



基于城域网的运营级 WLAN 组网技术

高 波,潘毅明,黄国瑾

(中国电信股份有限公司上海研究院 上海 200122)

摘 要: WLAN 作为有线宽带的延伸,也是无线宽带的重要组成部分。近年来,各地政府纷纷提出建设“无线城市”,将其作为城市第 5 项公共基础设施;中国电信股份有限公司也提出了将 WLAN 建设成为第 4 张基础网络,这些因素促进了 WLAN 的大规模建设和发展。分析了基于城域网的运营级 WLAN 的建设目标和组网架构,提出了运营级 WLAN 的组网技术以及 WLAN 的安全策略部署建议。

关键词: WLAN;集中控制型 AC+AP;AC 池化技术;BRAS;DHCP;大数据;安全

doi: 10.11959/j.issn.1000-0801.2015268

Technology of WLAN in Operation Level Based on Metropolitan Area Network

Gao Bo, Pan Yiming, Huang Guojin

(Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China)

Abstract: As an extension of the cable broadband network, WLAN is also an important part of the wireless broadband network. In recent years, local governments have put forward the construction of “wireless city” as the fifth city public infrastructure, China Telecom Co. Ltd. also put forward the WLAN construction as the forth basic network. These factors promoted the large-scale construction and development of WLAN. The construction goal and the network architecture of WLAN based on metropolitan area network were analyzed. The networking technologies and the security policy deployment of WLAN were proposed.

Key words: WLAN, centralized control AC+AP, AC pool technology, BRAS, DHCP, big data, safety

1 引言

随着移动互联网时代的到来,尤其是具有 WLAN (wireless local area network,无线局域网)无线模块的移动智能终端的普及推广,WLAN 接入需求也日益迫切,在某种程度上,WLAN 的普及程度已成为一个城市现代化的重要标志。政府要将 WLAN 打造成继水、电、气、交通之后的

城市第 5 项公共基础设施,以提升城市信息化水平;各地“无线城市”建设进一步促进了 WLAN 和热点的建设。中国电信股份有限公司(以下简称中国电信)也提出将 WLAN 建成第 4 张基础网络。

WLAN 技术以其标准统一、部署简单、性价比高的特点,成为无线宽带接入的重要手段。但 WLAN 本质是个局域网技术,要适应城域网的技术要求,需要对组网技术

收稿日期:2015-06-21;修回日期:2015-10-10

论文引用格式:高波,潘毅明,黄国瑾. 基于城域网的运营级 WLAN 组网技术. 电信科学, 2015268

Gao B, Pan Y M, Huang G J. Technology of WLAN in operation level based on metropolitan area network. Telecommunications Science, 2015268



进行创新,实现对 WLAN 用户接入的可管、可控,打造一张基于城域组网的运营级 WLAN。

本文以上海电信 WLAN 城域组网技术为基础,阐述基于城域组网的运营级 WLAN 组网技术和要求。

2 WLAN 组网架构选择和组网策略

运营级 WLAN 的特征是“大容量、高可靠、可扩展、可管理”,其建设需要从网络覆盖、组网架构、网络质量和网络管理维护等多方面着手,以提升用户体验为落脚点,全方位提升网络质量。运营级 WLAN 主要特征有以下几个方面。

- WLAN 覆盖将由零散热点向数据热区演进;对构建逻辑数据热区进行统一的网络管理、数据分析和特色业务开展。
- 网络架构扁平化,提高网络运营和管理效率。网络部署时要按组建整网的思路进行规划和建设,构筑集中、安全、扁平化的网络架构;同时能适应不同业务的承载需求。
- 着眼用户体验,全面提升网络质量:保证网络稳定性,使用户体验良好,满足多用户、高速率接入需求,支持各类 WLAN 终端方便接入;还需具备高安全性。
- 网络可管可控,提升维护和优化水平。确保在网 WLAN 设备纳入网管,快速定位网络故障,确保网络整体运行良好。图 1 为 WLAN 目标组网架构示意。

3 运营级 WLAN 组网方案

大规模 WLAN 组网均已采用集中控制型 AC (AP

controller,AP 控制器)+“瘦”AP(access point,接入点)架构。传统的组网方案是 AC 分散部署,就近旁挂 BRAS (broadband remote access server,宽带网络接入服务器)。一台 AC 只能管理该 BRAS 下同一厂商的 AP,覆盖范围有限。由于不同 BRAS 下 WLAN 业务发展的不平衡,使接入的 AP 数量、用户数量及流量不同,导致各台 AC 负载能力不均衡,部分 AC 设备利用率偏低;如果实现 AC 备份机制,将会大大提高设备成本。AC 分散部署,资源无法做到全网统一调度和管理,无法满足多业务、个性化需求。

为此,提出将不同厂商的 AC 集中部署,形成 AC 中心,通过采用 AC 池化技术提升 AC 覆盖范围和负载均衡能力,全网统一调度资源。图 2 为 WLAN 组网拓扑示意。

每台 AC 双上联到支持虚拟一体化的二台交换机 SW (switch,AC 专用接入交换机),AC 双上联均采用万兆接口跨框聚合,AP 专线接入的 BRAS 分别采用两个端口分别与 AC 接入交换机互联,端口绑定,确保网络安全可靠。任一台 AC 与 BRAS 均可通过 IP 路由可达,因此 AP 通过 BRAS 可接入任一台 AC;同时部署专用 DHCP(dynamic host configuration protocol,动态主机配置协议)服务器^[1]。通过上述组网形成 AC 中心。

其中,一部分 AC 设备配置私网地址,负责通过专线接入的 AP;另一部分 AC 设备配置公网地址,负责通过 Internet 接入的 AP。

3.1 AC 池化技术

将为 AP 分配管理地址和下发 AC 地址的功能,从 AC 设备中剥离出来,AC 仅负责 AP 接入注册、AP 管理和信息上报给网管平台。AC 池中心通过专用的 DHCP 服务

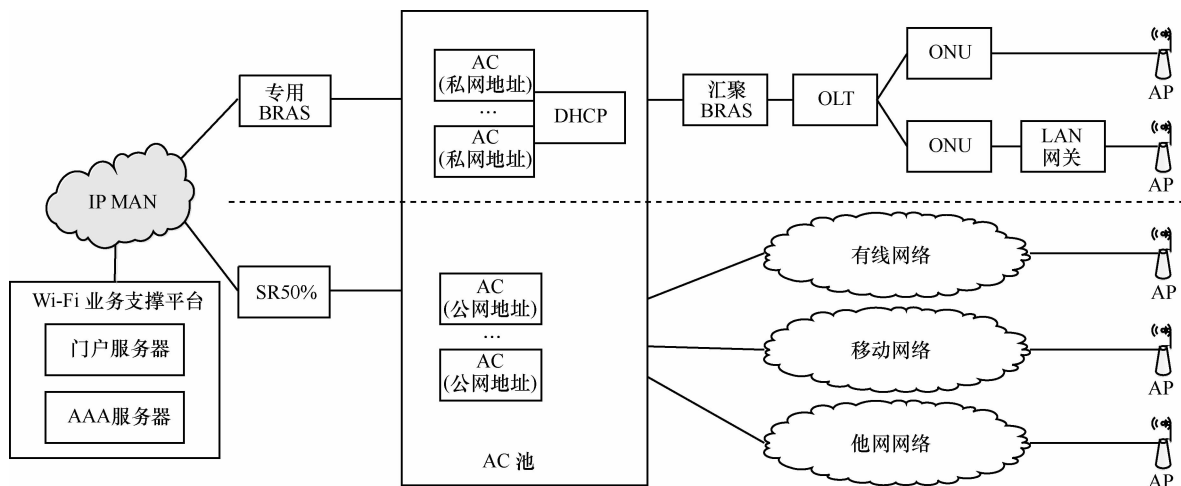


图 1 WLAN 目标组网架构

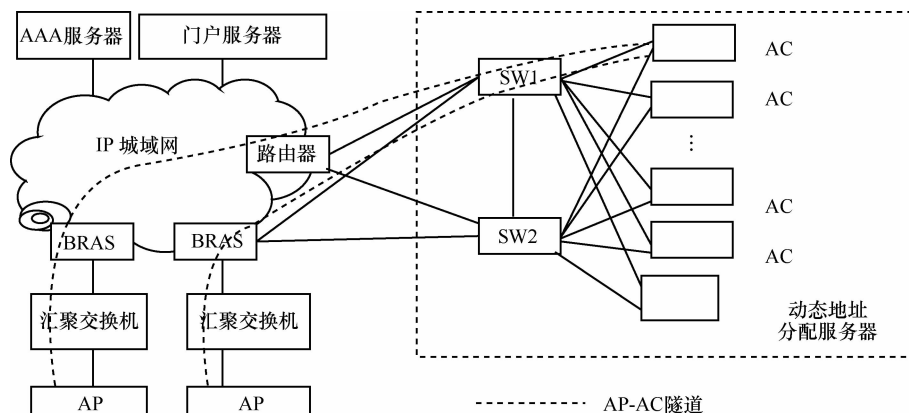


图2 WLAN组网拓扑

器系统负责为 AP 分配管理地址,同时通过 option 43 属性为 AP 下发 AC 地址。

WLAN 网管和后台的资源库根据新上线 AP 的需求、AC 池中各 AC 的负载、同一热点已在线 AP 所注册的 AC 等情况进行综合考虑,为新上线 AP 分配合适的 AC 设备,并将 AP 与 AC 的对应关系下发给专用 DHCP 系统和 AC 设备。

通过 AC 池化技术,可以集中调度 AC 设备;利用网管系统检测在网 AC 设备负载、设备 CPU (central processing unit, 中央处理器) 利用率等技术指标及实时检测 AC 设备的故障情况;灵活支持 $M+1$ 、 $M+N$ 或 $M:M$ 等多种 AC 备份机制。其中, $M+1$ 备份指用一台专用的备份 AC 设备作为 M 台主用 AC 的备份; $M+N$ 备份指用 N 台专用的备份 AC 设备作为 M 台主用 AC 的备份,任意 1 台主用 AC 出现故障时,可整机切换到备份 AC 设备上; $M:M$ 备份指不设置专用的备份 AC,所有的 M 台 AC 都正常工作,但不 100% 配置(如只配置 AC 能力的 80% 的 AP),留有一定的空余能力作为备份,当有 AC 发生故障时,将故障 AC 上的 AP 灵活地分散调度到其他若干台 AC 中。

3.2 AP 两种接入方式

AP 上联主要有两种接入方式,一种是专线接入,AP 通过预配置管理 VLAN (virtual local area network, 虚拟局域网) 接入 BRAS, BRAS 通过 VLAN 可识别 AP 业务并作相应的转发;另一种是 AP 通过 Internet 接入与部署在公网的 AC 组网。AP 通过 Internet 接入 AC 组网,作为 AP 专线接入组网的补充手段,极大地扩大了 WLAN 的覆盖范围,使任何场点都有可能接入基于城域网的 WLAN。

3.2.1 AP 专线接入方式

AP 通过专线接入。传统组网需要将不同厂商的 AP 分

别配置不同的管理 VLAN, BRAS 根据管理 VLAN 识别厂商,将 AP 的 DHCP 报文转发给对应的 AC^[2]。通过 AC 池化技术,实现将不同厂商的 AP 都配置成相同的管理 VLAN, BRAS 统一将 AP 的 DHCP 报文转发给专用 DHCP 系统。DHCP 系统为 AP 分配管理地址的同时,根据网管系统下发的 AP 和 AC 对应关系,通过 option43 属性为 AP 下发 AC 地址。

3.2.2 AP Internet 接入方式

AP 通过场点部署的企业网关/家庭网关接入 Internet,如中小商铺通过部署企业网关/家庭网关 PPPoE (PPP over ethernet, 以太网上传送 PPP) 拨号接入 Internet。AP 由网关设备分配地址,通过域名解析获得 AC 地址,与部署在公网的 AC 通信建立隧道^[3]。

3.3 AC 启用二、三层混用功能

中国电信的 WLAN 组网利用现网已有的 BRAS 设备,对 WLAN 用户实现地址分配、认证、管理等功能。用户数据通过 AP-AC 隧道,经 AC 二层转发至 BRAS,用户二层报文终结于 BRAS。

随着多 SSID (service set identifier, 服务集标识) 的开启,AC 二层透传各 SSID 用户数据到 BRAS,会过多消耗 BRAS 的资源,势必会影响到 BRAS 原来承载的宽带业务。为此,AC 会承载部分 SSID 的用户地址分配、认证和管理等功能,近阶段 AC 主要承载便捷认证业务的 SSID、行业 SSID 用户的认证和管理;其他 SSID 用户数据仍由 AC 二层转发到 BRAS。将结合 BRAS 功能的 AC 称为融合 AC,在现网中融合 AC 同时启用二层用户数据转发和三层用户数据终结的功能。

3.4 多业务承载

中国电信 WLAN 原本承载 ChinaNet 业务,随着广大



用户和终端类型对 WLAN 接入的日益普及,各地市级政府和区政府都有建设“无线城市”和应用的需求,不少行业也提出 WLAN 业务需求,互联网企业也与运营商合作开展 WLAN 后向经营业务的需求。为此,同一张 WLAN 网络需同时承载多种业务,且能够满足个性化业务需求。

采用 AC 集中部署的池化技术,可以很好地满足上述多业务需求。通过规划用户双层业务 VLAN,用外层 VLAN 标识业务类型、内层 VLAN 标识 AP 或场点,就能实现用户位置和业务的精确定位。集中部署的 AC 可以在全局层面灵活地部署个性化业务策略,可以推送全局性的个性化 portal 认证页面,也可在同一业务下根据不同 AP 或场点推送不同的 portal 认证页面,也支持基于场点和业务进行的个性化计费。

3.5 大数据挖掘

WLAN 以 AP、SSID 为单位对热点运营数据进行采集,包括 WLAN 终端的 MAC 地址、AP 设备地址、RSSI (received signal strength indication,接收的信号强度指示)、时间戳等信息,并发给大数据分析平台。大数据分析平台能按 AP、SSID、场点等进行数据统计;按 PV (page view, 页面浏览量或点击量)数据、UV (unique visitor, 访问某个站点或点击某条新闻的不同 IP 地址的人数)数据、CPC (cost per click, 每次点击付费广告)数据、CPM (cost per thousand click-through, 网上广告产生每 1 000 个广告印象(显示)数的费用)数据、流量/人均流量、时长/人均时长等多个维度进行数据展示和业务分析。

同时,将大数据平台分析得到的数据反馈回 WLAN,根据用户特征和场点性能,可实时对个性化 portal 页面的展示内容和热点接入带宽等进行动态调整。

4 WLAN 安全防范策略

在建设高效、灵活的 WLAN 的同时,还要考虑 WLAN 的安全^[4],其安全包括用户接入安全、用户数据空口传输安全、网络安全、设备安全等方面,下面分别进行描述。

4.1 用户接入安全防范

用户接入安全问题主要有:在同一 AP/AC 下用户二层互访、IP 地址欺骗、MAC (media access control, 媒体访问控制)地址欺骗。

如果在同一 AP/AC 下,用户通过二层网络能相互通信(用户未通过接入认证),则存在如下安全隐患:

- 用户通过某一用户作代理访问公网;
- 某一终端中毒,则会不断发送 ARP (address resolution protocol, 地址解析协议)广播或协议类攻击报文或进行病毒传播、木马植入等网络攻击,影响整个 WLAN 二层网络;
- 用户之间如处在同一个局域网,恶意用户(未通过接入认证)能够攻击其他同一个二层网络的用户或窃听其他用户信息。

IP 地址欺骗存在如下安全隐患:用户地址由 BRAS/融合 AC 负责分配,如果某一终端配置静态 IP 地址,会造成与其他终端地址冲突,造成合法用户不能正常上网;如果用户配置用户网关地址,会造成整个网络瘫痪。

MAC 地址欺骗存在如下安全隐患:在无线环境中,非法用户通过侦听等手段获得网络中合法站点的 MAC 地址比在有线环境中要容易得多,这些合法的 MAC 地址可以被用来进行恶意攻击。

用户接入应采取的安全防范措施为:

- 同一 AP 和同一 AC 下启用用户二层隔离功能,只有认证通过的用户才能通过三层相互访问;
- 在 BRAS 设备上启用 DHCP snooping 功能,用户地址与 MAC 地址绑定,防范 IP 地址和 MAC 地址欺骗。

4.2 用户数据传输安全防范

在 WLAN 中,在同一个 AP 下用户是共享带宽,如果个别用户使用 P2P (peer-to-peer, 伙伴对伙伴)、BT (bit torrent, 比特流)等这类占用大量带宽的应用,就会影响其他用户正常使用 WLAN 业务。

通过对用户限速,可以防止个别用户占用过多带宽,提升所有用户使用 WLAN 业务的体验。

4.3 无线网络安全防范

IEEE 802.11 网络很容易受到威胁网络安全的攻击,如 DoS (denial of service, 拒绝服务)/DDoS (distributed denial of service, 分布式拒绝服务)攻击、泛洪攻击、欺骗攻击等。通过启用 AC 设备的 WIDS (wireless intrusion detection system, 无线入侵检测系统)/WIPS (wireless intrusion detection system, 无线入侵保护系统)功能,监视分析无线用户的活动、判断入侵事件的类型、检测非法网络行为、对异常的网络流量进行报警,并根据策略采取相应的措施,确保 WLAN 的安全。

DoS/DDoS 利用软件(含操作系统)的缺陷、协议的漏洞(如 Syn flood 攻击)进行资源比拼(如发送大量的垃圾数

据侵占系统资源), 利用攻击程序 (如 smurf、trino、tfn、tfn2k、stacheldraht 告示 DoS 攻击程序) 进行攻击。

当一台无线设备试图在网络内泛洪时, 会在短时间内发送大量的同种类型的报文。此时 AC 和 AP 会被泛洪设备发送的攻击报文淹没而无法处理正常无线终端(合法用户)的报文。

泛洪攻击类型的报文主要有:

- 认证请求/解除认证请求;
- 关联请求/解除关联请求/重新关联请求;
- 探查请求;
- 空数据帧;
- action 帧。

欺骗攻击: 这种攻击是借合法终端 MAC 地址来发送攻击报文, 如一个欺骗的解除认证的报文会导致合法无线客户端下线。

通过启用 AC 设备的 WIDS/WIPS 功能, 监视分析无线用户的活动、判断入侵事件的类型、检测非法网络行为、对异常的网络流量进行报警, 并根据策略采取相应的措施, 以确保 WLAN 的安全。

4.4 WLAN 设备的安全防范

DHCP 池的安全性。当 AC 负责分配 AP 的地址时, 即 AC 启用 DHCP 池功能, 如果 AC 不检测 DHCP 请求的终端(如 AP)的合法性而直接分配 IP 地址, 则 DHCP 池的地址可能被耗尽并带来安全隐患。

对于 DHCP 池的安全性问题, 要求 AP 支持 DHCP option60, 即 AP 携带企业码, 这样 AC 就不会为任意一个 DHCP 请求的终端分配地址。

AC 设备的安全性, 主要有以下几个方面。

(1) AC 配置公网 IP 地址, 若黑客破解了 AC 设备账号, 入侵了主机, 植入了非法进程(如 tirqd)与非法服务项目(如 tblockd), 并启用 8080 端口发送了大量的垃圾邮件, 会造成恶劣的影响。

应采取的安全措施有: AC 配私网管理地址, 与公网隔离; AC 启用 ACL 策略, 只允许特定 IP 地址的终端访问, 并设置登入账号; 只打开特定端口, 其他端口关闭。

(2) 当 AP 到 AC 注册建立隧道时, 如果 AC 不检测/认证 AP 的合法性, 而直接允许 AP 注册, 则存在非法 AP 接入的风险。

应采取的安全措施有: AC 应检查 AP 的序列号、MAC 地址等, 确认所接入的 AP 是预先允许接入的 AP。

5 结束语

将 AC 集中部署、通过 AC 池化技术组网, 大大减少了 AC 部署数量和占用机房空间, 节省了管理、维护和人力成本; 支持 AP 通过中国电信的有线网络和移动网络以及其他运营商网络接入 AC 中心, 实现 WLAN 城域网, 极大地扩展了 WLAN 覆盖范围。利用丰富的 VLAN 资源实现外层业务 VLAN 标识业务、内层业务 VLAN 标识 AP 或场点等技术, 强化网络及设备的安全性能, 通过建设运营级 WLAN, 满足“无线城市”、行业 WLAN、商业 WLAN 和公共无线宽带上网需求。通过自建或与互联网企业合作开展后向经营, 极大地提升了 WLAN 价值, 为广大用户提供了高带宽、低资费的无线宽带接入。

参考文献

- 1 IETF RFC2131. Dynamic Host Configuration Protocol, 1997
- 2 IETF RFC3046. DHCP Relay Agent Information Option, 2001
- 3 IETF RFC5415. Control And Provisioning of Wireless Access Points(CAPWAP) Protocol Specification, 2009
- 4 刘杰. 浅析 WLAN 及 WLAN 网络安全问题. 网络安全, 2007(7)
Liu J. Analysis of WLAN and WLAN security issues. Network Security, 2007(7)

[作者简介]



高波, 男, 中国电信股份有限公司上海研究院教授级高级工程师, 主要研究方向为 WLAN 技术、安全和数据通信技术等。



潘毅明, 男, 中国电信股份有限公司上海研究院高级工程师, 主要研究方向为宽带接入及 WLAN 无线接入技术。



黄国瑾, 男, 中国电信股份有限公司上海研究院工程师, 主要研究方向为 WLAN 测试及组网技术。