第 42 卷 第 6A 期
2015 年 6 月

计 算 机 科 学
Computer Science

Vol. 42 No. 6A
June 2015

多 AP 无线网组建的关键点及扩展应用研究

周 铜 宋海军
(中州大学 郑州 450052)

摘 要 组网是一个工程,AP 的衔接配置是有要求的,必须明确哪些配置仅能在 AP 之间使用,哪些用在与主机连接之时,否则,组网将遇到障碍。经过实验研究,探索总结了组网过程中 AP 的基本配置规则,并在网络建设中实现了一个无线廉价可移动打印的应用系统。

关键词 无线网络,原理,廉价,移动打印
中图法分类号 TP393 文献标识码 A

Key Point Created by More AP Wireless Network and Extended Applied Research

ZHOU Tong SONG Hai-jun
(Zhongzhou University, Zhengzhou 450052, China)

Abstract Creating a wireless network is a project. AP interface configuration has requirements that which configuration can only be used between the AP and which can be used when connected to the host must be clear. Otherwise, the network will encounter obstacles. We tested explored the basic configuration of the network in the process of summarizing the AP rules, and implemented a cheap wireless mobile printing applications in the network construction.

Keywords Wireless networks, Principle, Inexpensive, Mobile printing

1 引言

无线网络应用是当今国内外较流行的一种技术,通信具有良好的灵活性,不受物理环境的限制,网络的传输范围可随意拓展,两点之间的传输距离可扩大到几十公里,对其进行普及应用是趋势。无线网络的主要设备之一是 AP,很多资料对 AP 的配置做了详细介绍,但少有在组网时明确指出 AP 的衔接配置规则。

组网是一个工程,AP 的衔接配置是有要求的,必须明确哪些配置仅能在 AP 之间使用,哪些用在与主机连接之时,否则,组网将遇到障碍。我们经过实验研究,探索总结了组网过程中 AP 的基本配置规则,并在网络建设中实现了一个无线廉价可移动打印的应用系统。

2 无线网络通信原理

2.1 通信基础条件

无线网络通信的主要硬件包括无线 AP、路由器及具有无线收发功能的计算机。无线网络的接入过程就是网络设备网络层以下的通信,在物理层主要处理无线信号的收发、信道选择等,而数据链路层主要控制帧在物理信道上传输、传输差错处理、发送速率调节等。在这个过程中,终端主机设备通过发送无线信号搜索 AP,当有相当强度的 AP 信号时就会与其建立无线连接,从而通过 AP 实现接入网络。如果网络中仅使用一个 AP 不会存在太大问题,但当 AP 数量增多时,无线信号相互干扰会影响接入的稳定性[1],这是造成复杂的局面的主要原因。

无线网络的另一个问题是有效传输距离,组建无线网络的主要设备是 AP,按照 IEEE 802.11b/g 协议标准来说,其覆盖范围应该是室内 10 米、室外 300 米。但这仅仅是理论数值,无线数据通信时与环境有关。可靠的通信范围是:室内 30 米、室外 10 米(没有障碍物)[2]。

无线网络通过无线信道进行数据传输,但在空间中充满各种无线信号,所以确保应用的安全性也是一个重要指标。

2.2 网卡与链路层原理

2.2.1 网卡

网卡不是组成计算机的内部逻辑部件,但却是计算机通信的必需设备,它负责通信数据的收发以及完成二层以下的功能。网卡的 48 位 MAC 地址是极其重要的,接收端通过查看所收到的数据帧之目的 MAC 来判断帧是否发给自己,该地址不是 IP 协议中的三层地址,而是网卡中的二层硬件地址。无线通信标准遵循 802.11,它在物理层和数据链路层之间还定义了一个媒体访问控制_物理子层,主要实现数据的打包与拆包。物理层使用信道空闲评估算法来判断信道是否空闲并发送信号,通过 MAC 层的控制来实现无线网络的多路访问协议[3]。

2.2.2 信道

信道类似于有线通信之中的通路,无线电波发送端到接收端传播路径不只一条,每条都称为信道。无线通信时必须首先建立一个信道,就像连接了一条有形链路。IEEE 802.11 定义无线网络连接是半双工模式的,发送方和接收方使用不同的频率。

关于 2.2.1 节和 2.2.2 节的相关内容有很多资料可供参考,这里不多做讨论。

2.2.3 802.11 帧头及数据路径

8021.11 帧的总体架构如图 1 所示。其中 preamble 域是

周 铜(1962—),男,教授,主要研究方向为网络技术;宋海军(1966—),男,教授,主要研究方向为网络与自动化。

前导同步等标识信息，以便接收设备能够识别 802.11 帧，PLCP 域包含一些物理层的协议参数。MAC 域开始是处理帧数据的。截取上图中 MAC 头开始的部分构成 MAC 帧格式，因为 802.11 帧类型不同，MAC 帧部分长短、格式也不同，但可用一个统一的形式来表示（见图 2），不同帧在该结构中会减少几个域。

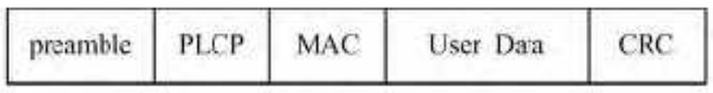

图 1　802.11 帧

图 2　MAC 帧头及控制帧各位

（1）不同类型帧头部的 MAC 地址个数不同，如 ACK 帧仅有一个 MAC 地址，而数据帧一般有 3 个 MAC 地址。但如果是在 WDS 模式下，帧头就有 4 个 MAC 地址。

（2）管理帧由无线 AP 发出，所携带的信息长度也会变化，该信息包含 MAC 地址、分片标志之类等信息，还包括关于安全设置、物理通信等信息，如 SSID 名称就是通过管理帧获得的。

（3）加密（wep、wpa 等）、QOS 信息，经过加密的数据帧比未加密据帧多了个加密头，用于解密，QOS 也是同样[4]。

802.11 定义了下列几类帧（见表 1）：

帧头的各个域以及帧控制的各个字段都有各自的意义，我们重点了解如下几个字段。表 2 指明控制帧两个字段能够显示数据包的方向与中转。

BSSID：在基本服务集中（后面介绍），BSSID 是一个 AP 的 MAC 地址。但是在独立基本服务集中，它是一个随机生成的 46 位二进制序列，它的最高两位分别是“全局/本地”标志位和“个人/组”标志位。独立基本服务集的 BSSID 中，全局/本地标志位为 1，表示本地 MAC；个人/组标志位为 0，表示是个人 MAC，其它位是随机的二进制数。注意：目前没有在 Windows 下抓取无线网络原始帧的工具，但网络上有很多实例程序，可以输入并运行它抓取原始帧，网络上的抓包软件一般是不能显示原始帧的。

可以看出，在 802.11 帧中除了有源和目的地 MAC 外，还有 RA 与 TA。在无线网络中有可能是通过 AP 把数据发送出去，所以数据帧中 RA 字段填的不是目的主机的 MAC 地址，这也是 802.11 与 802.3 的重要区别之一。RA 只是一个中转，它还有一个 DA 字段来指明该帧的最终目的地。SA 字段则是目的主机回应时必不可少的。如果无线网络中有多个 AP，那么在 WDS 模式下数据帧会有 4 个地址，这些地址结合帧控制的 To DS/From DS 字段共同决定数据包的走向。

表 1　802.11 的重要帧

管理帧（4 种）	控制帧（4 种）	数据帧
·信标帧：AP 定时发送信标（Beacon）帧用来声明某个网络。客户机通过信标帧就知道该网络还存在。信标帧还携带了网络的一些信息。 ·探测请求/回复帧 Probe Request/Response：客户机除了监听信标帧以了解网络信息外，还可以主动发送探测请求帧用于探测周围的无线网络。 ·关联请求/回复帧 Association Request：客户机需要关联到某个 AP 时发送此帧，而 AP 则会回复一个关联请求帧用于通知是否允许关联。 ·认证/取消认证帧 Authentication：用于身份验证，认证过程可能需要好几次帧交换，每个帧都有自己的编号。	控制对共享媒体，即物理媒介的访问； ·RTS（Request To Send）：RTS 用于申请无线媒介的使用时间。 ·CTS（Clear To Send）：清除发送数据包。 ·ACK：MAC 以及任何数据的传输都需要得到一个确认帧。这些数据包括普通的数据传输、RTS/CTS 交换之前帧以及分片帧。 ·PS-POLL：该控制帧被客户机用于从 AP 中获取因省电模式而缓存的数据。客户机和 AP 关联时，由 AP 赋给该客户信息。	传输数据

表 2　控制帧两个字段

网络模式\功能	To DS	From DS	目的端地址	源端地址	发出地址	接收地址
独立基本服务集 IBSS	0	0	DA	SA	BSSID	未用
To AP（基础型）	1	0	BSSID	SA	DA	未用
From AP（基础型）	0	1	DA	BSSID	SA	未用
WDS（无线分布式系统）	1	1	RA	TA	DA	SA

还有一点需要说明的就是 AP 的 IP 地址，因为 AP 具有部分有线网络交换机的作用，它起着数据中转作用，与交换机一样，通信中不涉及它的 IP 地址，因而不需要专门为它配置 IP 地址，但是需要一个 IP 管理它，因为很多 AP 都是通过 IP 登录的。

2.3　无线接入的实现

无线网络在二层以下的通信没有有形的传输介质，是靠空中电波进行的。无线网分为独立基本服务集（IBSS）和基本服务集（BSS），前者是指无线主机之间相互通信组成的网络，后者则是指网络中必须使用 AP 作为客户主机接入的中间设备的情况。在一个无线局域网中相关的通信设备的集合被称为服务集，其标识符（SSID）唯一，它是管理人员命名的一个不超过 32 位的文本字符串，信标帧、关联请求、探测请求等管理帧中都包含它，通过识别它是否相同来判断双方是否同属于同一个服务集，并决定是否允许通信。通过无线介质通信的设备数量取决于网络及设备的承载能力，但通信设备数量可能影响通信的可靠性[5]。

独立基本服务集属于两台主机之间的直接通信，相对简单。而基本服务集（BBS）包含一个接入点 AP，那么，所通信的局域网设备就都要通过它，所发出的数据帧就包含 AP 的 MAC 地址，它相当于有线网络中的汇集器，集中管理通过其无线设备。所有要接入该网络的客户主机都必须向 AP 提出申请，AP 要验证客户端是否满足：①SSID 是否匹配；② 是否兼容当前的无线数据率；③ 身份验证是否通过。

接入过程：客户主机向 AP 发出申请，即发送一条关联请求消息，这个帧包含 SSID，AP 通过发送关联应答消息来应答拒绝或批准，成功关联 AP 后，通信双方的数据都必须经过 AP，因为此时的数据帧内容是按 BSS 服务集方式打包生成的，与独立基本服务集方式下生成的帧 MAC 地址数据不同，所以，主机间无法直接通信。

无线 AP 也会定期主动发出信标帧通告自己，信标帧中

包含 SSID 以便让客户主机关联。AP 还具有管理功能，例如主机发送的每个数据帧都会得到一个确认，AP 负责将确认帧发回给发送主机。

消息的发送有单播、多(组)播和广播，广播的 MAC 地址直接是 48 位全 1。通过前述我们已经知道，802.11 帧有 48 位的 BSSID 地址，这是 AP 的无线接口 MAC 地址。无线主机可以通过定期扫描 AP 广播发送的信标帧(Beacon)来获取 AP 的 MAC 地址，另外，无线主机也可以主动发送扫描形式的探测请求帧(Probe Request)广播去获取 AP 的 MAC 地址，此时 AP 会先查看 SSID 名称是否匹配，并且 MAC 过滤表中是否允许连接，过滤后会用单播响应帧予以回复。

一个基本服务集模式的局域网只包含一个 AP 和其中所有的网络设备，且没有连接到以太网。如果网络连接到了以太网，则被称为 802.11 的扩展服务集(ESS)。扩展服务集中允许使用多个 AP，无线客户端可以在 AP 间漫游关联，当客户主机移动到另一个 AP 附近时，就可同该地信号更强的 AP 关联从而实现漫游。

3 应用网络的设计

通过上述分析看出，组件多 AP 无线网络的技术基础成熟，办公场所宜采用扩展服务集(ESS)模式设计网络，但系统配置设计也是关键问题。

3.1 设备选择

网络设计使用多个 AP 和一个无线路由器。无线路由器配置很简单，配置 WAN 口 IP 为学校分配的地址，启用 DHCP，配置 SSID 即可。AP 则根据工作需求进行合理配置。一般 AP 具有 5 种工作模式[6]分别是：(1)无线接入点模式；(2)AP 客户端模式；(3)无线桥接器模式；(4)无线桥接中心点模式；(5)无线放大器模式。在这些模式中只有客户端模式只接收信号不发送任何信号，此时它相当于一个无线客户，这种情况 AP 应处于网络的末端，其后面只有主机，不再桥接或中继其它局域网设备。

3.2 AP 漫游支持与网络安全性

无线网络的通信类似移动手机通信，AP 是基站，客户主机同 AP 关联后，所有通信数据都必须经过该 AP。只要客户主机在当前 AP 的信号覆盖范围中，就会维持同该 AP 的关联，当客户主机不断远离该信号范围时，接收到本 AP 的信号强度将逐渐降低，当信号强度低于一定的阈值时，客户端就会失去关联，即掉线，当客户主机接近另一个强信号的 AP 时，它会再次向新 AP 请求重新关联，且这个 AP 是允许关联的，就可完成关联过程，从而使客户主机继续处于通信网络中从而实现漫游。

虽然在无线网络中没有固定的信号轨迹，二层以下的信号可能非常多并且复杂，但是，由于无线网络通信有一定的规范，从基本原理上讲，目标不是本机的数据不会被上交。假如收到了危险信息，网络还有其它手段进行管理。比如基本服务集中 AP 可以管理它的客户，因为通信必需经过 AP，所以，每个客户主机需要通过关联、认证，AP 才能允许接入，那些凌乱、无效或者攻击信息，如果不能突破这些规则，很难被 AP 允许进入网络。因此，网络的安全性与否不取决于网络本身，而在于为网络安全设置的安全门槛，也就是说：认证和加密突出重要，为了保证安全，应该设计多种方法用于进行认证、加密或两者[7]。

3.3 设备布局

在入口房间信息点附近放置一台小型无线路由器，无线路由器需要配置 WAN 口 IP 为学校分配地址，LAN 口可根据需要配置或使用默认，即可以配置内网 IP 地址，也可以启用 DHCP，但必需要配置 SSID 和 WEP KEY。多个房间应用设计方法并不唯一，不过为了保证信号质量，应在区域中心位置放置一个 AP(见图 3)，设置为一点对多点桥接模式，并将与其关联的 AP 及路由器 MAC 地址填入配置表。其它除了连接打印机以外的 AP 都设置成中继模式，只有连接打印机的 AP 应设置成客户端模式，这种模式是通过无线接收而为用户提供有线接入的，是专用于连接网络打印服务器，构建网络移动打印系统的，所有 AP 要配置 SSID 和 WEP KEY，并且应关闭其 DHCP 服务。

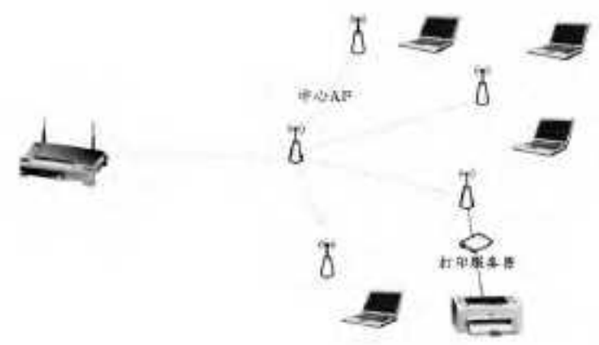

图 3

最初，我们没有意识到 AP 模式的重要性，前面的 AP 都设置为多点桥接模式，末端 AP 设置为中继模式，连接后也能联网通信。但是，当根据前面的 802.11 帧格式分析内容进行抓取原始帧分析后发现，原先的连接通信都是通过路中继 AP 和由器完成的，我们实验所作的漫游，表面上主机是到了桥接 AP 附近，但实质上信号仍在中继 AP 或路由器的覆盖范围内，所谓漫游没有经过桥接模式的 AP，说明桥接模式下它不与主机进行通信。因此我们调整了 AP 配置，将位于区域中心的一台 AP 设置为一点对多点桥接模式，其它除连接打印机的 AP 外均设置为中继模式，使连接步入正轨。

经过诸如上述的多次实验研究，得出如下结论：

(1)无线网络中 AP 之间通信的基础有赖于各个 AP 的 MAC 地址，但必须针对 AP 人工设置与之通信 AP 的地址。802.3 的数据包可根据交换机端口-MAC 表确定转发端口，但无线网络包是向空中发出的，只有明确目标 AP 的 MAC 地址才能使其接收并继续转发。

(2)多个 AP 组建无线网络时，能够连接无线客户主机的 AP 只能是无线接入点模式或者中继模式，桥接模式都不与客户主机进行通信，仅与 AP 通信，无线接入点模式只能用在从有线网络接入时，无法用在与其它 AP 的连接，它不需要设置上级 AP 的 MAC 地址。

(3)多点桥接 AP 必须填写上级与下联的各个 AP 的 MAC 地址。

(4)中继 AP 必须是末端的，它需要设置上级 AP 的 MAC 地址。

(5)距离较远时，中心应设置一台 AP 作为路由器连接其它 AP 的多点桥，该 AP 必须设置与之通信各个 AP 的 MAC 地址，相当于一个集中器，其它下级 AP 都对中心桥接 AP 连接，它们彼此之间没有关联。

由此可以进一步推断，如果继续扩大网络范围，可以在中心 AP 下再增加一台一点对多点桥接 AP，它向上连接上级中心 AP，它的下面可再连接多个中继 AP，以此类推，最终组成一个一定规模的无线网络。

设置完无线路由器及AP,并对其无线安全机制做了修改之后,要对无线网卡的参数做相应的设置,“SSID”这项要保持一致才能连入网络。对于无线网卡来说,允许两种类型的工作模式,即通过AP互连工作模式和对等点对点互连模式。如果选择了前者,无线网卡将会连接到一个信号好的AP;如果选择后者,无线网卡将会直接连接到另一个无线工作站。在AP互连工作模式中,主机的无线网卡使用的“信道”是自动检测的。只有在点对点对等模式中才需要设置信道值。

应当注意,多个AP同时使用时,其SSID应该相同,但每个AP信道设置不能相同,因为802.11定义的无线传输频率在2.4-2.4xxxGHz,这些频段又被划分为13个信道,信道号相近时其频率也接近,易产生干扰,所以,相邻AP所使用的信道号应该尽量数值差别大一些,如1、6、11。有人可能会问,两个AP的信道号不同,它们之间最初时使用哪个信道?这一点也是物理层完成的工作,从动者可以通过遍历方法寻找无线信号耦合。

此外,我们原有一台网络打印服务器(不支持WI-FI),将其连接在AP的网络接口,使用普通打印机也可构成无线可移动网络打印系统,并且价格非常低廉。

3.4 组建廉价可移动打印机系统

打印机连接在一个末端AP上,这个AP必须设置成为客户端模式,虽然此时AP仅接收上级AP发送的无线帧,但却可以通过自身网线将数据指令传输给打印服务器,而打印服务器也会再将这些指令发送到打印机接口,即可实现打印。

这时打印服务器的安装不同于无线网络打印服务器,它经过了AP,所以必须为其配置静态IP,且与路由器LAN口同网段,也不能使用DHCP,因为它的网卡直接连接的是AP而不是路由器,此时的AP不会将它的DHCP请求发给路由器,所以无法自动获取IP地址。安装打印驱动程序在每台需要使用打印机的计算机上,且应选择直接连接方式,而不能使用网络方式。最后再安装打印服务器软件,安装完毕就可以使用打印机了,并且多台计算机都可以共用(见图3)。

完成打印的过程是:客户主机的打印指令提交给打印服务器软件,该软件再将打印指令提交给网卡,无论是有线或无线网卡都能实现数据发送,无线网络发送给AP,AP将接收的无线打印指令数据通过有线网口传给打印服务器硬件,打印服务器再传输给打印机。可以看出,打印机虽然不是直接连在客户主机上,但主机上的打印服务器软件与打印服务器硬件建立了逻辑关系,它管理着打印服务器并在打印机与网络间建立了稳定的数据传输,从而实现送往打印机接口的指令数据通过网络能够发送到打印机。

结束语 无线网络最大的特点就是舍弃了错综复杂的布线,设备位置更加灵活,其优势明显。但组建网络也必须将关键技术点弄清楚才能更好地发挥其性能,否则有可能出现问题,尤其在AP的配置上,资料大多介绍的是基本方法,而组网时的组织衔接及规则要求,则需要我们自己探索。无线网络应用还可扩展到多种设备[8],我们在建设无线网络时,使用普通打印机及不足百元的打印服务器,提出了一种构建了廉价无线可移动打印系统的方法,扩展了网络应用。

参 考 文 献

[1] 无线局域网交换机操控无线网络接[OL]. http://network.51cto.com/art/201009/224792.htm

[2] 无线网桥和无线AP的区别[OL]. http://blog.sina.com.cn/s/blog_a63d5e5e0101d5vb.html

[3] 无线网卡的工作原理[OL]. http://www.elecfans.com/tongxin/119/2008063010029.html

[4] Wireless Fundamental(2)-802.11 MAC 头格式解析(updating)[OL]. http://hi.baidu.com/cnss_ay/item/6d772ff984c707703c198b25

[5] 常潘. Cisco无线局域网配置基础[M]. 电子工业出版,2011(3)

[6] 黄超毅. 5种常见的AP使用式[OL]. http://wenku.baidu.com/view/fdf8530d76c66137ee061908.html

[7] 51CTO. 无线网络架构及设计[OL]. http://networking.ctocio.com.cn/433/12238933.shtml 2012-01-09

[8] 企业如何部署Wi-Fi无线网络[OL]. http://www.edu.cn/wxjq_9863/20100702/t20100702_492211.shtml

(上接第293页)

[2] Ye W, Heidemann JEstrin D. An Energy Efficient MAC Protocol for Wireless Sensor Networks[C]// INFOCOM 2002. New York, June 2002:1567-1576

[3] Dam T V, Langendoen K. An Adaptive Energy Efficient MAC Protocol for Wireless Sensor Networks[C]// The First ACM Conference on Embedded Networked Sensor Systems(Sensys'03). Los Angeles, CA, USA, November, 2003:5-7

[4] Enz C, EL-Hoiydi A, Decotignie J-D, et al. WiseNET: An Ultra Low Power Wireless Sensor Network Solution[J]. Computer, 2004, 37(8):62-71

[5] El-Hoiydi A, Decotignie J D. WiseMAC: An Ultra Low Power MAC Protocol for the Downlink of Infrastructure Wireless Sensor Networks[C]// The 9th Int'l Symp. on Computers and Communications Alexandria. Egypt, 2004

[6] Polastre J, Hill J, Culler D. Versatile Low Power Media Access for Wireless Sensor Networks[C]// ACM Sensys 04. Baltimore, Maryland, USA, 2004

[7] Lu G, Krishnamachari B, Raghavendra C. An Adaptive Energy-Efficient and Low-Latency MAC for Data Gathering in Wireless Sensor Networks[C]// Proc 18th Int'l Parallel and Distributed Processing Symp(IPDPS'04). 2004:26-30

[8] Paxson V, Floyd S. Wide-Area Traffic: The Failure of Poisson Modeling[J]. IEEE ACM Transactions on Networking, 1995, 3(3):226-244

[9] Ganesan D, Govindan R, et al. Highly-resilient, energy-efficient multipath routing in wireless sensor networks[J]. Mobile Computing Review, 2002, 1(2):11-25

[10] Lisa A, Shay. The wireless network environment sensor: A technology independent sensor of faults in mobile wireless network links [D]. Rensselaer Polytechnic Institute Troy, New York, USA, 2002

[11] Sun Y, Xu L, Wu X, et al. A Chain Routing Algorithm Based on Traffic Prediction in Wireless Sensor Networks[J]. Communications and Network, 2013, 5:504-507

[12] Brockwell P J, Davis R A. Time Series: Theory and Methods (Second Edition)[M]. Springer Press, 1990:214-254, 189