

# 智能办公无线局域网组网 技术方案书

上海宜悦网络科技有限公司

# 目 录

1	网络详细设计及实行方案.....	3
1.1	网络设计原则.....	3
1.2	无线局域网技术.....	4
	无线局域网频道分派与调制技术.....	4
	无线局域网拓扑构造.....	5
	无线局域网的几种重要工作过程.....	7
	影响无线局域网性能的原因.....	7
	无线局域网的安全性.....	8
1.3	覆盖考虑.....	9
1.4	无线链路计算.....	9
2	智能小区无线网络覆盖背景简介.....	10
2.1	无线网络实行目的.....	10
2.2	无线网络需求分析.....	11
	应用需求.....	11
	功能需求.....	11
	方案选型.....	11
3	无线组网详细设计方案.....	12
3.1	无线网络产品的优势及特点.....	12
3.2	方案总体网络设计.....	13
	总体网络拓扑图.....	13

	无线覆盖原理.....	14
	机房网络设计.....	15
	方案阐明.....	17
	设备选型.....	18
	网络构造.....	18
3.5	远景规划.....	21
	硬件扩充.....	21

## 前 言

伴随通信事业的高速发展，无线数据通信已逐渐成为一种重要的通信方式。无线数据通信不仅可以作为有线数据通信的补充及延伸，并且还可以与有线网络环境互为备份。在某种特殊环境下，无线通信是重要的甚至唯一的可行的通信方式。从通信方式上考虑，多元化通信方式是现代化网络通信的重要特性。

# 1 网络详细设计及实行方案

## 1.1 网络设计原则

根据 802.11 无线局域网的国际规范和国家无线电管理委员会的原则，在进行实际的网络设计时，我们会遵照下列原则。

### 一〉 先进性原则

采用先进的设计思想，选用先进的网络设备，使网络在此后一定时期内保持技术上的先进性。

### 二〉 开放性原则

网络设计及网络设备选型遵从国际原则及工业原则，使网络具有开放性和兼容性。

### 三〉 可伸展性原则

网络设计在充分考虑目前状况的同步，必须考虑到此后较长时期内业务发展的需要，留有充足的升级和扩充的也许性。

### 四〉 安全性原则

网络系统的设计必须贯彻安全性原则，以防止来自网络内部和外部的多种破坏。

### 五〉 可靠性原则

网络系统的设计必须贯彻可靠性原则，使网络系统具有很高的可用性。

### 六〉 可管理性原则

网络系统应具有良好的可管理性，使得网络管理人员能以便及时地掌握诸如网络拓扑构造、网络性能记录、网络故障等信息，能简便地对网络进行配置和调整，保证网络工作在良好状态。

## 1.2 无线局域网技术

### 无线局域网频道分派与调制技术

无线局域网采用电磁波（RF）作为载体传送数据信息。对电磁波的使用分两种常见模式：窄带和扩频。窄带技术以微波为主，合用于长距离点到点的应用，可以到达 30 公里。由于它采用的频道较宽以及定向信号天线，因此其最大带宽可达 10Mbps，但受环境干扰较大。

无线局域网采用无线扩频(spread spectrum)技术，也称 SST，初期由军事部门研发，保证安全可靠的军事通讯。常见的扩频技术包括两种：调频扩频（FHSS）和直序扩频（DSSS），它们工作在 2.4-2.4835GHz。

**调频技术**将 835MHz 的频带划提成 79 个子频道，每个频道带宽为 1MHz。信号传播时在 79 个子频道间跳变，因此传播方与接受方必须同步，获得相似的跳变格式，否则，接受方无法恢复对的信息。调频过程中假如碰到某个频道存在干扰，将绕过该频道。受跳变的时间间隔和重传数据包的影响，调频技术的经典带宽限制为 2-3Mbps。

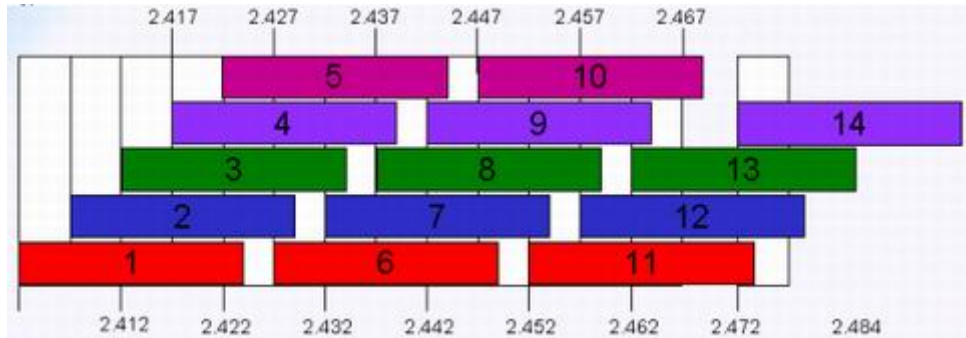
无线个人网采用的蓝牙技术就是采用调频技术，该技术提供非对称数据传播，一种方向速率为 720Kbps，另一种方向速率仅为 57Kbps。蓝牙技术也可以传送 3 路双向 64Kbps 的语音。

**直序扩频技术**是无线局域网 802.11b 采用的技术，将 83.5MHz 的频带划提成 14(中国)个子频道，每个频道带宽为 22MHz。直序扩频技术用一种冗余的位格式来表达一种数据位，这个冗余的位格式称为 chip，因此它可以抗拒窄带和宽带噪音的干扰，提供更高的传播速率。

直序扩频技术采用采用 DBPSK 和 DQPSK 调制技术，提供的最高带宽为 11

Mbps，并且可以根据环境原因的限制自动降速至 5.5Mbps，2Mbps，1Mbps。

14 个子频道分派如下图：



在多种频道同步工作的状况下，为保证频道之间不互相干扰，原则规定两个频道的中频间隔不能低于 25MHz。因此从上图可以看出，在一种蜂窝区内，直序扩频技术最多可以提供 3 个不重叠的频道同步工作，提供高达 33Mbps 的吞吐量。

## 无线局域网拓扑构造

无线局域网组网分两种拓扑构造：对等网络和构造化网络。

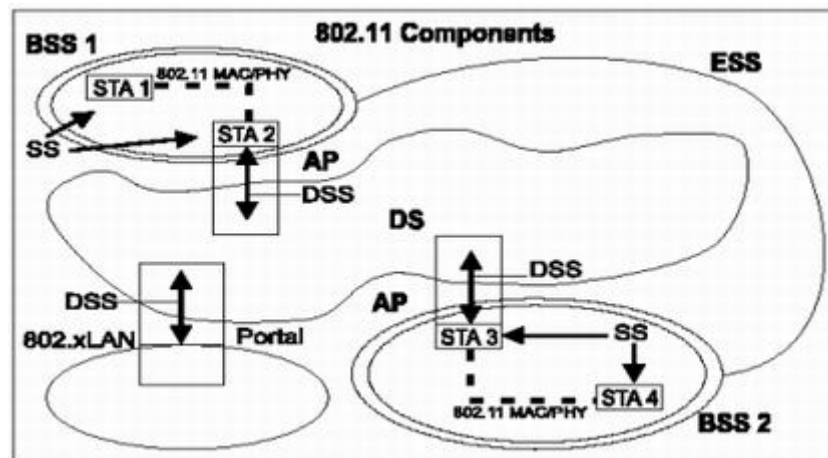
**对等网络**也成 Ad-hoc 网络，它覆盖的服务区称独立基本服务区。对等网络用于一台无线工作站和另一台或多台其他无线工作站的直接通讯，该网络无法接入有线网络中，只能独立使用。



对等网络中的一种节点必需能同步“看”到网络中的其他节点，否则就认为网络中断，因此对等网络只能用于少数顾客的组网环境，例如 4 至 8 个顾客，并且他们离得足够近。

**构造化网络**由无线访问点（AP）、无线工作站（STA）以及分布式系统（DSS）构成，覆盖的区域分基本服务区（BSS）和扩展服务区（ESS）。无线访问点也称无线 hub，用于在无线 STA 和有线网络之间接受、缓存和转发数据。无线访问点一般可以覆盖几十至几百顾客，覆盖半径达上百米。

基本服务区由一种无线访问点以及与其关联（associate）的无线工作站构成，在任何时候，任何无线工作站都与该无线访问点关联。换句话说，一种无线访问点所覆盖的微蜂窝区域就是基本服务区。无线工作站与无线访问点关联采用 AP 的基本服务区标示符（BSSID），在 802.11b 中，BSSID 是 AP 的 MAC 地址。



扩展服务区是指由多种 AP 以及连接它们的分布式系统构成的构造化网络，所有 AP 必需共享同一种扩展服务区标示符（ESSID），也可以说扩展服务区 ESS 中包括多种 BSS。分布式系统在 802.11 原则中并没有定义，不过目前大都是指以太网。扩展服务区是一种 Layer 2 网络构造，对于高层协议例如 IP 来说，它是一种子网。

## 无线局域网的几种重要工作过程

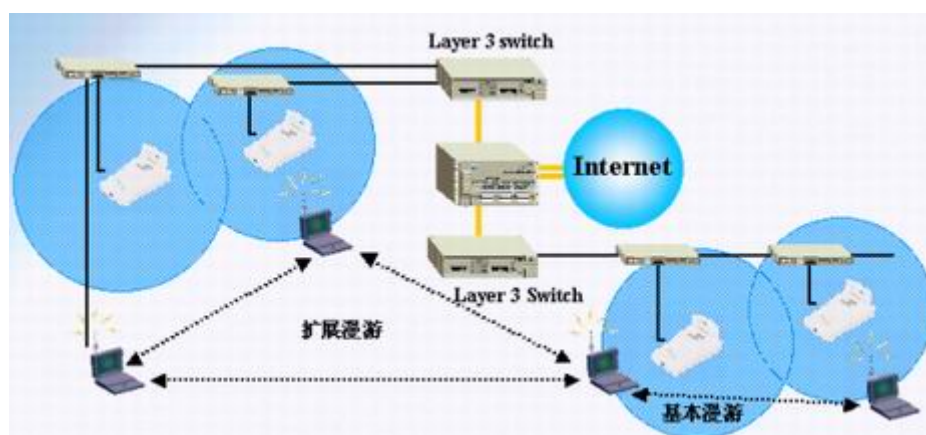
扫频：

STA 在加入服务区之前要查找哪个频道有数据信号，分积极和被动两种方式。积极扫频是指 STA 启动或关联成功后扫描所有频道；一次扫描中，STA 采用一组频道做为扫描范围，假如发现某个频道空闲，就广播带有 ESSID 的探测信号；AP 根据该信号做响应。被动扫频是指 AP 每 100 毫秒向外传送灯塔信号，包括用于 STA 同步的时间戳，支持速率以及其他信息，STA 接受到灯塔信号后启动关联过程。

**关联 (Associate):** 用于建立无线访问点和无线工作站之间的映射关系，实际上是把无线变成有线网的连线。分布式系统将该映射关系分发给扩展服务区中的所有 AP。一种无线工作站同步只能与一种 AP 关联。在关联过程中，无线工作站与 AP 之间要根据信号的强弱协商速率，速率变化包括：11Mbps, 5.5Mbps, 2Mbps 和 1Mbps。

**重关联 (Reassociate):** 当无线工作站从一种扩展服务区中的一种基本服务区移动到此外一种基本服务区时，与新的 AP 关联的整个过程。重关联总是由移动无线工作站发起。

**漫游:** 指无线工作站在一组无线访问点之间移动，并提供对于顾客透明的无缝连接，包括基本漫游和扩展漫游。基本漫游是指无线 STA 的移动仅局限在一种扩展服务区内部。扩展漫游指无线 STA 从一种扩展服务区中的一种 BSS 移动到另一种扩展服务区的一种 BSS，802.11b 并不保证这种漫游的上层连接。常见做法是采用 Mobile IP 或动态 DHCP。





## 影响无线局域网性能的原因

a、传播功率：

- b、天线类型和方向；
- c、噪声和干扰：授权顾客，微波炉，故意干扰等；
- d、建筑物构造：引起多路经，穿透效应等；
- e、无线访问点摆放的位置。

## 无线局域网的安全性

由于无线局域网采用公共的电磁波作为载体，因此与有线线缆不一样，任何人均有条件窃听或干扰信息，因此在无线局域网中，网络安全很重要。常见的无线网络安全分几种：

### **服务区标示符(SSID):**

无线工作站必需出示对的的 SSID 才能访问 AP，因此可以认为 SSID 是一种简朴的口令，从而提供一定的安全。假如配置 AP 向外广播其 SSID，那末安全程度将下降；由于一般状况下，顾客自己配置客户端系统，因此诸多人都懂得该 SSID，很轻易共享给非法顾客。目前有的厂家支持“任何”SSID 方式，只要无线工作站在任何 AP 范围内，客户端都会自动连接到 AP，这将跳过 SSID 安全功能。

### **物理地址 (MAC) 过滤:**

每个无线工作站网卡都由唯一的物理地址标示，因此可以在 AP 中手工维护一组容许访问的 MAC 地址列表，实现物理地址过滤。物理地址过滤属于硬件认证，而不是顾客认证。这种方式规定 AP 中的 MAC 地址列表必需随时更新，目前都是手工操作；假如顾客增长，则扩展能力很差，因此只适合于小型网络规模。

### **连线对等保密 (WEP):**

在链路层采用 RC4 对称加密技术，钥匙长 40 位，从而防止非授权顾客的监听以及非法顾客的访问。顾客的加密钥匙必需与 AP 的钥匙相似，并且一种服务区内的所有顾客都共享同一把钥匙。WEP 虽然通过加密提供网络的安全性，但也存在许多缺陷：一种顾客丢失钥匙将使整个网络不安全；40 位的钥匙在今天很轻易被破解；钥匙是静态的，并且要手工维护，扩展能力差。为了提供更高的安全性，802.11i 提供了 WEP2，该技术与 WEP 类似。WEP2 采用 128 位加密钥匙，从而提供更高的安全。WEP2 目前不保证互操作性。

#### **端口访问控制技术 (802.1x):**

该技术也是用于无线局域网的一种增强性网络安全处理方案。当无线工作站 STA 与无线访问点 AP 关联后，与否可以使用 AP 的服务要取决于 802.1x 的认证成果。假如认证通过，则 AP 为 STA 打开这个逻辑端口，否则不容许顾客上网。802.1x 规定无线工作站安装 802.1x 客户端软件，无线访问点要内嵌 802.1x 认证代理，同步它还作为 Radius 客户端，将顾客的认证信息转发给 Radius 服务器。802.1x 除提供端口访问控制能力之外，还提供基于顾客的认证系统及计费，尤其适合于公共无线接入处理方案。

#### **无线局域网络产品的兼容性:**

WECA 是无线以太网兼容性联盟，有 10 多种组员，包括 3Com, Symbol, Dell, Cisco 等，目的是保证各厂家的所有 802.11b 产品的互操作性，所有通过认证的产品将颁发 Wi-Fi 证书，贴 Wi-Fi 标志。Wi-Fi 代表 Ethernet for WLAN。目前有 40 多种厂家的 100 多种产品通过了 Wi-Fi 认证，因此它们之间的互操作将得到保证。

## **1.3 覆盖考虑**

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。

如要下载或阅读全文，请访问：

<https://d.book118.com/798131130070006107>