摘 要

无线局域网是指以无线信道作传输媒介的计算机局域网络，是计算机网络与无线通信技术相结合的产物，它以无线多址信道作为传输媒介，提供传统有线局域网的功能，能够使用户真正实现随时、随地、随意的宽带网络接入。

目前 WLAN 虽然剪断了电缆的束缚，现在只是“半移动”状态，移动终端只能在同一个区域内随时随地接入 Internet，提供区域性的漫游功能。目前这种业务主要是在数据业务方面，而在对实时性要求较高的业务如语音，视频支持不好,因为目前 WLAN 不能平滑切换漫游。WLAN 最热门的一个课题是 VoWLAN(Voice over Wireless LAN)，VoWLAN 是 WLAN 的新兴应用之一，从技术层面来说，语音业务对于延迟敏感度远远高于数据业务。VoIP 是指 IP 电话通过数据网络传输语音信号。WLAN 能够无线上网。VoWLAN 可以说是这两者的有机结合，它可以利用现有的 WLAN 网络实现无线的 VoIP 通话能力。

本课题以 VoWLAN 为应用背景，通过改进 IAPP 负载均衡协议，并且进行预认证等方面改进 WLAN 的切换性能，使得切换漫游平滑。最后对 WLAN 的完全漫游进行了展望。

关键词：无线局域网；漫游；VoWLAN；负载均衡；预认证

Abstract

Wireless LAN is a Lan which uses wireless channels to transfer information, result from the combination of computer network and wireless communication. WLAN uses wirless multiple access as the transfer medium, it can server as what the Wired LAN do. Whenever and wherever are people able to obtain access to wide-band network through WLAN.

At present WLAN has unchained the cable, however, the terminal could access the network only when it moves in a certain area. WLAN is good at providing data service, however, it doesn't support the voice and video well which require real-time handling. The reason for this is that WLAN doesn't support well the switching and roaming of a STA from one Access Point to another. Voice over WLAN is a popular topic today, it is a new service of WLAN, and will be widely used all around the world. As refer to technology, voice service is more sensitive than data service. VoIP can transfer voice by using TCP/IP protocols, and We can access Internet through WLAN. VoWLAN is something that can provide the VoIP service through WLAN.

Throughout this paper, reference is made to the application of VoWLAN. In order to make the WLAN's switching and roaming more smoothly, this paper has made improvement of the load balance of IAPP, as well as pre-authentication is introduced.

Finally, in order to meet the requirement of completely roaming, mobile IP and MESH may be renewed.

Keywords: Wireless LAN; roaming; VoWLAN; load balance; pre-authentication

哈尔滨工程大学
学位论文原创性声明

本人郑重声明：本论文的所有工作，是在导师的指导下，由作者本人独立完成的。有关观点、方法、数据和文献的引用已在文中指出，并与参考文献相对应。除文中已注明引用的内容外，本论文不包含任何其他个人或集体已经公开发表的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

作者（签字）：

日期：2006年 1 月 9日

第1章 绪论

1.1 引言

局域网 LAN 是处于同一建筑，同一单位或方圆几千米区域内的专用网络。局域网常用于连接公司办公室或工厂里的个人计算机和工作站，以便共享资源(如打印机)和交换信息。局域网采用的传输媒介多为有线电缆或者光纤，这种局域网称为有线局域网局域网。有线局域网应用非常广泛，而且传输速率高，构建成本低。

随着社会对计算机依赖性的迅速增加，用户要求互连的计算机数量更多，类型也更为复杂。现代固态电子技术的发展，使人们可以根据不同的要求选择不同的网络方案，但传统有线网络由于受设计或环境条件的制约，在物理、逻辑和资金方面普遍存在着一系列问题，特别是当涉及到网络移动和重新布局时，所以发展一种可行的无线通信网络技术作为现有数据连接的扩充已成为一种需要。进入 90 年代以来，随着个人数据通信的发展，功能强大的便携式数据终端以及多媒体终端的广泛应用，为了实现任何人在任何时间、任何地点均能实现数据通信的目标，要求传统的计算机网络由有线向无线，由固定向移动，由单一业务向多媒体发展，更进一步推动了无线局域网(Wireless LAN，以下简称 WLAN)的发展。

1.2 课题来源、背景及意义

目前 WLAN 虽然剪断了电缆的束缚，现在只是“半移动”状态，移动终端只能在同一个区域内随时随地接入 Internet，提供区域性的漫游功能。但是目前这种业务主要是在数据业务方面，而在对实时性要求较高的业务如语音，视频支持不好。现在的发展目标，将是完全漫游的能力，即在以一定速度行进时，可无中断地收发数据，这将是实现个人通信网(PCN)的一条有效途径[1]。

WLAN 当前最热门的一个课题是 VoWLAN(Voice over WLAN)，VoWLAN 是

WLAN 的新兴应用之一，从技术层面来说，语音业务对于延迟敏感度远远高于数据业务。VoIP 是指 IP 电话通过数据网络传输语音信号。WLAN 能够无线上网。VoWLAN 可以说是这两者的有机结合，它可以利用现有的 WLAN 网络实现无线的 VoIP 通话能力，企业内部员工可以通过 VoWLAN 在办公场所以外的地方随时访问语音、E-mail 和其他已连的网络资源，这样提高了网络资源的利用率并降低了每次电话呼叫的成本，从而节省企业的总体 IT 费用。对于住宅用户也可以通过与宽带 802.11 无线网络相连的 VoIP 电话降低话费。

因此 WLAN 要承载更多的业务，必须实现全移动，必须实现优良的切换性能才可以。本课题就是基于这样的应用需求下提出的。

1.3 课题研究工作简介

课题主要以 VoWLAN 这样一个典型的应用背景，来实现 WLAN 的无缝切换。当前国内国外的 WLAN 的切换研究也是刚刚开始，IEEE 工作组制定了 802.11F 协议，阐述了接入点内部协议 IAPP(Inter-Access Point Protocol)。IAPP 协议解决了 STA 在子网内 AP 间漫游的部分问题，但是发生 AP 切换时，STA 的 QoS 也不能得到可靠地保证，因为 IAPP 协议只是解决了用户移动而带来的链路层通信的问题。本课题的主要工作是实现 IEEE 802.11F 的功能，并在此基础上进行有效的改进：引入“预认证”措施，解决了当前安全认证所带来的一个负面效应—切换延时过大，从而容易导致业务中断；引入 MESH、移动 IP 技术解决了 WLAN 跨网段 IP 地址需要改变的问题，保证在高度分割的网络内切换保持平滑连续。

1.4 论文组织结构

本论文分为四章，按如下方式组织：

第一章是本论文的引言部分，介绍了 WLAN 的研究现状和发展阶段以及本课题的背景、目的和意义、提出了论文的主要工作内容及组织结构。

第二章首先介绍了 WLAN 的当前主要标准，随后讲述了 WLAN 的几个重要概念、组网方式，最后简单介绍了 WLAN 的网络安全、典型应用方案。

第三章首先介绍了目前 WLAN 的“半移动性”，这制约了很多新业务的应用，然后介绍WLAN移动切换的三种情形，最后给出当前最热门的话题VoWLAN，VoWLAN要求WLAN能够平滑切换。

第四章详细讲述了从负载均衡和预认证两个方面改进WLAN的切换性能，最后是实验部分，使用Chariot软件来测试VoWLAN的切换性能，从而验证了课题提出的方案的有效性。

第五章对WLAN漫游进行了展望，通过MESH技术和移动IP技术，将达到STA在有热点覆盖的地方可以任意接入。

第2章 无线局域网概述

2.1 WLAN的标准

目前的 WLAN 产品所采用的技术标准主要包括：IEEE 802.11、IEEE 802.11b、IEEE 802.11a、IEEE 802.11g、HomeRF、IrDA 和蓝牙等。

2.1.1 IEEE 802.11

1997 年 6 月，IEEE 推出了第一代 WLAN 标准——IEEE 802.11[14](1997 版本)，随后在 1999 年推出了新的 IEEE 802.11(1999 版本)。该标准制定了物理层和媒介访问控制子层(MAC)的技术规范，允许 WLAN 及无线设备制造商在一定范围内建立互操作网络设备。任何 LAN 应用、网络操作系统或协议(包括 TCP/IP 和 Novell NetWare)在遵守 IEEE 802.11 标准的无线局域网上运行时，就像在它们运行在以太网上一样容易。

IEEE 802.11 在物理层定义了数据传输的信号特征和调制方法，定义了两种无线电(RF)传输方式和一种红外线传输方式。其中 RF 传输标准包括直接序列扩频技术(DSSS, Direct Sequence Spread Spectrum)和跳频扩频技术(FHSS, Frequency Hopping Spread Spectrum)。DSSS 采用一个长度为 11 比特的 Barker 序列来对无线方式发送的数据进行编码，每个 Barker 序列表示一个二进制数据位(1 或 0)，并被转化成可以通过无线方式发送的波形信号。这些波形信号如果使用二进制相移键控(BPSK)调制技术，可以以 1Mb/s 的速率进行发射；如果使用正交相移键控(QPSK)调制技术，发射速率可以达到 2Mb/s。FHSS 利用 GFSK 二进制或四进制调制方式可以达到 2Mb/s 的工作速率[6][9]。

由于在无线网络中碰撞检测较困难，IEEE 802.11 规定媒介访问控制(MAC)子层采用碰撞回避(CA)协议，而不是碰撞检测(CD)协议。为了尽量减少数据的传输碰撞和重试发送，防止各站点无序争用信道，WLAN 中采用了与以太网 CSMA/CD 类似的 CSMA/CA(载波侦听多址访问/碰撞避免)协议[24][29]。CSMA/CA

基本上是一种 p 持续机制(一个站点在发送之前，首先监听信道，如果信道空闲，便以概率 p 传送，而以概率 q=1-p 把该次发送推迟到下一时隙)，加上空闲时间管理。当一个设备检测到传输介质空闲时，该设备在它可以竞争访问介质之前必须等待一个指定长度的时间。这个指定的等待时间称作帧间间隔(IFS 时间)。在 IFS 时间过后，想要发送的设备设置一个竞争定时器。竞争时间长度从预先定义的竞争窗口长度值中随机选取。在竞争定时器超时后，该设备在介质上发送数据，并等待应答。如果发送方没有收到应答，那么该设备认为发生了冲突。该设备选择另一个竞争定时器，等待定时器超时，重传信息。在第二次尝试中，从其得到竞争时间的时间长度加倍，因此这里所实现的是二进制指数退避。

如果在等待发送的站监听到介质在被使用，而竞争定时器的值在不断减少，那么就停止竞争定时器。当介质再次变成空闲时，竞争定时器的值继续减小。暂停定时器而不是重启定时器的理由是允许等待时间最长的站在下一竞争周期中得到比较高的优先级。另外，帧间间隔也可以用于优先级传输。如果一个设备被分配一个较小的帧间间隔值，那么它就有更多的机会得到对传输介质的访问。

2.1.2 IEEE 802.11b

由于现行以太网技术可以实现 10Mb/s,100Mb/s 乃至 1000Mb/s 等不同速率以太网络之间的兼容，为了支持更高的数据传速速率，IEEE 于 1999 年 9 月批准了 IEEE 802.11b[16]标准。IEEE 802.11b 标准对 IEEE 802.11 标准进行了修改和补充，其中最重要的改进就是在 IEEE 802.11 的基础上增加了两种更高的通信速率[2][3]。

802.11b 在无线局域网协议中最大的贡献就在于它在 802.11 协议的物理层增加了两个新的速率：5.5Mbps 和 11Mbps。为了实现这个目标，DSSS 被选作该标准的唯一的物理层传输技术，这个决定使得 802.11b 可以和 1Mbps 和 2Mbps 的 802.11 DSSS 系统互操作。最初 802.11 的 DSSS 标准使用 11 位的 chipping-Barker 序列来将数据编码并发送，每一个 11 位的 chipping 代表一个一位的数字信号 1 或者 0，这个序列被转化成波形(称为一个 Symbol)，

然后在空气中传播。这些 Symbol 以 1MSps(每秒 1M 的 symbols)的速度进行传送，传送的机制称为 BPSK(Binary Phase Shifting Keying)，在 2Mbps 的传送速率中，使用了一种更加复杂的传送方式称为 QPSK(Quandrature Phase Shifting Keying)，QPSK 中的数据传输率是 BPSK 的两倍，以此提高了无线传输的带宽[10][11][12]。

在 802.11b 标准中，一种更先进的编码技术被采用了，在这个编码技术中，抛弃了原有的 11 位 Barker 序列技术，而采用了 CCK(Complementary Code Keying)技术，它的核心编码中有一个 64 个 8 位编码组成的集合，在这个集合中的数据有特殊的数学特性使得他们能够在经过干扰或者由于反射造成的多方接受问题后还能够被正确地互相区分。5.5Mbps 使用 CCK 串来携带 4 位的数字信息，而 11Mbps 的速率使用 CCK 串来携带 8 位的数字信息。两个速率的传送都利用 QPSK 作为调制的手段，不过信号的调制速率为 1.375MSps。这也是 802.11b 获得高速的机理。

为了支持在有噪音的环境下能够获得较好的传输速率，802.11b 采用了动态速率调节技术，来允许用户在不同的环境下自动使用不同的连接速度来补充环境的不利影响。在理想状态下，用户以 11Mbps 的全速运行，然而，当用户移出理想的 11Mbps 速率传送的位置或者距离时，或者潜在地受到了干扰的话，这把速度自动按序降低为 5.5Mbps、2Mbps、1Mbps。同样，当用户回到理想环境的话，连接速度也会以反向增加直至 11Mbps。速率调节机制是在物理层自动实现而不会对用户和其它上层协议产生任何影响。

2.1.3 IEEE 802.11a

IEEE 802.11a[16]标准是已在办公室，家庭，宾馆和机场等众多场合得到广泛使用的 IEEE 802.11b 无线组网标准的后续标准。IEEE 802.11a 工作在 5GHz U-NII 频带，物理层速率可达 54Mb/s，传输层可达 25Mb/s。IEEE 802.11a 选择具有能有效降低多径衰落影响与有效使用频率的正交频分复用(OFDM)为调制技术，可提供 25Mb/s 的无线 ATM 接口和 10Mb/s 的以太网无线帧结构接口，以及 TDD/TDMA 的空中接口；支持语音、数据和图象业务。

2.1.4 IEEE 802.11g

由于下一代规格 IEEE 802.11a 与目前的 IEEE 802.11b 规范之间频段与调制方式的不同使得两者不能互通，已经拥有 IEEE 802.11b 产品的消费者可能不会在 IEEE 802.11a 设备问世之前就立即购买；IEEE 802.11g 就是为这段过渡时间所发展的规范，它构建在既有的 IEEE 802.11b 物理层与媒介访问控制层标准基础上，选择 2.4GHz 频段，让已经拥有 IEEE 802.11b 产品的用户能够以 IEEE 802.11g 的产品满足速度升级的需要。

在 2000 年初，IEEE 802.11g 的工作组接受了一项开发高速、向下兼容非常成功的 IEEE 802.11b 物理层标准的工作，新增的 IEEE 802.11g 标准将兼容 IEEE 802.11b 的 MAC，实现所有 IEEE 802.11b 所必要的功能并保证兼容、可交互，同时包括至少 20Mb/s 的速率，还包括 2.4GHz/5GHz 波段的融合，从而在 2.4GHz 频段获得更高的速率。IEEE 802.11g 工作组几乎用了一年半的时间，在集中的建议中取得了一个折衷的方案，这就是 2001 年 11 月的第一个 IEEE 802.11g 草案。工作组在 2002 年 1 月份的会议上还取得了一些附加的技术改善，整个 IEEE 802.11g 标准在 2003 年初完成。IEEE 802.11g 草案采用了 IEEE 802.11b 的要求，在 2.4GHz 频段上速率可以扩展至 54Mb/s。IEEE 802.11g 必须向 IEEE802.11b 兼容。

2.1.5 HomeRF

HomeRF 是专门为家庭用户设计的一种WLAN技术标准。HomeRF 利用跳频扩频方式，既可以通过时分复用支持语音通信，又能通过载波监听多重访问/冲突避免(CSMA/CA)协议提供数据通信服务。同时，HomeRF 提供了与TCP/IP 良好的集成，支持广播、多播和 48 位 IP 地址。目前，HomeRF 标准工作在 2.4GHz 的频段上，跳频带宽为 1MHz，最大传输速率为 2Mbps，传输范围超过 100 米。

美国联邦通信委员会(FCC)最近采取措施，允许下一代 HomeRF 无线通信网络传送的最高速度提升到 10Mbps，这个速度是目前此种网络速度的 5 倍，这将使 HomeRF 的带宽与 IEEE802.11b 标准所能达到的 11Mbps 的带宽相差无几，并且将使 HomeRF 更加适合在无线网络上传输音乐和视频信息。

除此之外，FCC 还接受了 HomeRF 工作组的要求，将 HomeRF/SWAP(共享无

线访问协议，Shared Wireless Access Protocol)使用的2.4GHz频段中的跳频带宽增加到5MHz。

2.1.6 IrDA

IrDA成立于1993年，是非营利性组织，致力于建立无线传播连接的国际标准，目前在全球拥有160个会员，参与的厂商包括计算机及通信硬件、软件及电信公司等。IrDA是一种利用红外线进行点对点通信的技术，其相应的软件和硬件技术都已比较成熟。它的主要优点是体积小、功率低，适合设备移动的需要，传输速率高，可达16Mbps，成本低，应用普遍。目前有95%的手提电脑上安装了IrDA接口，最近市场上还推出了可以通过USB接口与PC机相连接的USB-IrDA设备。

面对其他技术的挑战，IrDA并没有停滞不前。除了传输速率由原来FIR标准(FastInfrared)的4Mbps提高到最新VFIR标准的16Mbps；接收角度也由传统的30度扩展到120度。

但是，IrDA也有其不尽如人意的地方。首先，IrDA是一种视距传输技术，也就是说两个具有IrDA端口的设备之间传输数据时，中间就不能有阻挡物，这在两个设备之间是容易实现的，但在多个设备间就必须彼此调整位置和角度等，这是IrDA的致命弱点。其次，IrDA设备中的核心部件—红外线LED不是一种十分耐用的器件，对于不经常使用的扫描仪和数码相机等设备还可以，但如果经常用装配IrDA端口的手机上网，可能很快就不堪重负了。

2.1.7 蓝牙

蓝牙(Bluetooth)技术是由爱立信、诺基亚、Intel、IBM和东芝5家公司于1998年5月共同提出开发的。蓝牙技术的本质是设备间的无线联接，主要用于通信与信息设备。近年来，在电声行业中也开始使用。依据发射输出电平可以有3种距离等级，Class1为100m左右、Class2约为10m、Class3约为2-3m。一般情况下，其正常的工作范围是10m半径之内。在此范围内，可进行多台设备间的互联。但对于某些产品，设备间的联接距离甚至远隔100m也照样能建立蓝牙通信与信息传递。蓝牙技术的特点包括：

1. 采用跳频技术，数据包短，抗信号衰减能力强；

2. 采用快速跳频和前向纠错方案以保证链路稳定，减少同频干扰和远距离传输时的随机噪声影响；
3. 使用2.4GHz ISM频段，无须申请许可证；
4. 可同时支持数据、音频、视频信号；
5. 采用FM调制方式，降低设备的复杂性。

该技术的传输速率设计为1MHz，以时分方式进行全双工通信，其基带协议是电路交换和分组交换的组合。一个跳频频率发送一个同步分组，每个分组占用一个时隙，使用扩频技术也可扩展到5个时隙。同时，蓝牙技术支持1个异步数据通道或3个并发的同步话音通道，或1个同时传送异步数据和同步话音的通道。每一个话音通道支持64kb/s的同步话音；异步通道支持最大速率为721kb/s，反向应答速率为57.6 kb/s的非对称连接，或者是432.6 kb/s的对称连接。目前，蓝牙技术已被普遍应用在笔记本电脑上，以帮助两台(或多台)笔记本电脑之间实现无线通信。较红外线传输“必须保证传输信息的两个设备正对，且中间不能有障碍物”、“几乎无法控制信息传输的进度”、“没有成为被广泛接受的工业标准、设备种类不多”等致命的缺陷，蓝牙的优势显示出了勃勃生机。全世界已有2161家公司参加了SIG(Special Interest Group)组织，并正在共同制定蓝牙技术标准。SIG的核心公司除上述最初提出开发蓝牙技术的5家公司外，还有3com、Lucent技术、微软和摩托罗拉4家。SIG成员公司包括：PC个人电脑、移动电话、网络相关设备、外围辅助设备和A/V设备、通讯设备和汽车电子、自动售货机、医药器械、计时装置等诸多领域的设备制造公司。

总的来讲，IEEE 802.11系列标准比较适用于办公室中的企业无线网络，HomeRF较适用于家庭中移动数据/语音设备之间的通信，而蓝牙技术则可以应用于任何可以用无线方式替代线缆的场合。目前这些技术还处于并存状态，从长远看，随着产品与市场的不断发展，它们将走向融合。

2.2 WLAN的网络组成

IEEE 802.11体系结构中两个最重要的组成部分是STA和BSS(Basic Service Set)，STA是指接入无线媒介的部分，它包含MAC实体和PHY实体。

和有线网络对应，STA 也常被称作网络适配器或者网络接口卡。STA 可以是移动的，也可以是固定的。每个 STA 都支持站点服务，这些服务包括鉴权、去鉴权、加密和数据传输。BSS 是 IEEE 802.11 局域网的基本构成单元，如图 2.1 所示，两个 BSS，每个 BSS 含有两个 STA，作为其成员。

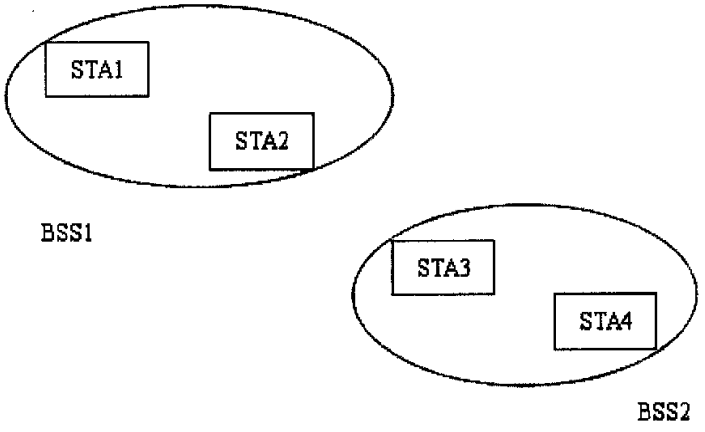

图 2.1 基本服务集(BSS)

2.2.1 Ad-Hoc 网络

独立的基本服务集(IBSS)是最基本的 IEEE 802.11 局域网类型。一个最小的 IEEE 802.11 局域网也许仅仅包含两个 STA。Ad-Hoc 网络不依赖固定网络，将地理位置分散的 STA 有效地组织在一起相互通信。由于没有中心基站的支持，组网的重担就落在各个 STA 上，因此这种网络也被称为自组织网。在移动的环境下，各 STA 间的通信链路是不固定的，甚至可能发生快速的变化。STA 与 BSS 之间的关系是动态的，STA 可以自由的开机、关机、进入或者离开 BSS 覆盖范围。为了成为 BSS 的组成成员，STA 必须与该 BSS 进行相互关系的沟通。这种关系是动态的，而且包含使用分发系统服务(DSS,Distribution System Service)。

2.2.2 Infrastructure 网络

物理层覆盖范围的有限决定了所能支持的 STA 与 STA 之间的直接通信距离。对有些网络，该距离足够；而对于另一些网络，则可能需要增加其物理层的覆盖范围。

为了解决覆盖范围的问题，BSS 可以不以单个的形式出现，而是由多个 BSS 构成一个扩展的网络。连接多个 BSS 的这个网络构件被称作分发系统(DS,Distribution System)。IEEE 802.11 逻辑上把无线媒介(WM,Wireless Medium)和分发系统媒介(DSM,Distribution System Medium)分开。每种逻辑媒介被不同的体系结构构件用于不同的目的。IEEE 802.11 定义既不排除也没有要求多个媒介是一样的，或者是不同的。分发系统如图 2.2。

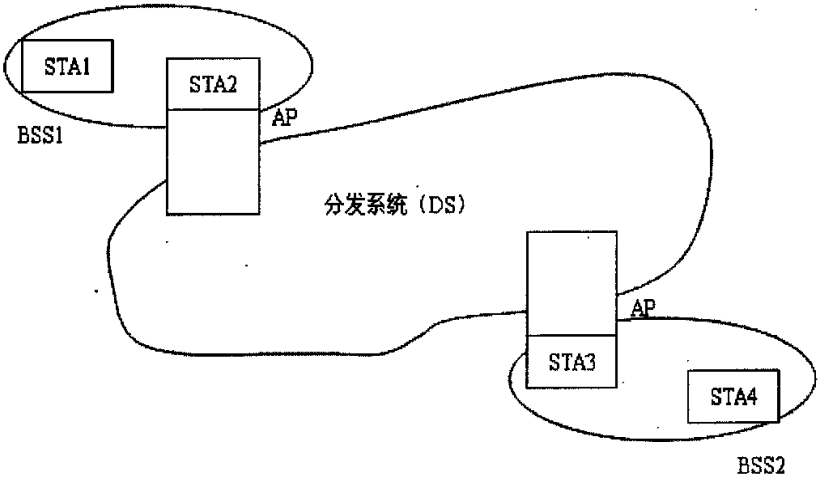

图 2.2 分发系统

访问点(AP，Access Point)也是一个 STA，该 STA 除了作为一个普通的 STA 工作外，它还通过提供分发服务来提供对 DS 的访问。数据通过 AP 在 BSS 和 DS 之间传输，所有访问点都是 STA，它们都是可编址单元。用于 AP 在 WM 上的通信地址和在 DSM 上的通信地址可以不必相同。

DS 和多个 BSS 允许 IEEE 802.11 构成一个任意大小和复杂的无线网络。

IEEE 802.11b 把这种网络称为扩展服务集(ESS, Extended Service Set)网络。对于 LLC 而言，ESS 网络显然等同于 IBSS 网络。ESS 网络内的 STA 可以通信，移动 STA 可以从一个 BSS 中移动到另一个 BSS 中(这些 BSS 在同一个 ESS 网络中)，这对 LLC 而言是透明的。

入口(Portal)是一个逻辑点，来自非 IEEE 802.11 局域网的 MSDU 通过该入口可以进入 IEEE 802.11 DS。Portal 在 IEEE 802.11 和有线局域网(如以太网)之间提供逻辑综合，在 IEEE 802.11 中，扩展服务集(ESS)体系结构提供传输分割和覆盖范围扩展的功能。IEEE 802.11 与其它局域网的逻辑连接·是通过入口完成的，入口实现了分发系统(DS)和局域网之间的互连。

2.3 WLAN的接入

IEEE 802.11 体系结构有如下服务：

1, Authentication (鉴权)

2, Deauthentication (取消鉴权)

3, Association (关联)

4, Disassociation (取消关联)

5, Reassociation (重新关联)

6, Distribution (分发)

7, Integration (综合)

8, Privacy (加密)

9, MSDU delivery (媒介访问控制服务数据单元交付)

鉴权

在有线局域网中，物理安全性可以用于防止未授权访问。但是在无线网络中，由于媒介物理边界的不确定性而不能防止未授权访问。IEEE 802.11 通过鉴权服务提供对局域网的访问控制。鉴权服务服务被所有 STA 用来确定与其通信的对方站点的身份。这对于 ESS 和 IBSS 两种网络确实如此。如果两

个 STA 之间没有建立相互可接收的鉴权级别，关联则不能建立。

IEEE 802.11 定义了两种 Authentication 机制：开放系统(Open System)鉴权机制和共享密码(Shared key)鉴权机制。开放系统鉴权允许鉴权帧交换结束后的结果一定是“成功”。此时 STA1 向 STA2 声明其身份，然后 STA2 将以“成功”的结果应答给 STA1。在此过程中没有相互验证身份的过程。因此当 IEEE 802.11 WLAN 要求严格的安全性后，都不能使用这种鉴权机制。在共享鉴权机制中，使用该机制的双方都必须使用一个共享密钥，同时要求双方支持 WEP 加码，然后使用 WEP 对测试文本进行加密和解密，以此来证明双方拥有相同密钥。在这种机制下，STA1 向 STA2 声明其身份，然后 STA2 将响应 STA1，在应答帧中 STA2 向 STA1 声明身份，并要求 STA1 通过正确加密测试文本。STA1 收到应答帧后用默认密钥或者密钥映射表中的密钥对测试文本进行加密，然后将结果发送给 STA2。STA2 收到此帧后用合适的密钥对其进行解密，然后将解密结果同原始文本进行比较，如果一致，则返回鉴权成功；反之返回鉴权失败。

关联

STA 在收到 MLME-ASSOCIATE.request(媒介访问控制管理实体关联请求原语)后，将按照如下过程与访问点 AP 建立关联关系：

1，STA 向已经鉴权的 AP 发送关联请求；

2，如果 STA 在发送关联请求后，收到状态值为“成功”的关联应答帧，则此 STA 已经与 AP 成功建立关联关系，此时媒介访问控制子层管理实体(MLME)将发出一条 MLME-ASSOCIATE.confirm(媒介访问控制子层管理实体关联证实原语)指示此类关联请求的成功完成；

3，如果 STA 在发出关联请求后收到的关联应答帧状态值不是“成功”，而是其它值，或者关联请求超时，则该 STA 未与 AP 成功关联。此时 MLME 将发送 MLME-ASSOCIATE.confirm 指出此次关联请求失败。

重新关联

STA 在收到 MLME-REASSOCIATATE.request(媒介访问控制子层管理实体重新关联请求原语)后，将按如下过程与 AP 建立重新关联关系：

1，STA 将发送一个重新关联请求帧到将要建立关联关系的 AP；

2，如果 STA 在发出重新关联请求后，收到状态值为“成功”的关联应答帧，则此 STA 已经与 AP 成功建立关联关系，此时媒介访问控制子层管理实体(MLME)将发出一条 MLME-REASSOCIATE.confirm(媒介访问控制子层管理实体重新关联证实原语)指示此类关联请求的成功完成；

3，如果 STA 在发出重新关联请求后收到的关联应答帧状态值不是“成功”，而是其它值，或者重新关联请求超时，则该 STA 未与 AP 成功关联。此时 MLME 将发送 MLME-REASSOCIATE.confirm 指出此次关联请求失败。图 2.3 是 WLAN 接入的鉴权和关联过程。

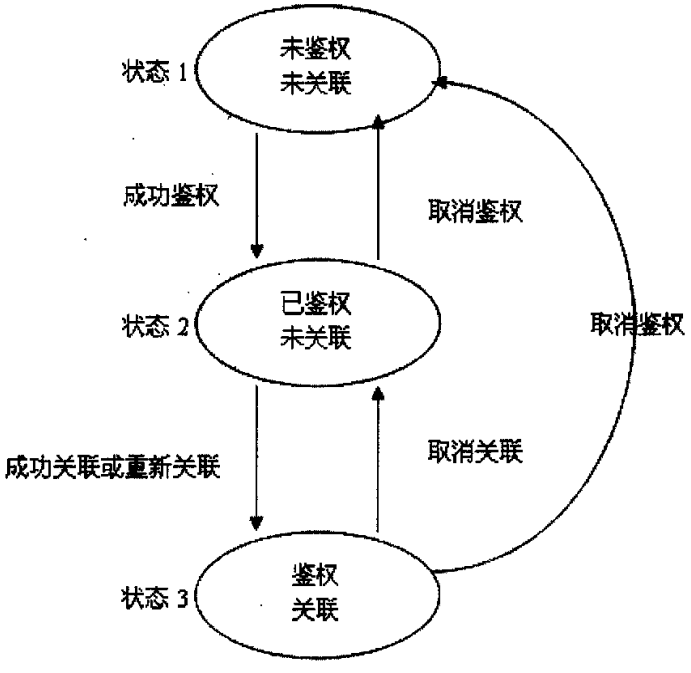

图 2.3 WLAN 接入的鉴权和关联过程

2.3.1 WLAN 的安全

近来，无线局域网发展的势头越来越猛，它接入速率高，组网灵活，在传输移动数据方面尤其具有得天独厚的优势。但是，随着无线局域网应用领域的不断拓展，其安全问题也越来越受到重视。在有线网络中，您可以清楚辨别哪台电脑连接在网线上。无线网络与此不同，理论上无线电波范围内的任何一台电脑都可以监听并登录无线网络。如果企业内部网络的安全措施不够严密，则完全有可能被窃听、浏览甚至操作电子邮件。为了使授权电脑可以访问网络而非法用户无法截取网络通信，无线网络安全就显得至关重要[7][8]。

安全性主要包括访问控制和加密两大部分。访问控制保证只有授权用户能访问敏感数据，加密保证只有正确的接收者才能理解数据。目前使用最广泛的 IEEE 802.11b 标准提供了两种手段来保证 WLAN 的安全——SSID 服务配置标示符和 WEP 无线加密协议。SSID 提供低级别的访问控制，WEP 是可选的加密方案，它使用 RC4 加密算法，一方面用于防止没有正确的 WEP 密钥的非法用户接入网络，另一方面只允许具有正确的 WEP 密钥的用户对数据进行加密和解密包括软件手段和硬件手段。

另外，802.11b 标准定义了两种身份验证的方法：开放系统(Open System)和共享密钥(Shared Key)。在缺省的开放系统方法中，用户即使没有提供正确的 WEP 密钥也能接入访问点，共享式方法则需要用户提供正确的 WEP 密钥才能通过身份验证。

很显然，基本的安全手段只能提供基本的安全性。对于不同的用户，有必要为他们提供不同级别的安全手段。目前 WLAN 设备提供了 3 种级别的安全措施。第一种是链路层的安全，也就是标准的 WEP 加密[36][37]。第二种则是用户身份验证层次的安全，代表性做法是利用 802.1x[39]。第三种是利用 VPN 手段。这三种级别的安全手段，适用于不同要求的用户，VPN 方法是最安全的。在简单应用中，目前用得最多的还是 WEP 方式，802.1x 将是趋势。本课题主要在 802.1x 安全认证的基础上研究 WLAN 的切换漫游。

2.3.2 IEEE 802.1x

IEEE 802.1x 称为基于端口的访问控制协议(Port based network access control protocol)[17][18]。基于端口的访问控制能够在利用 IEEE 802 LAN 的优势基础上提供一种对连接到局域网(LAN)设备或用户进行认证和授权的手段。通过这种方式的认证，能够在 LAN 这种多点访问环境中提供一种点对点的识别用户的方式。这里端口是指连接到 LAN 的一个单点结构，可以是被认证系统的 MAC 地址，也可以是服务器或网络设备连接 LAN 的物理端口，或者是在 IEEE 802.11 无线 LAN 环境中定义的工作站和访问点。图 2.4 是 IEEE 802.1x 体系结构图。

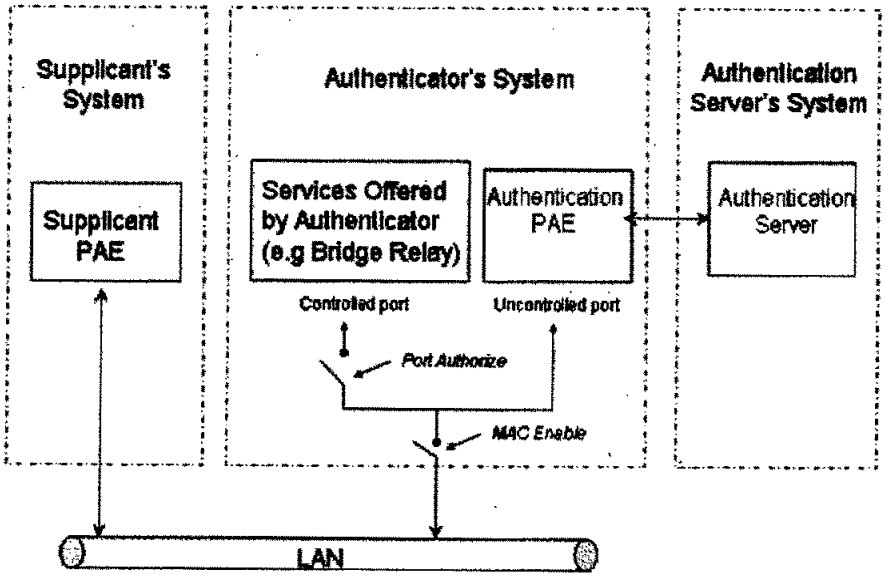

图 2.4 IEEE 802.1x 体系结构

客户端(Supplicant)

客户端指 LAN 所连接的一端的实体(entity)，它向认证系统(Authenticator 如下)发起请求，对其身份的合法性进行检验。

Authenticator 认证系统

认证系统指在LAN连接的一端用于认证另一端设备的实体(entity)。

认证服务器(Authentication Server)

认证服务器指为认证系统提供认证服务的实体。这里认证服务器所提供的服务是指通过检验客户端发送来的身份标识，来判断该请求者是否有权使用认证系统所提供的网络服务。

网络访问端口(Network Access Port)

网络访问端口指用户系统连接到LAN的访问端口。访问端口可以是物理端口，例如连接到用户的网络设备端口；也可以是逻辑端口，例如用户设备的MAC地址。

端口访问实体(PAE，Port Access Entity)

端口访问实体指一个端口的相关协议实体。PAE 能够支持的功能包括：客户端完成的功能、认证系统完成的功能或者两者功能同时具备。

系统(System)

系统是指通过一个或更多端口连接到LAN的设备，例如：终端、服务器、交换机或路由器等设备都称为系统。

IEEE 802.1x 认证流程

802.1x作为一个认证协议，在实现的过程中有很多重要的工作机制。

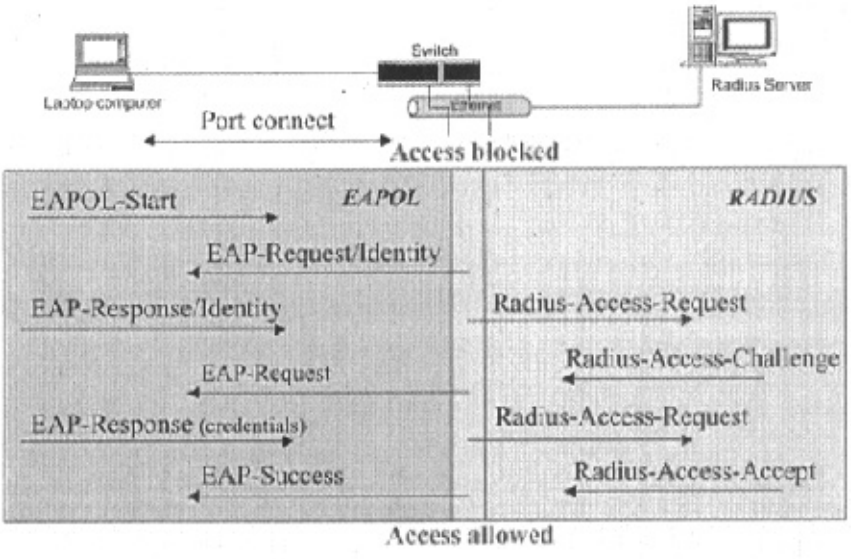

图 2.5 IEEE 802.1x 协议的工作机制

认证发起

认证的发起可以由用户主动发起，也可以由认证系统发起。当认证系统探测到未经过认证的用户使用网络，就会主动发起认证；用户端则可以通过客户端软件向认证系统发送 EAPOL-Start 报文发起认证。

由认证系统发起的认证

当认证系统检测到有未经认证的用户使用网络时，就会发起认证。在认证开始之前，端口的状态被强制为未认证状态。

如果客户端的身份标识不可知，则认证系统会发送 EAP-Request/Identity 报文，请求客户端发送身份标识。这样，就开始了典型的认证过程。

客户端在收到来自认证系统的 EAP-Request 报文后，将发送 EAP-Response 报文响应认证系统的请求。

认证系统支持定期的重新认证，可以随时对一个端口发起重新认证的过程。如果端口状态为已认证状态，则当认证系统发起重新认证时，该端口通过认证，那么状态保持不便；如果未通过认证，则端口的状态改变为未认证状态

由客户端发起认证

如果用户要上网，则可以通过客户端软件主动发起认证。客户端软件会向认证系统发送 EAPOL-Start 报文主动发起认证。

认证系统在收到客户端发送的 EAPOL-Start 报文后，会发送 EAP-Request/Identity 报文响应用户请求，要求用户发送身份标识，这样就启动了一个认证过程。

退出已认证态

有几种方式可以造成认证系统把端口状态从已认证状态改变成未认证状态。

1. 客户端未通过认证服务器的认证；
2. 由于管理性的控制端口始终处于未认证状态，而不管是否通过认证；
3. 与端口对应的 MAC 地址出现故障(管理性禁止或硬件故障)；
4. 客户端与认证系统之间的连接失败，造成认证超时；
5. 重新认证超时；
6. 客户端未响应认证系统发起的认证请求；
7. 客户端发送 EAPOL-Logoff 报文，主动下线。

退出已认证状态的直接结果就是导致用户下线，如果用户要继续上网则要再发起一个认证过程。

为什么要专门提供一个 EAPOL-Logoff 机制，是处于如下安全的考虑。

当一个用户从一台终端退出后，很可能其他用户不通过发起一个新的登录请求，就可以利用该设备访问网络。提供专门的退出机制，以确保用户与认证系统专有的会话进程被中止，可以防止用户的访问权限被他人盗用[19][20]。通过发送 EAPOL-Logoff 报文，可以使认证系统将对应的端口状态改变为未认证状态。

2.4 WLAN的应用

WLAN 可以为用户移动或者半移动状态下接入网络，得到高效率、高质量、低商业成本的数据。在这一方面，无线网络所提供的移动和无线接入却是有线网络无法相比的。适合于：

- 难以布线获布线成本太高的地区
- 校园会议室、展览厅、咖啡厅等人员变动频繁的地方
- 如餐厅、仓储超市等需要无线通信的场所
- 家庭和 SOHO 用户，享受高质量的家庭网络服务
- INTERNET 宽带接入，基于 WLAN 的宽带数据业务
- .....

除了在机场、宾馆和会议中心等首批 WLAN 的热点场所之外，无线互联网服务商和移动网络服务商目前正大范围的装置 WLAN，商业公共场所的 WLAN 供应商正将目光从首批用户转向办公室和家庭市场的新用户，以增加针对商务旅行者业务方面的营业收入。图 2.6 是运营商布置的典型解决方案：

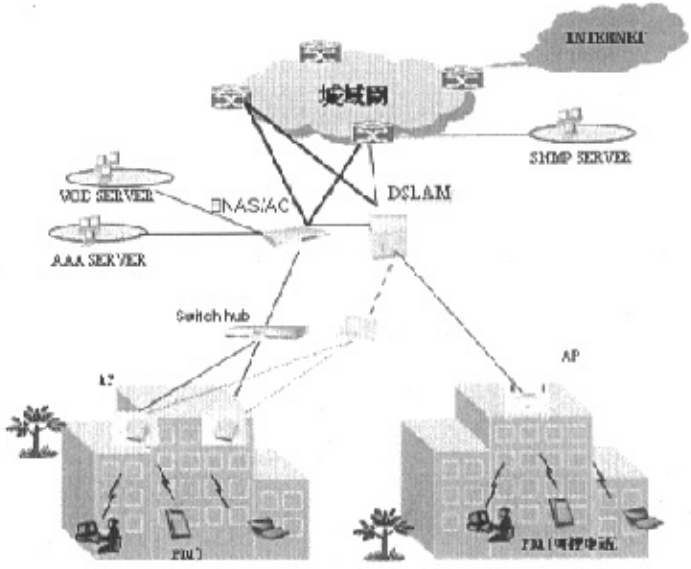

图 2.6 WLAN 典型解决方案

2.5 本章小结

本章首先介绍了 WLAN 主要标准，IEEE 802.11b，802.11a，802.11g 是当前主要使用的 WLAN 标准，电信运营商，企业用户比较欢迎这类标准。HomeRF，IrDA，蓝牙标准的无线局域网客户主要是家庭，个人等；然后介绍 WLAN 的网络组成，接入过程；接着介绍对于无线开放系统来说最重要的安全性，802.1x 定义的认证流程正在被越来越多的协议所使用，如中国自主研发的 WLAN 安全标准 WAPI，IEEE 制定的 802.11n 标准；最后阐述了 WLAN 的典型解决方案。

第3章 无线局域网漫游切换

目前 WLAN 虽然剪断了电缆的束缚，现在只是“半移动”状态，移动终端只能在同一个区域内随时随地接入 Internet，提供区域性的漫游功能。并且目前这种业务主要是在数据业务方面，对实时性要求较高的业务如语音，视频支持却不好。现在的发展目标，将是完全漫游的能力，即在以一定速度行进时，可无中断地收发数据，这将是实现个人通信网(PCN)的一条有效途径。语音，视频点播等实时性业务要求 WLAN 快速、顺利地切换。本论文就是在 VoWLAN 这样的应用背景下来研究 WLAN 的漫游切换的。

3.1 切换的种类

STA 的移动分为三种：

1. 同一 BSS 内；
2. BSS 的变化：这种类型定义为在同一 ESS 内，一个 STA 从一个 BSS 移动到另一个 BSS；
3. ESS 的变化：这种类型定义为一个 ESS 中的一个 BSS 内的 STA 移动到另一个 ESS 内的 BSS 下，这种情况只在 STA 可以移动的情况下才会得到支持。IEEE 802.11 不承诺上层连接的维护，事实上到目前为止，此种服务随时可能会中断。

图 3.1 是 WLAN 切换的三种情况。图中箭头 1 表示第一种移动：BSS 的变化，箭头 2 表示的可以是第二种移动：ESS 的变化。在更大型的网络中，将出现第三种移动。STA 从一个 AP 下移动到另一个 AP 下，都必须断开与第一个 AP 的连接，然后才能与第二个 AP 建立连接，因此这是一种硬切换。

WLAN 的安全认证时，STA 和 AP，认证服务器之间需要交互认证。IP 的尽力交付说明了其不完善的 QoS 机制，这使得交互时间没有保证。而 STA 每次与 AP 关联时时必须进行安全认证的。

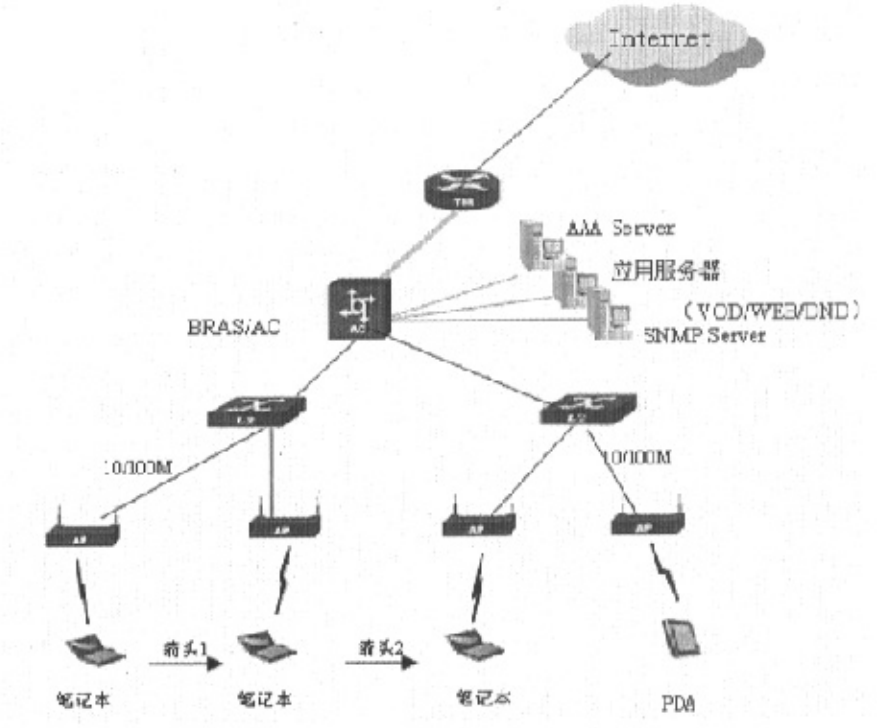

图 3.1 WLAN 的三种切换

3.2 VoWLAN

WLAN 目前最热门的一个课题是 VoWLAN(Voice over WLAN)，VoWLAN 是 WLAN 的新兴应用之一。

3.2.1 VoWLAN 发展现状

WLAN 技术的逐渐普及以及 VoIP 的迅速发展，使人们对将两者结合起来的 VoWLAN 技术投入了越来越多的关注，而将 VoWLAN 概念引入手机，并与蜂窝网络结合为用户提供无缝服务的移动 VoIP 更成为业界关注的焦点。VoIP 是指 IP 电话通过数据网络传输语音信号。WLAN 能够无线上网。VoWLAN 可以说是这两者的有机结合，它可以利用现有的 WLAN 网络实现无线的 VoIP 通话

能力，企业内部员工可以通过 VoWLAN 在办公场所以外的地方随时访问语音、E-mail 和其他已连的网络资源，这样提高了网络资源的利用率并降低了每次电话呼叫的成本，从而节省企业的总体 IT 费用。对于住宅用户也可以通过与宽带 802．11 无线网络相连的 VoIP 电话降低话费。

VoWLAN 业务可以由电信运营商提供，也可以由企业用户自主搭建 WLAN 环境，从而进行 VoIP 的业务等。电信运营商一般拥有公共场所的 WLAN 热点覆盖资源，从而可以开展 VoWLAN 业务。电信运营商主要面向最终用户提供服务，同时为 ISP 提供解决方案和业务批发；在终端应用上，以 Soft Phone为主，逐渐与 VoWLAN 终端厂家和手机厂家联盟，提供蜂窝-WLAN 双模终端，双模终端手机将会有很大的市场，在有热点覆盖的地方，使用 VoWLAN 呼叫 IP 电话，对等 VoWLAN,或者 PSTN 侧用户[38]。在没有热点覆盖的区域，使用 GSM/CDMA/3G 等无线接入手段，图 3.2 为 WLAN+GSM/CDMA/3G 组网图。

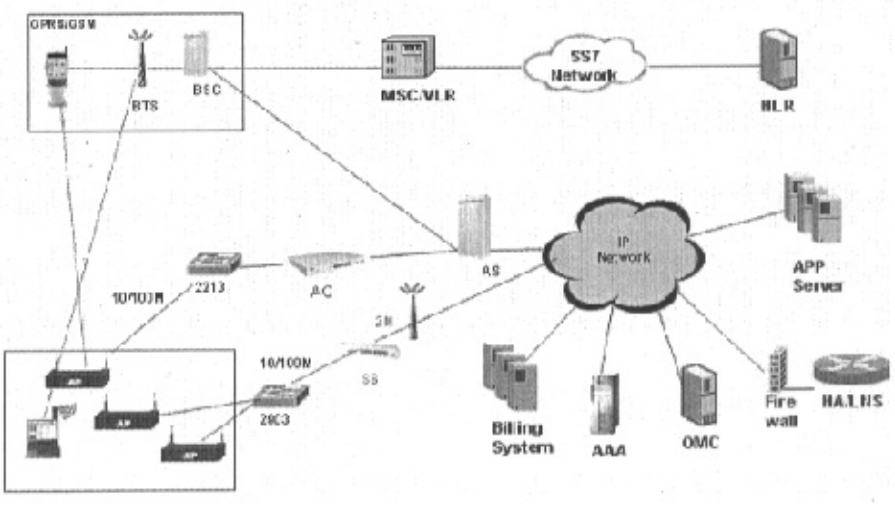

图 3.2 WLAN+GSM/CDMA/3G 组网图

现在很多企业已经布置了自己的 WLAN，原来仅仅作为有线局域网的补充：在会议室，外来客户，经常需要移动办公的员工提供快捷的网络接入手段。现在企业可以使用 VoWLAN 业务，提高了工作效率，如果企业和电信运营

商申请落地网关，则可以使用 IP 电话业务，降低了市话，长途电话等的呼叫成本，从而节省企业的总体生产成本。

3.2.2 WLAN 语音呼叫过程

VoIP 使用 SIP(Session Initiation Protocol)协议，组网图如图 3.3。IEEE 802.11 终端 STA 通过 ESSID 接入 AP，AP 有线连接交换机，接入控制服务器 AC(Access Control)作为接入控制设备，外接的 Radius Server，SIP Server 提供 AAA 服务和语音服务。IEEE 802.11 终端可以是硬终端如 WiFi 手机，也可以是软终端如笔记本+VoIP 客户端软件。

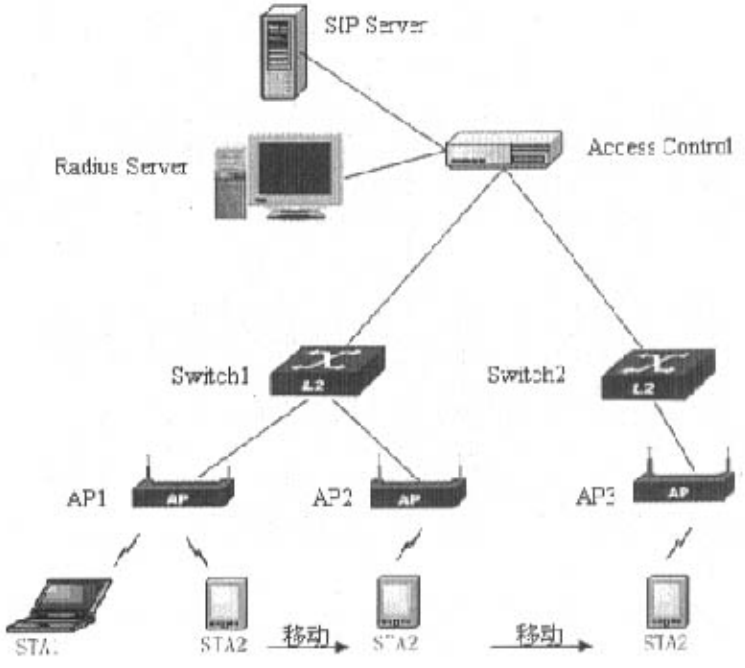

图 3.3 VoWLAN 组网图

AC 提供 Radius 认证服务，同时兼做 DHCP Server。STA1，STA2 接入 AC，在 Radius Server 上安全认证通过，此时 STA1，STA2 可以使用 WLAN 提供的接入业务如数据传输，无线接入 Internet 等。STA1，STA2 与 SIP Server 建立逻辑链路。STA1，STA2 发送 Register 报文，SIP Server 回复 200 OK，注

册成功后，STA1 可以向 STA2 发起呼叫请求，建立话路。

下面分析 STA 通话时在不同 AP 间移动的过程。开始 STA1，STA2 同在 AP1 下，STA2 向右移动，当 STA2 的物理层检测到与 AP1 的连接信号强度低于某个阈值 v 时，物理层通知 APME， STA2 开始搜索其它的 AP，此时它会搜索到 AP2，于是断开与 AP1 的连接，与 AP2 建立连接。STA2 需要重新发起 Radius 认证，SIP Server 的注册。假设 STA2 从 AP1 切换到 AP2 的时间为 t_1，进行 Radius 重认证的时间为 t_2，SIP Server 的注册时间为 t_3，则 $t_1+t_2+t_3$ 内 STA1，STA2 之间的语音数据将丢弃，严重的情况下，语音服务将会中断。下面一章主要讲述如何改进 WLAN 的切换性能。

3.3 本章小结

WLAN 的安全认证时，STA 和 AP，认证服务器之间需要交互认证。IP 的尽力交付说明了其不完善的 QoS 机制，这使得交互时间没有保证。而 STA 每次与 AP 关联时时必须进行安全认证的。

第4章 无线局域网切换改进

从第三章 WLAN 的切换过程可以看出，切换时的丢包主要在 $t_1+t_2+t_3$ 时间内，因此可以从减少这三个时间来改善切换性能。下面从负载均衡，预认证等措施改进切换性能。

4.1 基于负载均衡的策略

IEEE 802.11F[21]标准定义了 IAPP 协议，该协议解决了跨越支持 IEEE 802.11 业务分布系统的多无线接入点的部分互通性问题。在具体实现上，无线接入点管理实体(APME)启动 IAPP 的服务，在一个扩展服务集(ESS)内接收其他 AP 的服务指示，依据标准存在四种服务类型，分别是请求(Requests)，确认(Confirms)，指示(Indications)和应答(Replies)。服务请求和应答被高层无线接入点管理实体发布到 IAPP，IAPP 发布服务确认和指示到高层无线接入点管理实体。

IAPP 软件子系统在 AP 软件系统体系内的协议层次划分上，可以认为其处于第三层。IAPP 通过原语与 802.11 无线驱动模块进行交互，接收来自驱动模块的触发消息，发送相应的指示消息到驱动模块控制设备的运行。IAPP 发送 802.2 类型 1 逻辑链路控制交换标识更新响应帧到分布系统，刷新其他设备如网桥，交换机和其他 AP 的前传表。AP 之间交互的消息数据包采用了 IP/UDP 封装，在各自的高层无线接入点管理实体间传送。

依据软件系统方案中对负载均衡的设计要求，在 IAPP 软件子系统内能够比较方便的实现。因此在 IAPP 软件子系统，同时实现了两种可供选择的负载均衡实现方案：按用户数量负载均衡和按数据流量负载均衡。利用 IAPP 协议规定的 UDP 通信通道，AP 设备间交互有关各自负载的消息，形成对 STA 接入的负载均衡控制策略。

依据软件系统方案中对设备发现的设计要求，在 IAPP 软件子系统内利用 IAPP 协议规定的 UDP 通信通道，实现本地 AP 与分布系统内的发现设备

SERVER(通常担当者是 AC)之间的设备发现通信。

总之，IAPP 软件子系统在 AP 软件系统中的位置如图 4.1 所示：

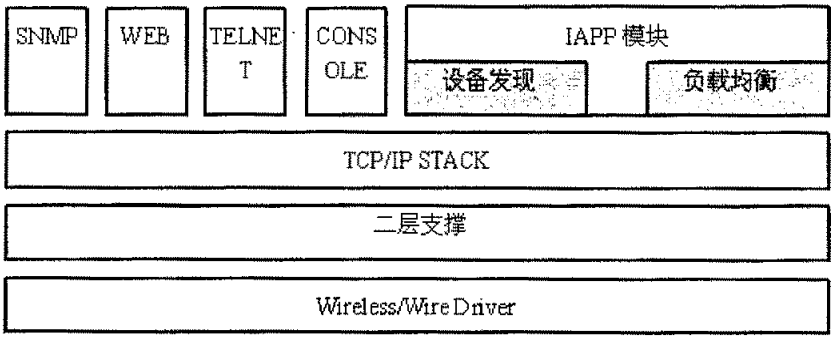

图 4.1 IAPP 在 AP 体系机构中的位置

4.1.1 服务原语

AP 体系结构中的部分服务原语描述如下：

1. IAPP-INITIATE request

1)功能：该服务原语触发AP初始化IAPP的数据结构，功能函数，和协议。

2)服务原语的语义：IAPP-INITIATE.request {

Port

}

其中，Port 为 IAPP 协议开放的端口号。

2. IAPP-INITIATE confirm

1)功能：该服务原语通知APME，IAPP-INITIATE.request开始的活动已经完成。

2)服务原语的语义：IAPP-INITIATE.confirm {

Status

}

其中，Status 指示 IAPP-INITIATE.request 响应的结果，Status 参数允许的取值是 SUCCESSFUL。

3. IAPP-TERMINATE request

1)功能：该服务原语触发 IAPP 终止 IAPP 的功能函数和协议。

2)服务原语的语义：IAPP-TERMINATE.request {

}

4. IAPP-TERMINATE confirm

1)功能：该服务原语通知 APME，IAPP-TERMINATE.request 开始的活动已经完成。

2)服务原语的语义：IAPP-TERMINATE. Confirm {

Status

}

其中，Status 指示 IAPP-TERMINATE.request 响应的结果，Status 参数允许的取值是 SUCCESSFUL。

5. IAPP-ADD request

1)功能：该服务原语被用于STA使用802.11关联请求帧连接到AP。触发一个帧发送到分布系统，更新前传表中该关联STA的信息；通知分布系统关于AP和STA间新的关联。

2)服务原语的语义：IAPP-ADD.request {

MAC Address,

Sequence Number,

Timeout

}

其中，MAC Address 是最近成功关联到 AP 的 STA 的地址；Sequence Number 是从该关联 STA 接收的 802.11 关联请求帧 SN 域的值；Timeout 是以秒为单位的值，当 ADD-notify 包和 L2 更新帧都没有被发出时，IAPP-ADD.confirm 原语将产生 TIMEOUT 状态。

6. IAPP-ADD confirm

1)功能：该服务原语被用于确认由 IAPP-ADD. Request 发起的行为已经完成，并且通知 APME 这些行为的状态。

2)服务原语的语义：IAPP-ADD.confirm {

Status

}

其中，Status参数指示相应IAPP-ADD.request成功或失败的状态。允许的值是SUCCESSFUL和TIMEOUT。SUCCESSFUL状态表明在超时期满前相应IAPP-ADD.request能够发送ADD-notify和L2更新帧;TIMEOUT状态表明在超时期满前不能发送ADD-notify包和L2更新帧之一或全部。

7. IAPP-ADD indication

1)功能：该服务原语被用于指示一个APME在分布系统内一个关联关系已经在一个移动STA和另一个AP间建立。

2)服务原语的语义：IAPP-ADD.indication {

MAC Address,

Sequence Number

}

其中，MAC Address 是接收的 IAPP-ADD.notify 包中移动 STA 的地址；Sequence Number 是从关联 STA 接收的 802.11 关联请求帧 SN 域的值。

8. IAPP-MOVE request

1)功能:该服务原语被用于一个 STA 使用 802.11 的重关联请求帧连接到 AP。触发一个帧被发送到分布系统更新前传表中该重关联 STA 的信息，以及通知分布系统该 AP 和 STA 的重关联关系。也尝试发送 IAPP Move-notify 包到该重关联 STA 以前关联的 AP。

2)服务原语的语义：IAPP-MOVE request {

MAC Address,

Sequence Number,

Old AP,
Context Block,
Timeout
}

其中，MAC Address 是最近成功重关联到 AP 的 STA 的地址；Sequence Number 是从重关联 STA 接收的 802.11 重关联请求帧 SN 域的值；Old AP 是重关联 STA 最后关联的 AP 的 IP 地址；Context Block 是送到 Old AP 的上下文，否则该参数为空。 Timeout 是以秒为单位的值，当 MOVE-notify 和 L2 更新帧都没有被发出并且 MOVE-reply 包没有被接收时，IAPP- MOVE.confirm 原语将产生 TIMEOUT 状态。

9. IAPP-MOVE confirm

1)功能：该服务原语被用于确认由 IAPP-MOVE. Request 发起的行为已经完成，并且通知 APME 这些行为的状态。

2)服务原语的语义：IAPP-MOVE confirm {
MAC Address,
Context Block,
Status
}

其中，MAC Address是从相应IAPP-MOVE.request中的STA地址；Context Block是当Status 为SUCCESSFUL时，由Old AP返回的上下文，否则为空；Status参数表明相应IAPP-MOVE. Request的结果，允许值是SUCCESSFUL和TIMEOUT，状态是TIMEOUT表明相应IAPP-MOVE. Request原语不能完成传送MOVE-notify包和L2更新帧，以及在IAPP-MOVE.request原语的超时参数期满之前不能接收到MOVE-reply包。

10. IAPP-MOVE indication

1)功能：该服务原语被用于指示一个 STA 已经重关联到另一个 AP。

2)服务原语的语义：IAPP-MOVE indication {

MAC Address,

Sequence Number,

AP Address,

Context Block

}

其中，MAC Address 是重关联到发送 IAPP MOVE-notify 包的 AP 的 STA 地址；Sequence Number 是从重关联 STA 接到的 802.11 重关联请求帧 SN 域的值；AP Address 是发送 IAPP MOVE-notify 包的 AP 的 IP 地址；Context Block 是由 AP Address 表明的 AP 发出的上下文，否则该参数为空。

11. IAPP-MOVE response

1)功能：该服务原语被用于发送任何常驻在发行该原语AP的有关的上下文。

2)服务原语的语义：IAPP-MOVE response {

MAC Address,

AP Address,

Sequence Number,

Context Block,

Status

}

其中，MAC Address 是重关联到由 AP Address 参数确定的 AP 的 STA 地址；AP Address 是 STA 已重关联到 AP 的 IP 地址；Sequence Number 是从重关联 STA 接到的 802.11 重关联请求帧 SN 域的值； Context Block 是重关联 STA 的上下文；Status 参数指出相应 IAPP-MOVE.indication 的结果，允许的值是 SUCCESSFUL 和 STALE_MOVE。

4.1.2 数据包格式

AP 体系结构 IAPP 的数据包格式描述如下图 4.2：

1. 一般IAPP数据包的格式

IAPP Version	Command	Identifier	Length	Data
Octets: 1	1	2	2	0-n

图4.2 一般IAPP数据包格式

其中，

(1) IAPP Version 域：长度为 1 个字节，指出 IAPP 协议的版本，取值为 0；

(2) Command 域：8 位整数，指出数据包的特定功能，取值为

ADD-notify 0

MOVE-notify 1

MOVE-response 2

Reserved 3-255；

(3) Identifier 域：两个字节的标识符有助于匹配请求和应答。发送任何接收到的其他 IAPP 数据包的响应包，应该将接收包 Identifier 域的值拷贝到响应包的 Identifier 域。以至于在一个时间范围内有相同源 IP 地址，端口和标识符的重复请求能被检测到。

(4) Length 域：两个字节的长度域指出整个数据包的长度，包括 Version，Command，Identifier，Length 和 Data 域。超过长度域规定长度范围的字节必须被处理成衬垫且接收时被忽略。如果数据包短于长度域规定的长度，应该被丢弃。

(5) Data域：数据域是一个可变长度域，内容依赖于Command域内容，数据域的内容分别在下面的2，3，4中描述。

2. ADD-notify数据包

ADD-notify 数据包在局域网段上用 IP/UDP 协议封装，使用 IAPP 协议发

送，通知任何接到该数据包的 AP，数据包中标识的移动 STA 已经关联到发送该数据包的 AP。该数据包被发送到广播地址子网，以至于该包将到达 DSM 局部子网的每一个设备，甚至交换 LAN。ADD-notify 数据包承载关联到 AP 的移动 STA 的 MAC 地址和 SN 序列号。该包的格式如图 4.3 所示。

Address Length	Reserved	MAC Address	Sequence Number
Octets: 1	1	n = Address Length	2

图4.3 ADD-notify数据域格式

其中，

(1)Address Length 域：是 8 位整数指出 MAC Address 的字节数量；

(2)Reserved 域：协议的保留域，设为 0，接收时应被忽略；

(3)MAC Address 域：是关联的移动 STA 的 MAC 地址，长度等于 Address Length 域值；

(4)Sequence Number 域：该域包含了 AP 从关联 STA 接到的关联请求帧的 SN 整数值，允许取值是 0-4095。

3. MOVE-notify 数据包

MOVE-notify数据包用IP/UDP协议封装，使用IAPP协议发送。该数据包从AP直接发送到重关联移动STA以前关联的老AP。该MOVE-notify包的数据域承载重关联到发送该数据包AP的移动STA的MAC地址和SN序列号值。该数据包数据域的格式如图4.4所示。

Address Length	Reserved	MAC Address	Sequence Number	Length of Context Block	Context Block
Octets: 1	1	n = Address Length	2	2	m=Length of Context Block

图 4.4 MOVE-notify 数据域格式

其中，

(1)Address Length 域：是 8 位整数指出 MAC Address 的字节数量；

(2)Reserved 域：协议的保留域，设为 0，接收时应被忽略；

(3)MAC Address 域：是重关联的移动 STA 的 MAC 地址，长度等于 Address Length 域值；

(4)Sequence Number 域：该域包含了 AP 从关联 STA 接到的重关联请求帧的 SN 整数值，允许取值是 0-4095；

(5)Length of Context Block 域：是一个 16 位整数，指出 Context Block 域的字节数量；

(6)Context Block 域：是一个变长域，包含了由 MAC Address 域确定的重关联 STA 传递的上下文信息，Context Block 的内容应该被 IAPP 解释。

Context Block 是一个由其他 802.11 标准定义的信息容器，需要从一个 AP 传递到另外一个重关联移动 STA，是一系列信息元素(Information Element)。信息元素的格式如图 4.5 所示。元素标识符和信息元素内容格式由使用 IAPP 从一个 AP 传送上下文到另一个的标准定义。信息元素被定义成一个通用一般格式，包含 2 字节 Element ID 域，一字节 Length 域，和一个变长特定元素 Information 域。每一个元素被分配一个唯一的由使用 IAPP 在 AP 间传送上下文的标准定义的 Element ID。Length 域规定了 Information 域的字节数量。IAPP 服务用户应该忽略它们不能理解的元素标识符的信息元素，而不是删掉整个 IAPP MOVE-response 数据包。

Element Identifier	Length	Information
Octets: 2	2	n = Length

图 4.5 信息元素格式

4. MOVE-response 数据包

MOVE-response 数据包用 IP/UDP 协议封装，使用 IAPP 协议发送。该数据包直接发送到那个发出 MOVE-notify 数据包的 AP。MOVE-response 数据包的数据域携带了重关联 STA 的 MAC 地址和与该 STA 有关的上下文。该数据包的数据域格式如图 4.6 所示。

Address Length	Reserved	MAC Address	Sequence Number	Length of Context Block	Context Block
Octets: 1	1	n=Address Length	2	2	m=Length of Context Block

图 4.6 MOVE-response 数据域格式

其中，

(1)Address Length 域：是 8 位整数指出 MAC Address 的字节数量；

(2)Reserved 域：协议的保留域，设为 0，接收时应被忽略；

(3)MAC Address 域：是关联的移动 STA 的 MAC 地址；

(4)Sequence Number 域：该域包含了引起生成该响应数据包的 MOVE-notify 数据包的 SN 值；

(5)Length of Context Block 域：是一个 16 位整数，指出 Context Block 域的字节数量；

(6)Context Block 域：是一个变长域，包含了由 MAC Address 域确定的重关联 STA 传递的上下文信息，Context Block 的内容应该被 IAPP 解释。

5. L2 更新帧

L2 更新帧是一个 802.2 类型 1 逻辑链路控制(Logical Link Control，LLC)交换标识(Exchange Identifier，XID)更新响应帧。该帧使用关联移动 STA 的 MAC 地址发送，以至于任何二层设备如网桥，交换机和其他 AP 能够更新它们的前传表，修正端口以达到移动 STA 的新位置。一个载于 802.3 上的 XID 更新帧格式如图 4.7 所示。

MAC DA	MAC SA	Length	DSAP	SSAP	Control	XID Information Field
Octets: 6	6	2	1	1	1	3

图 4.7 L2 更新帧格式

其中，

(1)MAC DA 域：是广播 MAC 地址(FF：FF：FF：FF：FF：FF)；

(2)MAC SA 域：是关联或重关联的移动 STA 的 MAC 地址；

(3)Length 域：是该域后面所有信息的长度；

(4)DSAP 域：设为空(NULL)；

(5)SSAP 域：设为空(NULL)；

(6)Control 域：IEEE 802.2 标准规定的值，为 0xAF；

(7)XID Information Field 域：IEEE 802.2 标准规定的值，为 0，0，0。

4.1.3 设备发现

设备发现，即 AP 和发现设备服务器之间通过交互设备发现消息，达到发现分布系统内的网络设备，了解网络拓扑结构的目的。通常在分布系统内担当发现设备服务器的是 AC 设备，在没有 AC 设备时，也可以是其他具有发现设备服务器功能的设备。

AP 和 AC 在初始化时都尝试发现对方设备，经过设备发现消息的交互各自建立了与对方的联系。AP 设备主要有四种状态："初始态"，"非受控态"，"等待态"，"控制态"。

"初始态"是指 AP 在初始化时或消息交互中设置的状态，在此状态下 AP 将清除设备发现其他状态机，重新开始设备发现。一般在初始态，AP 将连续 10 次广播发送 DISCOVER-INIT 消息，以尝试接收来自发现设备服务器的 DISCOVER-RESPONSE 消息，以及通知其他 AP 学习自己的相关信息。

"非受控态"是指 AP 在初始态时 10 次发送 DISCOVER-INIT 消息结束，没有接到发现设备服务器的 DISCOVER-RESPONSE 消息而转变的状态。此状态下，AP 继续定期发送 DISCOVER-HELLO 消息，来通知其他 AP 检测自己是否在线。

"等待态"是指 AP 在初始态时 10 次发送 DISCOVER-INIT 消息结束，接到发现设备服务器的 DISCOVER-RESPONSE 消息，由于消息附带信息超出以太网最大传输要求而分片传输时，AP 等待接收所处的状态。是"初始态"到"控

制态”的过渡状态。

“控制态”是指AP在初始态时10次发送DISCOVER-INIT消息结束，接到完整的发现设备服务器的DISCOVER-RESPONSE消息而转变的状态。此状态下，AP继续定期发送DISCOVER-HELLO消息，来通知其他AP检测自己是否在线。以及定期发送DISCOVER-ONLINE消息，来通知发现设备服务器检测自己是否在线。

AC设备的设计说明有其他相关文档描述，因此这里只介绍AP设备的设备发现设计。

4.1.3.1 AP的状态

在设备发现的消息交互中，AP有四种状态：“初始态”，“非受控态”，“等待态”和“受控态”。

1. AP处于“初始态”

1. AP初始化后状态设置为“初始态”；
2. 启动“DISCOVER-INIT定时器”，发送“DISCOVER-INIT消息”，等待AC的应答；
3. 侦听AC的“DISCOVER-RESPONSE消息”，如果收到AC的“DISCOVER-RESPONSE”消息，记录该AC相关信息(如MAC地址，IP地址等)，并转变为“等待态”或“受控态”，终止“DISCOVER-INIT定时器”；启动“DISCOVER-ONLINE定时器”，定期发送“DISCOVER-ONLINE消息”；
4. 侦听其他设备的“DISCOVER-INIT消息”，记录该设备相关信息(如MAC地址，IP地址等)；
5. 侦听其他设备的“DISCOVER-HELLO消息”，记录该设备相关信息(如MAC地址，IP地址等)；
6. 如果“DISCOVER-INIT定时器”超时，AP转变为“非受控态”，启动“DISCOVER-ONLINE定时器”，定期发送“DISCOVER-ONLINE消息”。

2. AP处于“非受控态”

1. AP状态设置为“非受控态”；
2. 侦听其他设备的“DISCOVER-INIT消息”，(如果发送方是其他AP时，记录该AP相关信息，并发送一个“DISCOVER-HELLO消息”；如果发送方是AC时，记录该AC相关信息，AP转变为“初始态”，终止“DISCOVER-ONLINE定时器”，重新发起设备发现。)
3. 侦听其他AP的“DISCOVER-HELLO消息”，记录该AP相关信息。
4. 侦听AC的“DISCOVER-RESPONSE消息”，AP转变为“初始态”，终止“DISCOVER-ONLINE定时器”，重新发起设备发现。

3. AP处于“等待态”

1. AP状态设置为“等待态”；
2. 侦听其他设备的“DISCOVER-INIT消息”，(如果发送方是其他AP时，记录该AP相关信息，并发送一个“DISCOVER-HELLO消息”；如果发送方是AC时，记录该AC相关信息，AP转变为“初始态”，终止“DISCOVER-ONLINE定时器”，重新发起设备发现。)
3. 侦听其他AP的“DISCOVER-HELLO消息”，记录该AP相关信息。
4. 侦听AC的“DISCOVER-RESPONSE消息”，如果是最后一个消息包时，AP转变为“受控态”。

4. AP处于“受控态”

1. AP状态设置为“受控态”；
2. 侦听其他设备的“DISCOVER-INIT消息”(如果发送方是其他AP时，记录该AP相关信息，并发送一个“DISCOVER-HELLO消息”；如果发送方是AC时，记录该AC相关信息，AP转变为“初始态”，终止“DISCOVER-ONLINE定时器”，重新发起设备发现)；
3. 侦听其他AP的“DISCOVER-HELLO消息”，记录该AP相关信息；
4. 侦听AC的“DISCOVER-RESPONSE消息”，如果是最后一个消息包时，AP转变为“受控态”。重新设置“DISCOVER-ONLINE定时器”，定期发送“DISCOVER-ONLINE消息”。

4.1.3.2 定时器设定

1. DISCOVER-INIT 定时器

该定时器用于在 AP 处于“初始态”时，发送“DISCOVER-INIT 消息”。系统缺省设置超时时间：1 秒；“DISCOVER-INIT 消息”发送最多：10 次。

2. DISCOVER-HELLO 定时器

该定时器用于 AP 之间互相确认是否在线。系统缺省设置超时时间：300 秒。

3. DISCOVER-ONLINE 定时器

该定时器用于 AP 与 AC 之间互相确认是否在线。系统缺省设置超时时间：3 秒。

4. DEV-AGING 定时器

该定时器用于老化 AP 学习到的外部设备。系统缺省设置超时时间：1200 秒。

4.1.3.3 拓展数据包格式

设备发现在 IAPP 子系统内实现，AP 与 AC 间设备发现信息的传递由于没有协议的支持，必须使用自定义的私有协议，在本软件系统内则利用 IAPP 协议原语及数据包的保留命令，在其上进行拓展的方法实现。一般 IAPP 数据包的格式如图 4.8 所示，

IAPP Version	Command	Identifier	Length	Data
Octets: 1	1	2	2	0-n

图 4.8 一般IAPP数据包格式

其中Command域标准规定的取值为，

ADD-notify 0

MOVE-notify 1

MOVE-response 2

3-255 是保留命令，自定义设备发现信息命令(10)作为在群组内 AP 与 AC 间交互设备发现的消息命令。由于 IAPP 的设备发现定义了多种报文，因此使用子命令加以区分，分别是：

DISCOVER-INIT	17
DISCOVER-ONLINE	18
DISCOVER-HELLO	19
DISCOVER-RESPONSE	33

在 AP 向 AC 或 AC 向 AP 发出的设备发现消息中，我们可以附加任意个信息元素属性，以达到拓展其他功能的目的。

设备发现拓展的数据包格式描述如下：

1. **Discover-init 数据包， Discover-online 数据包， Discover-hello 数据包**

Discover-init 数据包， Discover-online 数据包， Discover-hello 数据包具有相同的报文格式，该数据包被发送到广播地址(或多播地址)子网，将到达局部子网的每一个设备。

报文格式：省略。

2. **Discover-response 数据包**

该数据包被送达发起该发现请求数据包的设备。

报文格式：省略。

4.1.4 分析

IAPP 协议里的 APME(AP management entity)作为 AP 的管理实体，与 802.11 无线驱动模块进行交互，接收来自驱动模块的触发消息，发送相应的指示消息到驱动模块控制设备的运行，并且负责接收来自同一 ESS 内其它 AP 发来的服务，通过服务访问点 IAPP SAP 调用 IAPP 服务。

如图 3-1 STA2 断开与 AP1 的连接，与 AP2 建立新连接，这段时间 t_1 又

是由 AP2 的反应时间 t_{11}和交换机 Switch1 的转发表的老化时间 t_{12}组成(即 $t_1=t_{11}+t_{12}$)，因此可以通过减少 t_{12}来改进 WLAN 的切换性能。当 STA 关联或者重新关联一个 AP，APME 将发送 IAPP-ADD.request 或 IAPP-MOVE.request 报文给 IAPP 模块，IAPP 模块接收后，检测报文合法后，立刻广播或者组播 Layer 2 Update Frame。因此交换机，网桥，其它 AP 接收到该报文后更新转发表。IAPP 通过提前主动请求更新二层设备转发表的方法，来减少 STA 切换的时延。由于 IAPP 是在向本地传输层发送 ADD-notify 报文之前发送 Layer 2 Update Frame，t_{12}时间和 t_{11}时间已经重叠起来，因此可以认为 $t_1=t_{11}$。流程图如图 4.9：

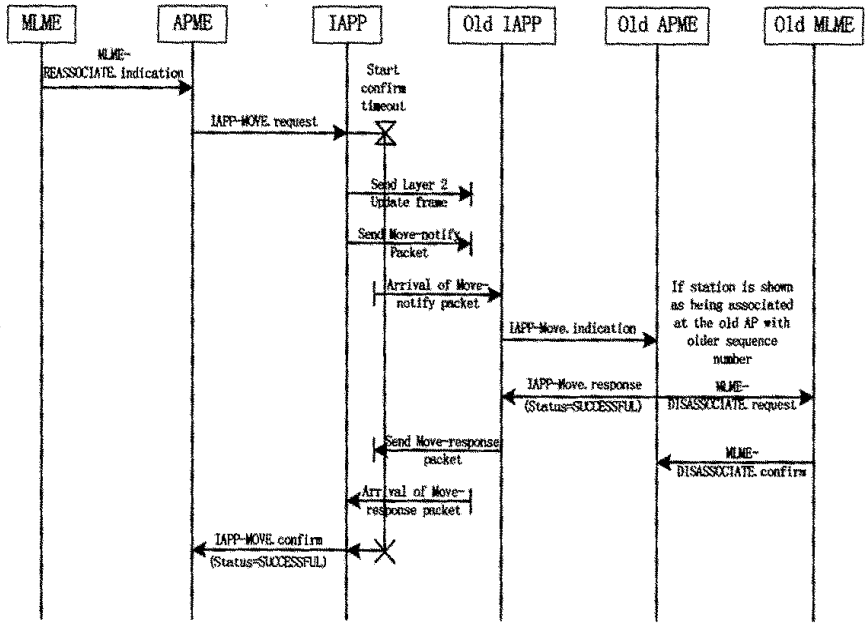

图 4.9 STA Reassociation

4.2 预认证策略

无线网络的安全问题越来越受到人们的关注。通常网络的安全性主要体

现在访问控制和数据加密两个方面域管理方法。对用户或设备访问网络的合法性提供认证是当然网络运营商惯用的手段，不仅可以控制非法用户的接入，而且对无线客户端的计费等管理。当 STA 关联一个 AP 时，因为 802.1x 支持 AP 与 RADIUS 进行信息交换而非用户与 Radius 直接交换，所以在无线认证中主要是以 802.1x 来提现移动性，而非 portal PPPOE。

AP 与 RADIUS 之间的交互信息包括 AP 的 BSS ID 到 IP 地址之间的映射，RADIUS 向 AP 发送密钥以保证 AP 之间的安全通信。当 STA 需要切换时，需向新 AP 发出关联或者重新关联消息，AP 应与 RADIUS 服务器进行消息交互，实现新 AP BSSID 与 IP 地址的映射，并且 RADIUS 服务器向 AP 发送相应的密钥。由于每次 STA 切换时 AP 都需要与 RADIUS 服务器进行消息交换，因此发生切换的时延比较长。

到目前为止，还没有预认证的标准，因此我们使用的是 IAPP 的 ESP(Encapsulating Security Payload)字段，这个字段是 IEEE 802 工作组预留的字段，各个设备厂家灵活使用，同时这也带来了一个问题，就是不同厂家的 AP 之间，目前来说预认证功能还不能生效，不过一般说来，一个热点区域的 AP 往往是同一个厂家生产的，所以影响比较小。

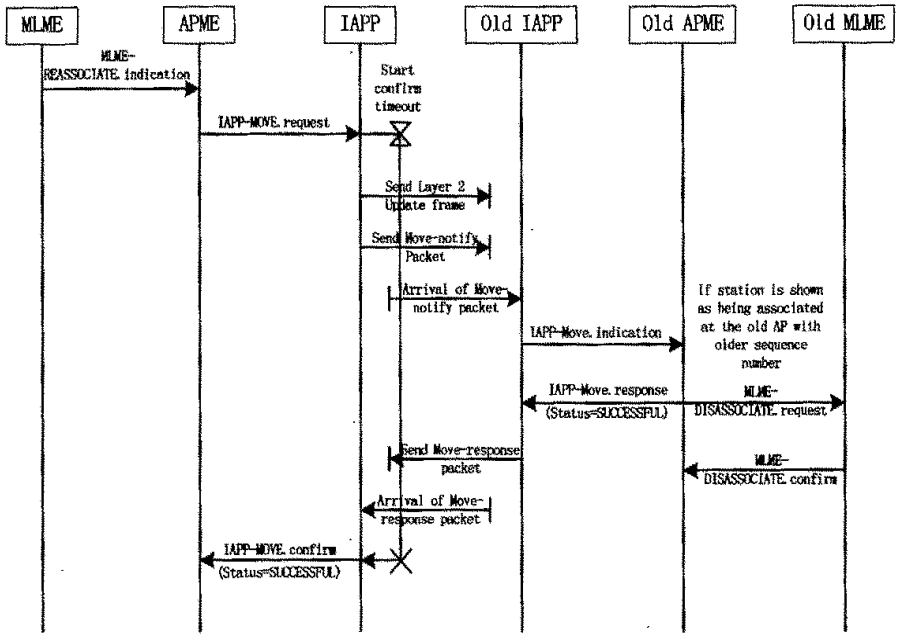

图 4.10 STA 预认证

如图 4.10，STA1 断开 AP1 的关联，切换到 AP2，AP2 的 APME 将发送 IAPP-ADD.request 或 IAPP-MOVE.request 报文给 IAPP 模块，IAPP 模块接收后，检测报文合法，广播或者组播 Layer 2 Update Frame 后，立刻检索 IAPP-ADD.request 中的 old AP 字段，从而得到 AP1 的 MAC 地址，AP2 与 Radius 服务器交互得到 AP1 的 MAC 地址，向 AP1 发送 Move-notify 报文。AP1 接受到 AP2 的 Move-notify 报文之后，立刻在回复报文 Move-response 的 ESP 字段中填入 STA 在 radius 服务器上的信息，从而免去了 STA 在切换时重新认证的过程。从而可以认为 $t_2 \rightarrow 0$。

4.3 实验

4.3.1 实验依据

实验组网如图 3.3，传统上，话音质量的测试是主观的：拿起电话，听一段通话，然后判断其话音质量。其中，比较突出的话音质量主观评估方法是 MOS(Mean Opinion Score)，具体参见 ITU (International Telecommunications Union)的 P.800 建议。ITU 的 P.800 建议描述了人们的这些反应，包括在听到不同延迟和丢包的语音时会给出的印象分。建立了网络特性，包括延迟和丢包等，与印象分之间的对应关系，使得 MOS 对于网络的 VoIP 的评估和调整十分有意义。

MOS 的评分从 1 分到 5 分，其中 1 分表示非常糟糕，而 5 分表示非常好。具体如表格 5.1：

表 5.1 MOS 值的分级

下限	上限	用户满意度
4.34	5.00	非常满意
4.03	4.34	满意
3.60	4.03	部分用户满意
3.10	3.60	很多用户不满意
2.58	3.10	几乎所有用户不满意
1.00	2.58	不可接受

4.3.2 Chariot 测试结果分析

对于 VoIP 测试而言，最重要的结果参数有：VoIP、One-way Delay、Jitter 和 Packet Loss(在 Datagram 中)。

首先看 VoIP，如果该 MOS 值低于 3.60，则可以认为该网络对 VoIP 的业务支持很差，下面检查相关的参数。如果 One-way Delay 超过了 150ms，则认为网络延迟太大；如果 Jitter 超过了 20ms，则认为抖动太大；如果 Packet Loss 超过了 1%，则认为丢包率太高。如果网络质量达不到要求，下面需要

和网络提供者对网络进行调整，包括增加带宽、寻找性能瓶颈点并升级或者改变路由、减少网络的跳数、提高 VoIP 数据流的优先级、减少同时并发的 VoIP 呼叫数等等。具体手段要根据测试结果和网络进行。

本次实验的组网图如图 3.3 所示，使用 802.1x 认证，SIP 协议。每种情况测试 3 次，取其平均值。

关闭 AP 的负载均衡和预认证功能

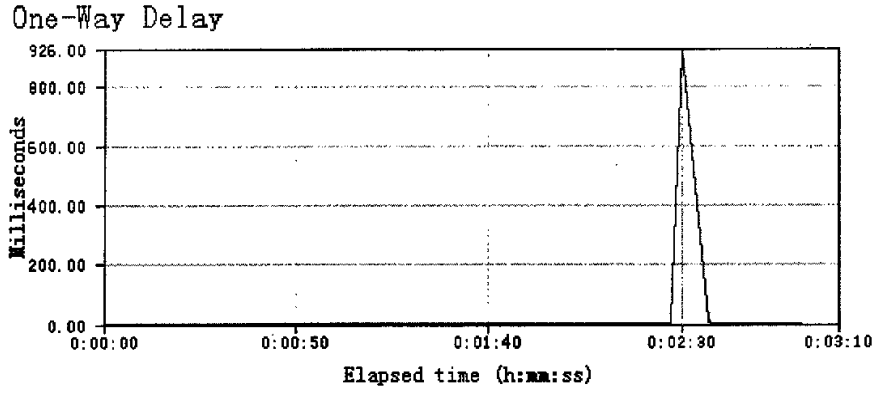

图 5.2 延时图

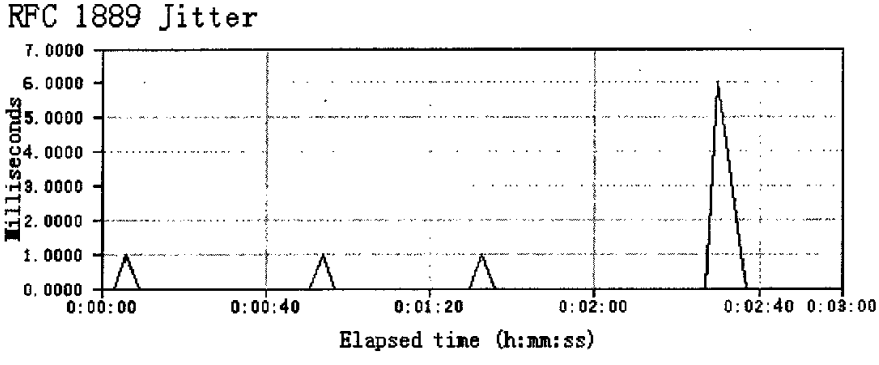

图 5.3 语音抖动图

启用 AP 的负载均衡和预认证功能

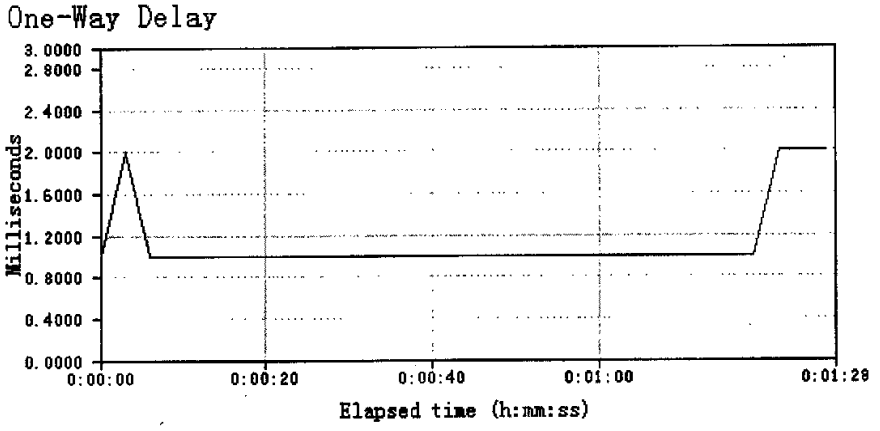

图 5.4 延时图

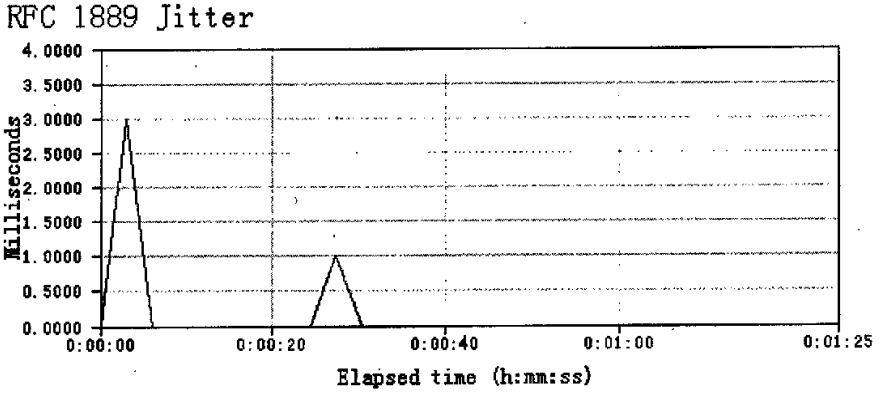

图 5.5 语音抖动图

从上面的数据可以看出，启用负载均衡和预认证功能后，时延从先前的 960ms 减少到 1.6ms，由此可以看出负载均衡和预认证措施起到了积极的作用。同时从启用负载均衡和预认证功能前后，语音的 Jitter 参数来看，并没有明显的改进，原因在于切换性能影响的只是语音的 mos 值、丢包、延时，而对 jetter 没有大的影响。另外的实验表明，负载容量对 mos 值，jetter

的影响比较大。

4.4 本章小结

本章详细讲述了 WLAN 切换的三个过程：二层设备转发表的更新时间；STA 与 Radius Server 注册时间；业务更新时间，对于 VoWLAN 来说就是 STA 在 SIP Server 上的注册时间。然后详细介绍了解决方案负载均衡和预认证措施。最后给出 VoWLAN 切换实验。

第5章 展望

目前 WLAN 的建设大部分都是以 Hotspot(热点)的形势出现的，当多个 Hotspots 组成 Hotzone(热点区域)时需要新技术支持 STA 在更大的移动范围内移动，譬如 MESH，移动 IP 技术。

5.1 MESH

目前 WLAN 的 DS 一般都是以太网连接，这样的网络拓扑结构相对固定，AP 与 AP 之间只能通过有线连接，如果有线出现故障，网络可能会瘫痪，因此目前 MESH 网络成为 WLAN 研究的热点

无线 MESH 网络是一种与传统的无线网络完全不同的网络。传统的无线网络必须首先访问集中的接入点(AP)才能进行无线连接。这样的话，即使两个节点互相挨着，它们也必须通过接入点才能进行通信。而在无线 MESH 网络中，每个节点都可以与一个或者多个对等节点进行直接通信。"MESH"这个词原来的意思就是指所有的节点都互相连接，当然实际上绝大多数现代的 MESH 网络只是通过部分节点相互连接。MESH 网络技术一度曾是一项军方技术，随着人们对 802.11a、802.11b 和 802.11g 等 LAN 技术了解的深入，MESH 网络才逐步成为企业界和消费者瞩目的焦点。图 5.1 是一个简单的 MESH 网络示意图。

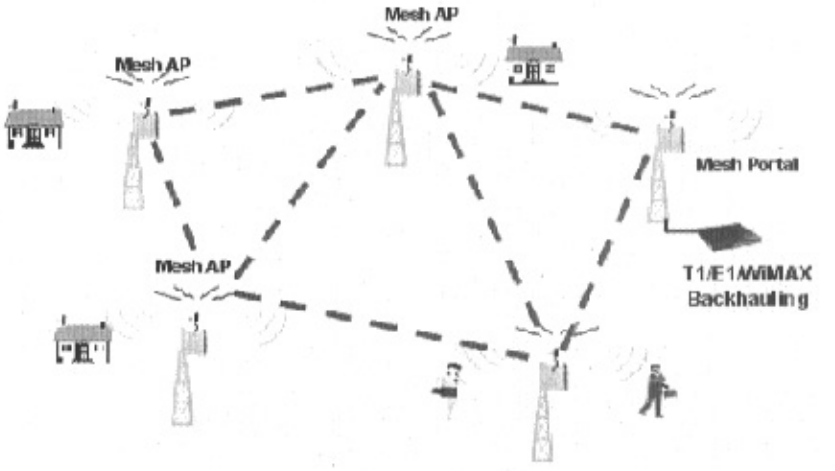

图 5.1 MESH 网络示意图

无线 MESH 网技术通过自动配置实现节点间的互联以及用户节点对骨干网的访问，摆脱了以往对中心节点(如基站)的依赖，可以灵活地应用于多种无线环境。目前，无线 Mesh 网技术处于初步发展的阶段，要充分发挥其潜力，还需要解决诸如智能天线设计、动态资源分配、无线路由算法等多项关键技术。但是，无线 MESH 网作为一种新的具有众多优点的技术，通过与其他无线网络技术相结合，将在下一代宽带无线网络中发挥重要的作用。

美国 Tropos Networks 公司采用其特有的 MetroMESH 体系结构。该结构可确保 Wi-Fi 在城域中的有效覆盖以及良好的无缝移动性。使之真正成为和今天移动 WiMAX 所宣传的高速移动宽带网络一样，具有很强的优势。利用 Tropos Networks 公司的 MetroMESH 技术，可以使服务供应商、公共安全机构和市政当局为用户提供定点或移动性的 IP 语音，数据和视频等应用和服务。而这是以前小规模 Wi-Fi 所达不到的，这也给运营商提供了一种规模部署、规模运营的可能。中国目前只有台湾的 ACCTON 公司在做 MESH 网络产品。

5.2 辅以移动IP和DHCP

当 STA 跨越不不同网段的时候，STA 的网络层应用就会中断，这时就需要

移动 IP 技术和 DHCP 技术[25][26]。

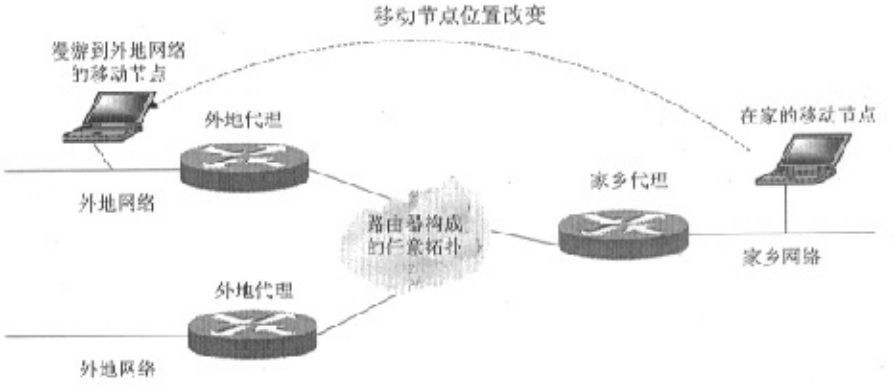

图 5.2 移动 IP 各个功能实体

如图 5.2，家乡代理有一个端口与移动节点家乡网络连接。当移动节点离开家乡网络时，家乡代理广播对移动节点家乡地址的网络前缀的可达性，从而吸引那些送往移动节点的家乡地址的 IP 包；同时解析送往移动节点的 IP 包，并将这些包通过隧道技术送到移动节点的转交地址。当移动节点漫游到外地网络时，外地代理帮助移动节点通知家乡代理它的转交地址，能够把家乡代理通过隧道送来的数据包拆封后转发给移动节点，同时作为连接在外地链路上的移动节点的缺省路由器。

结　论

无线局域网是指以无线信道作传输媒介的计算机局域网络，是计算机网络与无线通信技术相结合的产物，它以无线多址信道作为传输媒介，提供传统有线局域网的功能，能够使用户真正实现随时、随地、随意的宽带网络接入。WLAN 技术使网上的计算机具有可移动性，能快速、方便地解决有线方式不易实现的网络信道的连通问题。利用电磁波在空气中发送和接收数据，而无需线缆介质。随着个人数据通信的发展，功能强大的便携式数据终端以及多媒体终端的广泛应用，为了实现任何人在任何时间、任何地点均能实现数据通信的目标，要求传统的计算机网络由有线向无线，由固定向移动，由单一业务向多媒体发展，推动了无线局域网(WLAN)的发展。

IEEE 802.11 协议制定了无线局域网 MAC 层和物理层的规范及其基本结构，但并没有对无线局域网的构建做出规定。这给接入点 AP 和由其组成的分布式系统在功能设计留出了很大的自由空间，但同时也给无线站点 STA 的移动带来了问题，使 STA 不能自由地在不同厂商生产的 AP 间移动，抑制了 WLAN 的广泛推广和应用。

目前 WLAN 虽然剪断了电缆的束缚，现在只是“半移动”状态，移动终端只能在同一个区域内随时随地接入 Internet，提供区域性的漫游功能。但是目前这种业务主要是在数据业务方面，而在对实时性要求较高的业务如语音，视频支持不好。现在的发展目标，将是完全漫游的能力，即在以一定速度行进时，可无中断地收发数据，这将是实现个人通信网(PCN)的一条有效途径。

WLAN 当前最热门的一个课题是 VoWLAN，VoWLAN 是 WLAN 的新兴应用之一，从技术层面来说，语音业务对于延迟敏感度远远高于数据业务。VoIP 是指 IP 电话通过数据网络传输语音信号。WLAN 能够无线上网。VoWLAN 可以说是这两者的有机结合，它可以利用现有的 WLAN 网络实现无线的 VoIP 通话能力， 企业内部员工可以通过 VoWLAN 在办公场所以外的地方随时访问语音、E-mail 和其他已连的网络资源，这样提高了网络资源的利用率并降低了每次电话呼叫的成本，从而节省企业的总体 IT 费用。对于住宅用户也可以通过与宽带 802. 11 无线网络相连的 VoIP 电话降低话费。本课题通过改进 IAPP 负

载均衡协议，并且进行预认证等方面改进 WLAN 的切换性能，使得切换漫游平滑。实验证明，本课题提出的方案切实有效!

参考文献

[1] 刘元安. 宽带无线接入与无线局域网[M]. 北京：北京邮电大学出版社，2001

[2] 陈如明.中国宽带无线频率规划、频谱管理及相关策略考虑[J].中兴通讯技术.2002,8(6):1-6 页

[3] 赵新胜,尤肖虎.未来移动通信系统中的无线资源管理[J].中兴通讯技术.2002,8(6):7-10 页

[4] 吴伟陵.下一代移动通信探讨[J].中兴通讯技术.2002,8(6):11-15 页

[5] 刘元安.无线局域通信网[J].中兴通讯技术.2002,8(6):16-18 页

[6] 曹淑敏.移动通信的发展动态与前景[J].中兴通讯技术.2001,7(3)： 40-42 页

[7] 刘东苏,王新梅.移动接入系统的安全技术[J].中兴通讯技术.2001,7(5):10-13 页

[8] 王育民,刘建伟.通信网的安全--理论与技术[M].西安:西安电子科技大学出版社,1999

[9] 朱近康,邱玲.移动通信调制技术的进展[J].中兴通讯技术. 2001,7(3):52-55 页

[10]隆克平,Rodney S.Tucker,王重钢.一种新的 IP DiffServ over OBS 网络体系结构及性能分析[J].重庆邮电学院学报(自然科学版).2004,16(2):1-6 页

[11]李映,王汝传,徐小龙.卫星网络中 IP 路由技术的研究[J].重庆邮电学院学报(自然科学版).2004,16(2):39-43 页

[12]袁刚,甘家宝,王文东等.MPLS 网络的 QoS 及其管理框架实现方式[J].重庆邮电学院学报(自然科学版).2003,15(3):57-61 页

[13]Eric Ouellet 等著.构建Cisco无线局域网[M]. 张颖等译.科学出版社,2003 (6)

[14]IEEE Std 802.11.Standards for Local and Metropolitan Area Networks-WLAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications[S].1999

[15]IEEE Std 802.11b.Standards for Local and Metropolitan Area Networks -Part 11: WLAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer Extension in the 2.4 GHz Band[S].1999

[16]IEEE Std 802.11a.Standards for Local and Metropolitan Area Networks -Part 11: WLAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications:High-Speed Physical layer Extension in the 5GHz Band[S].1999

[17]Aboha B, Simon D. IETF RFC 2716. PPP EAP TLS Authentication Protocol[S].1999

[18]Blunk L, Vollbrecht J.IETF RFC 2284. PPP Extensible Authentication Protocol(EAP)[S].1998

[19]Tim Moore.Suggested Changes to Robust Security Network (RSN) for IEEE 802.11[R].IEEE P802.11 Task Group I Meeting Update, 2002

[20]IEEE 802.11i Group. Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems LAN/MAN Specific Requirements[S].2002

[21]IEEE 802.11f IEEE Recommended Practice for Multi -Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation

[22]Hedetniemi S, Liestman A. A survey of gossiping and broadcasting in communication networks.Networks,1998,18(4):319-349p

[23]Sohrabi K,Gao J, Ailawadhi V,Pottie GJ.Protocols for self-organization of a wireless sensor network.IEEE Personal Communications,2000,7(5): 16-27p

[24]Heinzelman W, Chandrakasan A, Baladrishnan H.Energy efficient communication protocol for wireless microsensor networks.In: Proceedings

of the 33rd Hawaii International Conference on System Sciences.Maui: IEEE Computer Society,2000.3005-3014p

[25]Internet draft (draft-choi-mobileip-Idext-O1.txt)-2001. Extension of LDP for Mobile IP Service through the MPLS Network[S]

[26]RFC2002-1996.IP Mobility Support[S]

[27]KIM H.Mobility-Aware MPLS in IP-based wireless access networks[A]. IEEE

[28]Globecom 2001[S].San Antonio,Tx,2001

[29]FABIOM. Chiussi. A Network Architecture for MPLS - Based Micro-Mobility[R].Bell Laboratories,Lucent Technologies

[30]YANGT, MAKRAKISD. Mobile MPLS: Supporting Delay Sensitive Applications Over Wireless Internet[A].International Conferences on Info-tech & Info-net(ICII2001)[C].Beijing,China,October 2001

[31]Schneier B.Applied Cryptography Protocols,Algorithms,and Source Code in C(Second Edition)[M].USA:John Wiley&sons,Inc,1996

[32]Fluhrer S, Mantin I, Shamir A.Weaknesses in the Key Scheduling Algorithm of RC4[EB/OL].http://www.drizzle.com/aboba/IEEE/rc4--ksaproc.pdf, 2001-08-16

[33]Borisov N.Wireless Privacy,Analysis of 802.11 security[EB/OL].http://download.nai.com/products/media/sniffer/pdf/sniffer wireless.pdf.2002-O9-O9.

[34]Potter B.Wireless Security and Privacy Future [M] IEEE Security and Privacy July/August,2003

[35]Jesse Walker 802.11 Security Series Part II:TKIP.[EB/OL]http://cedar.intel.com

[36]Russ Housley and Jesse Walker Security Flaws in 802.11 Data Link Protocols May,2003[Z]

[37]Paul Congdonetal. IEEE802.1x RADIUS Usage Guide-lines. Networking Group, 2003[Z]

[38]IEEE Std 802.1x, Port-based Network Access Control".2003[Z]

[39]National Institute of Standards and Technology.FIPS Pub 197:Advanced Encryption Standard(AES).Nov.26,2001[S]

攻读硕士学位期间发表的论文和取得的科研成果

[1] 顾国昌,尹浩，惠铁.WiMAX 技术的发展与应用.信息技术.已录用

致 谢

经过两年多的学习生活，在老师、亲友、同事、同学的关心和支持下，我的硕士论文终于如期完成了，论文的每一步工作都倾注着老师的心血！导师以其渊博的学识，敏锐的洞察力，严谨、求实的治学态度和勤奋、创新的钻研精神所树立的学者风范使我受益匪浅，并将为我终生效仿的楷模；导师高尚的敬业精神，平易近人的生活态度以及给予我的谆谆教诲，给我留下了深刻的印象，必将对我今后的人生产生深远的影响。值此论文完成之际，谨向辛勤培育和关心我的导师顾国昌教授致以崇高的敬意和衷心的感谢！同时也要感谢杨永田老师、张汝波老师、张国印老师、黄少滨老师、刘杰老师以及计算机学院的其他所有老师在我六年多的学习和生活中所给予的帮助和支持。

在我求学的过程中，得到了中兴通讯南京研究所的领导的关怀和培养，我的论文才能得以顺利完成，在此表示最真挚的感谢。此外，向南京数据事业部，网络事业部终端项目组的所有成员表示感谢，是他们在日常的工作和学习中给了我无私的帮助和耐心的辅导。感谢课题期间给予我关心和支持的史建军，郭仕刚，张磊，王占利，张远等同事，他们对于我的课题提出了许多中肯的建议。

最后，我要感谢我的家人，在我求学的每一级台阶上都有他们的鼓励和支持。

谨祝哈尔滨工程大学计算机学院明天更加美好，前途更加辉煌！