意味着能阻止黑客进行无线信号侦听。通过某些软件分析截获的数据，能够获得AP允许通信的STA□

MAC地址，这样黑客就能利用MAC地址伪装等手段入侵网络了。

3 .WLAN业界的安全技术

早期的无线网络标准安全性并不完善，技术上存在一些安全漏洞。但是另一方面，由于WLAN标准是公开的，随着使用的推广，更多的专家参与了无线标准的制定，使其安全技术迅速成熟起来。现在不只是在家庭，学校，中小企业里边WLAN

得到广泛的应用，在安全最敏感的大企业，大银行户头(例如全球财富500强)，政府机构，WLAN的安全可靠性也得到了认可，并大量地推广使用。

具体地讲，为了有效保障无线局域网(WLAN)的安全性，就必须实现以下几个安全目标：

1.提供接入控制:验证用户，授权他们接入特定的资源，同时拒绝为未经授权的用户提供接入；

2.确保连接的保密与完好:利用强有力的加密和校验技术，防止未经授权的用户窃听、插入或修改通过无线网络传输的数据；

3.防止拒绝服务(DoS)攻击:确保不会有用户占用某个接入点的所有可用带宽，从而影响其他用户的正常接入。

无线局域网的安全技术这几年得到了快速的发展和应用。下面是业界常见的无线网络安全技术:

- 服务区标识符(SSID)匹配；
- 无线网卡物理地址(MAC)过滤；
- 有线等效保密(WEP)；
- 端口访问控制技术(IEEE802.1x)和可扩展认证协议(EAP)；
- WPA (Wi-Fi 保护访问) 技术；
- 高级的无线局域网安全标准—IEEE 802.11i；

3.1 SSID

SSID(Service Set Identifier)将一个无线局域网分为几个不同的子网络，每一个子网络都有其对应的身份标识(SSID)，只有无线终端设置了配对的SSID才接入相应的子网络。所以可以认为SSID是一个简单的口令，提供了口令认证机制，实现了一定的安全性。但是这种口令极易被无线终端探测出来，企业级无线应用绝不能只依赖这种技术做安全保障，而只能作为区分不同无线服务区的标识。

3.2 MAC地址过滤

每个无线工作站网卡都由唯一的物理地址（MAC）标识，该物理地址编码方式类似于以太网物理地址，是48位。网络管理员可在无线局域网访问点AP中手工维护一组（不）允许通过AP访问网络地址列表，以实现基于物理地址的访问过滤。

MAC地址过滤的好处和优势

- 简化了访问控制
- 接受或拒绝预先设定的用户
- 被过滤的MAC不能进行访问
- 提供了第2层的防护

MAC地址过滤的缺点

- 当AP和无线终端数量较多时，大大增加了管理负担
- 容易受到MAC地址伪装攻击

3.3 802.11 WEP

WEP

IEEE80211.b标准规定了一种被称为有线等效保密（WEP）的可选加密方案，其目的是为WLAN提供与有线网络相同级别的安全保护。WEP是采用静态的有线等同保密密钥的基本安全方式。静态WEP密钥是一种在会话过程中不发生变化也不针对各个用户而变化的密钥。

WEP的好处和优势

WEP在传输上提供了一定的安全性和保密性，能够阻止有意或无意的无线用户查看到在AP和STA之间传输的内容，其优点在于：

- 全部报文都使用校验和加密，提供了一些抵抗篡改的能力
- 通过加密来维护一定的保密性，如果没有密钥，就难把报文解密
- WEP非常容易实现
- WEP为WLAN应用程序提供了非常基本的保护

WEP的缺点

- 静态WEP密钥对于WLAN上的所有用户都是通用的

  这意味着如果某个无线设备丢失或者被盗，所有其他设备上的静态WEP密钥都必须进行修改，以保持相同等级的安全性。这将给网络的管理员带来非常费时费力的、不切实际的管理任务。

- 缺少密钥管理

  WEP标准中并没有规定共享密钥的管理方案，通常是手工进行配置与维护。由于同时更换密钥的费时与困难，所以密钥通常长时间使用而很少更换。

- ICV算法不合适

  ICV是一种基于CRC-32的用于检测传输噪音和普通错误的算法。CRC-32是信息的线性函数，这意味着攻击者可以篡改加密信息，并很容易地修改ICV，使信息表面上看起来是可信的。

- RC4算法存在弱点

在RC4中，人们发现了弱密钥。所谓弱密钥，就是密钥与输出之间存在超出一个好密码所应具有的相关性。攻击者收集到足够使用弱密钥的包后，就可以对它们进行分析，只须尝试很少的密钥就可以接入到网络中。

- 认证信息易于伪造

  基于WEP的共享密钥认证的目的就是实现访问控制，然而事实却截然相反，只要通过监听一次成功的认证，攻击者以后就可以伪造认证。启动共享密钥认证实际上降低了网络的总体安全性，使猜中WEP密钥变得更为容易。

WEP2

为了提供更高的安全性，WiFi工作组提供了WEP2技术，该技术相比WEP算法，只是将WEP密钥的长度由40位加长到128位，初始化向量IV的长度由24位加长到128位。然而WEP算法的安全漏洞是由于WEP机制本身引起的，与密钥的长度无关，即使增加加密密钥的长度，也不可能增强其安全程度。也就是说WEP2算法并没有起到提高安全性的作用。

3.4 802.1x/EAP用户认证

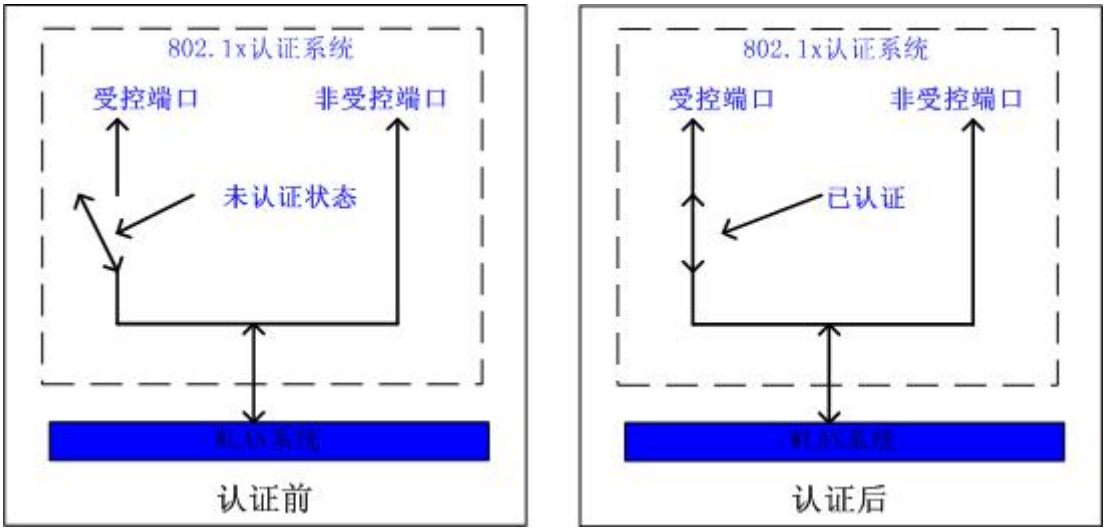
802.1x认证技术

802.1x是针对以太网而提出的基于端口进行网络访问控制的安全性标准草案。基于端口的网络访问控制利用物理层特性对连接到LAN端口的设备进行身份认证。如果认证失败，则禁止该设备访问LAN资源。

尽管802.1x标准最初是为有线以太网设计制定的，但它也适用于符合802.11标准的无线局域网，且被视为是WLAN的一种增强性网络安全解决方案。802.1x体系结构包括三个主要的组件：

- **请求方（Supplicant）**：提出认证申请的用户接入设备，在无线网络中，通常指待接入网络的无线客户机STA。
- **认证方（Authenticator）**：允许客户机进行网络访问的实体，在无线网络中，通常指访问接入点AP。
- **认证服务器（Authentication Sever）**：为认证方提供认证服务的实体。认证服务器对请求方进行验证，然后告知认证方该请求者是否为授权用户。认证服务器可以是某个单独的服务器实体，也可以不是，后一种情况通常是将认证功能集成在认证方Authenticator中。

802.1x草案为认证方定义了两种访问控制端口：即"受控"端口和"非受控"端口。"受控端口"分配给那些已经成功通过认证的实体进行网络访问；而在认证尚未完成之前，所有的通信数据流从"非受控端口"进出。"非受控端口"只允许通过802.1X认证数据，一旦认证成功通过，请求方就可以通过"受控端口"访问LAN资源和服务。下图列出802.1x认证前后的逻辑示意图。



802.1x技术是一种增强型的网络安全解决方案。在采用802.1x的无线LAN中，无线用户端安装802.1x客户端软件作为请求方，无线访问点AP内嵌802.1x认证代理作为认证方，同时它还作为Radius认证服务器的客户端，负责用户与Radius服务器之间认证信息的转发。

802.1x认证一般包括以下几种EAP(Extensible Authentication Protocol)认证模式：

- EAP-MD5
- EAP-TLS(Transport Layer Security)
- EAP-TTLS(Tunnelled Transport Layer Security)
- EAP-PEAP(Protected EAP)
- EAP-LEAP(Lightweight EAP)
- EAP-SIM

802.1x认证技术的好处和优势

- 802.1x协议仅仅关注受控端口的打开与关闭；
- 接入认证通过之后，IP数据包在二层普通MAC帧上传送；

- 由于是采用Radius协议进行认证，所以可以很方便地与其他认证平台进行对接；
- 提供基于用户的计费系统。

802.1x认证技术的缺点

- 只提供用户接入认证机制。没有提供认证成功之后的数据加密。
- 一般只提供单向认证
- 它提供STA与RADIUS服务器之间的认证，而不是与AP之间的认证
- 用户的数据仍然是使用的RC4进行加密。

3.5 WPA(802.11i)

802.11i——新一代WLAN安全标准

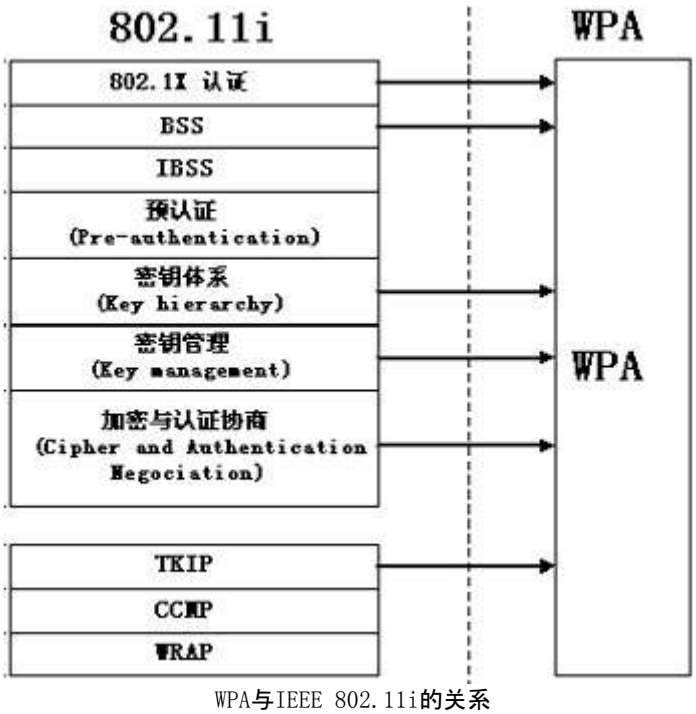
为了使WLAN技术从安全性得不到很好保障的困境中解脱出来，IEEE 802.11的i工作组致力于制订被称为IEEE 802.11i的新一代安全标准，这种安全标准是为了增强WLAN的数据加密和认证性能，定义了RSN（Robust Security Network）的概念，并且针对WEP加密机制的各种缺陷做了多方面的改进。

IEEE 802.11i规定使用802.1x认证和密钥管理方式，在数据加密方面，定义了TKIP（Temporal Key Integrity Protocol）、CCMP（Counter-Mode/CBC-MAC Protocol）和WRAP（Wireless Robust Authenticated Protocol）三种加密机制。其中TKIP采用WEP机制里的RC4作为核心加密算法，可以通过在现有的设备上升级固件和驱动程序的方法达到提高WLAN安全的目的

。CCMP机制基于AES（Advanced Encryption Standard）加密算法和CCM（Counter-Mode/CBC-
MAC）认证方式，使得WLAN的安全程度大大提高，是实现RSN的强制性要求。

WPA——向IEEE 802.11i过渡的中间标准

然而，市场对于提高WLAN安全的需求是十分紧迫的，IEEE 802.11i的进展并不能满足这一需要。在这种情况下，Wi-Fi联盟制定了WPA（Wi-Fi Protected Access）标准。WPA是IEEE802.11i的一个子集，其核心就是IEEE 802.1x和TKIP。WPA与IEEE 802.11i的关系如下图所示。



WPA与IEEE 802.11i的关系

WPA采用了802.1x和TKIP来实现WLAN的访问控制、密钥管理与数据加密。802.1x是一种基于端口的访问控制标准。TKIP虽然与WEP同样都是基于RC4加密算法，但却引入了4个新算法：

- 扩展的48位初始化向量（IV）和IV顺序规则（IV Sequencing Rules）；
- 每包密钥构建机制（per-packet key construction）；

- Michael（Message Integrity Code，MIC）消息完整性代码;
- 密钥重新获取和分发机制。

WPA系统在工作的时候，先由AP向外公布自身对WPA的支持，在Beacons、Probe Response等报文中使用新定义的WPA信息元素（Information Element），这些信息元素中包含了AP的安全配置信息（包括加密算法和安全配置等信息）。STA根据收到的信息选择相应的安全配置，并将所选择的安全配置表示在其发出的Association Request和Re-Association Request报文中。WPA通过这种方式来实现STA与AP之间的加密算法以及密钥管理方式的协商。

在STA以WPA模式与AP建立关联之后，如果网络中有RADIUS服务器作为认证服务器，那么STA就使用802.1x方式进行认证；如果网络中没有RADIUS，STA与AP就会采用预共享密钥（PSK，Pre-Shared Key）的方式。

在WPA中，AP支持WPA和WEP无线客户端的混合接入。在STA与AP建立关联时，AP可以根据STA的Association Request中是否带有WPA信息元素来确定哪些客户端支持使用WPA。但是在混合接入的时候，所有WPA客户端所使用的加密算法都得使用WEP，这就降低了无线局域网的整体安全性。

尽管WPA在安全性方面相较WEP有了很大的改善和加强，但WPA只是一个临时的过渡性方案，在WPA2（802.11i）中将会全面采用AES加密机制机制。

4 .企业/校园无线网安全解决方案

4.1无线网安全性现状

分析企业对无线网络的需求特征，安全因素被放在了首位，因安全方面的担心而不愿采用Wi-Fi，是目前很多企业存在的现象。实际上，目前大多数企业或校园无线网络提供的安全性如何？能否满足企业或校园的需求呢？

由于历史原因，大多数企业或校园的无线局域网主要是依靠WEP方式对数据进行加密，数据加密后的微波信号即使被人截获，也不易破解，从而保证客户传输的数据安全性。但是WEP存在着不理想的地方：一是密钥共享。由于每个人都知道密钥，则密钥很容易泄漏不易管理。二是弱密钥缺陷，导致WEP不能很好地抵御密码学破解攻击。

其次，如果AP不做任何安全设定，则任何一个符合Wi-Fi的网卡都可以接入网络，所以大多数无线局域网的用户接入安全保障是采用MAC地址控制。但是这种接入控制方法对于大型企业或校园无线网，会存在管理麻烦、扩展能力受限制等问题。另外，黑客还可能会使用MAC欺骗技术入侵网络。

所以对于企业或校园无线网络系统，如果不从整体上进行规划和设计，只孤立地采用单一的某项安全技术是无法满足企业或校园的高安全性的要求的。反而会造成无线网络不安全的印象，导致不能充分利用无线网络所能提供的诸多特性和优点来进行资源共享和提高工作效率。下面就将介绍根据企业或校园无

线网络应用的需求和要达到的目标，整体规划设计的一套适用于企业及校园的无线安全解决方案。

4.2 解决方案概述

为了解决企业无线应用的首要难题——安全性，该解决方案采用了WPA安全架构的设计。同时，为了向企业外部来访的用户提供无线接入的灵活性和方便性，该方案还应用了基于英特尔架构的无线网络控制器（WNC）和支持多SSID的AP（Cisco 1100/1230），使企业无线网络在保证企业信息安全的前提下，对多种接入认证方式提供了必要的支持。为了使无线网络系统能满足企业或校园在功能性、灵活性和可扩展性方面的众多需求，中采用Ocamar WNC（昂科无线网络控制器）作为无线网络管理和控制设备。昂科WNC除了实现了AC设备应该具备的接入控制、身份认证等功能，还能够向企业提供策略路由、流量控制、无线设备管理、用户管理和计费等极具价值的功能，这使其成为对企业和校园无线应用架构起关键作用的设备。

上海交通大学无线网案例

下面以上海交通大学校园无线网项目为例，具体地阐述典型的企业及校园无线解决方案：

上海交通大学是我国历史最悠久的高等学府之一。近年来，随着学校教学规模逐步扩大，除拥有古色古香的百年徐家汇老校区外，还有现代化闵行新校区以及法华镇路校区、上中校区、七宝校区等五个位于上海不同位置的校区。

由于存在不同地点的校区，交大的教员和学生不得不在不同的校区来回，同时教学场所也经常在各校区之间变换。这让校园网络出现了难题:

1□ 如何在不大幅度提高成本的情况下，校园网络覆盖五个不同位置的校区？

2□ 如何在校园的各个教学场所之间，提供无缝的网络连接，完成教学任务？

3□ 如何连接五个不同位置的校区，同时又提供足够的安全特性，保证安全通畅的网络连接？

4□ 如何充分利用现有的资源，帮助教员和学生利用现代互联网技术，提高教学效率和学习效率？

针对学校面临的以上难题，对无线网络解决方案的要求确定如下：

1. 无线网络信号覆盖五个不同位置的校区；
2. 提供无缝的互联网IP连接特性，保持教学网络在校园之间无缝漫游；
3. 保障无线网络安全性，对用户和资源访问权限进行管理；
4. 对不同的无线用户提供不同的接入认证方式，并对其应用合适的路由策略；
5. 普及基于无线连接的笔记本电脑，充分提高教学和学习效率。

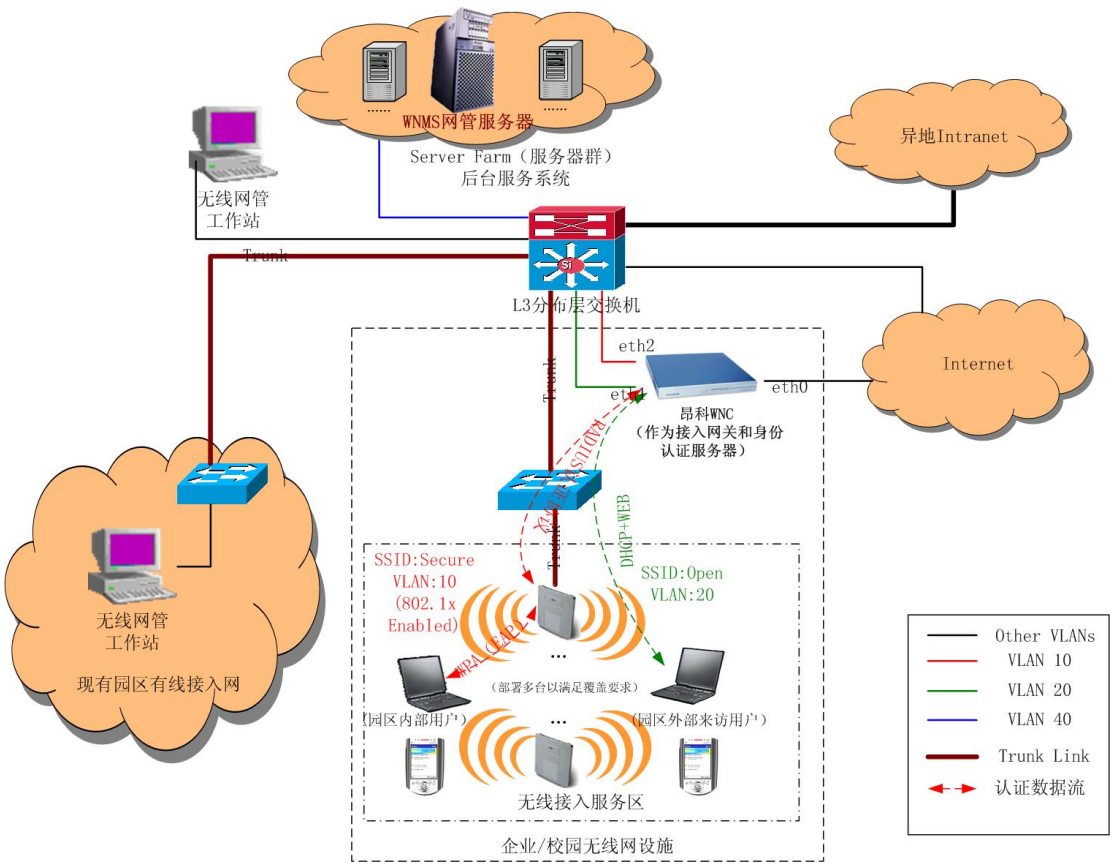
为让网络应用的价值最大化，从而为上海交通大学五个分散的校区内构建一个统一的、易接入、稳定安全的校园无线网络环境。针对解决方案的要求，经过多次比较和反复技术论证，决定为上海交通大学无线网络采用以下的解决方案：

1. 全面采用基于英特尔公司迅驰移动技术的笔记本电脑作为无线终端，提高教与学的效率和移动便利，同时保证高速的互联网接入；

2. 采用符合802.11标准及通过Wi-Fi认证的无线网络产品，核心安全架构采用WPA标准；
3. 采用具有多SSID和VLAN特性的Cisco Aironet 1200系列AP进行基础覆盖；
4. 采用昂科WNC无线网络接入控制器作为无线校园网的安全接入产品，为网络安全和扩展提供保证；
5. 采用昂科WNMS无线网络管理系统，对整个无线网络的基础设施、用户、安全策略和相关资源进行统一管理和监控。

该解决方案还使得上海交大整个校园无线网络具有高度可扩展性和可升级性，为将来实现网络升级和扩展提供了极高的资源保护。整个方案由昂科信息技术（上海）公司提供系统集成和方案实施。

昂科信息技术（上海）有限公司在充分了解上海交大现有网络建设后，针对上海交大的实际情况，提出了校园无线网络的整体解决方案。具体方案如拓扑图所示：



如图，各无线覆盖区域的AP就近接到接入层交换机上。因为存在校内教师、学生和校外来访用户等不同的无线用户群，出于不同用户群对安全性、易用性要求不同的考虑，采取802.1x和WEB认证相结合的方式来提供用户身份认证。为了区分这两种接入方式并将其分别关联到一个对应的VLAN，采用了支持多SSID（Multi-SSID）和802.1q VLAN特性的Cisco Aironet 1200 系列AP。

对于在校内的学生和教师用户，将采用符合WPA安全架构的802.1x标准认证的接入方式，认证通过的用户将获得一个每用户唯一的主密钥，通过该主密钥客户端和负责接入的AP将根据TKIP方法动态生成每数据包唯一的加密密钥，通信双方以此进行通信加密。在校园有线网L3分布层交换机上配置VLAN的子接口，利用该子接口作为这个SSID所代表的VLAN的网关，对其进行路由转发。从而使通过认证的企业内部用户能够如同用有线接入一样访问整个企业网络，但是由

于对无线通信进行了动态加密，保证了校园的敏感数据在空中传输的安全，有效地解决了校园无线应用的首要问题。

对于用WEB方式认证的校外来访用户，当利用基于英特尔公司迅驰移动技术的笔记本电脑连接上无线接入点后，可以通过AC设备的DHCP服务或企业的专用DHCP服务器获得IP地址、网关和DNS信息，无须安装客户端软件，直接利用浏览器就可以通过充当WNC设备进行WEB方式认证，认证通过后就可以接入到Internet。为保证整个园区网络的安全性，对于该SSID接入的用户必须以WNC作为其网关设备，所以L3分布层交换机无须对该SSID所代表的VLAN进行路由转发，从而统一该虚网的出口为昂科AC2010无线网络控制器。

如果这些用户需要访问校园内部网络，可以通过在这一WNC设备上启用用户级的策略路由来实现。这样在保证一定安全性的基础上方便了来访用户或漫游用户的接入，提高了无线网络的易用性和灵活性。

4.3 解决方案特点

4.4.1安全性高

这套专门为大中型企业和校园定制的无线局域网系统支持符合WPA安全架构的802.1x认证方式，

借助TKIP技术动态生成的数据加密密钥使空中无线数据通信如同在一条加密隧道中传输，保证了信息传输的高安全性。

而且通过利用Ocamar

WNC灵活的配置方式和支持多种认证接入方法的特性，还支持Web方式认证以

及无线链路层的VPN加密方式PPTP、L2TP，以及支持协议过滤、策略路由、流量控制等访问控制策略，过滤掉非法的用户访问，确保网络的安全。

4.4.2支持多SSID和VLAN划分

Cisco Aironet 1200系列AP支持多SSID特性，
每一个都可以映射到有线网络的一个VLAN，将符合802.1q标准的VLAN
延伸到无线网络上。网络管理员可以将无线网络上用户分组和网络分段管理与有限网络一同规划，大大减轻了管理负担、保证了企业安全策略的一致性。

4.3.4利用策略路由进行访问控制

昂科WNC的策略路由功能对于拥有多个网络出口、多种用户群体的企业或组织机构有相当的应用价值。针对不同的用户采用不同的路由策略，可以很好地划分和引导用户数据流，便于管理和资源分配。在企业中，策略路由功能更是可以用来区分用户权限级别，以限制不同的用户访问不同的网络，从而强化了企业信息系统的安全性。

比如交大无线校园解决方案中，学校的网络有两个出口，一个连到中国教育科研网（CERNET），另一个与Internet相连。该案例中将校园无线用户分成两类，一是教师用户，一是学生用户。为了让学生能通过教育网与其他高校的师生进行交流，但是又不想Internet上的垃圾信息和不良网站干扰学生的正常网上生活，就可以设置学生用户的下一跳路由到CERNET，而教师用户的下一跳则是路由到Internet出口，从而实现了不同无线用户群体的访问需求。

4.3.5流量控制保证用户带宽

□□通过Ocamar

WNC的流量控制功能将不同用户的带宽按不同需要进行管理，保证某些重要用户的带宽，从而保证了任务关键性的无线企业应用的畅通，有效防止了带宽过量占用的拒绝服务攻击。

4.3.6 AP管理和用户管理

通过Ocamar

WNC的AP管理功能，可以对其下所连的AP作为一个网络单元进行管理，结合昂科WNMS网管系统还可以将Ocamar

WNC作为SNMP代理对这些AP进行管理。另外，Ocamar

WNC还提供完善的用户管理，无线网络管理员可以通过“Web Manager”图形化配置界面，方便地填加、删除用户，或对用户的接入控制属性进行设置，定制用户级别的接入控制策略。

4.3.4支持漫游用户

当企业或校园里的终端用户在移动中进行网络通信时，用户可能会在AP之间漫游，甚至跨越不同的IP子网，无线接入点必需瞬间完成客户的重新认证和密钥分配，并为客户建立由所在网段的AP提供通往原网段AP的隧道，继续保持用户的通话。该方案通过采用符合Wi-Fi认证标准的无线接入产品，以及功能强大、能提供移动IP和策略路由支持的Ocamar WNC，将使各种漫游用户在异地无线接入仍能顺利访问到原地网络。

4.3.7无线网络管理

该无线解决方案通过采用Ocamar WNMS，能够把各无线局域网内的AP设备以及其相连的的运行状况实时纳入网管系统的管理范围；面向全网，为网络维护人员提供统一的、完备的全网视角，准确、快速把握全网的实时性能与潜在的问题，及时采取相应的措施确保企业WLAN的高可靠性。

采用一个完整的无线局域网网管系统WNMS。WNMS采用网络管理的标准协议SNMP对相关无线局域网设备进行配置、管理数据、性能数据、故障数据的采集和分析，同时也可通过WNMS对具体设备上的参数进行配置、调整、故障诊断。WNMS还提供拓扑发现、管理的功能，可以直观的反映出AC、AP和其他相关设备之间的对应关系。网络监视基于网络拓扑图进行，在性能、告警、配置等方面动态反映网络的变化,因此成为保障无线网络稳定运行不可缺少的重要组成部分。

4.4无线产品选型原则

目前在市面上销售的无线接入产品类型多种多样，就算无线芯片来自同一家厂商，产品的集成制造厂家和实现的方法也各不一样。所以为了保护投资以及确保产品的兼容性、互操作性和可扩展性，产品除了要求符合电气和电子工程师协会（IEEE）802.11系列标准，还应该一致选用符合Wi-Fi认证标准的无线产品。功能完备、安全性好、使用简易是规划一套信息系统基础设施的永恒目标，选择合适的产品将是实现这一目标的前提。上海交通大学无

线网络项目之所以成功，正是因为解决方案提供商昂科信息技术（上海）有限公司依据合理的产品选型原则，结合客户的需求选择了合适的无线产品和架构标准。

根据在无线接入网络系统中所扮演的角色的不同，接下来将从无线接入基础设施、无线终端设备、接入控制设备以及后台服务系统几个方面阐述产品选型需要考虑的要素和应该遵循的原则。

4.3.1无线接入基础设施

无线接入基础设施是实现无线网络覆盖的最基础的设备，这方面的产品的选型应该遵循以下的原则：

1、首先要根据应用需求确定无线接入设备的规格标准，如选用802.11系列的a、b或g标准；

2、确保所选用的产品都是通过Wi-Fi组织认证的；

3、根据特殊应用需求，选择合适的、提供这些应用支持的产品；

4、从产品可靠性、可扩展性、性能、成本和保护投资等方面综合考虑。

比如，选用Cisco Aironet 1200系列AP可以保护现有的和未来的网络基础设施投资。这种符合电气和电子工程师协会（IEEE）802.11b标准的接入点目前可以支持高达11Mbps的数据传输速率，并完全符合Wi-Fi认证标准，可以为想要采用WPA安全架构的企业用户提供安全的无线网络解决方案支持。

Cisco Aironet 1200系列的模块化设计可以实现单段和双段配置，以及可现场升级能力，一个单

独的接入点可以在提供一个802.11b波段传输的同时，为高速的802.11a提供另外一个无线电连接。Cisco Aironet 1200系列可以支持所有802.1X认证类型，包括EAP思科无线认证（LEAP）、EAP-TLS和利用EAP-TLS的类型，完全能够满足WPA标准的要求。

Cisco Aironet 1200系列的多SSID（Multi-SSID）特性为需要同时部署多种方式的无线接入方式的企业提供了最大的灵活性。使得企业将无线网络的认证方式从传统迁移到WPA标准变得更容易更灵活。多SSID特性结合VLAN技术，企业还可以部署针对不同用户群采用不同得认证方式的无线接入系统，可以同时满足企业高安全性的要求和来访用户简便接入的需求。

4.3.2无线终端设备

无线移动终端一般指的是用户直接使用并具有无线网络接入能力的数字终端，目前市面上主要有迅驰笔记本电脑、带有WLAN无线网卡的台式PC机、具有WLAN接入功能的PDA等等，甚至现在还有带WLAN通信功能的摄像、监控设备。选择这些设备也应该遵循符合Wi-Fi认证、可靠性高、使用方便的产品。

其中基于CMT（迅驰移动技术）的笔记本电脑是最广泛使用的WLAN终端，这项技术的采用与WLAN的应用部署几乎同步增长。迅驰移动技术是国际知名芯片设计制造商英特尔专为无线应用而设计的，采用这种创新技术的笔记本电脑将获得以下的特性：

- 集成的无线局域网连接能力；
- 突破性的移动计算性能；
- 延长的电池使用时间；

- 更轻、更薄的外形设计。

4.3.3无线接入控制设备

由于WLAN与其他有线网络间的明显区别，原则上都应该在WLAN与传统网络之间部署一种接入控制机制，以加强企业网络的安全性以及WLAN接入方式的灵活性。通常这种接入控制机制是由一种通称为接入控制器（AC）的设备来实现。

昂科无线网络控制器(Ocamar Wireless Network Controller，以下简称Ocamar WNC)就很好的实现了AC的各项功能定义，除了具有常用的身份认证、接入控制等AC的必备功能之外，还具有流量控制、策略路由等增值功能。昂科WNC提供了建立具备安全性、可升级性和对业务至关重要的802.11无线网络的基础。在无线以太网的核心部分，Ocamar
WNC提供包括严密的访问控制、集中式管理、无缝漫游等关键性服务，并且整合了计费功能。

4.3.4无线网络后台服务系统

基于英特尔体系结构的服务器为企业提供了构建高性能、高可用信息系统的基础设施平台。比如DHCP服务器、RADIUS服务器、WEB服务器等企业信息化必备的组件都可以采用英特尔体系结构的服务器实现，利用这些基本组件可以实现WPA标准规定的系统性要求，并且为将来的扩展和升级提供了足够的空间和灵活性。

在硬件基础设施的基础上，同时也要选择合适的、功能完备、可靠性高的相关软

件系统，如无线网络管理系统、身份验证系统等等。比如选用Ocamar WNMS无线网络管理系统就能对无线网基础设施进行有效的管理，因为该系统具有设备配置和性能管理、负载均衡、故障预警、故障告警等功能，对简化网络管理负担都是非常有价值的。

5.结论

WLAN技术是当今世界上最令人振奋的、全新的无线技术之一。实现了无论是在工作中、在家中，还是国内外旅行中的安全的、健壮的高速无线访问。现在有笔记本电脑、PDA支持它，而且马上将被手机支持。该技术的采用正快速地在很多地方增长，包括企业、机场、医院、酒店、家庭、餐馆、咖啡厅、仓库，甚至也应用在停车场和汽车站，让人们能随时与同事和家人保持联系，从而更大的提升自由度和工作效率。

无论是企业、运营商还是个人用户，如果能构建符合标准、易于使用且属于自己的WLAN设施，将能强占先机、提高效率和降低成本。特别是对于企业，如果能按照Wi-Fi组织定义的安全标准实施企业WLAN，那么将对企业信息化应用产生极大的价值。采用文中安全解决方案中描述的WLAN安全架构，并灵活运用符合Wi-Fi认证要求的产品来搭建WLAN系统，将是迈向最终实现安全接入、无缝漫游的踏脚石。

昂科信息技术（上海）有限公司采用了基于英特尔公司迅驰移动技术的笔记本电脑以及思科功能齐全、性能稳定的无线接入点产品，并结合昂科WNC无线网络控制器和WNMS网管软件系统来构架交大无线网解决方案。这些要素构成

了上海交通大学无线校园网络的最佳平台和框架，它提供了无线、移动、高速和安全的互联网连接，帮助上海交通大学成为中国最成功的校园网实施案例。同时，该案例中的解决方案也成为值得其他大中型企业和学校在部署无线网络之前应借鉴的成功典范。