

无线网络的构建和安全策略研究

许高建

(安徽农业大学 信息与计算机学院, 安徽 合肥 230036)

摘要:随着现代化通讯工具的发展,人们对通讯设备之间互联互通的需求日益增加。目前许多通讯设备都是基于某种特定的技术规格设计和生产的,是独立的,它们往往只能和其配套的伙伴产品相互兼容,而无法与其他设备互联互通。近来一些公共场所开始提供无线局域网服务,但如果用户使用的无线网卡和这些场所的设施不兼容,就很可能无法享受这些便利的通信服务。无线局域网能利用简单的存取构架让用户随身、随时、随地获取信息。文中主要讨论现在流行的无线局域网的构建、调试和维护,并介绍 WLAN 技术及在智能小区网络应用中的设计方案。详细说明无线网络的安全防护和维护,无线访问控制和安全解决方案的实施。

关键词:WLAN; 802.11; 无线适配器; 安全策略

中图分类号:TN925+.93

文献标识码:A

文章编号:1673-629X(2007)07-0156-04

Research on Constructing Wireless Network & Safety Tactic

XU Gao-jian

(School of Information Technology, Anhui Agricultural University, Hefei 230036, China)

Abstract: As the development of modern communication devices, the demands that those devices can communicate each other are increasing. At present, most of those devices are designed and produced in some specifical technique. They are unattached. They are compatible with their associated products sometimes. Now some wireless network services are provided in public. But if the wireless network adapter isn't compatible with the devices there, they can't achieve the convenience of communication. Wireless network can use simple store-fetch structure to get information anywhere or anytime. The article talks over the prevalent construction, debugging, and maintenance on wireless network mainly. It discusses the techniques of WLAN and designation of applied in intelligence residential area briefly. It also describes the safety defending and maintenance about wireless network. And wireless visit control, the safety-solve way are put in practice.

Key words: WLAN; 802.11; wireless adapter; safety tactic

0 引言

WLAN 为 Wireless Local Area Networks 的简称,即无线局域网。它是一种借助无线技术取代以往有线网络的新手段,可提供传统有线局域网的所有功能。WLAN 是计算机网络与无线通信技术相结合的产物,是通用无线接入的一个子集,可支持较高的传输速率(可达 2~108Mbps)。利用射频无线正交频分复用(OFDM),借助直接序列扩频(DSSS)或跳频扩频(UWB)技术^[1],可实现固定的、半移动的以及移动的网络终端对因特网进行较远距离的高速连接访问。

智能小区^[2]的设计方案是基于小区进行设计,无

线网络的覆盖面较大,硬件设备的要求较高,需要全方向天线和定向引向反射天线配合使用。在小区中还必须配有大量的 AP,保证用户在任何时间、任何地点都可以使用无线网络。这样的设计需要对网络进行合理的规划,硬件和系统配置要合理。在客户端和网络之间采用 MAC 地址访问控制和安全 VPN 应用软件,再结合无线网络间的 128 位 WEP 加密机制,可以确保最大程度的安全。

1 WLAN 的基本结构和相关术语

1.1 无线网络技术简介

随着网络的飞速发展,笔记本电脑的普及,人们对移动办公的要求越来越高。传统的有线局域网要受到布线的限制,如果建筑物中没有预留的线路,布线以及调试的工程量将非常大,而且线路容易损坏,给维护和扩容等带来不便,网络中的各节点的搬迁和移动也非

收稿日期:2006-09-22

基金项目:安徽省高校省级自然科学基金项目(2006KJ168B)

作者简介:许高建(1974-),男,安徽肥东人,讲师,研究方向为计算机应用、计算机网络。

常麻烦。因此高效快捷、组网灵活的无线局域网应运而生。

无线局域网是利用无线技术实现快速接入以太网的技术。综观现在的市场,IEEE 802.11b^[3]技术在性能、价格各方面均超过了蓝牙、HomeRF 等技术,逐渐成为无线接入以太网应用最为广泛的标准。

1.2 无线网络的优势

与有线网络相比,WLAN 最主要的优势在于不受布线条件的限制,因此非常适合移动办公用户的需要,具有广阔市场前景。目前它已经从传统的医疗保健、库存控制和管理服务等特殊行业向更多行业拓展开去,甚至开始进入家庭以及教育机构等领域。IEEE 802.11 规定的发射功率不可超过 100mW,实际发射功率约 60~70mW,而手机的发射功率约 200mW 至 1W 间,手持式对讲机高达 5W。而且无线网络使用方式并非像手机直接接触人体,因此是安全的。

1.3 无线网络的协议

最常见的有 IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g。其中:IEEE 802.11 是 IEEE (电气和电子工程师协会)最初制定的一个无线局域网标准。IEEE 802.11b 又被称为 Wi-Fi^[3],使用开放的 2.4GHz 直接序列扩频,最大数据传输速率为 108Mbps,也可根据信号强弱把传输率调整为 54Mbps、11Mbps、5.5Mbps、2Mbps 和 1Mbps 带宽。无需直线传播传输范围为室外最大 300m,室内有障碍的情况下最大 100m,是现在使用的最多的传输协议。

1.4 无线局域网的工作模式

无线局域网的工作模式一般分为两种:Infrastructure 和 Ad-hoc。Infrastructure 是指通过 AP(Access Point)互连的工作模式,也就是可以把 AP 看作是传统局域网中的 Hub(集线器);Ad-hoc 是一种比较特殊的工作模式,它通过把一组需要互相通讯的无线网卡的 ESSID 设为同值来组网,这样就可以不必使用 AP,构成一种特殊的无线网络应用模式。几台计算机装上无线网卡,即可达到相互连接、资源共享的目的。

1.5 WLAN 的基本构件

一般架设无线网络的基本配备就是无线网卡及一台 AP,如此便能以无线的模式,配合既有的有线架构来分享网络资源。如果只是几台电脑的对等网,也可不要 AP,只需要每台电脑配备无线网卡。AP 为 Access Point 简称,一般翻译为“无线访问节点”,或“桥接器”。它主要在媒体存取控制层 MAC 中扮演无线工作站及有线局域网的桥梁。有了 AP,就像一般有线网络的 Hub 一般,无线工作站可以快速且轻易地与网络相连。

2 智能小区的设计方案和实施

2.1 应用需求分析

根据提供的资料分析,宽带已接入到小区的网络中心(100M),小区内的 8 幢住宅楼没有宽带接入,共有 800 户居民,楼内居民户数一般在 100 户以内,只有 1 幢超过 100 户(175 户),为了保证用户网上冲浪、视频点播,网络中心与住宅楼采用点对点的无线接入,无线接入设备采用 IEEE 802.11b 标准,为数据流量提供了 11Mbps 的数据速率,其传送信息的速度要快于租赁的 T1 线路(1.544Mbps),高于一条 E1 线路(2Mbps),传输距离最远达 30km。楼内用户通过架设的无线设备,使居民无论是在楼前的花园还是家里,没有上网时间、地点的限制,只需插入笔记本电脑一张小小的无线网卡,即可随时随地上网,享受网络服务。

2.2 小区无线网络方案设计说明

本套方案的无线产品采用 Z-COM 公司的 AP 和无线网卡。AP 用 XI-1500 系列,无线网卡用 XI-300、XI-600、XI-750、XI-800 系列。台式机的无线网卡用 XI-750(USB)系列或 XI-600(PCI→PCMCIA)+XI300 系列;笔记本电脑网卡用 XI-300;掌上电脑用 XI-800 系列。使用有线接入,存在布线困难、施工不便、费用高、周期长等问题,所以,本方案从宽带接入到用户终端使用的连接方式均采用无线方式。

各住宅楼间的 AP,若放在室内,则有破坏原建筑物、增加室内 AP 的数量、布线难度加大、施工周期加长等缺点。所以,计划将住宅楼间的 AP 放在室外。中心站点设在主楼,AP 放在楼顶。主楼和住宅楼通过 AP XI-1500 通信。住宅楼顶的 AP 与住宅楼间的 AP 连接。用户在终端设备装上无线网卡,即可自由访问 Internet。

2.3 流量分析

宽带的总流量为 100Mbps,每个 AP 的总流量为 11Mbps,8 个仅需 88Mbps,宽带流量完全能满足 AP 的流量需求。本小区是 8 幢 800 户,假设每幢楼有 100 户,使用率 100%,每幢楼同时上网人数假设有 80 人,每人的传输速率约 140kbps。所以,住宅楼间装有 AP 的住宅楼顶只需 1 个 11Mbps 的 AP,足可满足用户要求。

2.4 中心机房网络设计

中心机房^[4]的无线网络接入情况如图 1 所示。其中,电信宽带 100Mbps 到小区,接到中心机房的代理服务器,百兆口的交换机也与代理服务器连接,主楼的 AP 直接连到交换机即可。代理服务器(proxy),PC 机+proxy,代理服务器装上防火墙、计费软件及其它管理软件,便可实现对小区的无线局域网进行管理,既能

防止非法用户登陆本网络,又能对无线终端进行计费。

百兆交换机(switch)提供了所有与之连接的 AP 共享 100Mbps 频宽。switch 的位置可以根据实际情况放置,若主楼顶有电源等设备的控制室,可以考虑将 switch 放到楼顶。switch 使用的是 8 口交换机。

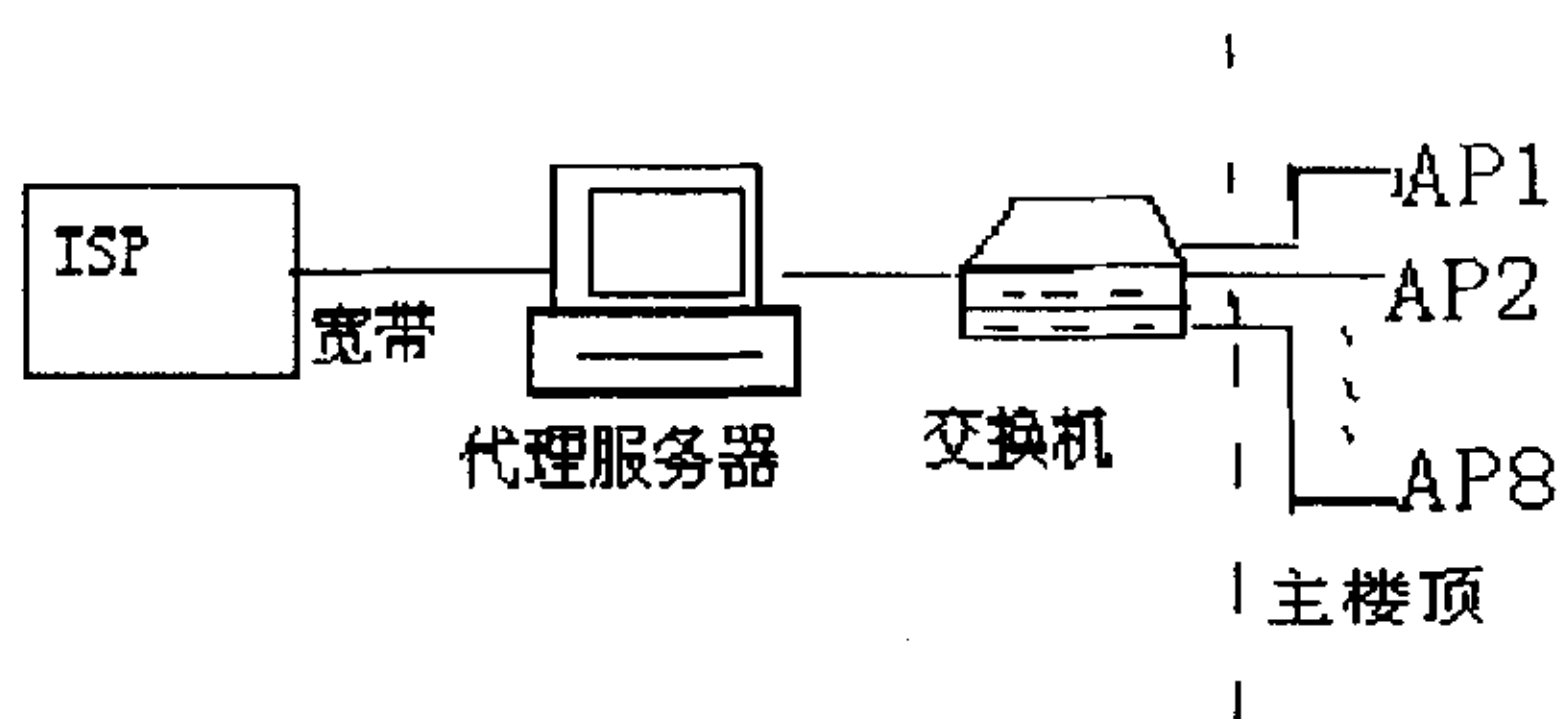


图 1 中心机房结构图

2.5 主楼和住宅楼的网络设计

宽带接入在主楼的中心机房,将中心机房设为中心接入点,通过中心接入点将宽带连接到各住宅的楼顶 AP。由于 1 个 AP 最高传输速率为 11Mbps,所以主楼用 1 个 AP 不能满足用户的上网要求。根据实际需要,设计如下:主楼有 6 个 AP 共享 100Mbps 的带宽,8 幢中的 6 幢住宅楼顶各用 1 个 AP。为了确保用户的通信质量,主楼与住宅楼均采用 24dBi 的网状定向天线。AP 均放在楼顶。

2.6 住宅楼的无线网络设计

8 幢住宅楼的网络结构是一样的,只是建筑面积有点差别。为了扩大覆盖面,住宅楼间的 AP 均采用全向天线,根据实际要求可在 5dBi~10dBi 范围内选择。每幢住宅楼间的 AP 通过 1 个 4 口的 Hub 与各自楼顶的 AP 连接。

2.7 网络的配置

小区使用的是商业 DSL 服务,它将为用户提供一套固定的 IP 地址。并且有路由器和防火墙提供一些安全功能,当无线用户连到网络时,需要网络地址转换和 DHCP 服务对之进行配置。配置过程中,还需要配置网络地址转换、网关地址、子网以及 DNS 服务器等信息。以下是配置方案:

ISP 提供的 IP 地址为 60.166.44.165(然后这个地址作为客户端及其他设备连到它的网关地址);

ISP 提供的网关地址是 60.166.44.1(需服务商预先设置);

ISP 将 DNS 地址分配为 202.102.192.68 和 202.102.199.68;

下面可以配置 WLAN 访问点:

将无线局域网 WLAN 访问点的 WAN 网关地址设为 60.166.44.165;

将无线局域网 WLAN 访问点的 WAN IP 地址设为 60.166.44.165;

该地址也是唯一地确定所有到 Internet 的 WLAN 访问点,需要的时候可以追踪通信量;

将无线局域网 WLAN 访问点的 DNS 设置为 202.102.192.68 和 202.102.199.68;

配置 WLAN 访问点的路由器的 LAN 地址为 10.10.1.1;

配置 WLAN 访问点的路由器的 LAN 地址为 255.255.0.0;

配置 WLAN 访问点的路由器以提供 NAT,并让它作为一个 DHCP 地址;

配置 WLAN 访问点的路由器以发布足够的 DHCP 地址——根据小区的实际情况,需要同时满足 640 个人的上网需求。那么至少就需要 640 个 DHCP 地址;

将 WLAN 访问点的服务标识符 SSID 设为小区用户认可的名字;

使用 WEP 加密密码,对非法用户作点限制。

3 无线网络的安全防护和维护

3.1 无线网络的安全性

由于无线局域网采用公共的电磁波作为载体,更容易受到非法用户入侵和数据窃听。无线局域网必须考虑的安全因素有三个:信息保密、身份验证和访问控制^[5]。为了保障无线局域网的安全,主要有以下几种技术:

(1) 物理地址(MAC)过滤。

每个无线工作站的无线网卡都有唯一的物理地址,类似以太网物理地址。可以在 AP 中建立允许访问的 MAC 地址列表,如果 AP 数量太多,还可以实现所有 AP 统一的无线网卡 MAC 地址列表,现在的 AP 也支持无线网卡 MAC 地址的集中 Radius 认证。这种方法要求 MAC 地址列表必须随时更新,可扩展性差。

(2) 服务集标识符(SSID)匹配。

对 AP 设置不同的 SSID,无线工作站必须出示正确的 SSID 才能访问 AP,这样就可以允许不同的用户群组接入,并区别限制对资源的访问。

(3) 有线等效保密(WEP)。

有线等效保密协议是由 802.11 标准定义的,用于在无线局域网中保护链路层数据。WEP 使用 40 位钥匙,采用 RSA 开发的 RC4 对称加密算法,在链路层加密数据。WEP 加密采用静态的保密密钥,各无线工作站使用相同的密钥访问无线网络。WEP 也提供认证功能,当加密机制功能启用,客户端要尝试连接上 AP 时,AP 会发出一个 Challenge Packet 给客户端,客户端再利用共享密钥将此值加密后送回存取点以进行认证

比对,如果正确无误,才能获准存取网络的资源。40位 WEP 具有很好的互操作性,所有通过 Wi-Fi 组织认证的产品都可以实现 WEP 互操作。现在的 WEP 也一般支持 128 位的密钥,能够提供更高等级的安全加密。

3.2 WLAN 的防护

在明白了一个毫无防护的 WLAN 所面临的种种问题后,应该在问题发生之前作一些相应的应对措施,下面就是介绍针对各种不同层次的入侵方式时采取的各种应对措施。

在一个无任何防护的无线 LAN 前,要想攻击它的话,并不需要采取什么特别的手段,只要任何一台配置有无线网卡的机器就行了,能够在计算机上把无线网卡开启的人就是一个潜在的入侵者。在许多情况下,有人无心地打开了他们装备有无线设备的计算机,并且恰好位于你的 WLAN 覆盖范围之内,这样他们的机器不是自动地连接到了你的 AP,就是在“可用的”AP 列表中看到了它。其实,在平常的统计中,有相当一部分的未授权连接就是来自这样的情况,并不是别人要有意侵犯你的网络,而是有时无意中在好奇心的驱使下的行为而已。

(1)更改默认设置。

最基本的是要更改默认的管理员密码,而且如果设备支持的话,最好把管理员的用户名也一同更改。对大多数无线网络设备来说,管理员的密码可能是通用的,因此,一般情况下更改这个密码,使其他用户无法获得整个网络的管理权限。

(2)更新 AP 的 Firmware。

有时,通过刷新最新版本的 Firmware 能够提高 AP 的安全性,新版本的 Firmware 常常修复了已知的安全漏洞,并在功能方面可能添加了一些新的安全措施。

(3)屏蔽 SSID 广播。

许多 AP 允许用户屏蔽 SSID 广播,这样可防范 NetStumbler 的扫描,不过这也将禁止 Windows XP 的用户使用其内建的无线 Zero 配置应用程序和其他的客户端应用程序。

(4)关闭机器或无线发射。

关闭无线 AP,是一般用户来保护他们的无线网络所采用的最简单的方法,在无需工作的整个晚上的时间内,可以使用一个简单的定时器来关闭 AP。不过,如果拥有的是无线路由器的话,那因特网连接也被切断了,这倒也不失为一个好的办法。在不能够关闭因特网连接的情况下,就不得不采用手动的方式来禁止

无线路由器的无线发射了(当然,也要求无线路由器支持这一功能)。

(5)MAC 地址过滤。

MAC 地址过滤是通过预先在 AP 写入合法的 MAC 地址列表,只有当客户机的 MAC 地址和合法 MAC 地址表中的地址匹配,AP 才允许客户机与之通信,实现物理地址过滤。

(6)降低发射功率。

虽然只有少数几种 AP 拥有这种功能,但降低发射功率仍可有助于限制有意或偶然的未经许可的连接。但现在无线网卡的灵敏度在不断提高,甚至这样的网卡随便都可购买得到,特别是在一幢大楼或宿舍中尝试阻止一些不必要的连接时,这可能没什么实际意义了。

(7)使用一些应用程序对无线网络进行探测。

通常情况下,还可以用一些软件对无线网络进行监控或探测。NetStumbler 最经常使用的一种软件,是广泛应用于监测无线网络运行的工具。它对可以接受到的每一个无线访问点都提供了大量的数据,能显示运行中的无线设备的 MAC 地址、使用信道、信号强度、SSID 或者其中的缺陷,以及对某个特别访问点是否采取了编码。

4 小 结

无线局域网是相当便利的数据传输系统,它利用射频(Radio Frequency, RF)的技术,取代旧式碍手碍脚的双绞铜线(Coaxial)所构成的局域网络,使得无线局域网络能利用简单的存取架构让用户透过它,达到“信息随身化、便利走天下”的理想境界。主要介绍了智能小区无线局域网的组建和管理方法,及如何运用手中的软件和硬件设备达到局域网的最佳配置。对局域网的设备、术语和操作方法描述的较详细,具有一定的实用价值。

参考文献:

- [1] Aspinwall J. Installing, Troubleshooting and Repairing Wireless Networks[M]. 北京:电子工业出版社,2004.
- [2] 蔡一郎. Windows 2000 Server 网络技术与构架管理[M]. 北京:清华大学出版社,2002:302-378.
- [3] Lixing. 热门无线局域网标准的比较[EB/OL]. 2005-09-10. www.huawei-3com.com.
- [4] 胡道元. 计算机网络学习辅导[M]. 北京:清华大学出版社,2005:60-107.
- [5] Steinmetz R. 计算机通信与应用[M]. 北京:人民邮电出版社,2002.