

ICS 33.060.20
M 36



中华人民共和国通信行业标准

YD/T 3101-2016

公众无线局域网组网技术要求

Technical requirements for networking of public wireless LAN

2016-07-11 发布

2016-10-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 术语和定义.....1

4 缩略语.....2

5 应用场景.....3

6 网络架构.....4

7 网络功能要求.....8

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位： 中国联合网络通信集团有限公司、中国信息通信研究院、国家无线电监测中心、中兴通讯股份有限公司、华为技术有限公司。

本标准主要起草人：邱 勇、党梅梅、许 玲、魏 元、温 蕾、王俊峰、胡 云、唐春梅。

公众无线局域网组网技术要求

1 范围

本标准规定了公众无线局域网的组网技术要求，包括应用场景、网络架构、网络功能要求。
本标准适用于由电信运营商提供服务的公众无线局域网。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 15629.11-2003 信息技术 系统间远程通信和信息交换局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范

GB 15629.1101-2006 信息技术 系统间远程通信和信息交换局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范：5.8GHz频段高速物理层扩展规范

GB 15629.1102-2003 信息技术系统间远程通信和信息交换局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范：2.4GHz频段较高速物理层扩展规范

GB 15629.1104-2006 信息技术 系统间远程通信和信息交换局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范：2.4GHz频段更高数据速率扩展规范

IEEE 802.11-2012 信息技术系统间过程通信和信息交换局域网和城域网特定要求第11部分无线局域网媒体设备访问控制和物理层规范（IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications）

YD/T 2615.3-2013 公众无线局域网网络管理 第3部分：接口技术要求

IEEE Std 802.1X-2010 基于端口的网络接入控制（Port-Based Network Access Control）

IETF RFC 2865 拨入用户远程认证服务（Remote Authentication Dial In User Service (RADIUS)）

IETF RFC 2866 RADIUS计费（RADIUS Accounting）

IETF RFC 2869 RADIUS 扩展（RADIUS Extensions）

3 术语和定义

下列术语和定义适用于本文件。

3.1

接入点 Access Point

具有STA功能一个实体，连接到它的其他STA通过认证授权后可以接入到运营商网络。

3.2

接入控制器 Access Controller

AP的控制和管理设备，通常有接入控制功能。

YD/T 3101-2016

3.3

站点 Station

单独可寻址的具有802.11 MAC的逻辑实体及其PHY接口。

3.4

移动AP Mobile AP

用无线做回传且可移动的AP。

3.5

切换 Handover

WLAN终端退出当前AP，并连接到新AP，保持IP业务不中断。

3.6

漫游 Roaming

WLAN终端离开归属网络，使用原账号密码，接入拜访网络。

3.7

用户ID User ID

手机号码、固网宽带号码、固网电话号码、专用WLAN号码等可唯一标识该用户的号码。

3.8

公众无线局域网 Public Wireless LAN

利用WLAN技术，由运营商为用户分配ID，提供认证方法，从而为用户提供互联网接入服务的电信级WLAN网络，具有可靠性、安全性、可管理性。

3.9

无线局域网 Wireless Local Area Network

利用射频的技术，取代双绞线等有线连接所构成的局域网络。在本标准中特指基于IEEE802.11标准的无线局域网。

3.10

城域网 Metropolitan Area Network

IP城域网，由路由器、二、三层交换机、BAS通过光纤、波分复用系统等连接组成，在城市范围内，为宽带用户提供服务。

3.11

共享模式 Sharing Mode

用户设备除自用的私有SSID之外，共享出部分带宽资源，并广播运营商的SSID，以供临时到访的运营商用户使用，此时该SSID通过VLAN或隧道与运营商的WLAN AAA系统相连完成认证等功能。

3.12

安全超文本传输协议 Hypertext Transfer Protocol over Secure Socket Layer

用以提供加密通讯及对网络服务器身份的鉴定的协议。

4 缩略语

下列缩略语适用于本文件。

AAA	Authentication、Authoritation、Accounting	认证、授权和计费
AC	Access Controller	接入控制器
AKA	Authentication and Key Agreement	认证与密钥协商
AP	Access Point	接入点
BAS	Broadband Access Server	宽带接入服务器
BSS	Basic Service Set	基本服务集
CAPWAP	Control And Provisioning of Wireless Access Points	无线接入点控制和配置
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
EAP	Extensible Authentication Protocol	可扩展认证协议
EAPoL	EAP over LAN	基于局域网的可扩展认证协议
EAP-SIM	Extensible Authentication Protocol-SIM	基于 SIM 卡的可扩展认证协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
HTTPs	Hypertext Transfer Protocol over Secure Socket Layer	安全超文本传输协议
IP	Internet Protocol	互联网协议
LAN	Local Area Network	局域网
LTE	Long Term Evolution	长期演进
MAC	Media Access Control	媒质接入控制
PEAP	Protected Extensible Authentication Protocol	受保护的可扩展认证协议
PHY	Physical Layer	物理层
PLMN	Public Land Mobile Network	公共陆地移动网络
RADIUS	Remote Authentication Dial In User Service	拨入用户远程认证服务
SSID	Service Set Identifier	服务集标识
STA	Station	站点
UE	User Equipment	用户设备
WLAN	Wireless Local Area Network	无线局域网
(U) SIM	(Universal) Subscriber Identity Module	(全球) 用户识别卡

5 应用场景

5.1 概述

公众无线局域网有5种基本接入场景，分别是热点场景、交通场景1、交通场景2、机构共享场景和家庭共享场景，如图1所示。凡是不需要通过运营商的认证即可访问网络的，WLAN仅作为网络末端的局域网技术使用，完全由用户控制，则该场景不属于本标准范围，比如用户通过支持3G或LTE的移动AP或移动终端设置的私有WLAN上网的场景。

YD/T 3101-2016

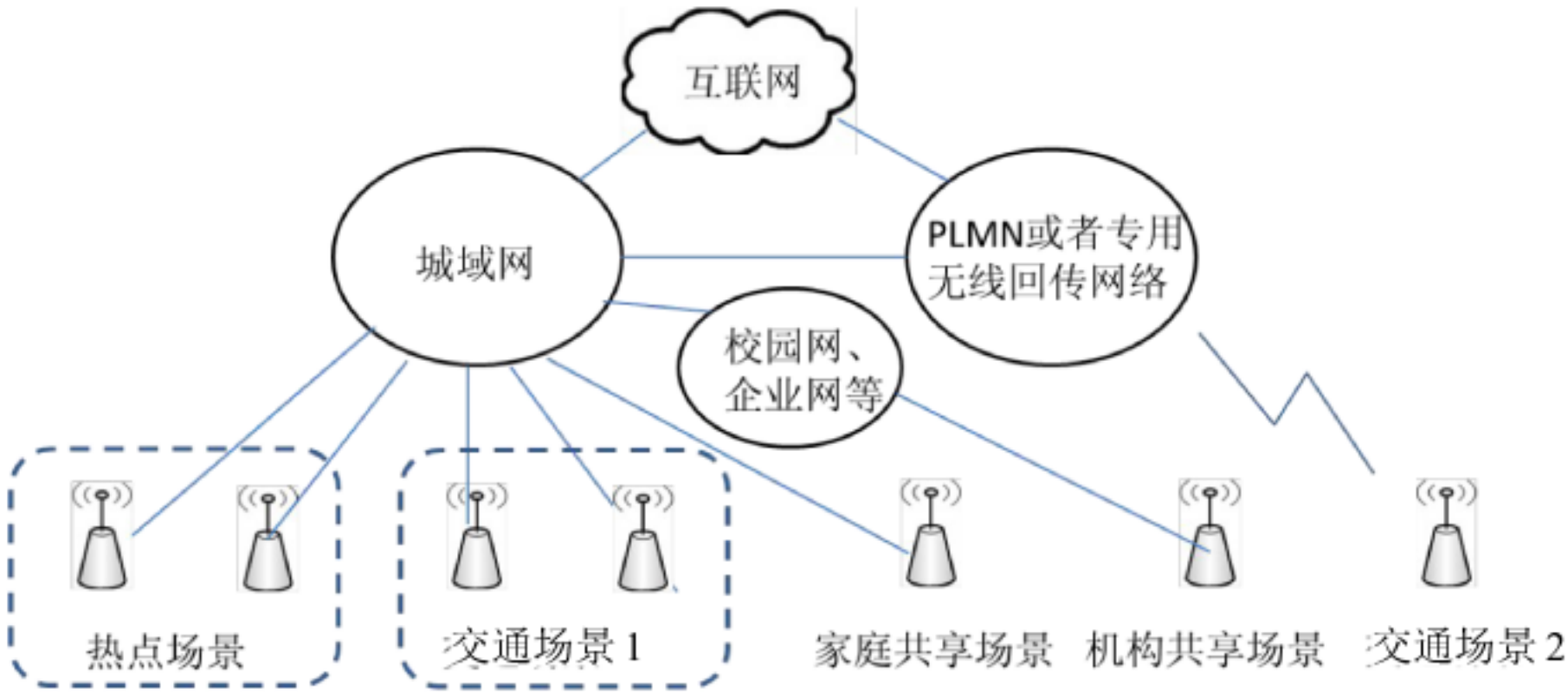


图1 WLAN的接入场景

5.2 热点场景

运营商签约用户通过运营商安装在机场、车站、购物中心、村镇等公共热点区域的AP，使用运营商提供的认证方式接入互联网。这种场景下，AP位置基本固定。用户STA静止或以步行速度移动。

5.3 交通场景 1

在中低速运行的城市交通工具上的运营商签约用户，通过运营商设置在路边的AP，使用运营商提供的认证方式接入互联网。这种场景下，AP位置基本固定。该场景与5.2类似，但组网上可根据场景特点进行优化。用户STA随交通工具移动。

5.4 交通场景 2

运营商签约用户通过设置在交通工具上的AP，使用运营商提供的认证方式接入互联网。AP回传采用如3G、LTE、卫星等技术手段。这种场景下，AP位置相对于交通工具固定。

如果AP使用交通工具拥有者局部定义的认证方式供用户使用，甚至不做认证，则该场景不属本标准的范围。

5.5 机构共享场景

运营商签约用户通过企业、学校、酒店等机构的工作在共享模式的AP，使用运营商提供的认证方式访问运营商的网络。此应用场景下，AP位置基本固定，AP中有一个SSID为运营商的SSID，可供临时到访的运营商签约用户使用。

如果AP使用机构用户局部定义的认证方式供用户使用，甚至不做认证，则该场景不属于本标准的范围。

5.6 家庭共享场景

运营商签约用户通过家庭、小型商户等工作在共享模式的AP，使用运营商提供的认证方式访问运营商的网络。此应用场景下，AP位置基本固定，AP中有一个SSID为运营商的SSID，可供临时到访的运营商签约用户使用。

如果AP使用用户自己局部定义的认证方式供用户使用，甚至不做认证，则该场景不属于本标准的范围。

6 网络架构

6.1 WLAN 网络架构

WLAN网络总体架构如图2所示。

该图中BAS、AC、AP为逻辑实体，BAS和AC在物理上可以是合一的设备，AC与AP也可以是合一的设备（胖AP）。

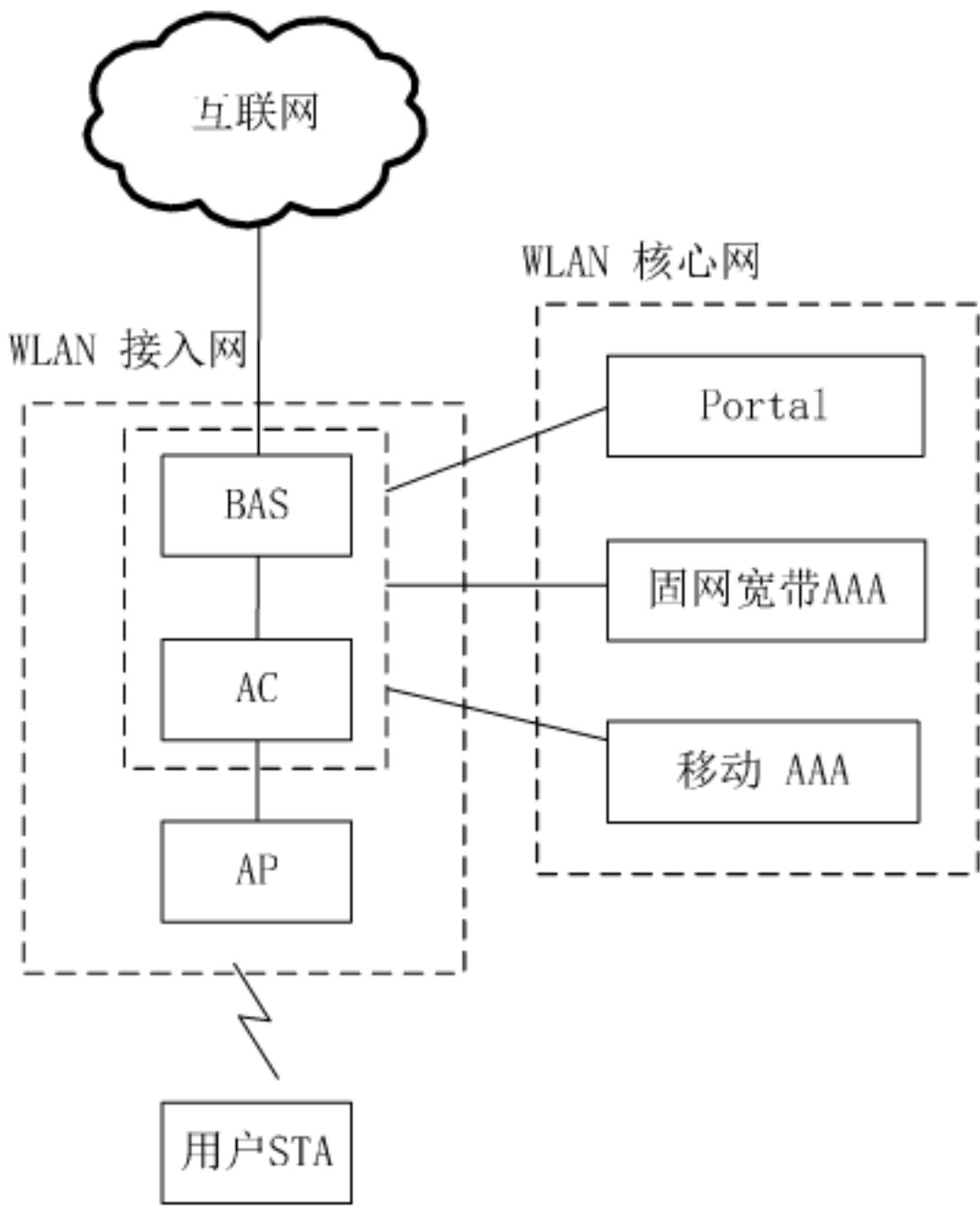


图2 WLAN网络总体架构

该架构中，运营商的固网宽带AAA系统、移动AAA系统实际在内部形成账号漫游，并形成统一账单。

对于AC和BAS是两个物理设备的情况，AC可以串接在AP与BAS之间，可以旁挂于BAS上，旁挂于AP与BAS之间的交换机上，甚至放置于BAS之后。但AP与AC之间始终保持可靠的IP连接或者2层连接。

另有几种网络架构，AP与BAS之间连接要通过隧道或者其他网络实现。分别是机构共享场景、交通场景2和家庭共享场景，分别如图3~5所示。

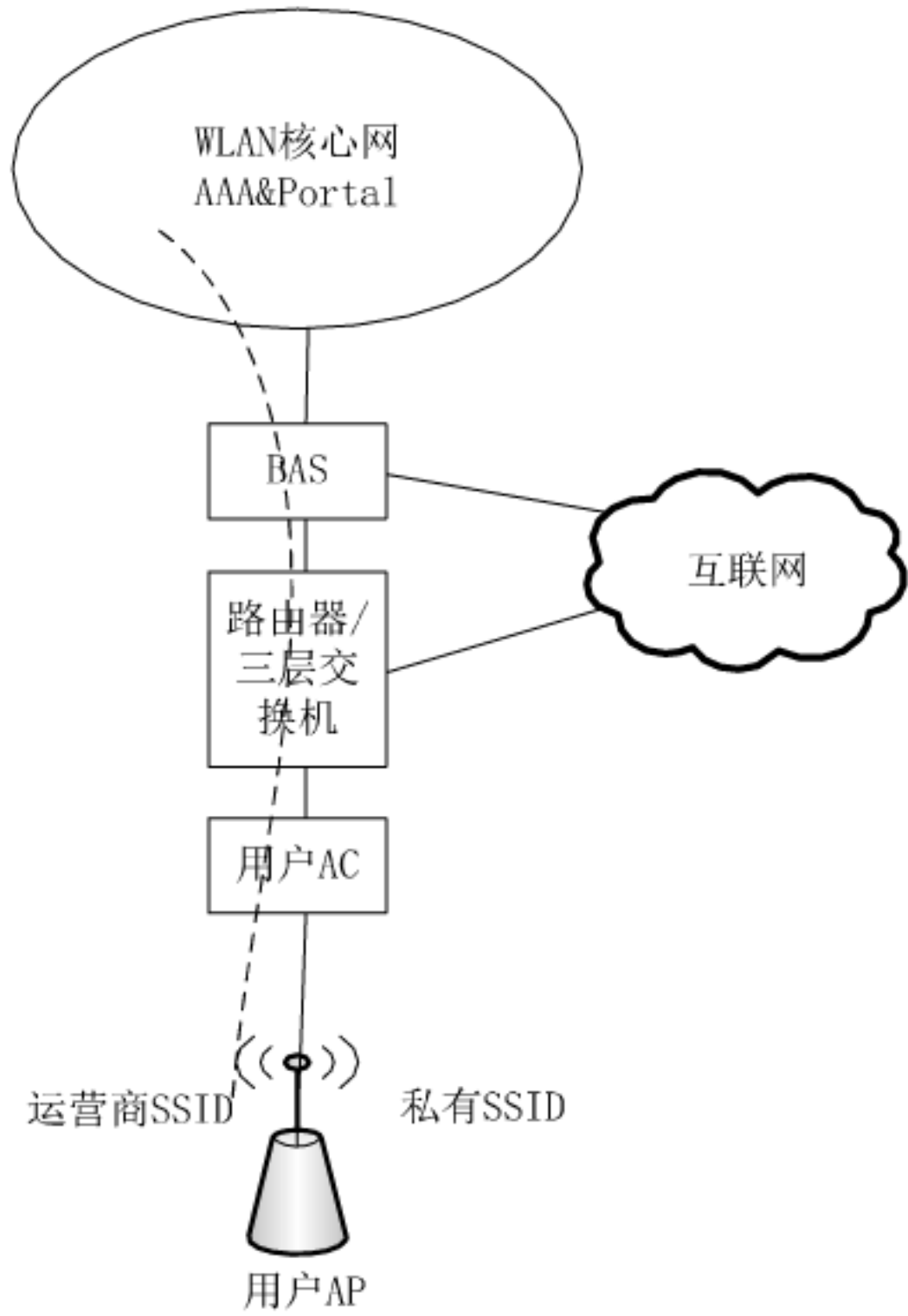


图3 机构共享场景

YD/T 3101-2016

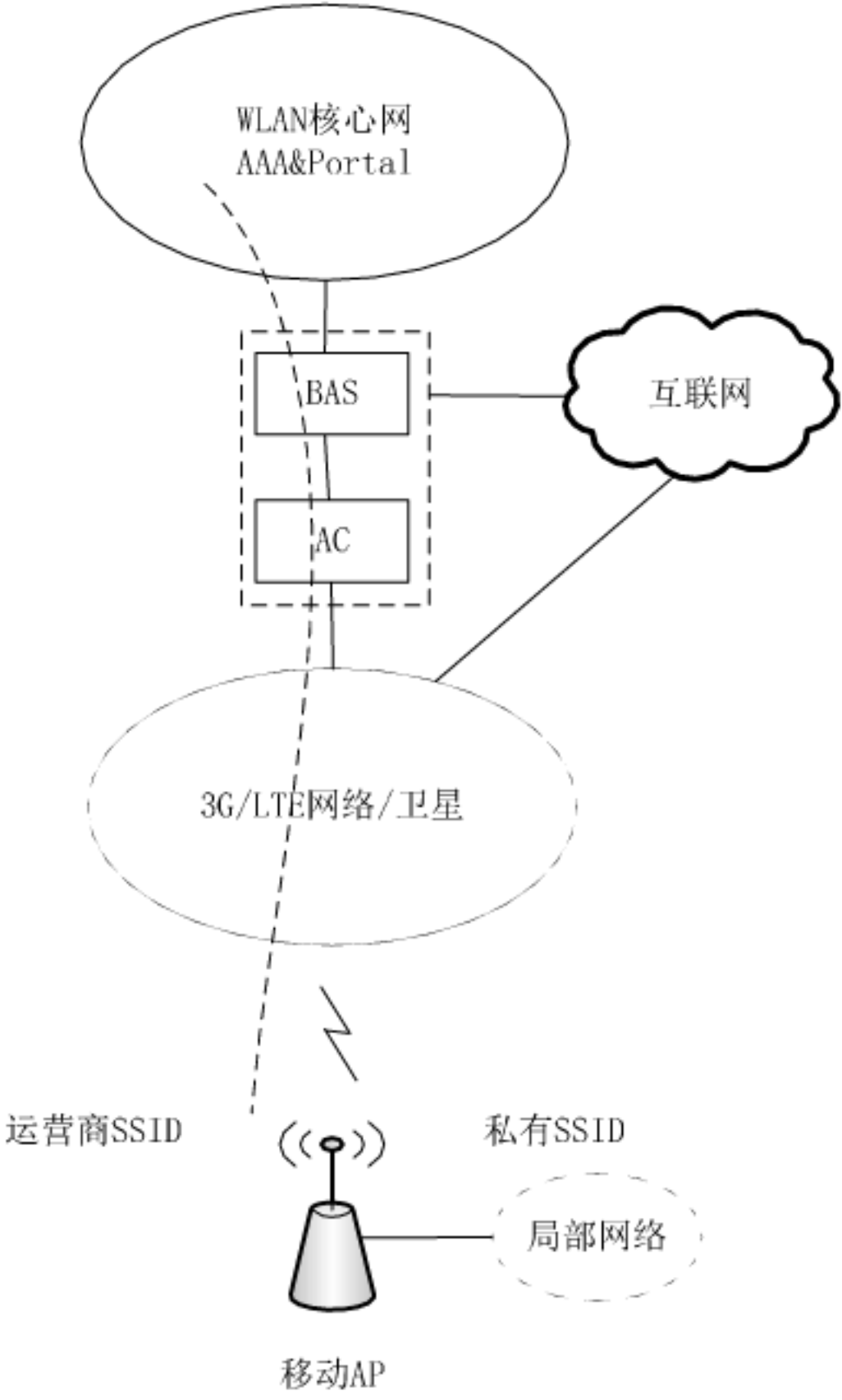


图4 交通场景2

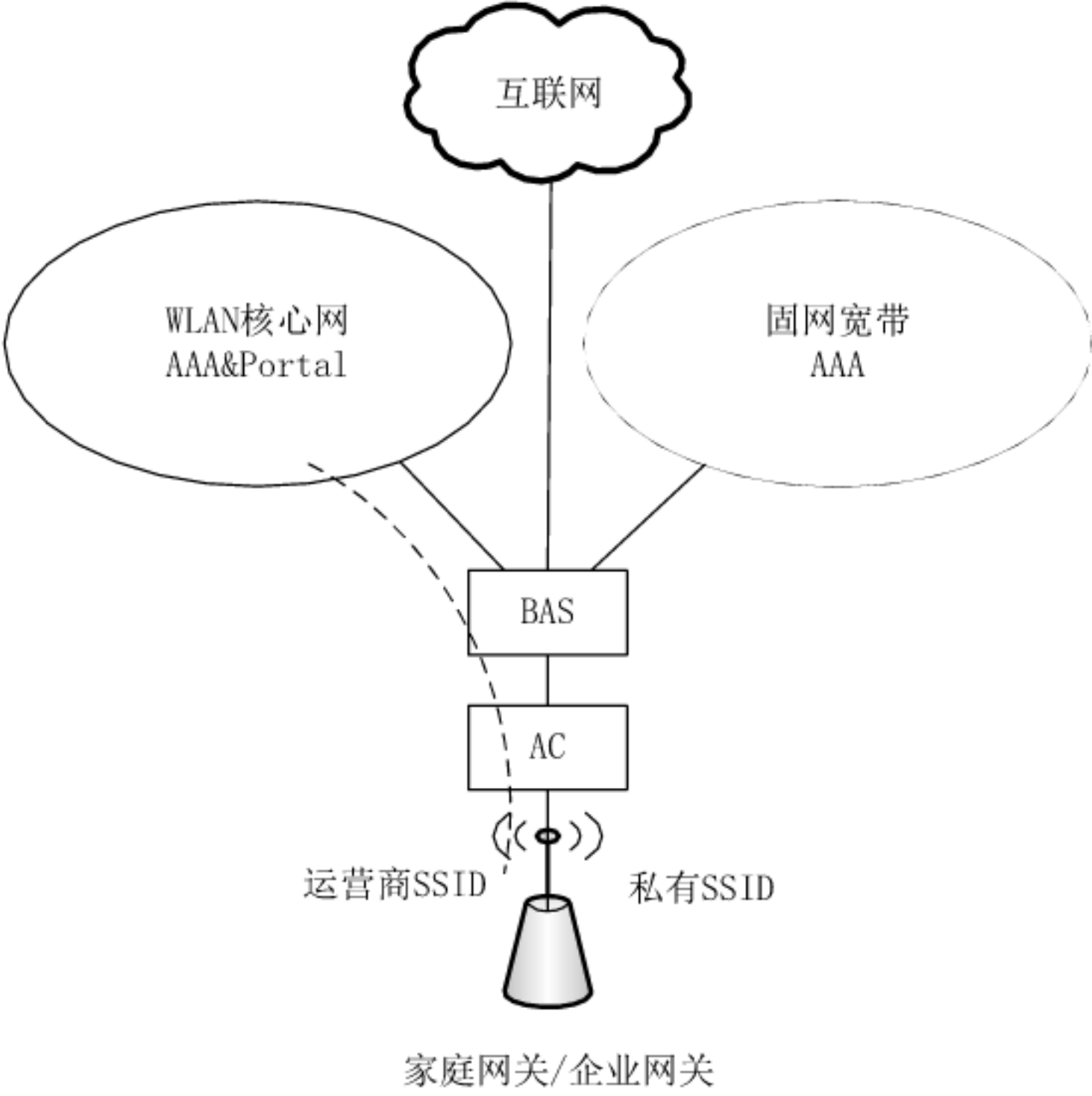


图5 家庭共享场景

6.2 网元

6.2.1 WLAN 网络的网元概述

WLAN接入网络的逻辑网元包含用户STA、接入点AP、接入控制器AC和宽带接入服务器BAS。

WLAN核心网由Portal服务器、固网宽带AAA、移动AAA组成。

AC也可以同时具备BAS功能，此时AC对AAA系统提供接入认证点功能。

6.2.2 用户 STA

应符合IEEE 802.11-2012定义的STA功能。

用户STA负责发起认证，一般支持Web+Portal认证方式，即通过web浏览器输入用户名和密码。

对于既支持WLAN STA功能又支持3G/4G移动通信功能的多模终端，还支持通过EAP-SIM/EAP-AKA发起认证。

6.2.3 AP

AP接入点，是具有STA功能一个实体，连接到它的其他STA通过认证授权后可以接入到运营商网络。

AP主要有两类，集中控制型AP和独立控制型AP。

集中控制型AP，也称FIT AP或瘦AP，须与AC配合实现接入控制、认证、负载均衡、切换等功能。AP的控制和管理通过AC实现。

独立控制型AP，也称FAT AP或胖AP，支持用户数据的路由和桥接方式转发，可独立实现控制、认证、管理，有路由能力。

另外，有些AP为可转换式，可以通过软件设置选择工作在独立控制模式或者集中控制模式。

还有些AP同时具有其他功能，如家庭网关、企业网关等，可以工作在共享模式。也有些共享功能是结合用户私有的AC来实现的，用户私有的AC通常规模较小，并具有接入控制器的功能。

交通场景下，移动AP采用3G、LTE、卫星或者专用网络做回传。

6.2.4 AC

AC的主要功能是AP控制，配合集中控制型AP使用，控制AP进行无线信道选择、切换、负载均衡等，对AP实现集中控制、管理，提供统一的网管接口。

6.2.5 BAS

BAS的主要功能是做为接入网关，对AAA系统提供接入认证点功能，与Portal系统、认证系统、计费系统相配合实现用户的认证、计费等，完成用户的接入会话的终结和认证功能，支持RADIUS认证和计费，实现流量的汇聚、用户的带宽和QoS的控制，支持对数据IP层的处理能力。

运营商可以使用独立的BAS设备完成接入控制功能，也可不用独立的BAS设备，而由AC同时完成BAS的功能。此时AC与BAS是一体的。

6.2.6 Portal 服务器

Portal服务器主要提供强制弹出认证页面的功能，用于实现Web+Portal认证方式。

用户浏览器发起互联网访问请求后，BAS将该请求重定向至Portal服务器。

Portal服务器支持二级重定向功能，以实现网间漫游功能。

Portal服务器与运营商的短信网关系统等配合，支持用户获取接入WLAN网络的密码。

6.2.7 固网宽带 AAA

主要是RADIUS服务器和证书服务器，为固网宽带用户提供PPPoE认证，为WLAN用户提供基于802.1X的接入认证，并支持运营商内异构网络间的用户账号漫游。

6.2.8 移动 AAA

运营商移动核心网的认证系统，用于支持EAP-SIM/AKA认证，并支持运营商内异构网络间的用户账号漫游。

6.3 网元接口

6.3.1 网元接口概述

包括用户STA与AP、BAS、Portal服务器的接口，AP与AC、BAS的接口，BAS与Portal的接口。

6.3.2 用户 STA 与 AP 之间的接口

用户STA与AP之间的接口是空中接口，符合GB15629.11、GB 15629.11-2003、GB 15629.1101-2006、GB 15629.1102-2003、GB 15629.1104-2006和IEEE802.11-2012。

6.3.3 用户 STA 与 BAS 之间的接口

用户STA与BAS之间为认证交互接口，无物理接口。

6.3.4 用户 STA 与 Portal 之间的接口

用户STA与Portal之间为业务控制接口，采用HTTP或HTTPS协议，支持Web认证页面推送，支持用户上下线通知。

6.3.5 AP 与 AC 之间的接口

AP与AC之间可以是2层或3层网络接口，集中控制型AP与AC之间应符合CAPWAP协议。

不同厂商的AP与AC之间应该能够互通，一个厂家的AC可以管理另外一个厂家的AP，至少可以实现设备发现功能和批量配置数据下发功能等基本管理功能。

6.3.6 AP 与 BAS 之间的接口

AP与BAS之间是3层网络接口。

在家庭共享场景下，AP是用户的家庭网关，该接口通过家庭用户宽带接入线路实现。

在机构共享场景下，该接口通过用户的内部网络及到运营商的专线实现。

交通场景2情况下，该接口通过移动网络实现。

6.3.7 BAS 与 Portal 之间的接口

BAS与Portal之间为业务控制接口。

7 网络功能要求

7.1 认证

7.1.1 认证方式

用户接入的认证方式有多种，如Web+Portal方式、EAP-SIM/AKA方式、PEAP方式等。

7.1.2 认证协议栈模型

Web+Portal认证方式下，认证协议栈模型如图6所示。

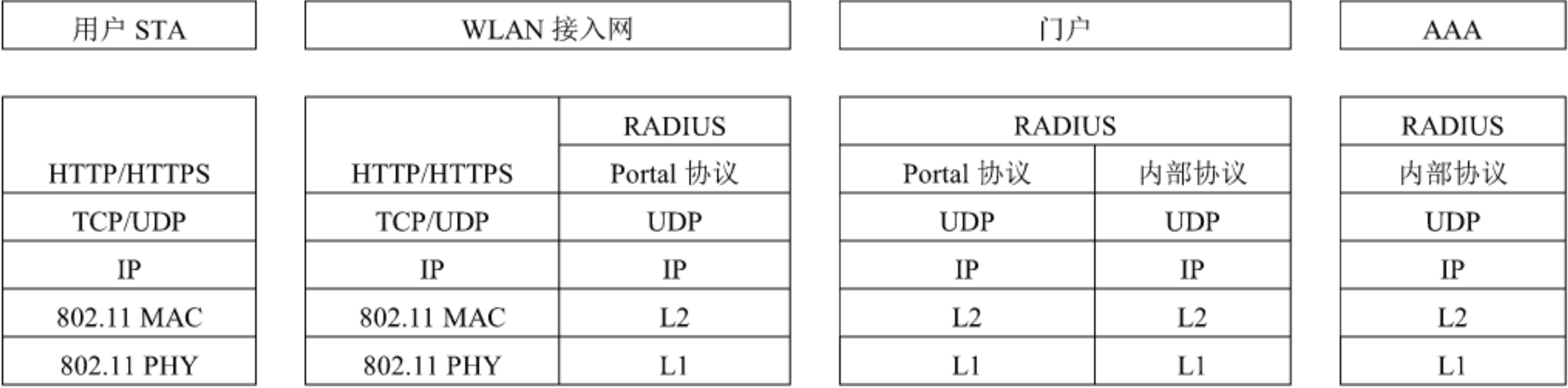


图6 Web+Portal认证协议栈模型

EAP-SIM/AKA和PEAP认证方式下，AAA对WLAN用户进行认证时，使用基于802.1X架构的EAPoL认证协议栈模型，如图7所示。

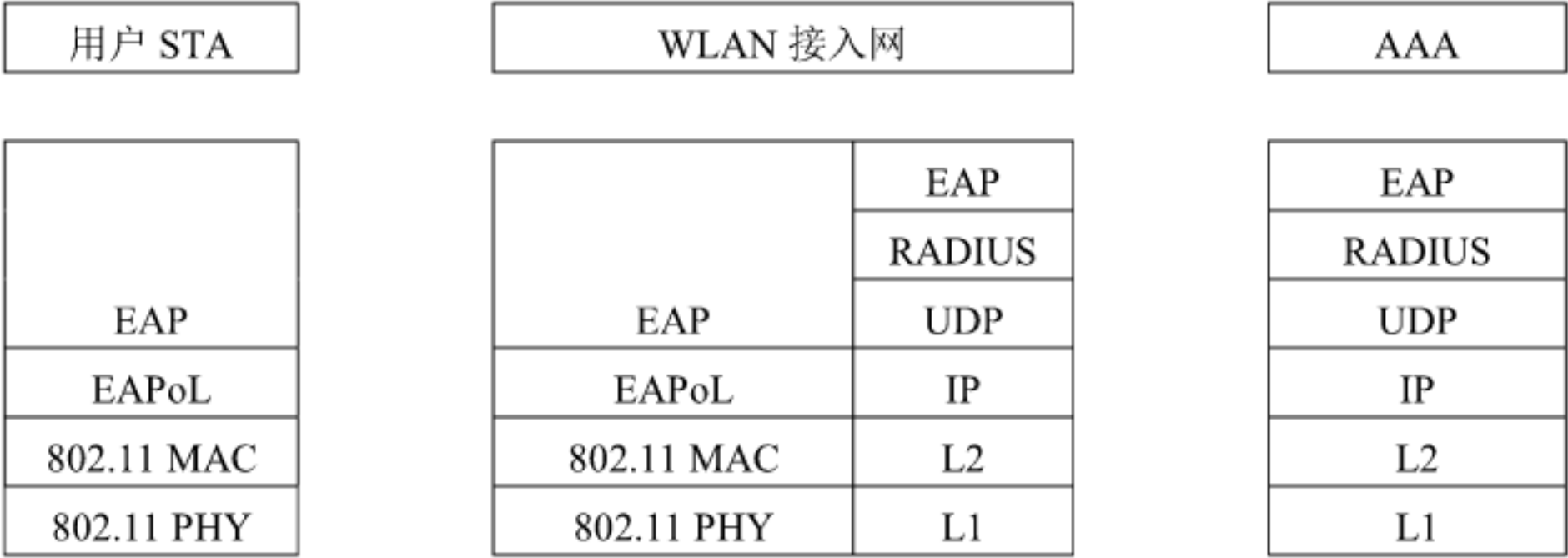


图7 EAP-SIM/AKA和PEAP认证协议栈模型

7.2 网络管理

WLAN网络管理系统实现对所辖范围内WLAN接入网中各类网元设备的集中监管。WLAN网络管理系统应支持拓扑、配置、性能、安全、故障等方面的管理功能。

WLAN网络管理网络逻辑拓扑结构图如图8所示。

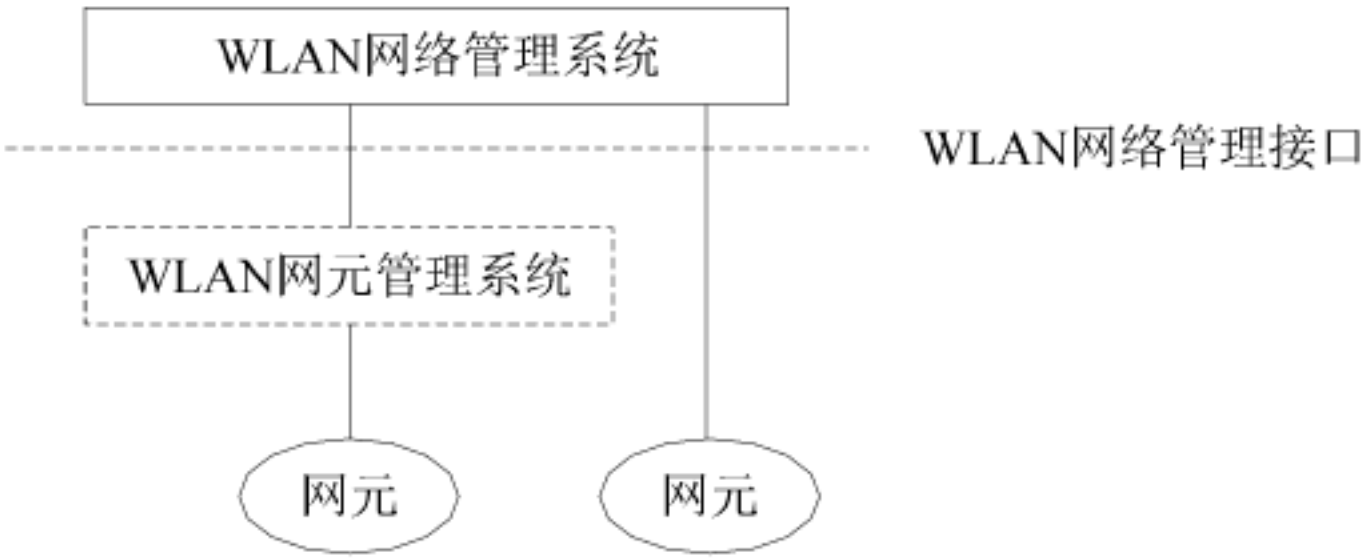


图8 WLAN网管网络逻辑拓扑结构图

其中WLAN网络管理系统与网元管理系统或网元设备之间的WLAN网元管理接口实现对网元设备和用户接入信息的采集，可通过设备厂商提供的WLAN网元管理系统间接采集，或从网元设备直接采集，一般采用直接采集方式，WLAN网元管理功能可选。WLAN网络管理接口应支持配置管理功能、告警管理功能和性能管理功能，要求WLAN网络管理系统和网元设备应支持统一的传输协议和数据参数，公众无线局域网网元管理接口技术要求详见YD/T 2615.3-2013。

7.3 切换

在同一运营商WLAN网络热点连续覆盖的范围内，通过网络调整，使AP由同一AC管理。在该范围内，当用户STA在AP之间切换时，要求IP业务不中断。

用户STA搜索到AP1信号小于可接入阈值，并且AP2的信号大于可接入阈值后，启动切换流程。首先断开与AP1的连接，然后接入AP2，通过AP2完成身份认证，通过AC获得IP地址。

AC根据用户STA的收发信号强度与上下行流量、AP的信号强度、连接用户数、与上下行流量等，来决定是否接纳用户STA的切换请求，以及将某些STA下线。对允许切换的用户，在切换过程中AC临时保留其IP地址，如图9所示。

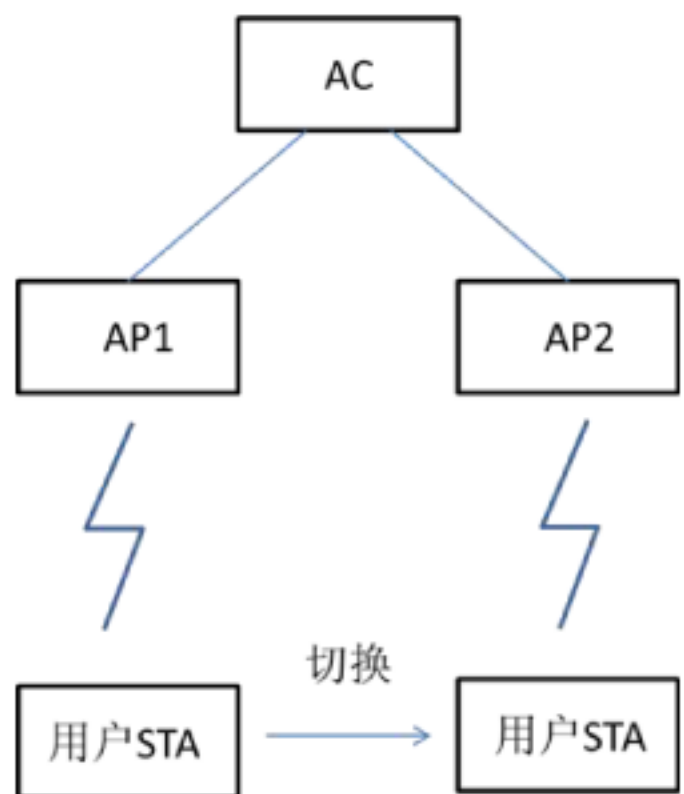


图9 切换示意

7.4 漫游

7.4.1 漫游实现方式

WLAN网络的漫游是指用户从归属网络到访问网络后，仍然能够以原有身份通过WLAN接入的过程。归属网络（Home Network）为用户签约网络，在用户的生命周期中唯一。访问网络（Visited Network）是指在某个具体时刻，为用户提供WLAN接入服务的网络。

实现跨运营商漫游的前提是不同运营商之间建立互信任机制，通常是双方相互签订漫游协议，或者同时与某第三方漫游组织签订漫游协议。

漫游一般通过AAA代理方式实现：指拜访地AAA充当AAA代理，将消息路由给漫游用户归属的AAA进行认证和计费，如图10所示。

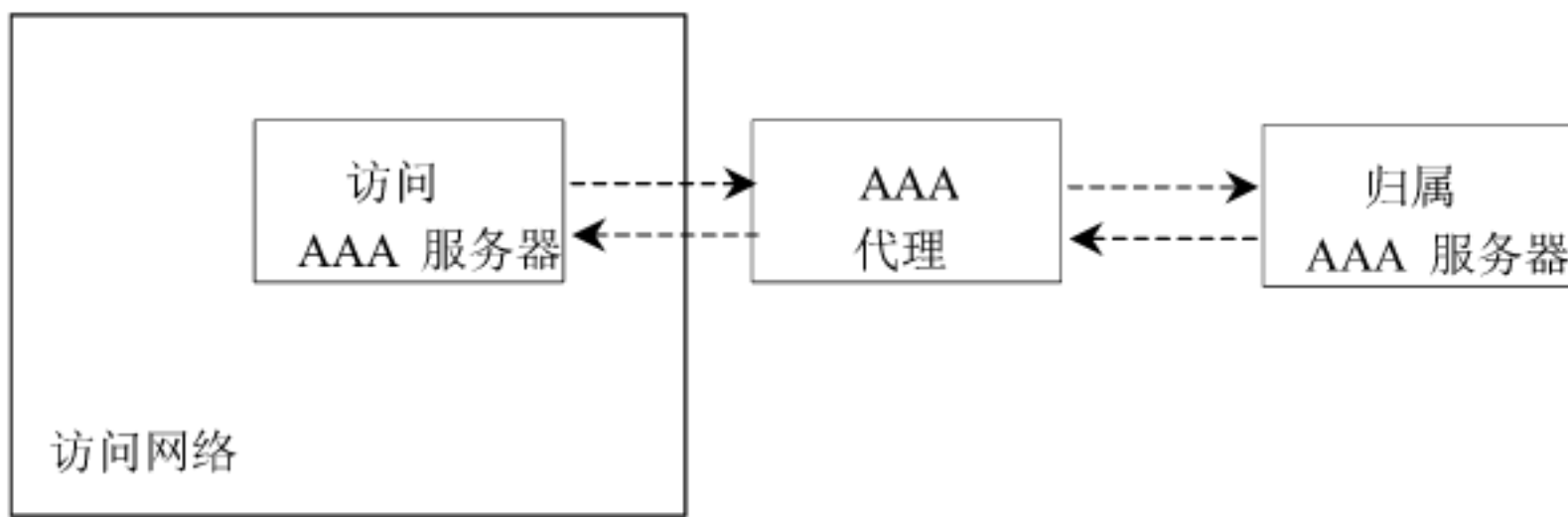


图10 漫游示意

Home AAA Server为归属AAA，是漫游用户的数据保存地，用户漫游时的真正认证和计费服务器，隶属于归属网络。

Visited AAA Server为拜访AAA，是漫游用户实际接入网络的AAA服务器，在用户漫游时充当AAA代理的作用，隶属于访问网络。

AAA Proxy是AAA代理，提供AAA信息的路由，支持RADIUS Client和RADIUS Server协议，漫游时所有的代理消息均通过这里转发。RADIUS协议符合IETF RFC 2865、IETF RFC2866以及IETF RFC2869的要求。

漫游用户从拜访网络接入时，拜访网络的AP将用户的认证/计费消息通过拜访BAS或者有BAS功能的AC上报给拜访AAA进行认证，拜访AAA再将该认证消息通过Proxy AAA转发给归属AAA进行认证/计费。因此，用户的认证/计费实际是在归属AAA中进行的。

7.4.2 漫游协议栈模型

Visited AAA服务器、AAA Proxy、Home AAA服务器的协议栈模型如图11所示。

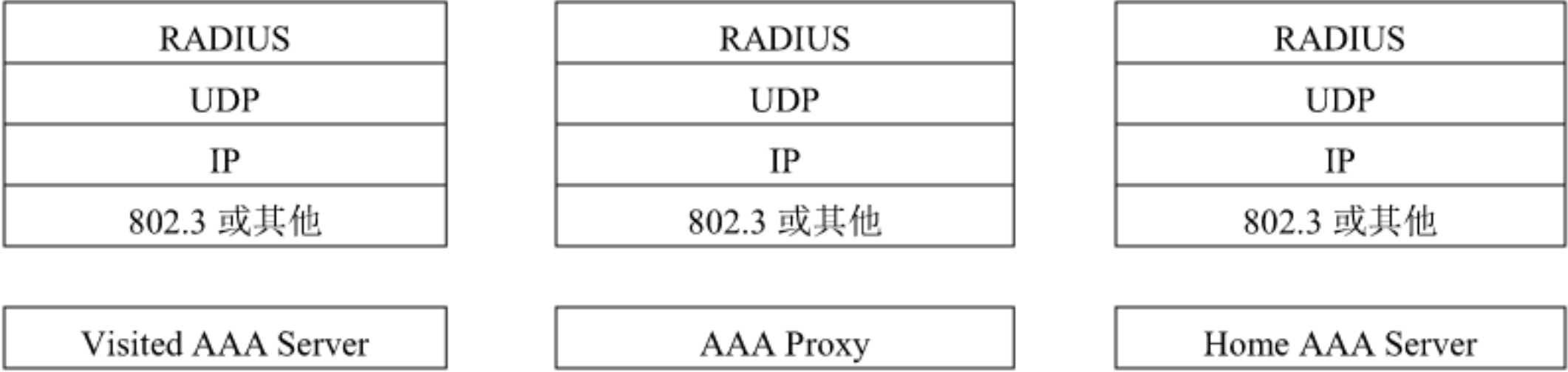


图11 漫游协议栈