ICS 33.040.01
M 10

YD

中华人民共和国通信行业标准

YD/T 2842-2015

宽带网络接入服务器支持 WLAN 接入及用户认证的技术要求

Technical specification for network equipment BRAS to support user authentication in WLAN access network scenario

2015-04-30 发布　　2015-07-01 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

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：中国电信集团公司、中国联合网络通信集团有限公司、华为技术有限公司。

本标准主要起草人：高　波、王　波、潘毅明、黄国瑾、夏俊杰、华一强、王泽林、王晓箴、薛　莉、杜宗鹏、胡俊理、钱国锋。

引　言

本文件的发布机构提请注意，声明符合本文件时，可能涉及到《一种无线局域网中密钥传递的方法、设备和系统》中密钥传递的方法与本文件附录A中的PMK下发方案相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得：

专利持有人姓名：华为技术有限公司

地址：深圳市龙岗区坂田华为基地

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

宽带网络接入服务器支持WLAN接入及用户认证的技术要求

1 范围

本标准规定了宽带网络接入服务器（BRAS）支持WLAN接入及用户认证的技术要求。

本标准适用于公共热点WLAN网络AC和BRAS分离部署场景下，支持用户认证的宽带网络接入服务器技术要求。本标准不适用于公共热点WLAN网络AC和BRAS合为一体部署场景（AC具有BRAS对用户地址分配、认证、管理等功能）。

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。

YD/T 1148 网络接入服务器技术要求——宽带网络接入服务器

IETF RFC2548 微软特定的RADIUS属性（Microsoft Vendor-specific RADIUS Attributes）

IETF RFC2759 微软的点到点协议的CHAP扩展第二版（Microsoft PPP CHAP Extensions, Version 2 (MSCHAPv2)）

IETF RFC2865 远程认证拨号用户服务（Remote Authentication Dial In User Service (RADIUS)）

IETF RFC3748 扩展认证协议（Extensible Authentication Protocol (EAP)）

IETF RFC4186 针对全球移动通信系统用户标示模块的扩展认证协议方法（Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)）

IETF RFC4187 针对第三代移动通信系统认证和密钥协商的扩展认证协议方法（Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)）

IETF RFC5176 RADIUS的动态授权扩展（Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)）

IEEE 802.1X 基于端口的访问控制（Port-Based Network Access Control）

IEEE 802.11 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）

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件：

3.1.1

无线接入点　Access Point

WLAN网络中的用户无线接入设备。

3.1.2

无线控制点　Access Controller

WLAN网络中管理AP的设备，它通过CAPWAP协议来实现对AP的管理。

3.1.3

宽带网络接入服务器　Broadband Remote Access Server

面向宽带网络应用的新型接入网关，它位于骨干网的边缘层，可以完成用户宽带网络的数据接入。

3.1.4

无线局域网　Wireless Local Area Networks

以无线信道作传输媒介的计算机局域网，遵循IEEE 802.11系列协议。

3.1.5

远程认证拨号用户服务　Remote Authentication Dial in User Service

广泛应用的AAA协议，它是一种同时兼顾验证、授权及计费三种服务的网络传输协议。

3.1.6

扩展认证协议　Extensible Authentication Protocol

一个认证框架，它提供一些公共的功能，并且允许协商所希望的认证机制，这些机制被称为EAP方法，例如PEAP、EAP-SIM/AKA。

3.1.7

802.1X认证　802.1X Authentication

IEEE为了解决基于端口的接入控制而定义的一个标准，它在运营商WLAN网络部署被广泛采用。802.1X认证体系结构包括三个重要的组成部分：客户端、认证点和认证服务器。

3.1.8

认证点　Authenticator

802.1X认证中的认证点，用于连接客户端和认证服务器实现对客户端的认证。

3.1.9

成对主密钥　Pairwise Master Key

对于使用RADIUS服务器的802.1X身份验证，PMK由无线客户端和RADIUS服务器共同确定，RADIUS服务器通过RADIUS Access-Accept消息将PMK传输给WLAN设备。接收到PMK后，WLAN设备与用户终端启动临时密钥消息交换机制，协商出来的密钥将作为802.11数据传输过程中的加密/解密密钥。

3.2　缩略语

以下缩略语适用于本文件：

3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
AAA	Authentication Authorization Account	认证授权计费
AC	Access Controller	WLAN接入控制节点
AKA	Authentication and Key Agreement	3G的认证与密钥协商

AP	Access Point	WLAN接入节点
BRAS	Broadband Remote Access Server	宽带网络接入服务器
CAPWAP	Controlling and Provisioning of Wireless Access Point	AP控制与配置协议
CHAP	Challenge-Handshake Authentication Protocol	挑战-握手验证协议
DHCP	Dynamic Host Configuration Protocol	动态主机设置协议
DM	Disconnect Message	断开连接消息
EAP	Extensible Authentication Protocol	扩展认证协议
EAPoL	Extensible Authentication Protocol over LAN	承载于局域网上的扩展认证协议
MAC	Medium Access Control	媒体介入控制层
PAP	Password Authentication Protocol	口令验证协议
PC	Personal Computer	个人电脑
PEAP	Protected EAP	受保护的EAP
PMK	Pairwise Master Key	成对主密钥
QoS	Quality of Service	服务质量
RADIUS	Remote Authentication Dial In User Service	远程认证拨号用户服务
SIM	Subscriber Identity Module	用户身份模块
UE	User Equipment	用户终端
USIM	Universal Subscriber Identity Module	全球用户识别卡
URL	Uniform Resource Locator	统一资源定位符
VPN	Virtual Private Network	虚拟局域网
WLAN	Wireless Local Area Networks	无线局域网络

4 AC/BRAS 分设的 WLAN 网络总体架构

WLAN网络架构中主要包括如下设备：AP、AC、BRAS、Portal服务器、RADIUS 服务器。其中AC设备的部署位置会直接影响WLAN网络架构，本标准主要关注AC和BRAS分设的WLAN网络架构，其中AC负责无线资源管理、AP的配置和管理，BRAS负责用户的地址分配、接入认证、用户管理等功能。该场景下，用户数据可以经AC集中转发，也可以本地直接转发，WLAN网络架构有如下四种：

——网络架构(一)：AC 旁挂于 BRAS。该架构中，AC 旁挂 BRAS，AP 和 AC 之间可以采用三层组网，AC 实现对 BRAS 以下 AP 进行配置和管理，如图 1 所示。

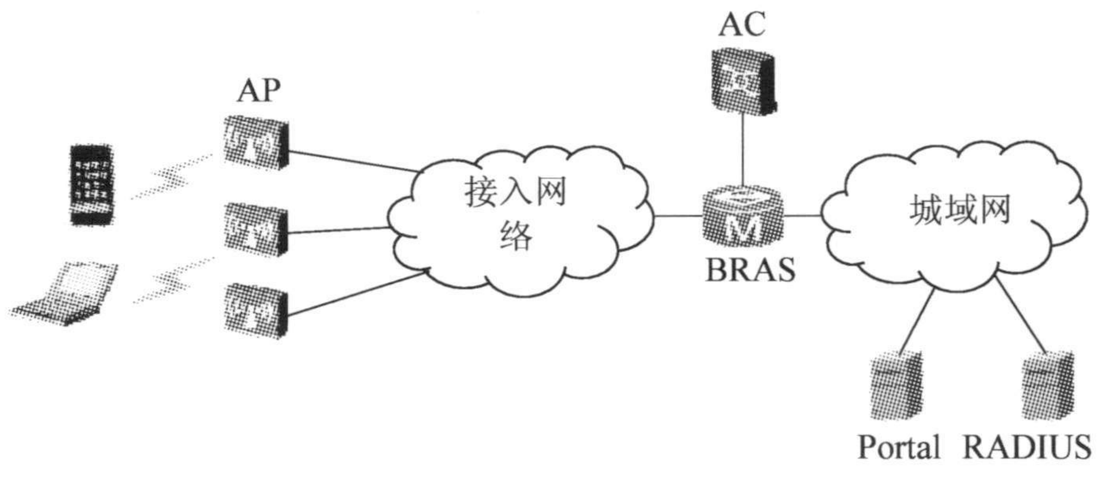


图1　AC 旁挂于 BRAS

——网络架构(二)：AC 旁挂于接入网络交换机。该架构中，AC 旁挂在二层交换机上，AP 和 AC 之间可以采用二层组网，AC 实现对所在二层网络的 AP 进行配置和管理，如图 2 所示。

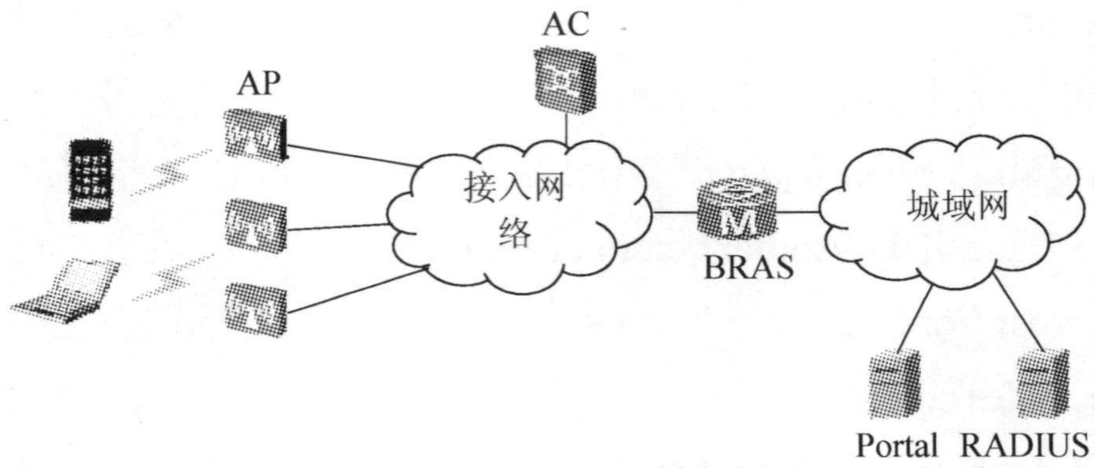


图2　AC 旁挂于接入网络交换机

——网络架构(三)：AC 旁挂于城域核心网。该架构中，AC 旁挂于城域核心网的汇聚设备上，AP 和 AC 之间可以采用三层组网，AC 实现对一个或多个 BRAS 以下的 AP 进行配置和管理。此组网模式下，若用户数据经 AC 集中转发，需 BRAS 与 AC 之间开通 VPN 通道。如图 3 所示。

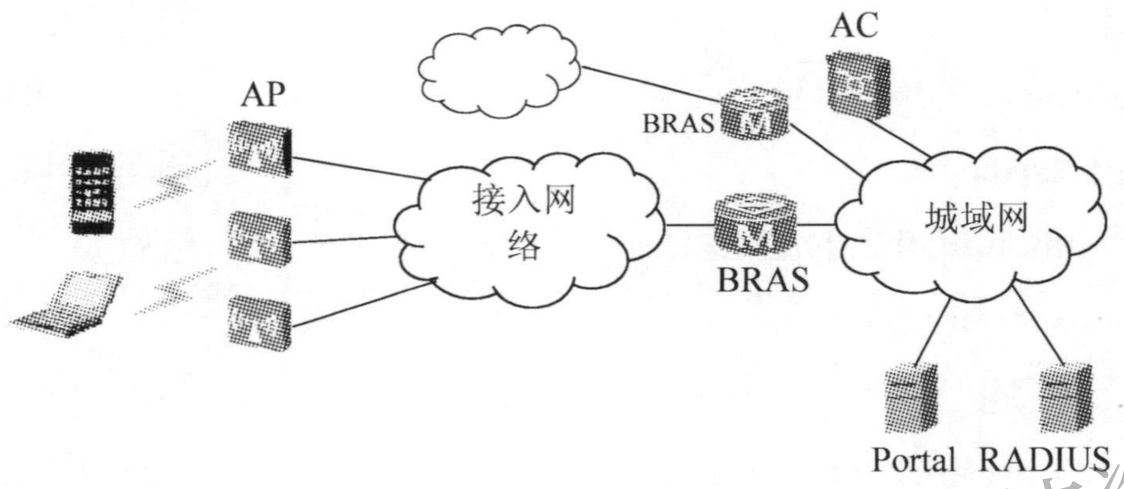


图3　AC 旁挂于城域核心网

——网络架构(四)：AC 直连模式。该架构中，AC 部署为直连模式。AC 实现对其下连的 AP 进行配置和管理。如图 4 所示。

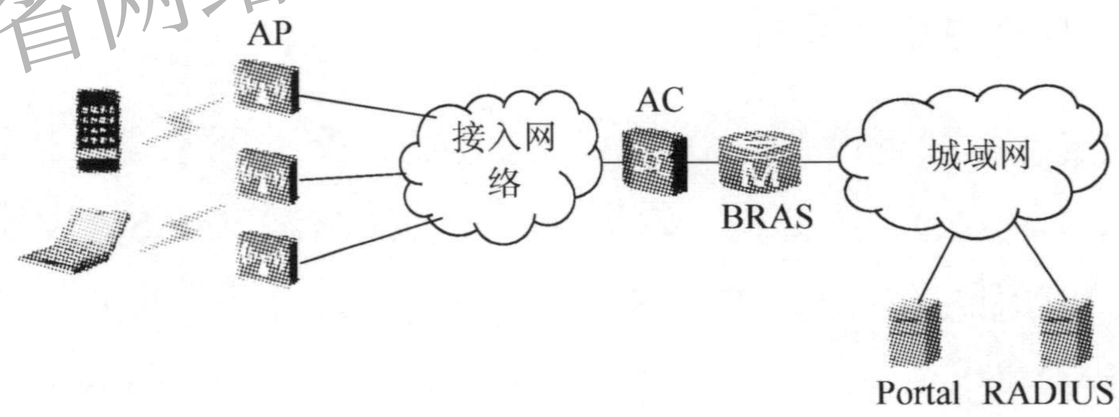


图4　AC 直连模式

本标准基于上述组网模式，制定了BRAS支持用户认证技术要求。

5　BRAS 支持 Portal 认证的技术要求

5.1　Portal 认证流程

Portal认证体系架构如图5所示。

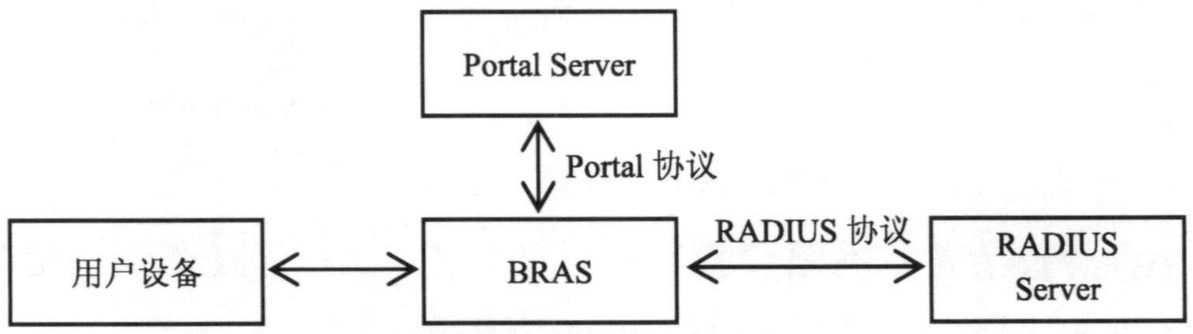


图5　Portal 认证体系结构

Portal认证流程如图6所示。在Portal认证之前，需要用户终端接入指定的SSID（OPEN模式）。

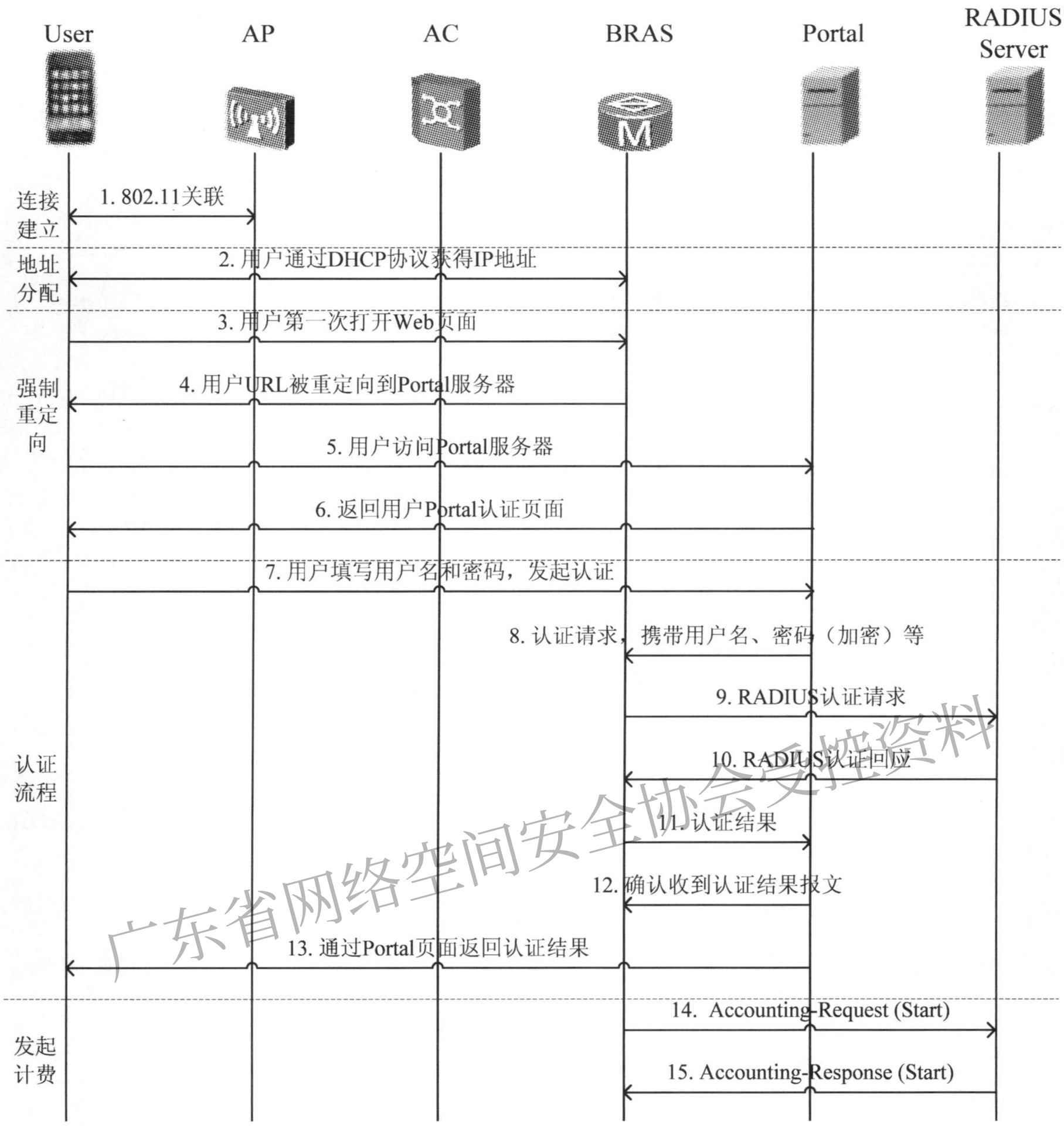


图6　Portal 认证工作流程

Portal认证流程可划分为下面几个步骤：

a）连接建立过程

- 该过程中用户终端和 AP 设备通过 802.11 协议建立关联。

b）地址分配过程

- 用户终端通过 DHCP 协议获得 BRAS 分配的 IP 地址。

c）强制重定向过程

- 未认证前，用户的 Web 访问被 BRAS 强制重定向到 Portal 页面。

d）认证流程

- 用户提交用户名和密码，相关网络设备完成认证流程。
- 在该过程中，为了传递用户名和密码，Portal 服务器和 BRAS 之间的消息交互采用 CHAP 或 PAP 方式。

e）计费流程

- BRAS 通过发送计费报文发起计费流程。

Portal认证方式中，用户下线流程包括用户主动下线、强制下线和异常下线。具体如下：

——用户主动下线流程：用户通过 Portal 控制触发的用户下线，如图 7 所示。Portal 服务器收到用户的下线请求后，发起用户下线流程。

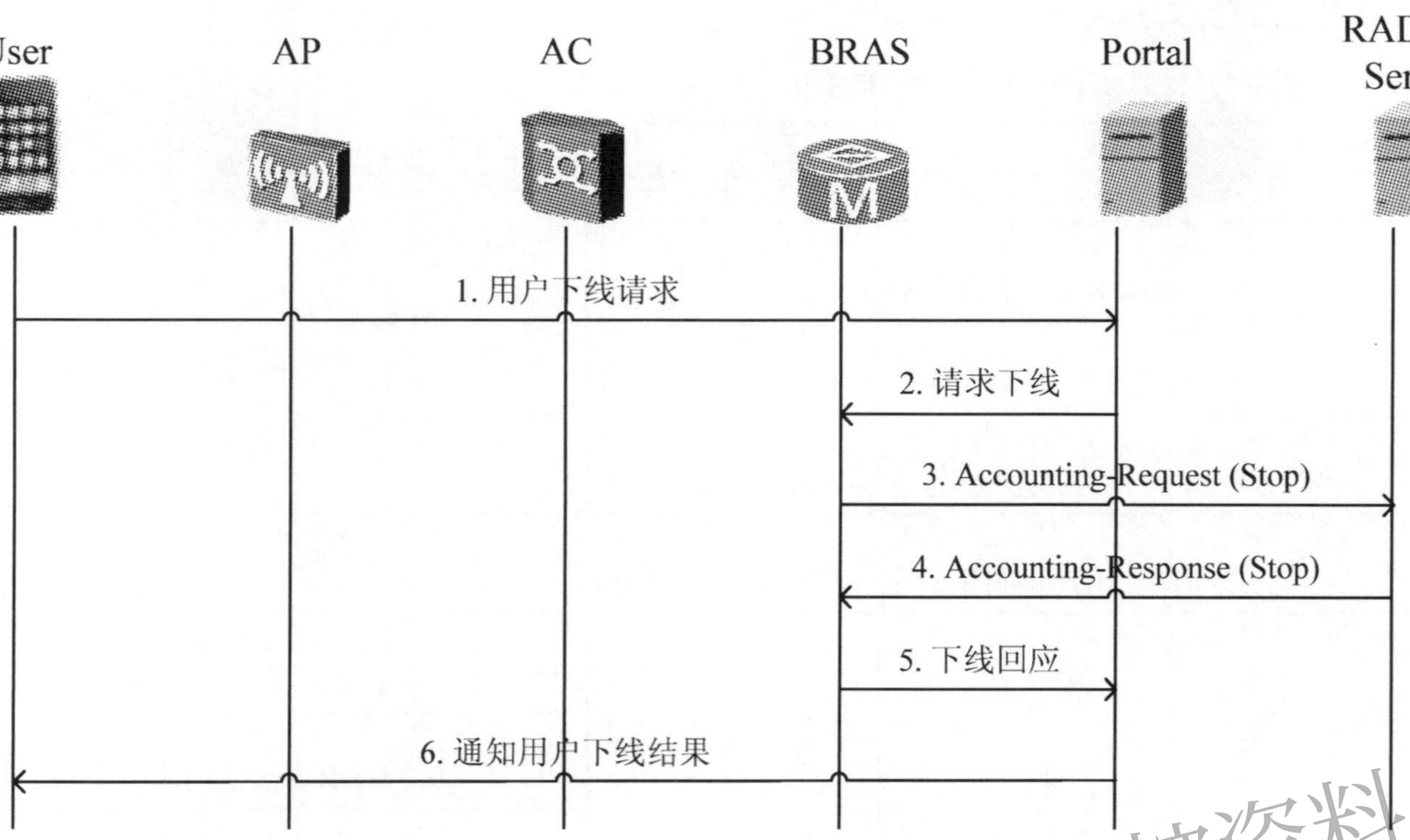
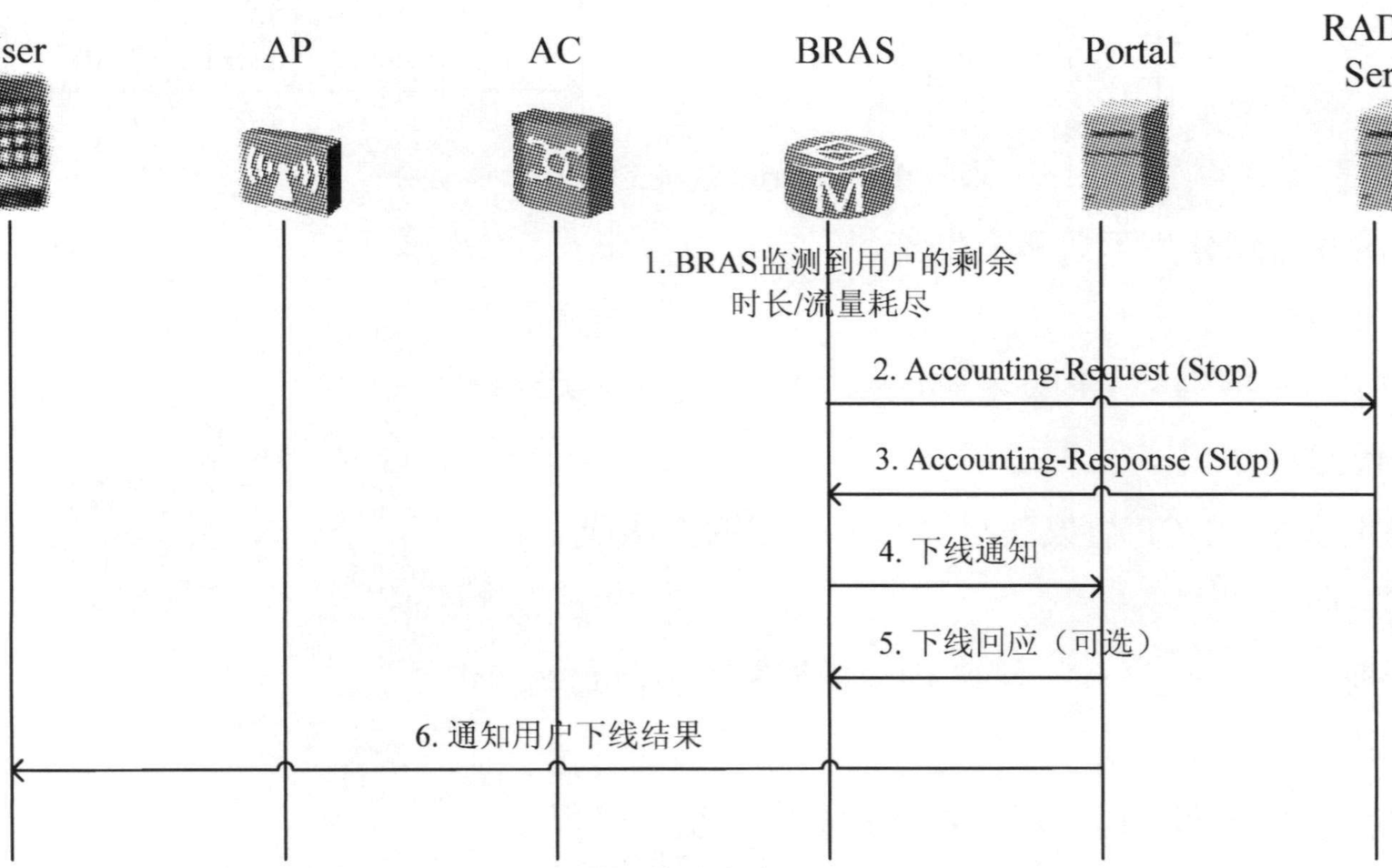


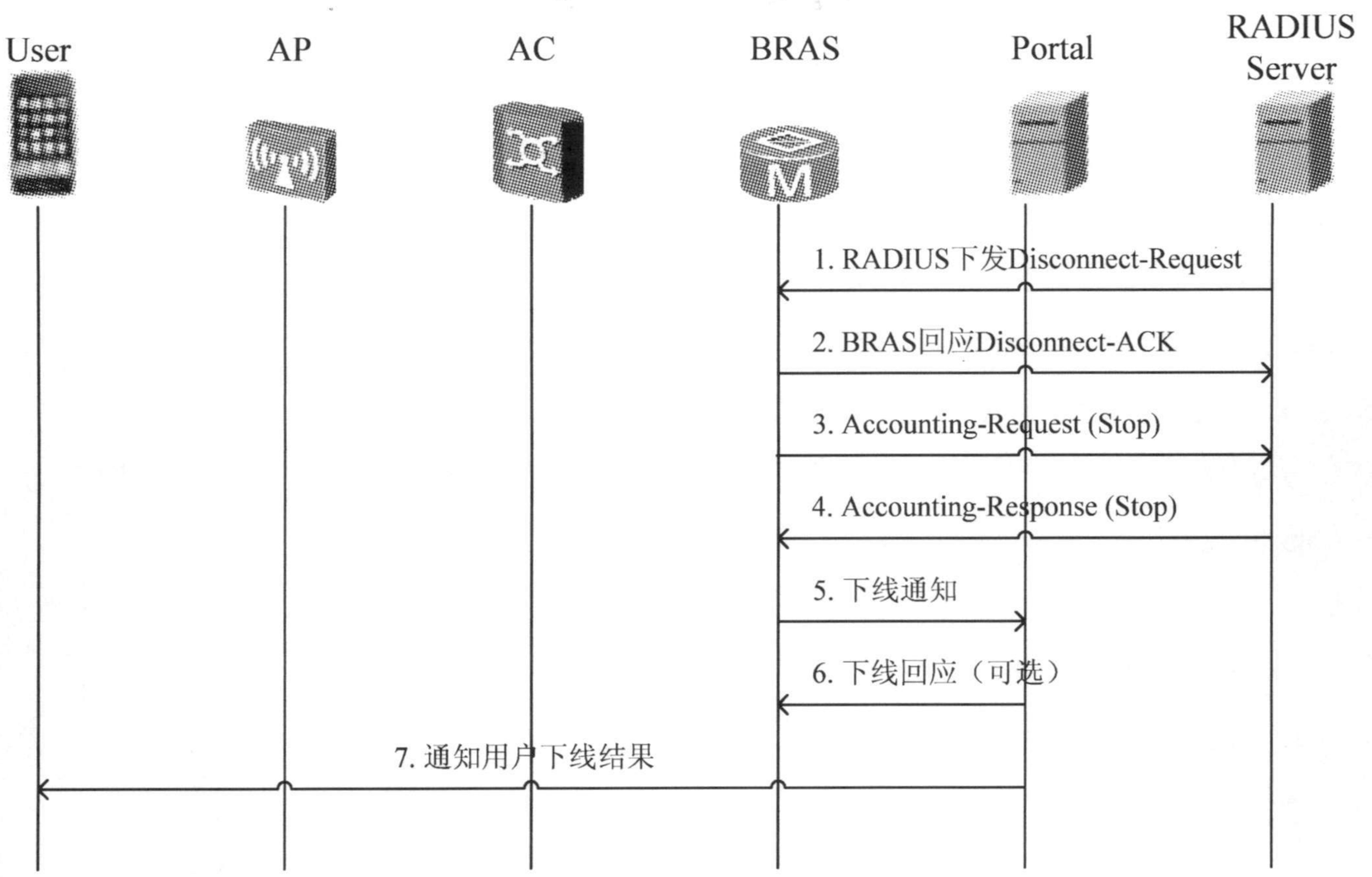
图7　Portal 认证用户主动下线流程

——用户（预付费）强制下线流程：用户强制下线流程可分为 BRAS 触发用户下线和 RADIUS 服务器触发用户下线两种方式。

- BRAS 触发：BRAS 监测到用户的剩余时长/流量耗尽，向 Portal 服务器请求下线，如图 8 a)所示；
- RADIUS 服务器触发：RADIUS 服务器下发的 DM（Disconnect Messages）消息强制用户下线，如图 8 b)所示。



a) BRAS触发



b) RADIUS服务器触发

图8　Portal 认证用户（预付费）强制下线流程

——用户异常下线流程：用户异常下线是指用户未执行主动退出操作而断开网络连接的情形，如用户关机、重启、或网络故障等。BRAS 通过 ARP 报文探测或流量监测功能感知用户下线，如图 9 所示。

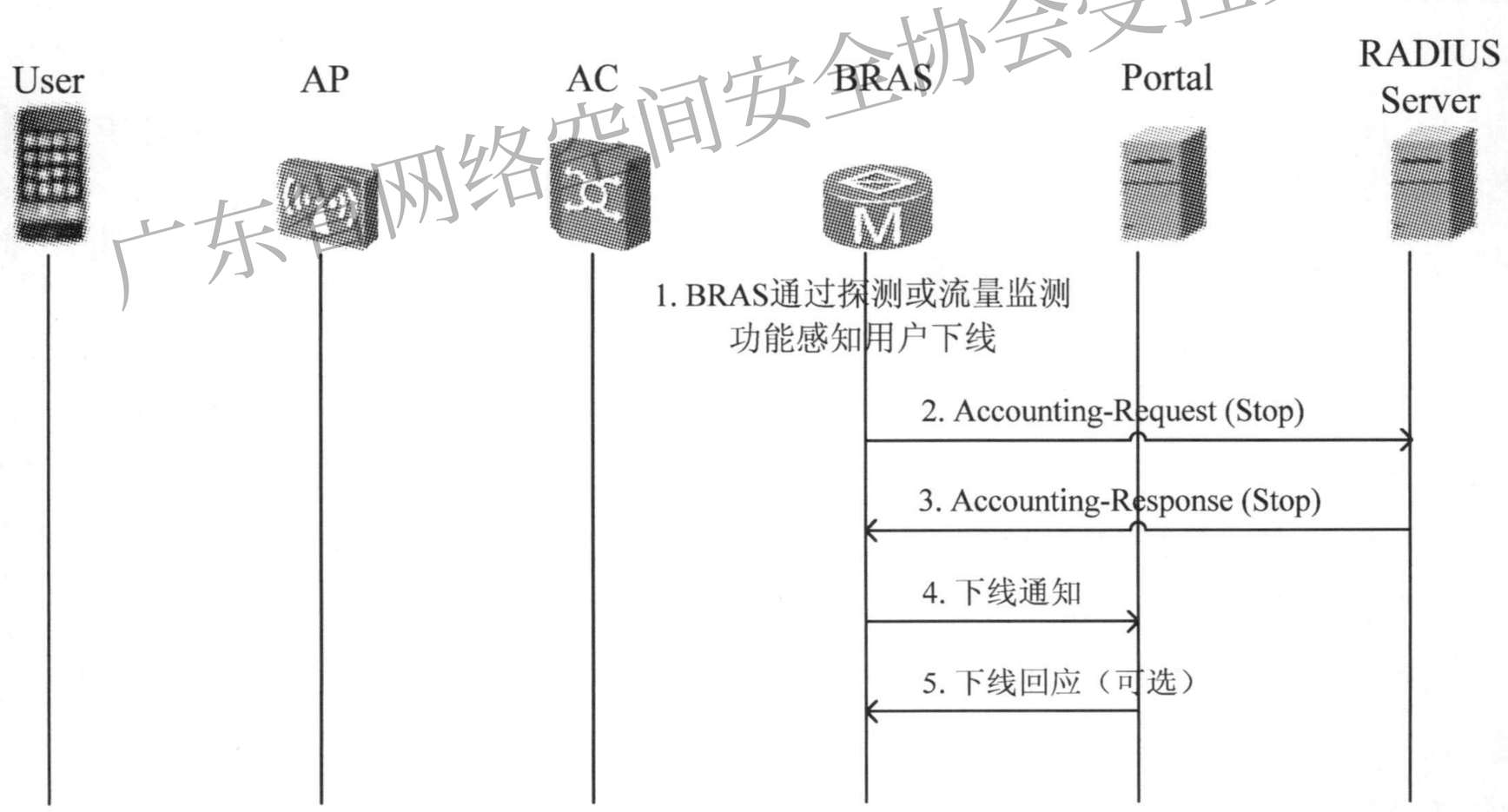


图9　Portal 认证用户异常下线流程

5.2　BRAS 技术要求

宽带网络接入服务器支持Portal认证技术要求应满足以下技术要求。

5.2.1　接口功能技术要求

Portal认证系统主要包括四个组件：用户终端，BRAS，Portal服务器和RADIUS服务器。在支持Portal认证的场景中，BRAS应支持以下接口：

——BRAS 设备应支持与 Portal 服务器的接口。接口的功能要求包括：用户名密码交互，认证信息交

互，用户管理等。

——BRAS 设备应支持与 RADIUS 服务器的接口。接口的功能要求包括：用户认证计费信息交互，用户管理等。

5.2.2 协议功能技术要求

Portal认证中，BRAS应支持如下协议和功能的技术要求：

——BRAS 应支持自动地址配置协议，如 DHCPv4 协议，在 IPv6 下的 SLAAC 协议和 DHCPv6 协议。

——BRAS 应支持 HTTP 协议和 TCP 协议的侦听能力，支持 Portal 认证的功能。

——BRAS 应支持向用户发送 HTTP 重定向响应，该重定向地址指向 Portal 的 URL。

——BRAS 应支持 Portal 协议，以保证与 Portal 服务器正确交互。

——BRAS 应支持 RADIUS 协议，以保证与 RADIUS 服务器正确交互。BRAS 应支持根据接受到的用户名和密码封装成认证请求报文，向 RADIUS 服务器发送认证请求。

——为了增加安全性，防止 Portal 服务器仿冒，BRAS 需要支持身份验证功能，如 IP 地址校验和/或 MD5 校验。

——为了保证用户认证信息的传输的安全性，BRAS 需要支持 IPSec 安全隧道协议（可选）。

Portal认证中，BRAS应支持受控逻辑端口和非受控逻辑端口的功能。在完成用户认证流程之前，BRAS设备受控逻辑端口关闭，连接在受控逻辑端口的非授权用户不能访问网络资源。非受控逻辑接口允许用户的控制层协议报文通过。

BRAS应支持下述受控逻辑端口和非受控逻辑端口功能要求：

——BRAS 应支持受控逻辑端口初始状态为关闭，未完成或未通过授权的用户终端不能访问受保护网络资源；在用户终端认证成功后，BRAS 设备的受控逻辑端口打开，用户终端可通过 BRAS 访问受保护网络资源。

——BRAS 的受控逻辑端口可以配置为双向受控或单向受控状态。当实行双向受控时，禁止数据的发送和接受；实行单向受控时，禁止从用户终端接受数据，但允许向用户终端发送数据。

——为保证 Portal 方式的接入身份认证，需要保证用户终端满足一定的网络基础条件。例如用户终端需要预先获得 IP 地址，且能够进行地址解析,以保证浏览器能够正常发起网络请求。为此，需要 BRAS 支持非受控逻辑端口允许授权的控制信令通过，如 ARP 协议，自动地址配置协议（如 DHCPv4 协议，IPv6 下的 SLAAC 协议和 DHCPv6 协议）。非受控端口的转发状态不受制于受控端口的状态。

——为支持基于 Portal 接入身份认证，需要用户终端具备一定的网络访问能力。在用户完成 Portal 认证之前，需要保证用户终端能够访问 DNS 服务器、Portal 服务器地址。因此，BRAS 设备应支持允许目的地地址为这类地址的用户报文通过。

——BRAS 受控逻辑端口和非受控逻辑端口应可支持 IPv4、IPv6 协议。

——用户正常下线，BRAS 可通过获取 Portal 服务器的用户下线通知，关闭受控逻辑端口。

——用户异常下线，BRAS 可通过 ARP 报文探测或流量监测功能感知用户下线，关闭受控逻辑端口。

5.2.3 用户和业务管理技术要求

Portal认证中，BRAS应支持对用户流量进行管理，以实现认证阶段用户流量重定向、用户管理等功能。BRAS应支持下述用户流量管理功能：

——BRAS 支持在截获到未授权用户 HTTP 流量后，将用户请求的 Web 页面重定向到 Portal 服务器。

——BRAS 支持对授权用户的时长/流量信息进行监测，在监测到用户的剩余时长/流量已耗尽时，发起强制用户下线流程。

——BRAS 支持对授权用户的在线状态进行 ARP 报文探测、或流量监测功能，BRAS 感知用户下线并通知 Portal 服务器。

5.2.4 安全性技术要求

Portal认证中，为了防止仿冒攻击和用户认证信息的安全性，BRAS应满足以下安全功能要求：

——BRAS 应支持共享密钥等方式防止 Portal 服务器仿冒攻击。

——BRAS 应支持安全性协议以防止用户认证信息（用户名和密码）的嗅探攻击。

——BRAS 应支持限制用户重定向流量的最大上行带宽。

6 BRAS 支持 MAC 认证的技术要求

6.1 MAC 认证流程

MAC认证的实现原理是网络首先对用户MAC进行比对，如果比对成功则直接允许用户访问网络，如果比对不成功则退回Portal认证。MAC认证以Portal认证流程为基础。MAC认证存在MAC地址仿冒的风险，在实际网络部署中可采用一些安全机制进行规避。MAC认证体系结构如图10所示。

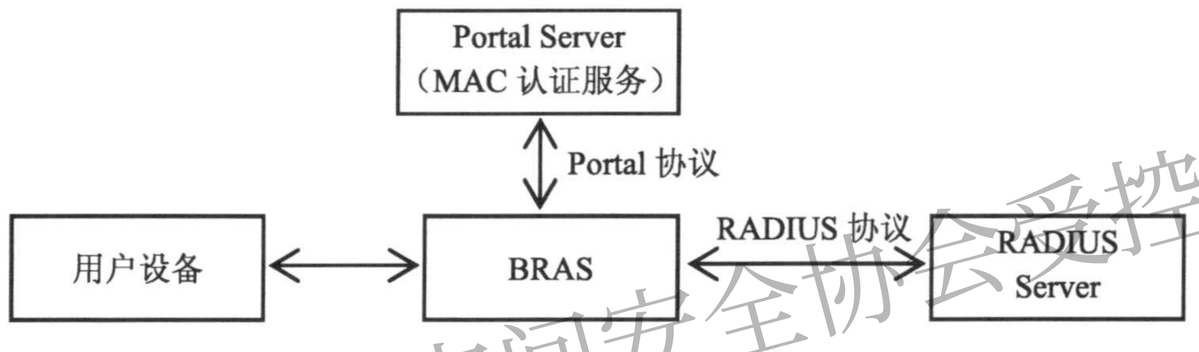


图10 MAC 认证体系结构

MAC认证中，Portal服务器需要支持部署一个子模块监测用户流量。如果Portal服务器监测到用户上网流量，则触发MAC认证。

用户首次接入WLAN网络，MAC认证流程如图11所示（其中MAC认证服务被部署在Portal服务器中）。在MAC认证之前，需要用户终端接入指定的SSID（OPEN模式）。

MAC认证主要流程包括：

a）连接建立过程

- 该过程中用户终端和 AP 设备通过 802.11 协议建立关联。

b）地址分配过程

- 用户终端通过 DHCP 协议从 BRAS 获得 IP 地址。

c）强制重定向过程

- 用户 HTTP 流量被强制重定向到 Portal 服务器，并触发 MAC 认证判断。具体的，若该用户终端是首次连接 WLAN 网络，MAC 认证服务模块中无此终端的 MAC 地址信息，不启动 MAC 认证，用户的 Web 访问被重定向到 Portal 页面（如图 11 所示）；若该用户终端已通过 Portal 页面成功登录 WLAN 网络并开通 MAC 认证，MAC 认证服务模块中有此终端的 MAC 地址与其用户名和密码的绑定关系，启动 MAC 认证，MAC 认证服务模块自动代替用户将用户名和密码发给 BRAS 进行认证（如图 12 所示）。

d）认证流程

- 相关网络设备根据用户名和密码完成认证流程。

e）计费流程

- BRAS 通过发送计费报文发起计费。

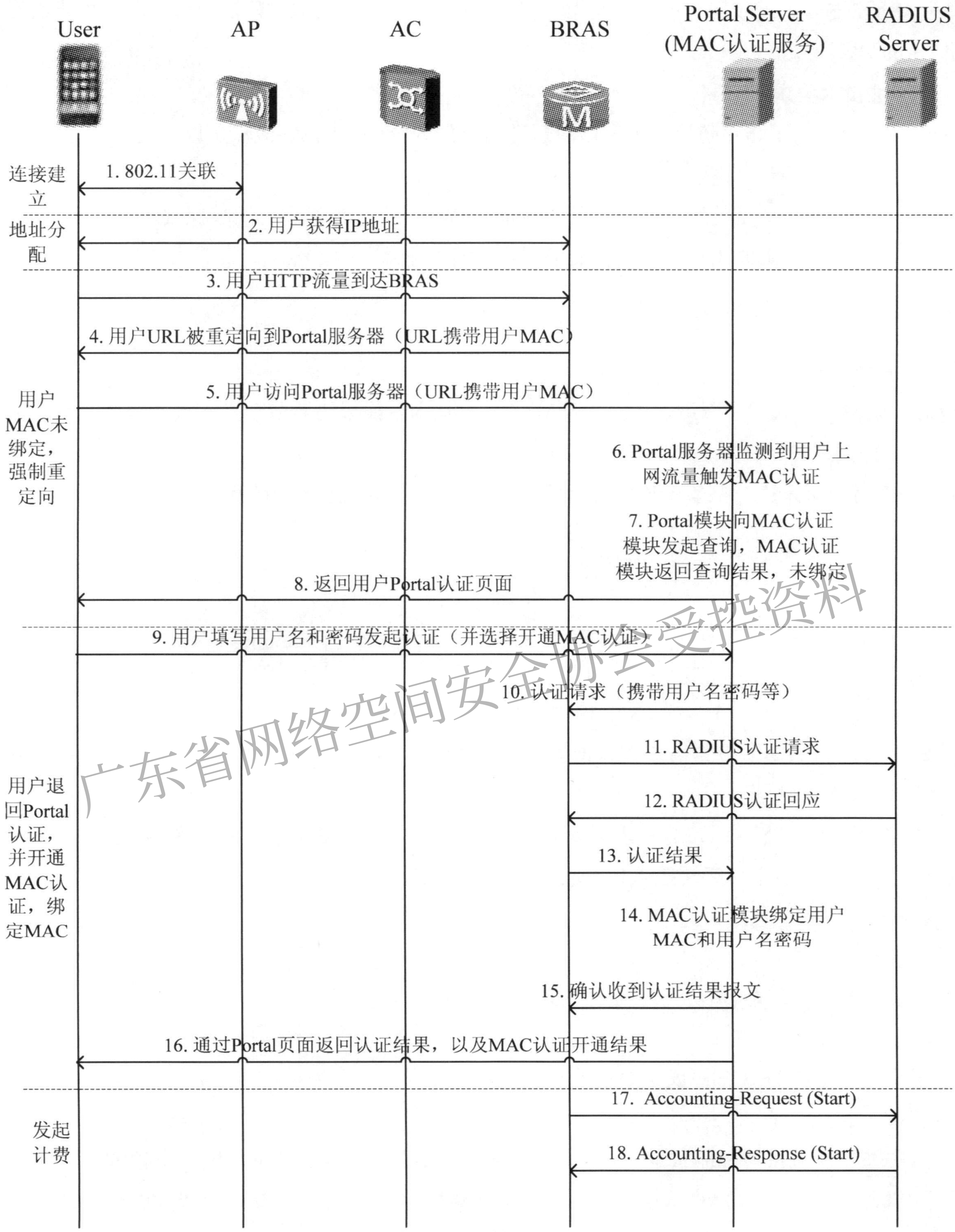


图11　MAC 认证工作流程（首次认证）

用户终端在首次登录WLAN网络时，需要进行Portal认证。选择MAC认证并在Portal认证通过后，该用户终端在后续认证过程中，不再需要输入用户名和密码，可直接通过Portal服务器、RADIUS服务器和BRAS之间的信息交互完成MAC认证。

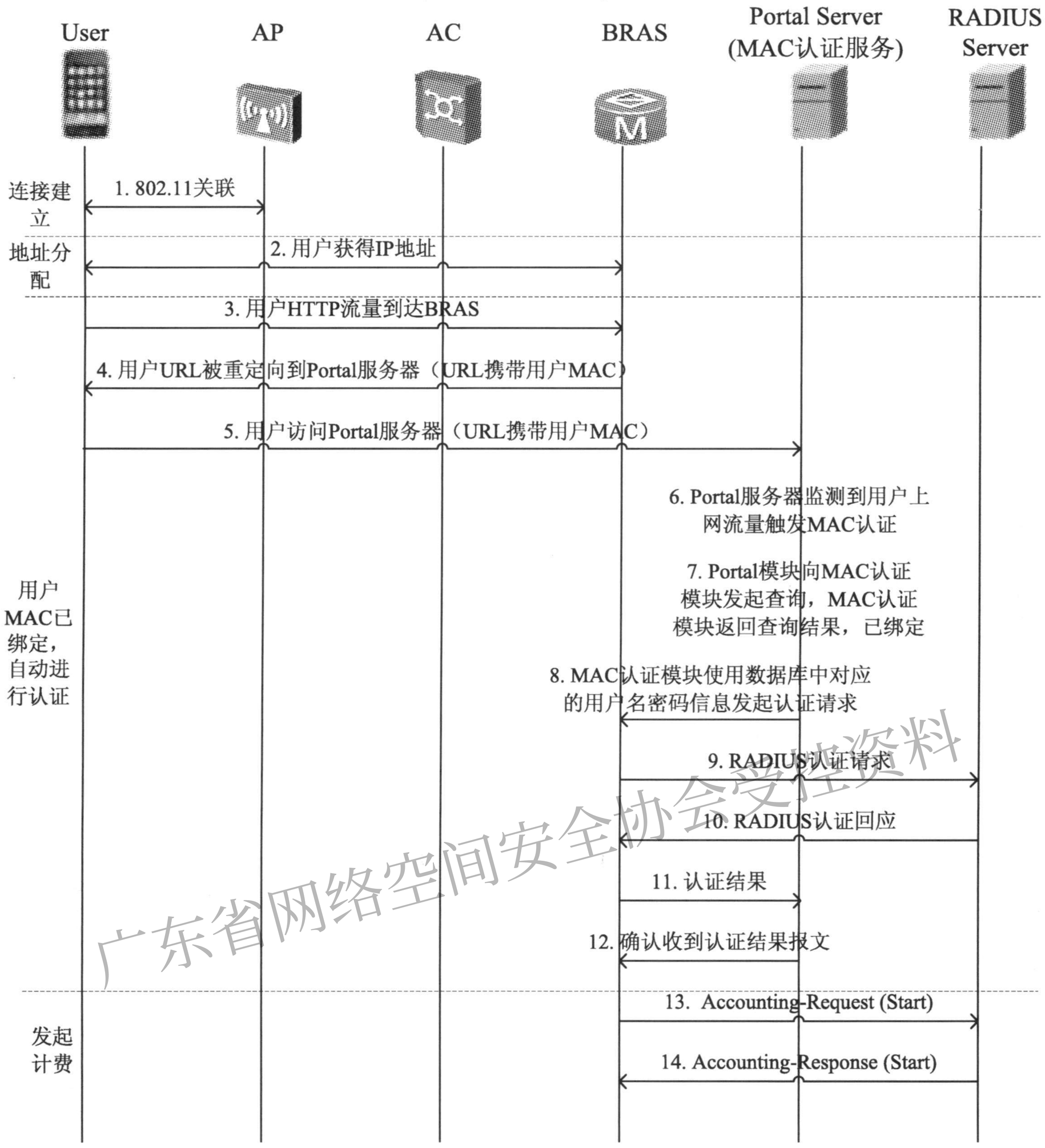
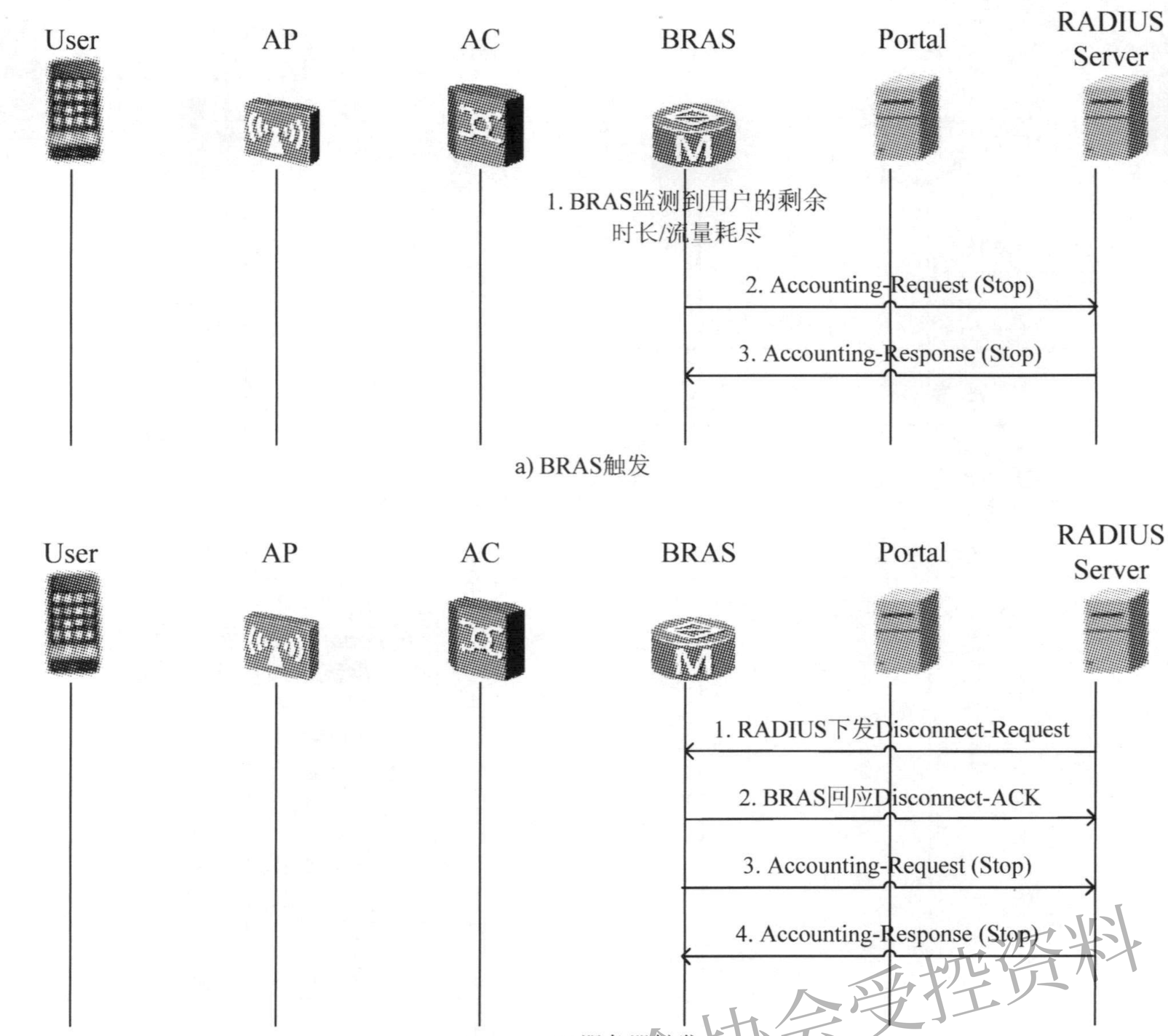


图12　MAC 认证工作流程（后续认证）

MAC认证中，用户下线流程包括用户强制下线和异常下线两种情况，其中BRAS在执行下线操作中不需要通知Portal服务器。具体如下：

——用户（预付费）强制下线流程：用户强制下线流程可分为 BRAS 触发用户下线和 RADIUS 服务器触发用户下线两种方式。

- BRAS 触发：BRAS 监测到用户的剩余时长/流量耗尽，执行用户下线，如图 13 a）所示；
- RADIUS 服务器触发：RADIUS 服务器下发的 DM（Disconnect Messages）消息强制用户下线，如图 13 b）所示。



a) BRAS触发

b) RADIUS服务器触发

图13　MAC认证用户（预付费）强制下线流程

——用户异常下线流程：BRAS 通过 ARP 报文探测或流量监测功能感知用户下线，之后执行用户下线操作，如图 14 所示。

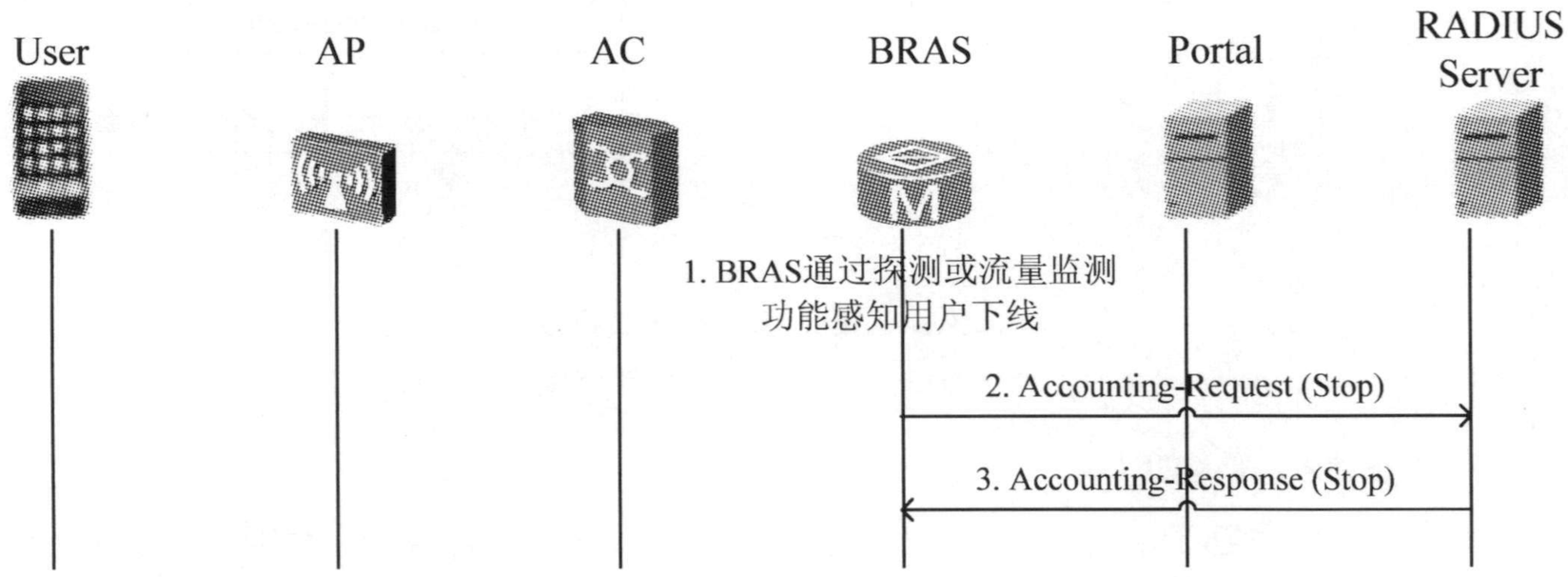


图14　MAC 认证用户异常下线流程

6.2　BRAS 技术要求

宽带网络接入服务器支持MAC认证技术应满足以下技术要求。

6.2.1　接口功能技术要求

MAC认证系统主要包括四个组件：用户终端，BRAS，Portal服务器（包括MAC认证服务模块）和RADIUS服务器。在支持MAC认证的场景中，BRAS应支持以下接口：

——BRAS 设备应支持与 Portal 服务器的接口。接口的功能要求包括：用户名密码交互，认证信息交互等。

——BRAS 设备应支持与 RADIUS 服务器的接口。接口的功能要求包括：用户认证计费信息交互，用户管理等。

6.2.2 协议功能技术要求

MAC认证中，BRAS应支持如下协议和功能的技术要求：

——BRAS 应支持自动地址配置协议，如 DHCPv4 协议，在 IPv6 下的 SLAAC 协议和 DHCPv6 协议。

——BRAS 应支持 HTTP 协议和 TCP 协议的侦听能力，支持 Portal 认证功能。

——BRAS 应支持向用户发送 HTTP 重定向功能，将用户的访问重定向到 Portal 服务器，该重定向地址指向 Portal 的 URL。

——BRAS 应支持 Portal 协议，以保证 MAC 认证过程中与 Portal 服务器的交互。

——BRAS 应支持 RADIUS 协议，以保证 MAC 认证过程中与 RADIUS 服务器的交互。BRAS 应支持根据接受到的用户名和密码封装成认证请求报文，向认证服务器发送认证请求。

——为了增加安全性，防止 Portal 服务器仿冒，BRAS 需要支持身份验证功能，如 IP 地址校验和/或 MD5 校验。

——为了保证用户认证信息的传输的安全特性，BRAS 需要支持 IPSec 安全隧道协议（可选）。

MAC认证中，BRAS需要支持受控逻辑端口和非受控逻辑端口。在完成用户认证流程之前，BRAS设备受控逻辑端口关闭。连接在受控逻辑端口的非授权用户不能访问网络资源。非受控逻辑接口允许用户的控制层协议通过。

BRAS应支持下述受控逻辑端口和非受控逻辑端口功能要求：

——BRAS 应支持受控逻辑端口初始状态为关闭，未完成或者未通过授权的用户终端不能访问受保护网络资源；在用户终端认证成功后，BRAS 设备的受控逻辑端口打开，用户终端可通过 BRAS 访问受保护网络资源。

——BRAS 的受控逻辑端口可以配置为双向受控或单向受控状态。当实行双向受控时，禁止数据的发送和接受；实行单向受控时，禁止从用户终端接受数据，但允许向用户终端发送数据。

——为保证 MAC 方式的接入身份认证，需要保证用户终端满足一定的网络基础条件。例如用户终端需要预先获得 IP 地址，且能够进行地址解析，以保证浏览器能够正常发起网络请求。为此，需要 BRAS 支持非受控逻辑端口允许授权的控制信令通过，如 ARP 协议，自动地址配置协议（如 DHCPv4 协议，IPv6 下的 SLAAC 协议和 DHCPv6 协议）等。非受控端口的转发状态不受制于受控端口的状态。

——为支持 MAC 认证，需要用户终端具备一定的网络访问能力。在用户完成 MAC 认证之前，需要保证用户终端能够访问 DNS 服务器、Portal 服务器地址。因此，BRAS 设备应支持允许目的地地址为这类地址的用户报文通过。

——BRAS 受控逻辑端口和非受控逻辑端口应可支持 IPv4，IPv6 协议。

——在用户下线过程中，BRAS 可通过 ARP 探测或流量监测功能感知用户下线，关闭受控逻辑端口。

6.2.3 用户和业务管理技术要求

MAC认证中，BRAS应支持对用户流量进行管理，以实现认证阶段用户流量重定向，用户管理等。BRAS应支持下述用户流量管理功能：

——BRAS 支持在截获到未授权用户 HTTP 流量后，将用户请求的 Web 页面重定向到 Portal 服务器。

——BRAS 在重定向用户的 HTTP 流量到 Portal 服务器时，支持在重定向的 URL 中携带用户的 MAC。

——BRAS 支持对授权用户的时长/流量信息进行监测，在监测到用户的剩余时长/流量已耗尽时，发起强制用户下线流程。

——BRAS 支持对授权用户的在线状态进行 ARP 探测，或者在定义时间内用户的流量小于阈值，BRAS 感知用户下线并执行用户下线操作。

6.2.4 安全性技术要求

MAC认证中，为了防止仿冒攻击和用户认证信息的安全性，BRAS应满足以下安全功能要求：

——BRAS 应支持共享密钥等方式防止 Portal 服务器仿冒攻击。

——BRAS 应支持安全性协议以防止用户认证信息（用户名和密码）的嗅探攻击。

——BRAS 应支持限制用户重定向流量的最大上行带宽。

7 BRAS 支持 PEAP 认证的技术要求

7.1 PEAP 认证流程

PEAP是EAP认证结构的一种实现方式。用户终端通过配置的PEAP客户端发起PEAP认证，经过认证点识别并传送到RADIUS认证服务器。通过用户终端与RADIUS认证服务器间建立的TLS隧道，在隧道内完成用户认证。

PEAP认证需要用户在初次认证过程中输入用户名和密码，后续终端关联到AP后自动认证。该认证方式安全性较高，支持主流终端操作系统。在PEAP认证之前，需要用户终端以PEAP方式接入指定的SSID（加密模式）。

PEAP认证体系架构如图15所示。

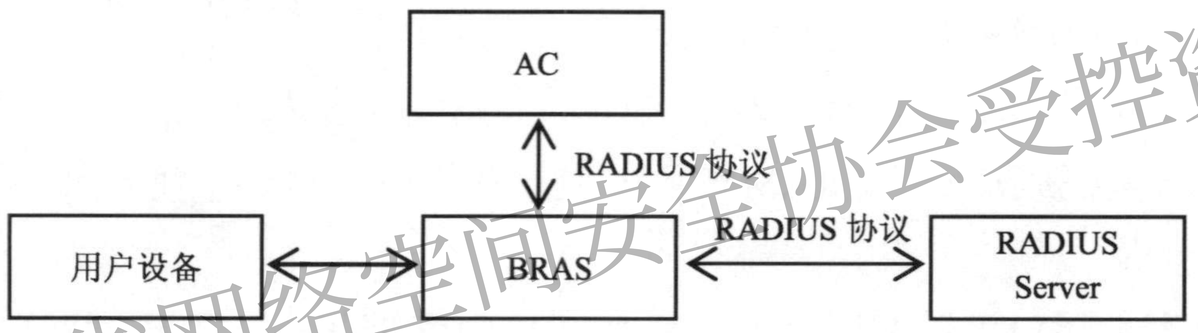


图15 PEAP 认证体系结构

WLAN网络中AC和BRAS分设场景下，PEAP认证系统的认证点部署在AC设备，BRAS需支持RADIUS Proxy功能。AC负责接收并终结用户的EAPoL报文，并根据需要将用户认证信息封装为RADIUS报文。AC将封装的RADIUS报文发送给RADIUS服务器。

具体认证流程如下：

a）连接建立过程

- 该过程中用户终端和 AP 设备通过 802.11 协议建立关联。

b）PEAP 认证流程

- 该过程中用户终端和 RADIUS 服务器执行 PEAP 认证流程，AC 作为 802.1X 认证的认证点，BRAS 对相关的 RADIUS 消息执行 Proxy 操作。
- 该过程中，用户首先与和认证服务器交互建立安全通道，其中客户端采用证书认证服务端，完成 TLS 握手。
- 建立安全隧道以后，其后的 EAP 通信都在 TLS 通道中进行，这时服务器对用户和客户端进行身份验证，具体方法由 EAP 类型决定，在 PEAP 内部可以选择使用 EAP-TLS 或 EAP-MS-CHAPv2 等。

c）密钥协商

- 认证授权通过以后，AC/AP 与用户执行密钥协商。其中 AC 与用户执行密钥协商对应步骤 14，AP 与用户执行密钥协商对应步骤 14a，14a'（用虚线表示）。这两种方案在 WLAN 部署时需要选择其中一种。为了简略，本标准之后的 EAP 认证图中都只标明了 AC 与用户执行密钥协商。

d）地址分配过程

- 用户终端通过 DHCP 协议从 BRAS 获得 IP 地址。

e）计费流程

- BRAS 通过发送计费报文发起计费。

BRAS支持RADIUS Proxy方案的认证流程（PEAP）如图16所示。

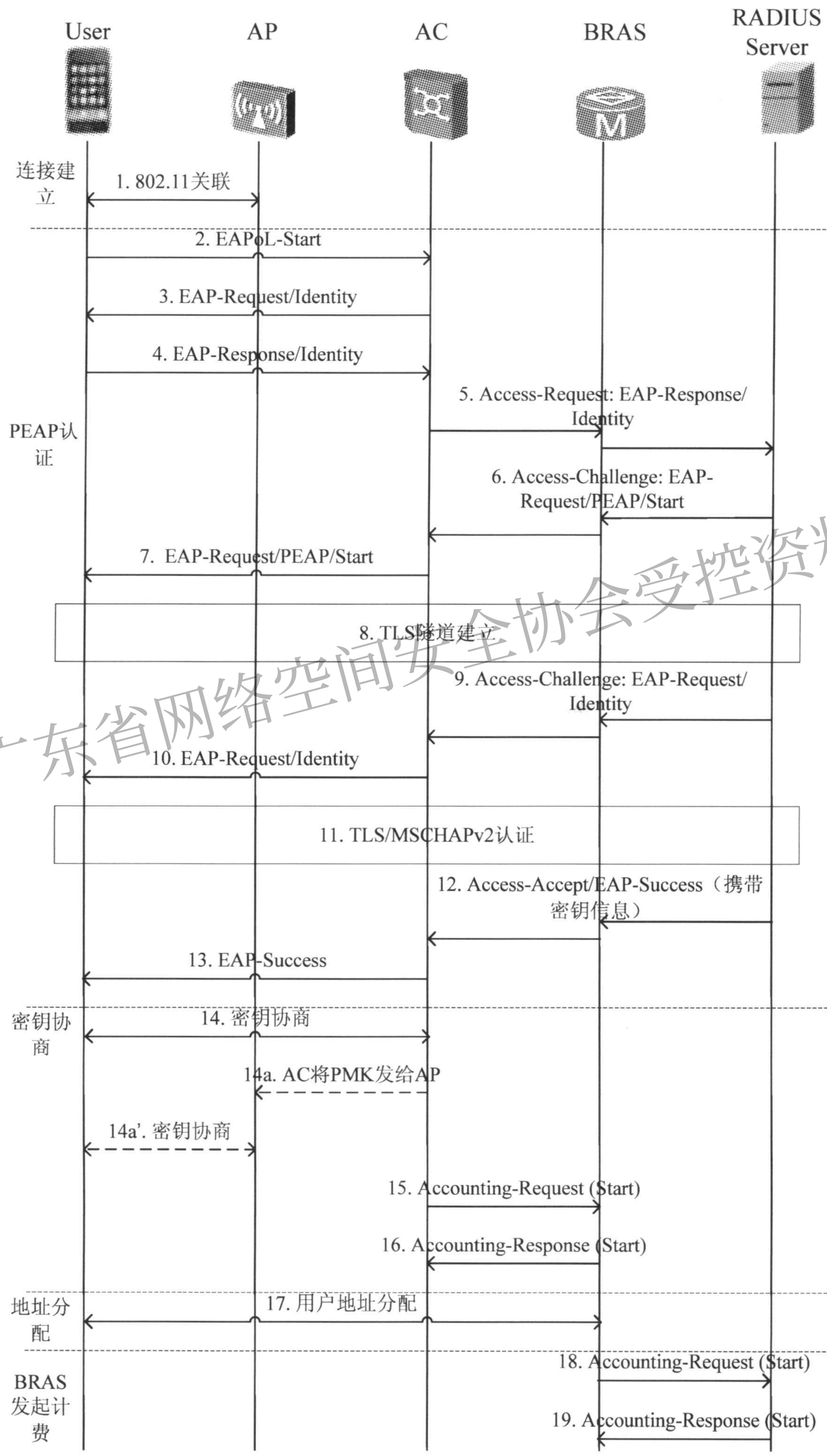
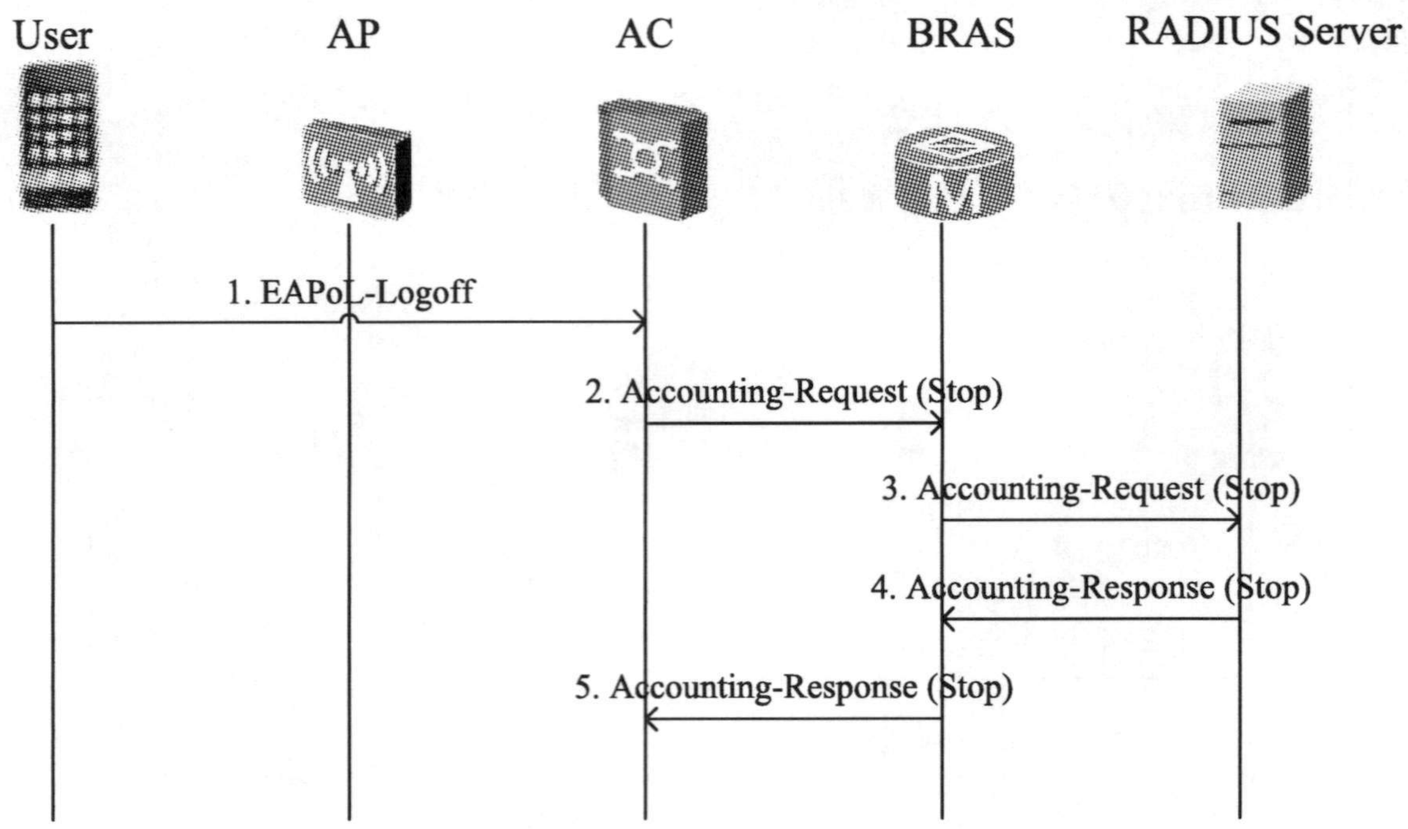


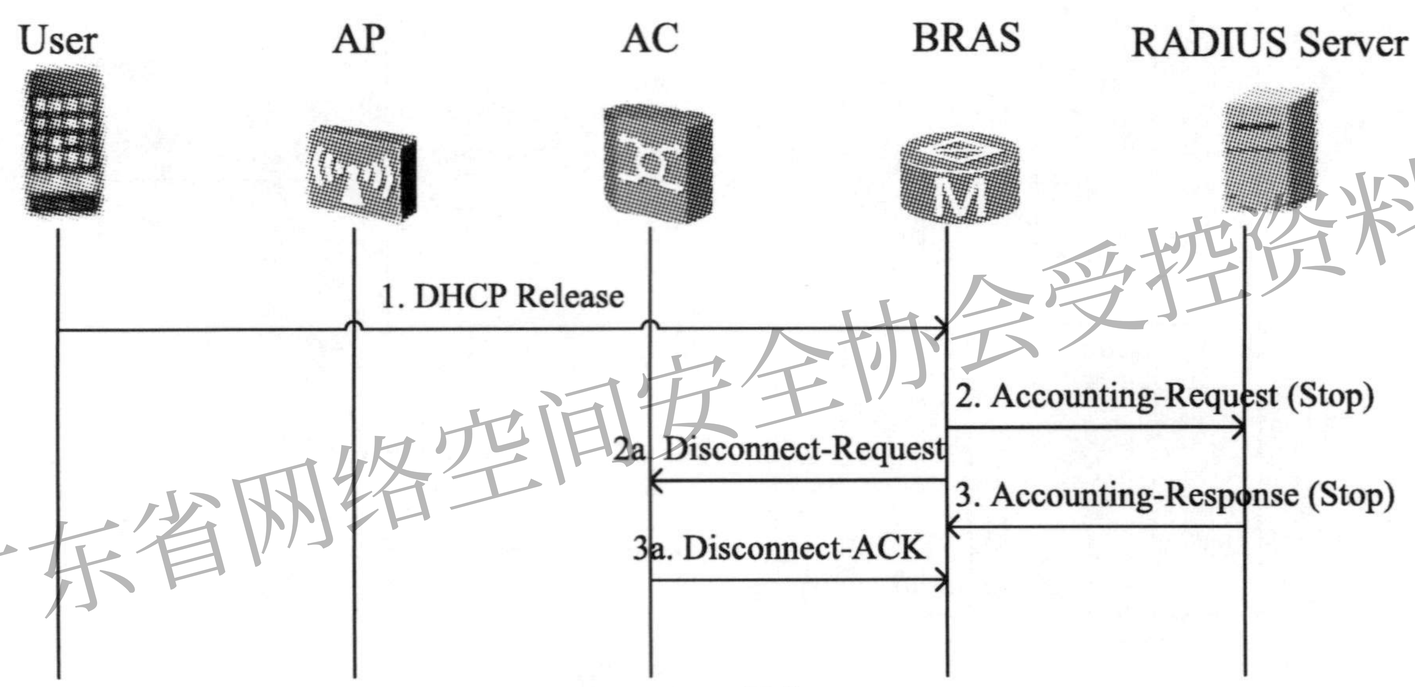
图16　BRAS 支持 RADIUS Proxy 方案认证流程（PEAP）

EAP用户下线流程包括用户主动下线、强制下线和异常下线。具体如下：

——用户主动下线流程：由用户发送 EAPoL-Logoff 或 DHCP Release 消息触发，如图 17 所示。



a) EAPoL-Logoff触发



b) DHCP Release触发

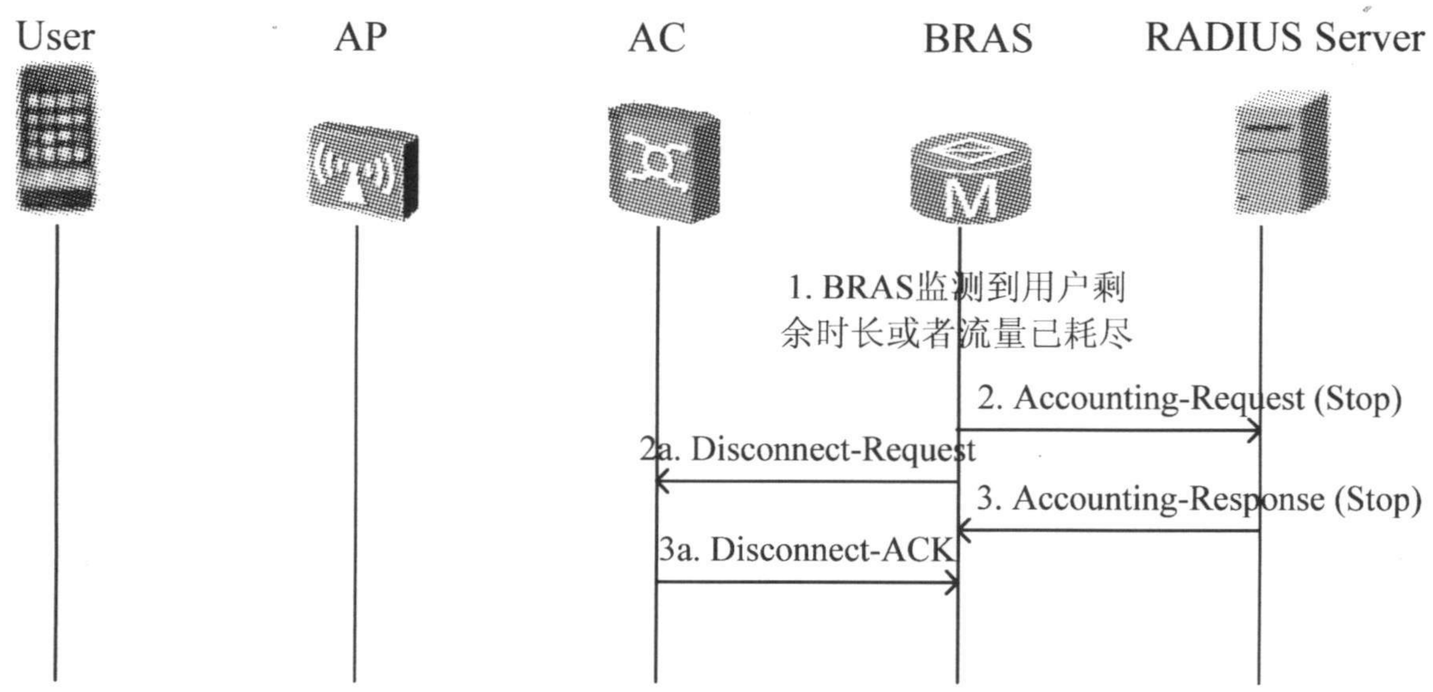
图17　EAP 用户主动下线流程

——用户（预付费）强制下线流程：用户强制下线流程可分为 BRAS 触发用户下线和 RADIUS 服务器触发用户下线两种方式。

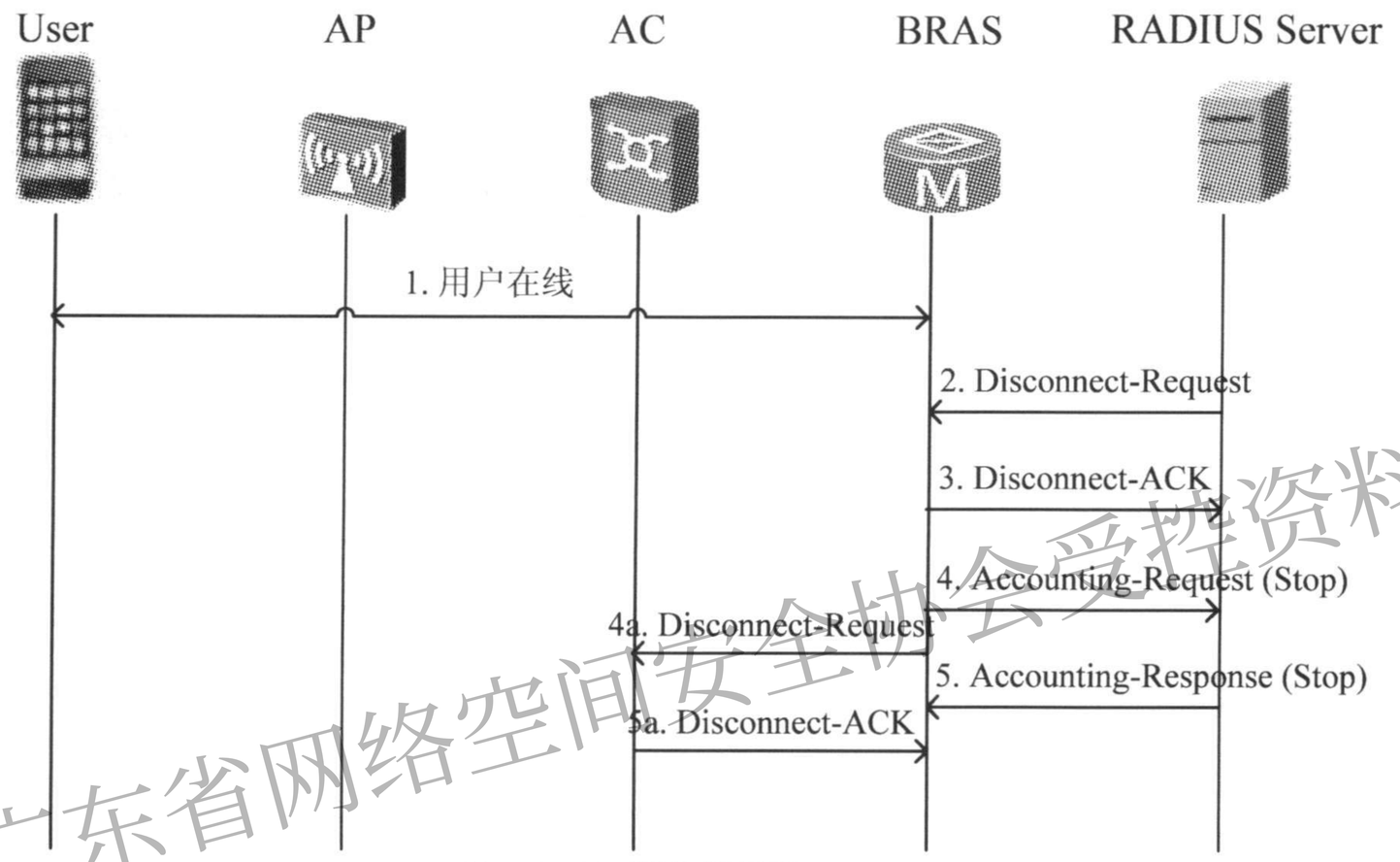
- BRAS 触发：BRAS 监测到用户的剩余时长/流量耗尽，向 AC 通告用户下线，如图 18a）所示；
- RADIUS 服务器触发：RADIUS 服务器下发的 DM（Disconnect Messages）消息强制用户下线，如图 18b）所示。

——用户异常下线流程：用户异常下线分为 BRAS 感知和 AC/AP 感知用户下线两种方式。两种方式在实际应用中至少采用一种，或两种方式同时采用。

- BRAS 感知：BRAS 通过 ARP 报文探测或流量监测功能感知用户下线，如图 19a）所示；
- AC/AP 感知：AC/AP 通过 WLAN 关联、流量监测等手段感知用户下线，如图 19b）所示。



a) BRAS触发



b) RADIUS服务器触发

图18　EAP 认证用户（预付费）强制下线流程

7.2　BRAS 技术要求

宽带网络接入服务器支持PEAP认证要求应满足以下技术要求。

7.2.1　接口功能技术要求

PEAP认证系统主要包括四个组件：用户终端，AC，BRAS和RADIUS服务器。在支持PEAP认证的场景中，BRAS应支持以下接口：

——BRAS设备应支持与AC的接口。在BRAS支持RADIUS Proxy的方案中，BRAS作为RADIUS协议的服务端与AC交互认证，计费消息，并且BRAS可以通过该接口通告AC用户下线。

——BRAS设备应支持与RADIUS服务器的接口。接口的功能要求包括：用户认证计费信息交互，用户管理等。

7.2.2　协议功能技术要求

PEAP认证中，BRAS应支持如下协议和功能的技术要求：

——PEAP认证中，BRAS应支持自动地址配置协议，如DHCPv4协议，在IPv6下的SLAAC协议和DHCPv6协议。

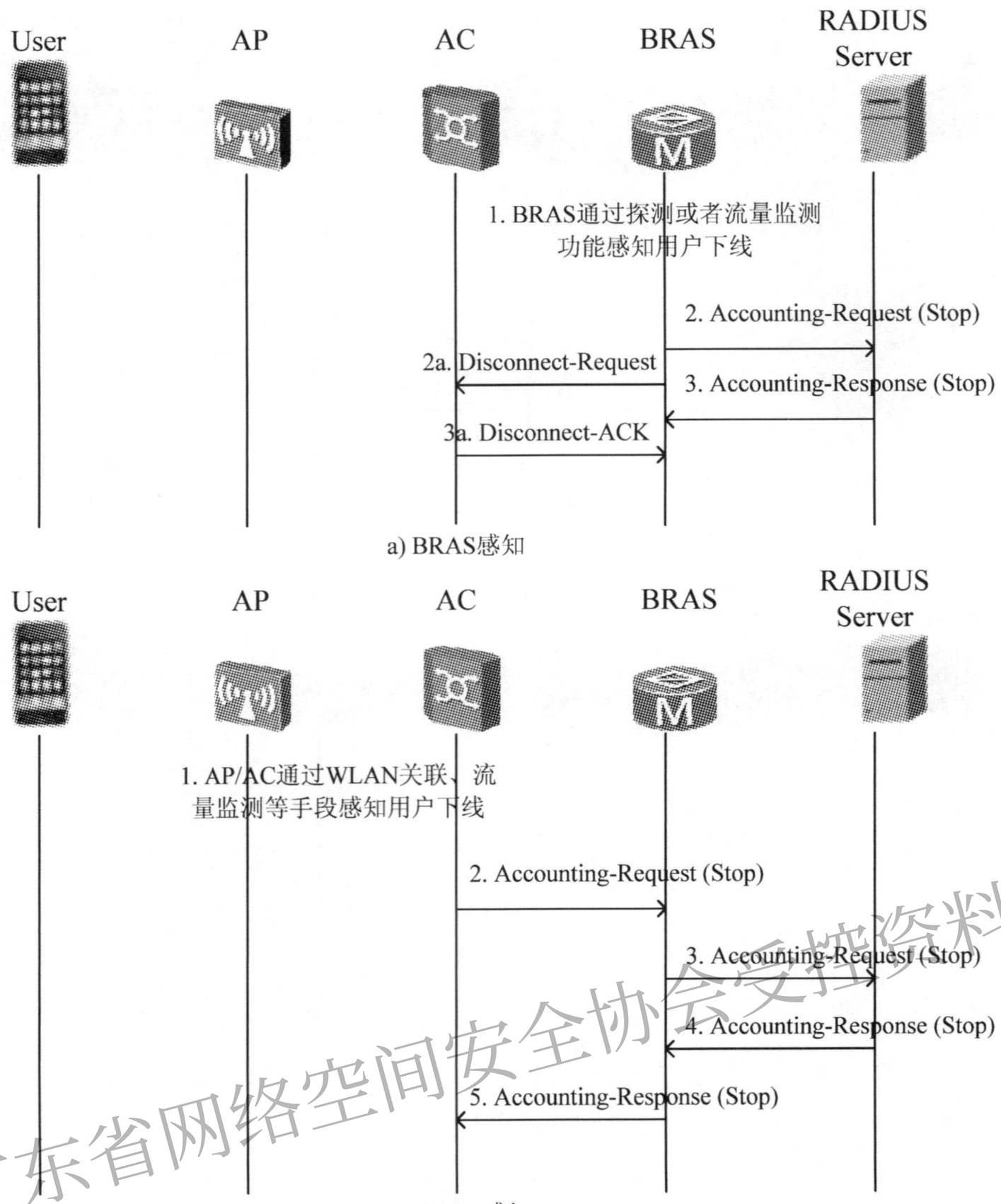


图19　EAP 认证用户异常下线流程

——BRAS应支持EAP认证协议，以及PEAP认证方法和流程。

——BRAS 应支持 RADIUS 协议，以保证认证计费过程中与 RADIUS 服务器的交互。

——BRAS 支持 RADIUS Proxy 的功能。BRAS 支持监听 AC 发送的 RADIUS 认证和计费报文，获取用户信息，用于用户管理和用户计费。

PEAP认证中，BRAS需要支持受控逻辑端口和非受控逻辑端口。在完成用户认证流程之前，BRAS设备受控逻辑端口关闭。连接在受控逻辑端口的非授权用户不能访问网络资源。非受控逻辑接口允许用户的控制层协议报文通过。

BRAS应支持下述受控逻辑端口和非受控逻辑端口功能要求：

——BRAS 应支持受控逻辑端口初始状态为关闭，未完成或者未通过授权的用户终端不能访问受保护网络资源；在用户终端认证成功后，BRAS 设备的受控逻辑端口打开，用户终端可通过 BRAS 访问受保护网络资源。

——BRAS 的受控逻辑端口可以配置为双向受控或单向受控状态。当实行双向受控时，禁止数据的发送和接受；实行单向受控时，禁止从用户终端接受数据，但允许向用户终端发送数据。

——BRAS 受控逻辑端口和非受控逻辑端口应可支持 IPv4，IPv6 协议。

——在用户下线过程中，BRAS 可通过 ARP 探测或流量监测功能感知用户下线，关闭受控逻辑端口。

7.2.3 用户和业务管理技术要求

PEAP认证中，BRAS的用户和业务管理技术要求包括用户流量和时长监测要求，以及用户下线感知要求等。具体如下：

——BRAS 支持对授权用户的时长/流量信息进行监测，当监测到用户的剩余时长/流量已耗尽时，发起强制用户下线流程。

——BRAS 支持对授权用户的在线状态进行 ARP 探测，或流量监测功能，BRAS 感知用户下线并执行用户下线操作。

7.2.4 安全性技术要求

PEAP认证中，BRAS需要保证与AC，以及RADIUS服务器的通信安全。具体要求如下：

——BRAS 应支持 RADIUS 协议中定义的安全机制。

7.3 BRAS 支持 PEAP 认证点的认证流程（可选）

当BRAS作为认证点时，BRAS负责接收并终结用户的EAPoL报文，并根据需要将用户认证信息报文封装为RADIUS报文。BRAS将封装的RADIUS报文发送给RADIUS服务器。

在该方案中，AC主要负责AP和无线资源管理；BRAS负责用户认证、管理、计费、IP地址分配等功能。其具体认证流程如下：

a）连接建立过程

- 该过程中用户终端和 AP 设备通过 802.11 协议建立关联。

b）PEAP 认证流程

- 该过程中用户终端和 RADIUS 服务器执行 PEAP 认证流程，BRAS 作为 802.1X 认证的认证点。

c）密钥协商

- 认证授权通过以后，AC/AP 与用户终端执行密钥协商。此时 BRAS 为认证点，AC 需要从认证点获取密钥信息（具体的密钥获取流程涉及到引言中提到的专利）。

d）地址分配过程

- 用户终端通过 DHCP 协议从 BRAS 获得 IP 地址。

e）计费流程

- BRAS 发送计费报文发起计费。

BRAS支持PEAP认证点的方案的认证流程如图20所示。

下线流程包括用户主动下线、强制下线和异常下线。具体如下：

——用户主动下线流程，由用户发送的 EAPoL-Logoff 或 DHCP Release 消息触发，如图 21 所示。

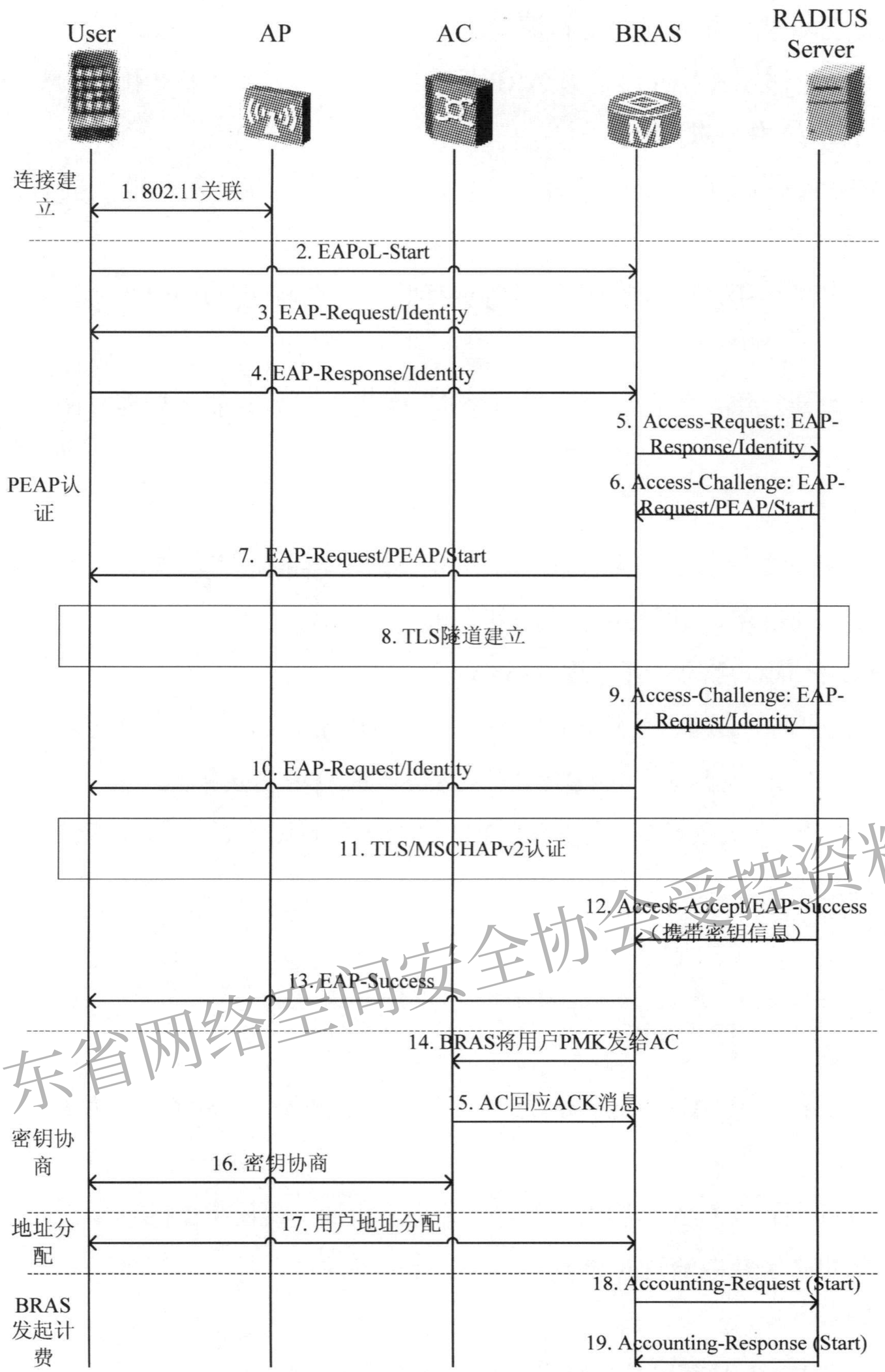
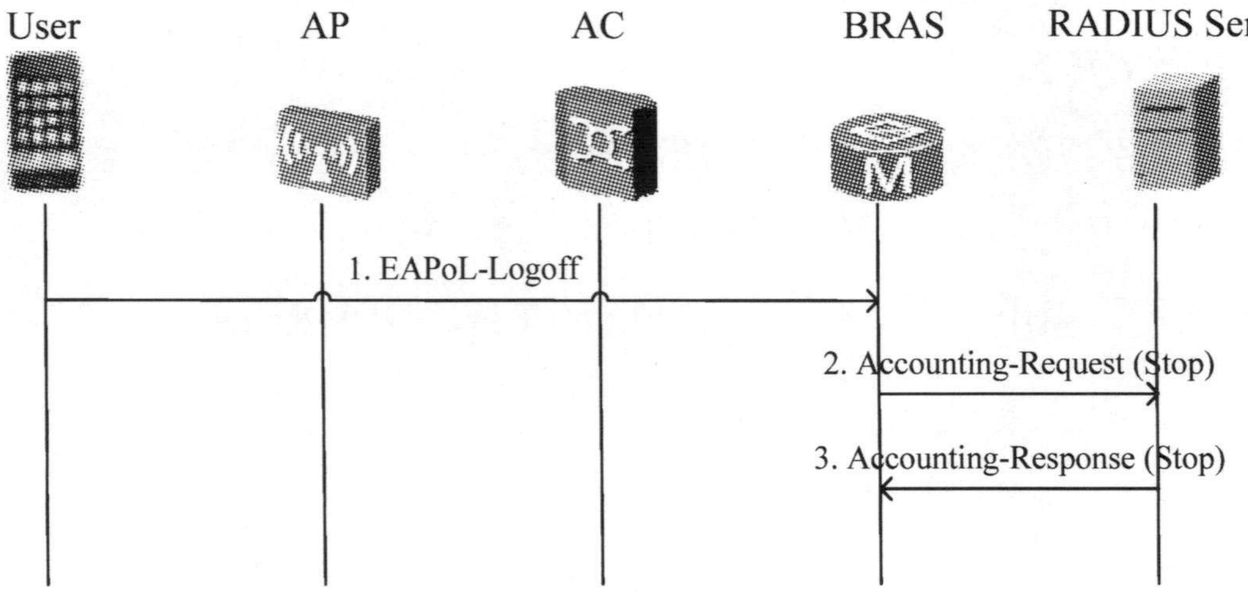
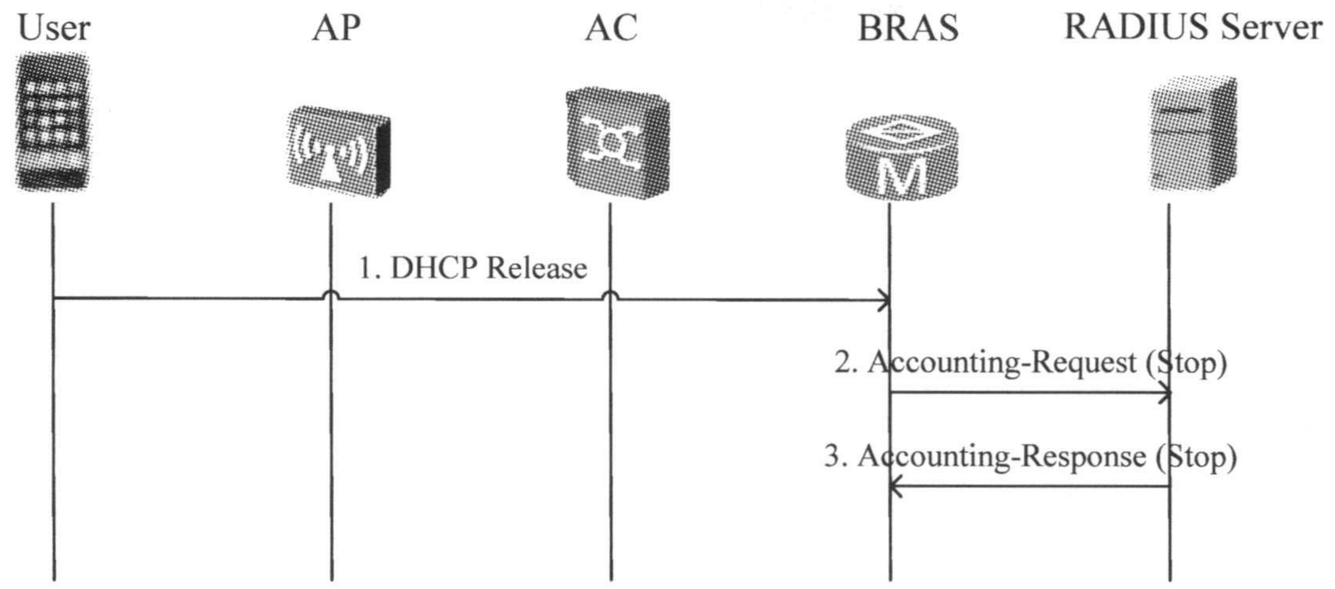


图20　BRAS 支持 PEAP 认证点方案认证流程



a) EAPoL-Logoff触发

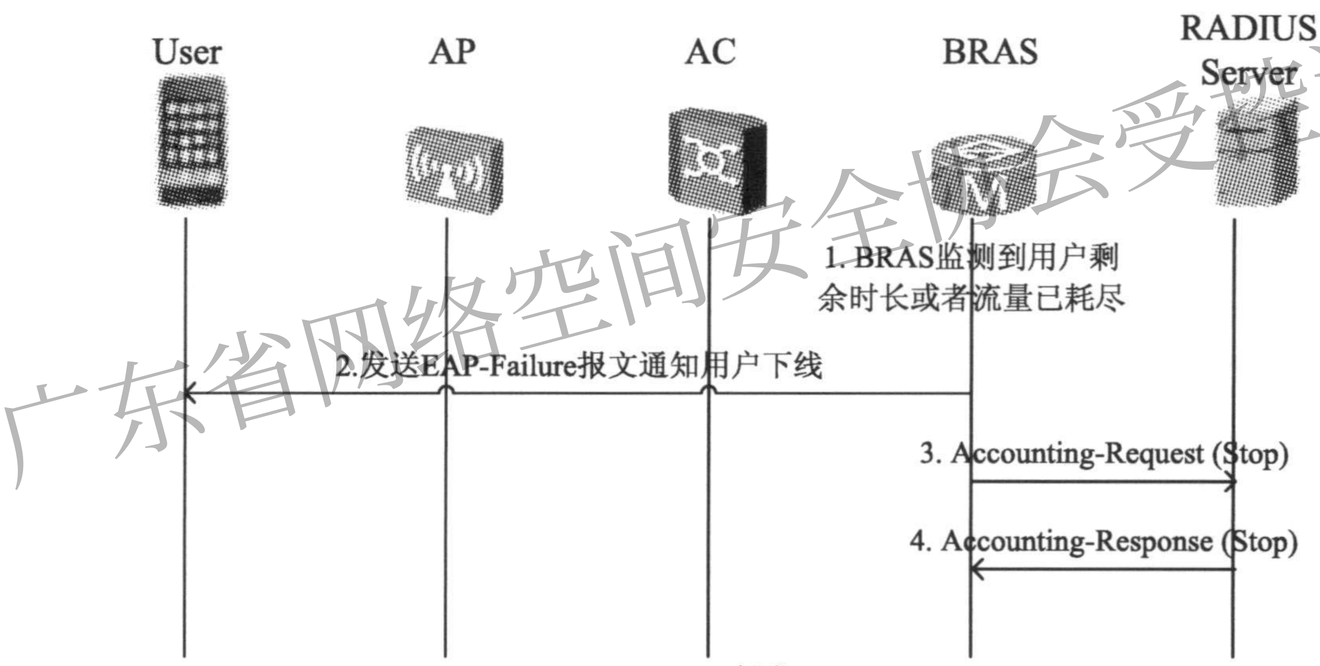


b) DHCP Release触发

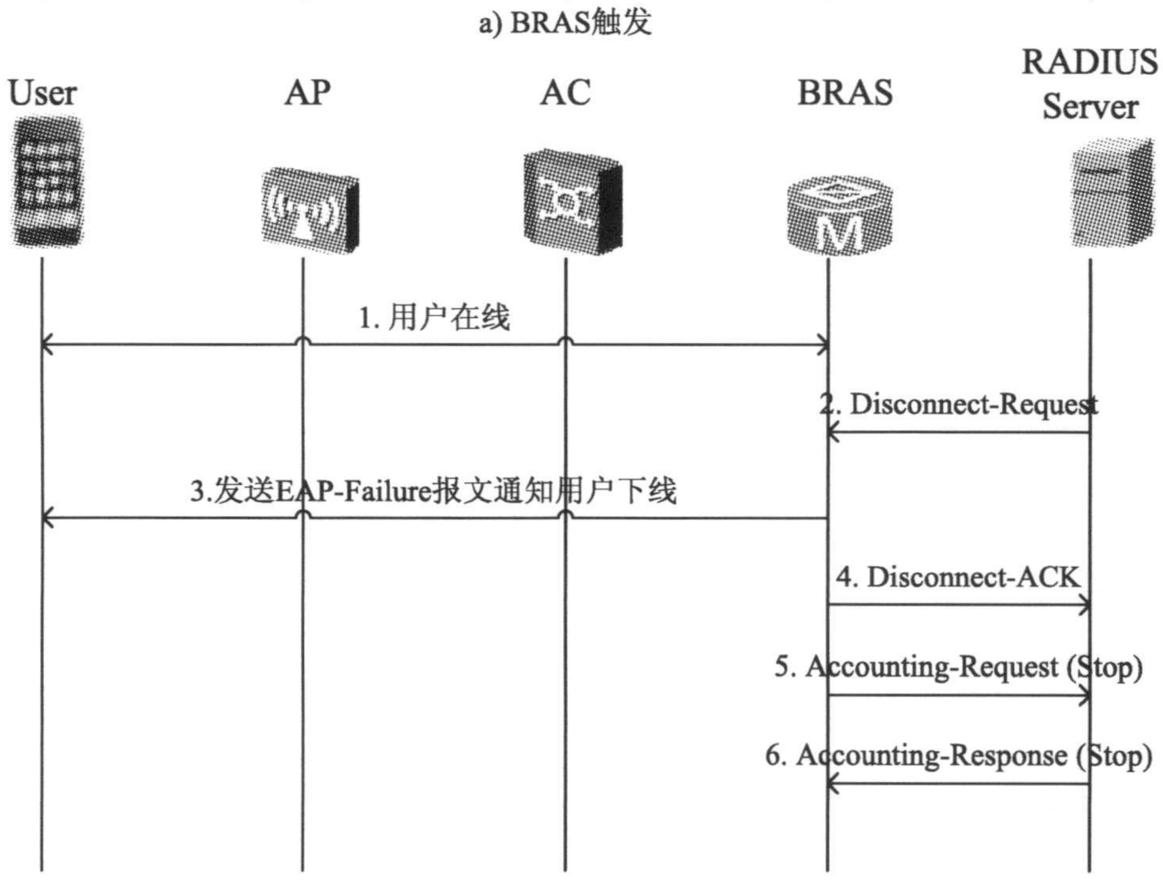
图21　EAP 用户主动下线流程

——用户（预付费）强制下线流程：用户强制下线流程可分为 BRAS 触发用户下线和 RADIUS 服务器触发用户下线两种方式。

- BRAS 触发：BRAS 监测到用户的剩余时长/流量耗尽，向用户通告用户下线，并且停止计费，如图 22a）所示；
- RADIUS 服务器触发：RADIUS 服务器下发的 DM（Disconnect Messages）消息强制用户下线，如图 22b）所示。



a) BRAS触发



b) RADIUS服务器触发

图22　EAP 用户（预付费）强制下线流程

——用户异常下线流程：即 BRAS 通过 ARP 报文探测或流量监测功能感知用户下线，如图 23 所示。

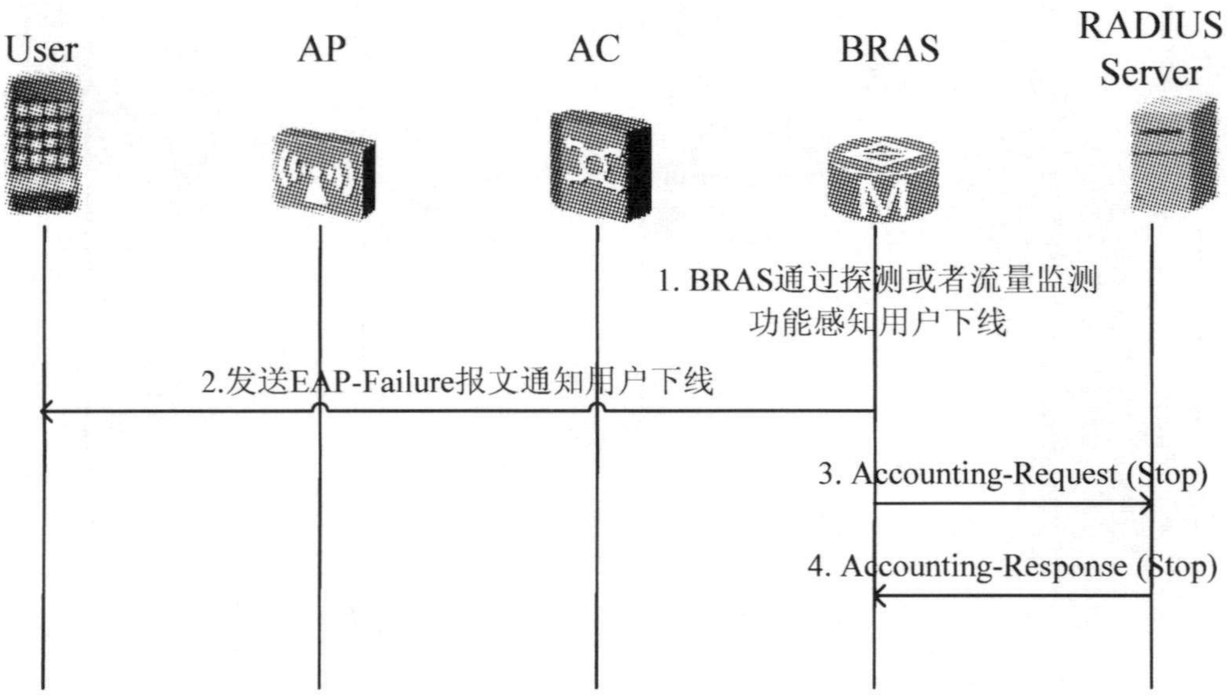


图23　EAP 用户异常下线流程

7.4　BRAS 支持 PEAP 认证点的技术要求（可选）

在BRAS作为认证点的方案中，BRAS除了需要支持前述AC做认证点方案中的技术要求，还需要支持通过RADIUS协议向AC下发密钥信息。其具体消息格式请见附录A。

在该方案中，BRAS应支持802.1X认证中的认证点的功能，接受用户的EAPoL消息，负责用户与移动AAA服务器之间的认证消息的转发。

8　BRAS 支持 EAP-SIM/AKA 认证的技术要求

8.1　EAP-SIM/AKA 认证流程

EAP-SIM/AKA认证机制提供基于(U)SIM卡的认证和密钥分发机制，该机制是一种双向的认证机制，即服务器认证用户终端，用户终端也认证服务器。只有双向认证通过之后，服务器端才发送EAP-Success消息，完成用户认证。EAP-SIM/AKA认证过程中，通过多次挑战响应机制产生会话密钥信息。

EAP-SIM/AKA认证过程用户无感知。在接入WLAN网络时，用户终端接入移动AAA服务器进行认证，该认证方式安全度较高。在EAP-SIM/AKA认证之前，需要用户终端以EAP-SIM/AKA认证方式接入指定的SSID(加密模式)。

EAP-SIM/AKA认证体系架构图与PEAP的认证体系架构图相同，参照图15。

BRAS支持RADIUS Proxy方案的认证流程如下（以EAP-AKA为例）：

a）　连接建立过程

- 该过程中用户终端和 AP 设备通过 802.11 协议建立关联。

b）　EAP-AKA 认证流程

- 该过程中用户终端和移动 AAA 服务器执行 EAP-AKA 认证流程，AC 作为 802.1X 认证的认证点，BRAS 对相关的 RADIUS 消息执行 Proxy 操作。
- 该过程中，用户终端和移动 AAA 服务器通过 EAP 请求和回应消息中的 AKA-Challenge 报文中携带的信息进行双向认证。

c）　密钥协商

- 认证授权通过以后，AC/AP 与用户执行密钥协商。

d）　地址分配过程

- 用户终端通过 DHCP 协议从 BRAS 获得 IP 地址。

e） 计费流程

- BRAS 通过发送计费报文发起计费。

BRAS支持RADIUS Proxy方案的认证流程（EAP-AKA），如图24所示。

图24 BRAS 支持 RADIUS Proxy 方案认证流程（EAP-AKA）

该方案中的EAP用户下线流程与BRAS支持RADIUS Proxy方案（PEAP）相同，包括用户主动下线、强制下线和异常下线，参照图17、18、19。

8.2 BRAS 技术要求

宽带网络接入服务器支持EAP-SIM/AKA认证技术要求应满足以下技术要求。

8.2.1 接口功能技术要求

EAP-SIM/AKA认证系统主要包括四个组件：用户终端，AC，BRAS和移动AAA服务器。在运营商网络部署支持EAP-SIM/AKA认证的场景中，BRAS需要支持以下接口：

——BRAS 设备应支持与 AC 服务器的接口。在 BRAS 支持 RADIUS Proxy 的方案中，BRAS 作为 RADIUS 协议的服务端与 AC 交互认证，计费消息，并且 BRAS 可以通过该接口通告 AC 用户下线。

——BRAS 设备应支持与移动 AAA 服务器的接口。接口的功能要求包括：用户认证计费信息交互，用户管理等。

8.2.2 协议功能技术要求

EAP-SIM/AKA认证中，BRAS应支持如下协议和功能的技术要求：

——EAP-SIM/AKA 认证中，BRAS 应支持自动地址配置协议，如 DHCPv4 协议，在 IPv6 下的 SLAAC 协议和 DHCPv6 协议。

——BRAS 应支持 EAP 认证协议，以及 EAP-SIM/AKA 认证方法和流程。

——BRAS 应支持 RADIUS 协议，以保证认证计费过程中与移动 AAA 服务器的交互。

——BRAS 支持 RADIUS Proxy 的功能。BRAS 支持监听 AC 发送的 RADIUS 认证和计费报文，获取用户信息，用于用户管理和用户计费。

EAP-SIM/AKA认证中，BRAS需要支持受控逻辑端口和非受控逻辑端口。在完成用户认证流程之前，BRAS设备受控逻辑端口关闭。连接在受控逻辑端口的非授权用户不能访问网络资源。非受控逻辑接口允许用户的控制层协议通过。

BRAS应支持下述受控逻辑端口和非受控逻辑端口功能要求：

——BRAS 应支持受控逻辑端口初始状态为关闭，未完成认证或者未通过授权的用户终端不能访问受保护网络资源；在用户终端认证成功后，BRAS 设备的受控逻辑端口打开，用户终端可通过 BRAS 访问受保护网络资源。

——BRAS 的受控逻辑端口可以配置为双向受控或单向受控状态。当实行双向受控时，禁止数据的发送和接受；实行单向受控时，禁止从用户终端接受数据，但允许向用户终端发送数据。

——BRAS 受控逻辑端口和非受控逻辑端口应可支持 IPv4，IPv6 协议。

——在用户下线过程中，BRAS 可通过 ARP 探测或流量监测功能感知用户下线，关闭受控逻辑端口。

8.2.3 用户和业务管理技术要求

EAP-SIM/AKA认证中，BRAS的用户和业务管理技术要求包括用户流量时长监测要求，以及用户下线感知要求。具体如下：

——BRAS 支持对授权用户的时长/流量信息进行监测，在监测到用户的剩余时长/流量已耗尽时，发起强制用户下线流程。

——BRAS 支持对授权用户的在线状态进行 ARP 探测，或者在定义时间内用户的流量小于阈值，BRAS 感知用户下线并执行用户下线操作。

8.2.4 安全性技术要求

EAP-SIM/AKA认证中，BRAS应保证与AC，以及移动AAA服务器的通信安全。具体要求如下：

——BRAS 应支持 RADIUS 协议中定义的安全机制。

8.3 BRAS 支持 EAP-SIM/AKA 认证点的认证流程（可选）

BRAS支持EAP-SIM/AKA认证点的方案的认证流程如下（以EAP-AKA为例）：

a）连接建立过程

- 该过程中用户终端和 AP 设备通过 802.11 协议建立关联。

b）EAP-AKA 认证流程

- 该过程中用户终端和移动 AAA 服务器执行 EAP-AKA 认证流程，BRAS 作为 802.1X 认证的认证点。

c）密钥协商

- 认证授权通过以后，AC/AP 与用户终端执行密钥协商。此时 BRAS 为认证点，AC 需要从认证点获取密钥信息（具体的密钥获取流程涉及到引言中提到的专利）。

d）地址分配过程

- 用户终端通过 DHCP 协议从 BRAS 获得 IP 地址。

e）计费流程

- BRAS 发送计费报文发起计费。

BRAS支持EAP-SIM/AKA认证点方案的认证流程（EAP-AKA）如图25所示。

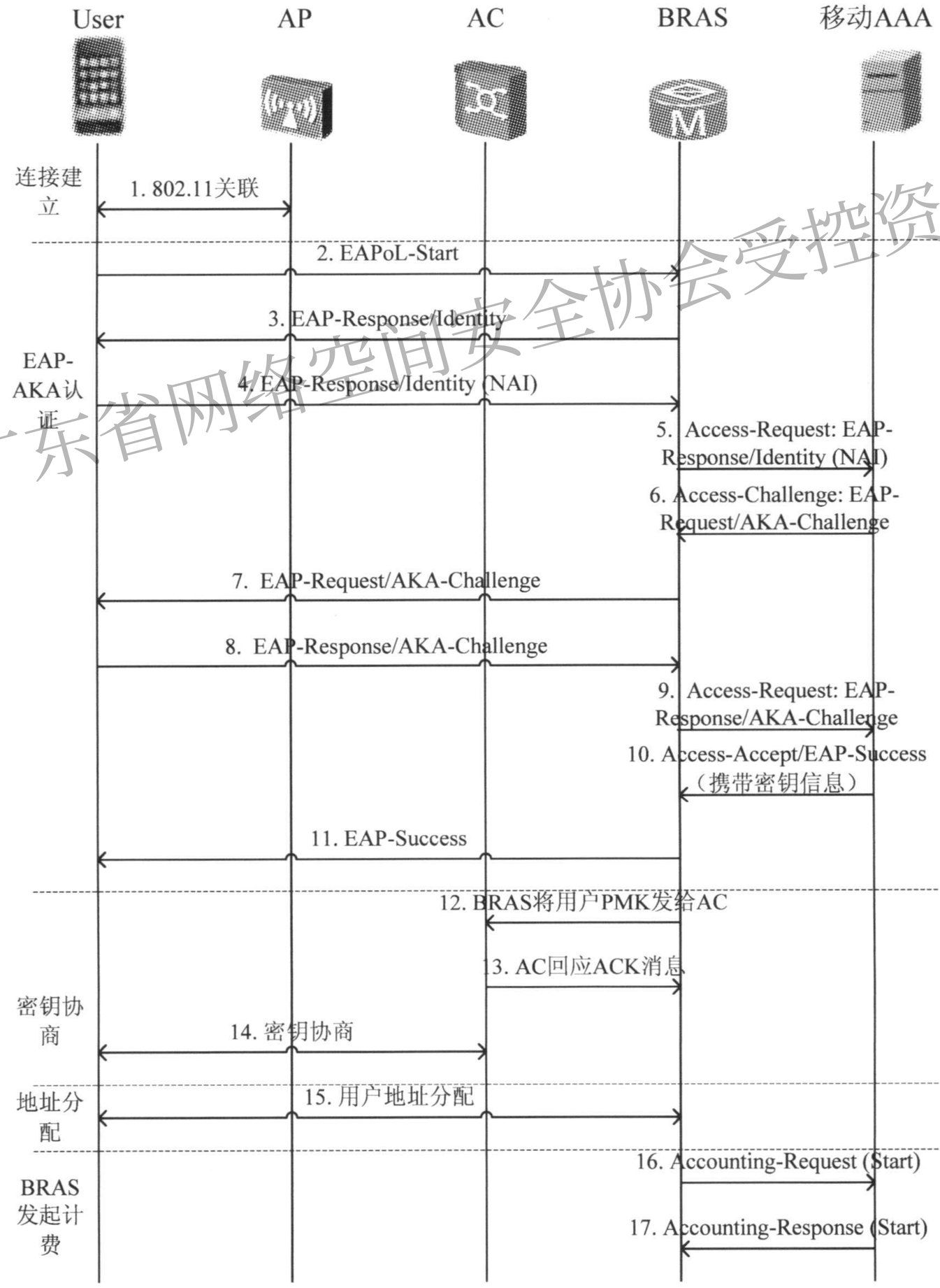


图25　BRAS 支持 EAP-AKA 认证点方案认证流程

该方案中的EAP用户下线流程与BRAS支持PEAP认证点的方案相同。包括用户主动下线、强制下线和异常下线，参照图21，22，23。

8.4 BRAS 支持 EAP-SIM/AKA 认证点的技术要求（可选）

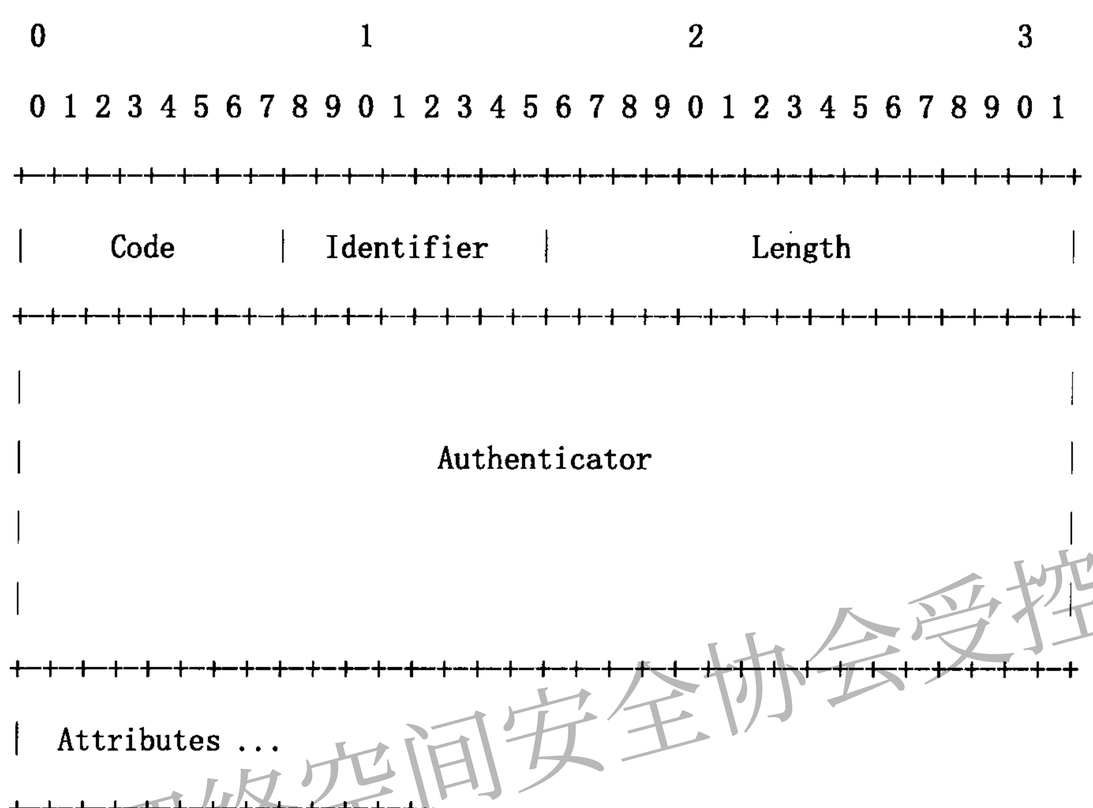
在BRAS作为认证点的方案中，BRAS的相关技术要求与本标准7.4节相同。

附 录 A
（资料性附录）
PMK下发交互报文字段定义

A.1 PMK下发交互报文字段格式

BRAS支持EAP认证点的方案的认证流程中，BRAS接收到RADIUS的认证成功回应后，需要将用户PMK发给AC，其具体的实现方案中需要定义两个新的RADIUS报文：Key-of-Announcement和KoA-ACK。

BRAS首先需要构建Key-of-Announcement报文发送给AC，AC接收后，回复KoA-ACK。Key-of-Announcement和KoA-ACK报文格式与RADIUS COA（IETF RFC 5176）中定义的报文格式相同，如图A.1所示。



图A.1 RADIUS 报文格式

Code: 1字节，代表RADIUS报文的类型；

Identifier: 1字节，取值范围为0~255，代表交互报文的标识，该值由BRAS填充，标识一对Key-of-Announcement和KoA-ACK；

Length: 2字节，代表消息长度，包括Code，Identifier，Length，Authenticator，Attribute字段；

Authenticator: 16字节，MD5校验码；

Attributes: TLV格式，封装携带的属性。

RADIUS协议需要扩展支持以下两种报文（数值为Code的取值）：

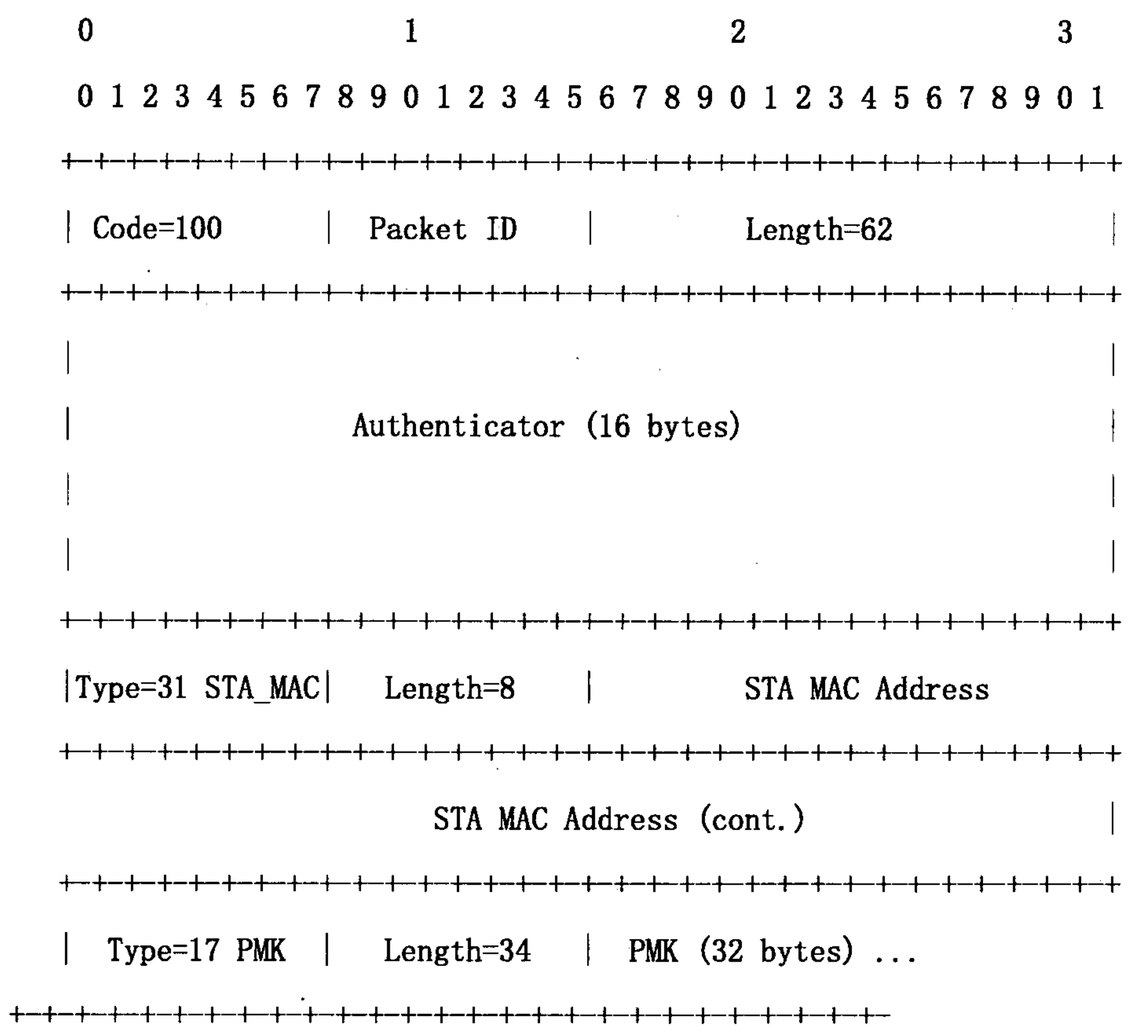
100（暂定）: Key-of-Announcement

101（暂定）: KoA-ACK

注：目前本标准中采用的RADIUS报文的编号是暂定的，如果将来IETF分配了其他的编号则需要按照IETF的编号修改，如果IETF分配了目前采用的编号给其他报文也需要修改目前采用的编号。

A.2 Key-of-Announcement报文格式

Key-of-Announcement 报文格式如图 A.2 所示。



图A.2 Key-of-Announcement 报文格式

Key-of-Announcement报文属性包括以下两个部分：

（1）MAC地址属性

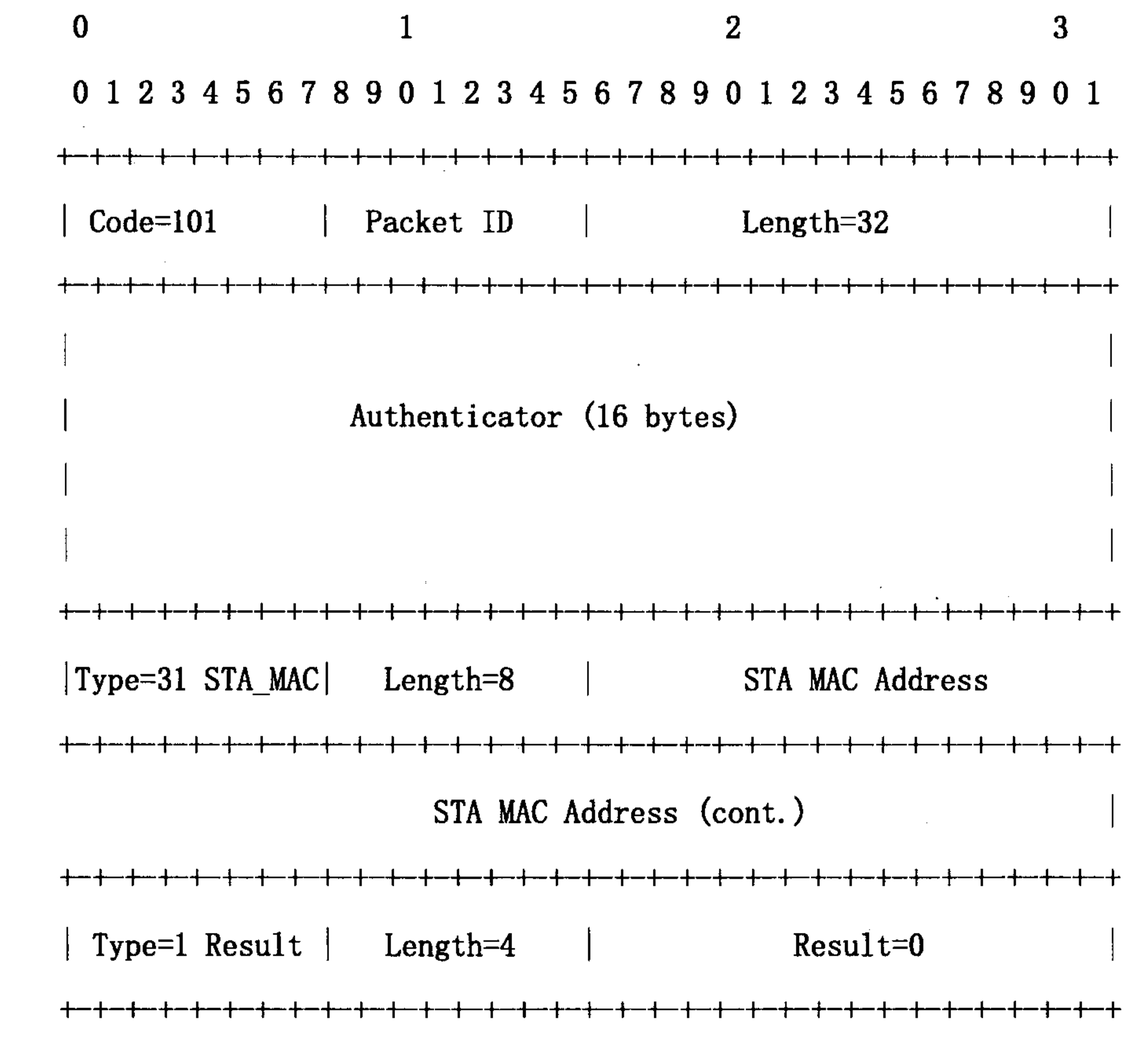
类型为31，长度为8，内容为用户MAC。

（2）密钥属性

类型为17，长度为34。使用Microsoft的17号属性MS-MPPE-Recv-Key的前32字节，请参考IETF RFC2548。

A.3 KoA-ACK报文格式

KoA-ACK报文格式如图A.3所示。



图A.3 KoA-ACK 报文格式

KoA-ACK报文属性包括以下两个部分：

（1）MAC地址属性

类型为31，长度为8，内容为用户MAC。

（2）错误码属性

类型为1，长度为4，内容为错误码(类型为ushort)，0表示成功，其他表示失败。

A.4 BRAS支持PMK下发的技术要求

PMK下发和PMK应答的使用对BRAS设备的技术要求包括：

——BRAS 需要支持配置对端 AC 的 IP，发送的目的端口号，以及使用的共享密钥（Shared-Key）。

——主备 AC 情况下，BRAS 需要支持在认证成功后向主备 AC 同时发送 Key-of-Announcement 消息。

对应的，该方案需要WLAN设备实现：

——保证发送到 BRAS 的 WLAN 用户 EAP 认证报文目的 MAC 为广播或者组播；也可以 EAPoL-Start 报文为广播或者组播，根据 BRAS 回应的 EAP 报文 WLAN 设备学习 BRAS 的 MAC 地址，以后发送的 EAP 认证报文直接封装 BRAS 的 MAC 地址做单播转发。

——AC 支持配置 BRAS IP，接收端口号和 Shared-Key；在 BRAS 双机备份场景中，需要支持配置两组。

——主备 AC 情况下，只需要主 AC 回应 KoA-ACK 消息。

参 考 文 献

[1] 2012-1365T-YD　公众无线局域网组网技术要求

[2] IETF草案　受保护的可扩展的身份验证协议（Protected EAP Protocol (PEAP) Version 2）

中华人民共和国
通信行业标准
宽带网络接入服务器支持 WLAN 接入
及用户认证的技术要求
YD/T 2842-2015
*
人民邮电出版社出版发行
北京市丰台区成寿寺路 1 号邮电出版大厦
邮政编码：100164
北京康利胶印厂印刷

*
开本：880×1230 1/16 2015 年 12 月第 1 版
印张：2.5 2015 年 12 月北京第 1 次印刷
字数：62 千字
15115・717
定价：30 元
本书如有印装质量问题，请与本社联系 电话：(010)81055492