



(12) 发明专利

(10) 授权公告号 CN 101621802 B

(45) 授权公告日 2012. 02. 08

(21) 申请号 200910091230. 2

CN 101212297 A, 2008. 07. 02, 全文.

(22) 申请日 2009. 08. 13

US 2006/0179307 A1, 2006. 08. 10, 全文.

(73) 专利权人 杭州华三通信技术有限公司

审查员 陈文军

地址 310053 浙江省杭州市高新技术产业开发区之江科技工业园六和路 310 号华为杭州生产基地

(72) 发明人 赵玄 王君菠

(74) 专利代理机构 北京德琦知识产权代理有限公司 11018

代理人 谢安昆 宋志强

(51) Int. Cl.

H04W 12/06 (2009. 01)

H04W 8/12 (2009. 01)

(56) 对比文件

CN 1455556 A, 2003. 11. 12, 全文.

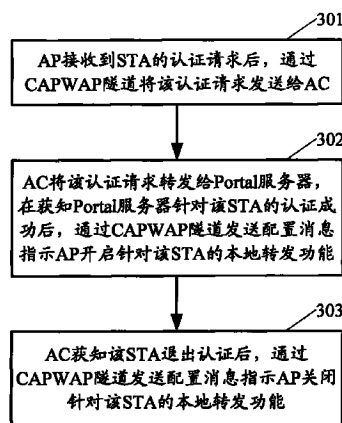
权利要求书 4 页 说明书 9 页 附图 5 页

(54) 发明名称

一种无线网络中的入口认证方法、系统和装置

(57) 摘要

本发明提供了一种无线网络中的入口 (Portal) 认证的方法、系统和装置, 其中方法包括: 无线接入点 (AP) 接收到移动终端 (STA) 的认证请求后, 通过无线接入点控制与供应协议 (CAPWAP) 隧道将该认证请求发送给接入控制器 (AC), 由 AC 转发给 Portal 服务器; AC 在获知 Portal 服务器针对该 STA 认证成功, 通过 CAPWAP 隧道发送配置消息指示 AP 开启针对该 STA 的本地转发功能; 在获知 STA 退出认证后, 通过 CAPWAP 隧道发送配置消息指示 AP 关闭针对该 STA 的本地转发功能。本发明可以利用已有网络认证架构实现 AP 本地转发情况下的 Portal 认证, 无需额外增加认证设备, 节约组网成本。



1. 一种无线网络中的入口 Portal 认证方法,其特征在于,该方法包括:

A、无线接入点 AP 接收到移动终端 STA 的认证请求后,通过无线接入点控制与供应协议 CAPWAP 隧道将该认证请求发送给接入控制器 AC;

B、所述 AC 将所述认证请求发送给 Portal 服务器,在获知所述 Portal 服务器针对所述 STA 的认证成功后,通过所述 CAPWAP 隧道发送配置消息指示所述 AP 开启针对所述 STA 的本地转发功能;

C、所述 AC 获知所述 STA 退出认证后,通过所述 CAPWAP 隧道发送配置消息指示所述 AP 关闭针对所述 STA 的本地转发功能。

2. 根据权利要求 1 所述的方法,其特征在于,在所述步骤 A 之前还包括:

D1、所述 STA 连接到所述 AP 后,发送动态主机配置协议 DHCP 请求报文;

D2、所述 AP 将所述 DHCP 请求报文通过 CAPWAP 隧道发送给所述 AC,并由所述 AC 发送至 DHCP 服务器;

D3、所述 AC 将所述 DHCP 服务器返回的所述 STA 的 IP 地址和所述 STA 的用户网关 IP 地址通过 CAPWAP 隧道发送给所述 AP;

D4、所述 AP 将所述 STA 的 IP 地址和所述用户网关 IP 地址转发给所述 STA,并存储所述 STA 的 IP 地址、STA 的 MAC 地址和用户网关 IP 地址之间的对应关系。

3. 根据权利要求 2 所述的方法,其特征在于,该方法还包括:预先在所述 AC 上配置包含用户网关的 IP 地址和 MAC 地址的 ARP 表项,利用该 ARP 表项进行针对所述用户网关的 ARP 应答。

4. 根据权利要求 1 或 3 任一权项所述的方法,其特征在于,AP 初始默认开启针对所述 STA 的下行本地转发功能,关闭针对所述 STA 的上行本地转发功能;

步骤 B 中获知所述 Portal 服务器针对所述 STA 的认证成功包括:所述 Portal 服务器在针对所述 STA 认证成功后,向所述 AC 发送认证成功消息,并发送目的 IP 地址为 STA 的 IP 地址的认证成功响应;中央路由器将所述认证成功响应发送给用户网关,由所述用户网关将该认证成功响应经由所述 AP 发送给所述 STA;其中,所述中央路由器为所述 Portal 服务器和所述 AC 之间的路由器或路由器网络。

5. 根据权利要求 4 所述的方法,其特征在于,由所述用户网关将该认证成功响应经由所述 AP 发送给所述 STA 包括:

所述用户网关接收到所述认证成功响应后,向与该用户网关连接的 AP 广播包含所述 STA 的 IP 地址的 ARP 请求;

与所述 STA 连接的 AP 接收到所述 ARP 请求后,向所述用户网关回复包含所述 STA 的 MAC 地址的 ARP 响应;

所述用户网关接收到所述 ARP 响应后,存储包含所述 STA 的 IP 地址和 MAC 地址的 ARP 表项,并利用该 ARP 表项发送所述认证成功响应。

6. 根据权利要求 4 所述的方法,其特征在于,步骤 B 中所述开启针对所述 STA 的本地转发功能为:开启针对所述 STA 的上行本地转发功能;

步骤 C 中所述关闭针对所述 STA 的本地转发功能为:关闭针对所述 STA 的上行本地转发功能。

7. 根据权利要求 1 至 3 任一权项所述的方法,其特征在于,该方法还包括:预先在所述

AC 上启动动态路由协议, AC 将收集到的所述 STA 的主机明细路由发送至中央路由器;

步骤 B 中获知所述 Portal 服务器针对所述 STA 的认证成功包括:所述 Portal 服务器在针对所述 STA 认证成功后,发送目的 IP 地址为 STA 的 IP 地址的认证成功响应;中央路由器根据所述 STA 的主机明细路由将所述认证成功响应发送给所述 AC;其中,所述中央路由器为所述 Portal 服务器和所述 AC 之间的路由器或路由器网络;所述 AC 通过所述 CAPWAP 隧道将所述认证成功响应发送给所述 AP,由所述 AP 发送给所述 STA。

8. 根据权利要求 7 所述的方法,其特征在于,步骤 B 中所述开启针对所述 STA 的本地转发功能为:开启针对所述 STA 的上行和下行本地转发功能;

步骤 C 中所述关闭针对所述 STA 的本地转发功能为:关闭针对所述 STA 的上行和下行本地转发功能;

所述步骤 C 还包括:所述 AC 通知所述中央路由器删除所述 STA 的主机明细路由。

9. 一种无线接入点 AP,其特征在于,该 AP 包括:报文收发单元和功能配置单元;

所述报文收发单元,用于接收到移动终端 STA 的认证请求后,通过无线接入点控制与供应协议 CAPWAP 隧道将该认证请求发送给无线控制器 AC;接收 AC 通过 CAPWAP 隧道发送的配置消息;在所述功能配置单元开启了针对所述 STA 的本地转发功能后,采用本地转发的方式对所述 STA 进行报文转发;

所述功能配置单元,用于在所述报文收发单元接收到指示开启针对所述 STA 的本地转发功能的配置消息时,开启针对所述 STA 的本地转发功能;在所述报文收发单元接收到指示关闭针对所述 STA 的本地转发功能的配置消息时,关闭针对所述 STA 的本地转发功能。

10. 根据权利要求 9 所述的 AP,其特征在于,所述报文收发单元,还用于将接收到的动态主机配置协议 DHCP 请求报文通过 CAPWAP 隧道发送给所述 AC;通过 CAPWAP 隧道接收 AC 发送的所述 STA 的 IP 地址和 STA 的用户网关 IP 地址,将该所述 STA 的 IP 地址和所述用户网关 IP 地址转发给所述 STA,并存储所述 STA 的 IP 地址、STA 的 MAC 地址和用户网关 IP 地址之间的对应关系。

11. 根据权利要求 9 或 10 所述的 AP,其特征在于,所述功能配置单元初始默认开启针对所述 STA 的下行本地转发功能,关闭针对所述 STA 的上行本地转发功能;在所述报文收发单元接收到指示开启针对所述 STA 的本地转发功能的配置消息时,开启针对所述 STA 的上行本地转发功能;在所述报文收发单元接收到指示关闭针对所述 STA 的本地转发功能的配置消息时,关闭针对所述 STA 的上行本地转发功能。

所述报文收发单元,还用于接收到入口 Portal 服务器经由中央路由器和用户网关发送来的认证成功响应后,将该认证成功响应发送给所述 STA。

12. 根据权利要求 11 所述的 AP,其特征在于,该 AP 还包括:ARP 代答单元;

所述报文收发单元,还用于接收到所述用户网关的 ARP 请求后,将该 ARP 请求发送给 ARP 代答单元;将所述 ARP 代答单元提供的 ARP 响应发送给所述用户网关;

所述 ARP 代答单元,用于判断所述 ARP 请求中包含的 IP 地址是否为自身所连接 STA 的 IP 地址,如果是,则将该 IP 地址对应的 STA 的 MAC 地址包含在 ARP 响应中提供给所述报文收发单元。

13. 根据权利要求 9 或 10 所述的 AP,其特征在于,所述功能配置单元在所述报文收发单元接收到指示开启针对所述 STA 的本地转发功能的配置消息时,开启针对所述 STA 的上

行和下行本地转发功能；在所述报文收发单元接收到指示关闭针对所述 STA 的本地转发功能的配置消息时，关闭针对所述 STA 的上行和下行本地转发功能。

所述报文转发单元，还用于接收到 Portal 服务器经由所述 AC 发送来的认证成功响应后，将该认证成功响应发送给所述 STA。

14. 一种无线控制器 AC，其特征在于，该 AC 包括：报文收发单元、认证确定单元和管理配置单元；

所述报文收发单元，用于通过无线接入点控制与供应协议 CAPWAP 隧道接收到无线接入点 AP 发送来的移动终端 STA 的认证请求后，将该认证请求发送给入口 Portal 服务器；

所述认证确定单元，用于在获知所述 Portal 服务器针对所述 STA 的认证成功后，向所述管理配置单元发送第一配置通知；在获知所述 STA 退出认证后，向所述管理配置单元发送第二配置通知；

所述管理配置单元，用于接收到所述第一配置通知后，通过所述 CAPWAP 隧道发送配置消息指示所述 AP 开启针对所述 STA 的本地转发功能；接收到所述第二配置通知后，通过所述 CAPWAP 隧道发送配置消息指示所述 AP 关闭针对所述 STA 的本地转发功能。

15. 根据权利要求 14 所述的 AC，其特征在于，该 AC 还包括：ARP 代答单元，用于根据预先配置在该 AC 上的包含用户网关的 IP 地址和 MAC 地址的 ARP 表项，进行针对所述用户网关的 ARP 应答。

16. 根据权利要求 14 或 15 所述的 AC，其特征在于，当所述 AP 初始默认开启针对所述 STA 的下行本地转发功能，关闭针对所述 STA 的上行本地转发功能时，所述认证确定单元在所述报文收发单元接收到所述 Portal 服务器发送的认证成功消息后，获知所述 Portal 服务器针对所述 STA 的认证成功。

17. 根据权利要求 14 或 15 所述的 AC，其特征在于，该 AC 还包括：路由发送单元，用于利用预先在该 AC 上启动的动态路由协议，将收集到的所述 STA 的主机明细路由发送至中央路由器；在所述认证确定单元获知所述 STA 退出认证后，通知所述中央路由器删除所述 STA 的主机明细路由；其中，所述中央路由器为所述 Portal 服务器和所述 AC 之间的路由器或路由器网络；

所述认证确定单元在所述报文收发单元接收到所述 Portal 服务器发送的认证成功响应后，获知所述 Portal 服务器针对所述 STA 的认证成功；

所述报文收发单元，还用于接收到所述认证成功响应后，将所述认证成功响应通过所述 CAPWAP 隧道发送给所述 AP。

18. 一种无线网络中的入口 Portal 认证系统，其特征在于，该系统包括：无线接入点 AP、无线控制器 AC 和 Portal 服务器；

所述 AP，用于接收到移动终端 STA 的认证请求后，通过无线接入点控制与供应协议 CAPWAP 隧道将该认证请求发送给所述 AC；接收到第一配置消息后，开启针对所述 STA 的本地转发功能；接收到第二配置消息后，关闭针对所述 STA 的本地转发功能；

所述 AC，用于将接收到的所述认证请求发送给所述 Portal 服务器，在获知所述 Portal 服务器针对所述 STA 的认证成功后，通过所述 CAPWAP 隧道向所述 AP 发送第一配置消息；获知所述 STA 退出认证后，通过所述 CAPWAP 隧道向所述 AP 发送第二配置消息；

所述 Portal 服务器，用于接收到所述认证请求后，对所述 STA 进行认证。

19. 根据权利要求 18 所述的系统,其特征在于,该系统还包括:动态主机配置协议 DHCP 服务器;

所述 AP,还用于接收所述 STA 在连接到该 AP 后发送的 DHCP 请求报文,并将该 DHCP 请求报文通过 CAPWAP 隧道发送给所述 AC;将接收到的 STA 的 IP 地址和 STA 的用户网关 IP 地址转发给所述 STA,并存储所述 STA 的 IP 地址、STA 的 MAC 地址和用户网关 IP 地址之间的对应关系;

所述 AC,还用于将接收到的 DHCP 报文发送给 DHCP 服务器;将所述 DHCP 服务器返回的 STA 的 IP 地址和 STA 的用户网关 IP 地址通过 CAPWAP 隧道发送给所述 AP;

所述 DHCP 服务器,用于接收到所述 DHCP 报文后,为所述 STA 分配 IP 地址,并将分配的 STA 的 IP 地址和 STA 的用户网关 IP 地址返回给所述 AC。

20. 根据权利要求 19 所述的系统,其特征在于,所述 AC,还用于利用预先配置的包含用户网关的 IP 地址和 MAC 地址的 ARP 表项,进行针对所述用户网关的 ARP 应答。

21. 根据权利要求 18 至 20 任一权项所述的系统,其特征在于,该系统还包括:用户网关以及在所述 Portal 服务器和所述 AC 之间的中央路由器;

所述 AP 初始默认开启针对所述 STA 的下行本地转发功能,关闭针对所述 STA 的上行本地转发功能;接收到所述第一配置消息后,开启针对所述 STA 的上行本地转发功能,接收到所述第二配置消息后,关闭针对所述 STA 的上行本地转发功能;

所述 Portal 服务器,还用于在针对所述 STA 认证成功后,向所述 AC 发送认证成功消息,并发送目的 IP 地址为 STA 的 IP 地址的认证成功响应;

所述 AC 接收到所述认证成功消息后,获知所述 Portal 服务器针对所述 STA 的认证成功;

中央路由器,用于接收到所述认证成功响应后,将所述认证成功响应发送给用户网关;

所述用户网关,用于将接收到的所述认证成功响应经由所述 AP 发送给所述 STA。

22. 根据权利要求 18 至 20 任一权项所述的系统,其特征在于,该系统还包括:用户网关以及在所述 Portal 服务器和所述 AC 之间的中央路由器;

所述 AC,还用于利用预先启动的动态路由协议,将收集到的所述 STA 的主机明细路由发送至所述中央路由器;

所述 Portal 服务器,还用于在针对所述 STA 认证成功后,发送目的 IP 地址为 STA 的 IP 地址的认证成功响应;

所述中央路由器,用于根据所述 STA 的主机明细路由,将所述 Portal 服务器发送的认证成功响应发送给所述 AC;

所述 AC 接收到所述认证成功响应后获知所述 Portal 服务器针对所述 STA 的认证成功,并通过所述 CAPWAP 隧道将所述认证成功响应发送给所述 AP;获知所述 STA 退出认证后,通知所述中央路由器删除所述 STA 的主机明细路由;

所述 AP,还用于将接收到的所述认证成功响应发送给所述 STA;接收到所述第一配置消息后,开启针对所述 STA 的上行和下行本地转发功能;接收到所述第二配置消息后,关闭针对所述 STA 的上行和下行本地转发功能。

一种无线网络中的入口认证方法、系统和装置

技术领域

[0001] 本发明涉及无线局域网 (WLAN) 技术领域,特别涉及一种无线网络中的入口认证方法、系统和装置。

背景技术

[0002] 在目前的无线网络中,集中式无线局域网由于其管理性强和适用于大规模部署的优点得到越来越广泛的应用。在集中式无线局域网中,AC 与 AP 之间可以通过专有的协议隧道进行连接,常用的是无线接入点控制与供应 (CAPWAP,Controlling and Provisioning of Wireless Access Point) 协议,通过 CAPWAP 隧道可以进行 AP 和 AC 之间数据的传输和配置管理。

[0003] 在传统集中式无线局域网中,入口 (Portal) 认证通过 AC 发送至 Portal 服务器进行,在用户的 Portal 认证通过后,由 AC 进行该用户的移动终端 (STA) 的数据的转发,集中式无线局域网的现有认证架构如图 1 所示。

[0004] 但随着无线通信技术的不断发展,AC 的性能已经逐渐无法满足各 AP 下的用户数据转发,因此,本地转发技术应运而生,即 AP 和 STA 仍通过 CAPWAP 隧道由 AC 进行管理,但 STA 的数据则通过与其连接的 AP 进行转发,不再通过 CAPWAP 隧道集中由 AC 进行转发。由于数据不再通过 AC,因此,无法通过现有的认证架构实现用户的 Portal 认证,而需要在与 AP 二层可达的地方额外增设 Portal 服务器,如图 2 所示。这样,在采用 AP 本地转发的情况下,就无法直接利用已有的网络架构,而不得不增加组网的设备数量,进而增加了成本。

发明内容

[0005] 有鉴于此,本发明提供了一种无线网络中的 Portal 认证方法、系统和装置,以便于利用已有网络认证架构实现 AP 本地转发情况下的 Portal 认证,不额外增加认证设备,节约组网成本。

[0006] 一种无线网络中的 Portal 认证方法,该方法包括:

[0007] A、AP 接收到 STA 的认证请求后,通过 CAPWAP 隧道将该认证请求发送给 AC;

[0008] B、所述 AC 将所述认证请求发送给 Portal 服务器,在获知所述 Portal 服务器针对所述 STA 的认证成功,通过所述 CAPWAP 隧道发送配置消息指示所述 AP 开启针对所述 STA 的本地转发功能;

[0009] C、所述 AC 获知所述 STA 退出认证后,通过所述 CAPWAP 隧道发送配置消息指示所述 AP 关闭针对所述 STA 的本地转发功能。

[0010] 一种 AP,该 AP 包括:报文收发单元和功能配置单元;

[0011] 所述报文收发单元,用于接收到 STA 的认证请求后,通过 CAPWAP 隧道将该认证请求发送给 AC;接收 AC 通过 CAPWAP 隧道发送的配置消息;在所述功能配置单元开启了针对所述 STA 的本地转发功能后,采用本地转发的方式对所述 STA 进行报文转发;

[0012] 所述功能配置单元,用于在所述报文收发单元接收到指示开启针对所述 STA 的本

地转发功能的配置消息时,开启针对所述 STA 的本地转发功能;在所述报文收发单元接收到指示关闭针对所述 STA 的本地转发功能的配置消息时,关闭针对所述 STA 的本地转发功能。

[0013] 一种 AC,该 AC 包括:报文收发单元、认证确定单元和管理配置单元;

[0014] 所述报文收发单元,用于通过 CAPWAP 隧道接收到 AP 发送来的 STA 的认证请求后,将该认证请求发送给 Portal 服务器;

[0015] 所述认证确定单元,用于在获知所述 Portal 服务器针对所述 STA 的认证成功后,向所述管理配置单元发送第一配置通知;在获知所述 STA 退出认证后,向所述管理配置单元发送第二配置通知;

[0016] 所述管理配置单元,用于接收到所述第一配置通知后,通过所述 CAPWAP 隧道发送配置消息指示所述 AP 开启针对所述 STA 的本地转发功能;接收到所述第二配置通知后,通过所述 CAPWAP 隧道发送配置消息指示所述 AP 关闭针对所述 STA 的本地转发功能。

[0017] 一种无线网络中的入口 Portal 认证系统,该系统包括:AP、AC 和 Portal 服务器;

[0018] 所述 AP,用于接收到 STA 的认证请求后,通过 CAPWAP 隧道将该认证请求发送给所述 AC;接收到第一配置消息后,开启针对所述 STA 的本地转发功能;接收到第二配置消息后,关闭针对所述 STA 的本地转发功能;

[0019] 所述 AC,用于将接收到的所述认证请求发送给所述 Portal 服务器,在获知所述 Portal 服务器针对所述 STA 的认证成功后,通过所述 CAPWAP 隧道向所述 AP 发送第一配置消息;获知所述 STA 退出认证后,通过所述 CAPWAP 隧道向所述 AP 发送第二配置消息;

[0020] 所述 Portal 服务器,用于接收到所述认证请求后,对所述 STA 进行认证。

[0021] 由以上技术方案可以看出,本发明提供的方法、系统和装置中,AP 将 STA 的认证请求通过 CAPWAP 隧道发送给 AC,由 AC 转发给 Portal 服务器,并且 AC 在获知 Portal 服务器针对该 STA 认证成功后,通过 CAPWAP 隧道发送配置消息指示 AP 开启针对该 STA 的本地转发功能;在获知 STA 退出认证后,通过 CAPWAP 隧道发送配置消息指示 AP 关闭针对该 STA 的本地转发功能。也就是说,在认证通过之前,认证请求集中发送至 AC,在认证通过之后,由 AC 配置 AP 开启通过认证的 STA 的本地转发功能。通过本发明可以利用已有网络认证架构实现 AP 本地转发情况下的 Portal 认证,无需额外增加认证设备,节约组网成本。

附图说明

[0022] 图 1 为集中式无线组网的现有认证架构图;

[0023] 图 2 为现有技术中 AP 本地转发情况下的认证架构图;

[0024] 图 3 为本发明实施例提供的主要方法流程图;

[0025] 图 4 为本发明实施例提供的详细方法流程图;

[0026] 图 5 为本发明实施例一中的 DHCP 报文流向示意图;

[0027] 图 6 为本发明实施例一中的认证报文流向示意图;

[0028] 图 7 为本发明实施例二提供的详细方法流程图;

[0029] 图 8 为本发明实施例提供的 AP 结构示意图;

[0030] 图 9 为本发明实施例提供的 AC 结构示意图。

具体实施方式

[0031] 为了使本发明的目的、技术方案和优点更加清楚,下面结合附图和具体实施例对本发明进行详细描述。

[0032] 本发明所提供的方法可以如图 3 所示,主要包括以下步骤:

[0033] 步骤 301:AP 接收到 STA 的认证请求后,通过 CAPWAP 隧道将该认证请求发送给 AC。

[0034] 步骤 302:AC 将该认证请求转发给 Portal 服务器,在获知 Portal 服务器针对该 STA 的认证成功,通过 CAPWAP 隧道发送配置消息指示 AP 开启针对该 STA 的本地转发功能。

[0035] 步骤 303:AC 获知该 STA 退出认证后,通过 CAPWAP 隧道发送配置消息指示 AP 关闭针对该 STA 的本地转发功能。

[0036] 下面结合具体实施例对本发明提供的上述方法进行详细描述。

[0037] 实施例一:

[0038] 图 4 为本发明实施例一提供的详细方法流程图,在该流程中仍使用如图 1 所示的现有认证架构来实现 AP 本地转发情况下的认证,在该方法中,在 AP 上配置 STA 认证通过前关闭本地转发功能,且默认开启下行本地转发功能。如图 4 所示,该方法可以包括以下步骤:

[0039] 步骤 401:STA 连接到 AP 后,发送动态主机配置协议 (DHCP) 请求报文。

[0040] 在 STA 初始连接到 AP 后,会发现该 STA 没有任何 IP 地址设定,就会发送一个携带该 STA 的 MAC 地址的 DHCP 请求报文,该 DHCP 请求报文的源地址会为 0.0.0.0,而目的地址则为 255.255.255.255。

[0041] 步骤 402:AP 通过与 AC 之间的 CAPWAP 隧道将 DHCP 请求报文发送给 AC,由 AC 转发给 DHCP 服务器。

[0042] 由于 AP 在用户认证通过前不开启本地转发功能,因此,AP 会将 STA 发送来的所有报文都通过 CAPWAP 隧道发送给 AC。在 AC 接收到 DHCP 请求报文后,对该 DHCP 请求报文进行 DHCP 中继 (DHCP Relay) 操作,转发至与其连接的 DHCP 服务器。

[0043] 步骤 403:DHCP 服务器为该 STA 分配 IP 地址,并确定该 STA 在后续的 AP 本地转发时使用的用户网关 IP 地址,将这些 IP 地址信息发送给 AC。

[0044] 步骤 404:AC 将该 IP 地址信息通过 CAPWAP 隧道发送给 AP,再由 AP 发送给 STA。

[0045] 本步骤中,仍通过 AC 的 DHCP Relay 功能将 DHCP 服务器回复的 IP 地址信息通过 CAPWAP 隧道发送给 AP,再进一步由 AP 发送给 STA。

[0046] 经过上述步骤后,STA 便获取到分配的 IP 地址,并且,AC 上会保存 STA 的 IP 地址和 MAC 地址之间对应关系的 ARP 表项。AP 上会存储该 STA 的 IP 地址、MAC 地址以及该 STA 对应的用户网关 IP 地址之间的对应关系,在开启针对该 STA 的本地转发功能后,使用该对应关系进行本地转发时使用。

[0047] 上述 DHCP 请求过程的报文流向可以如图 5 所示。

[0048] 步骤 405:STA 发送目的 IP 地址为用户网关 IP 地址的 HTTP 请求报文,AP 接收到该 HTTP 请求报文后通过 CAPWAP 隧道发送至 AC。

[0049] 用户打开 Internet 上的超文本传输协议 (HTTP) 页面后,由于该用户尚没有通过认证,会触发认证过程的开始。首先会发送目的 IP 地址为用户网关 IP 地址的 HTTP 请求报

文来获取用户网关的 MAC 地址,以便进行后续的二层转发。AP 接收到该 HTTP 请求报文后,仍会将该 HTTP 请求报文通过 CAPWAP 隧道发送至 AC。

[0050] 步骤 406 :AC 接收到该 HTTP 请求报文后,利用预先配置的 ARP 表项代替用户网关通过 CAPWAP 隧道向 STA 进行 ARP 应答。

[0051] 由于 AC 尚并不存在用户网关的 MAC 地址信息,因此,需要预先在该 AC 上配置各用户网关的 ARP 表项,即 IP 地址与 MAC 地址之间的对应关系,并在 AC 上配置用户网关的 ARP 代答功能。AC 接收到 HTTP 请求报文后,将用户网关的 MAC 地址通过 CAPWAP 隧道发送给 AP,再由 AP 发送给 STA。AP 和 STA 都会存储该用户网关的 ARP 表项。

[0052] 步骤 407 :STA 发送认证请求,AP 通过 CAPWAP 隧道将认证请求发送给 AC,AC 接收到该认证请求后将该认证请求重定向至 Portal 服务器。

[0053] 通常,该认证请求中的目的地址为用户网关的地址,AC 在接收到认证请求后,会向 STA 回复 HTTP 重定向告知 Portal 服务器的 IP 地址。STA 根据该 HTTP 重定向,重新发送认证请求,由 AC 将该认证请求转发至 Portal 服务器。

[0054] 需要说明的是,如果用户直接使用登录页面,也可以不执行步骤 405 和 406,直接执行步骤 407 发送认证请求,并在步骤 407 中进行 ARP 应答。

[0055] 步骤 408 :Portal 服务器接收到认证请求后,对该用户进行认证,认证通过后,告知 AC 认证成功,并向 STA 发送认证成功响应。

[0056] 其中,告知 AC 认证成功可以通过向 AC 发送认证成功消息的方式实现,该方式是 Portal 认证已有的标准方式。

[0057] 该认证成功响应的目的 IP 地址为 STA 的 IP 地址。向 STA 发送的认证成功响应首先发送至中央路由器,由于 STA 的 IP 地址是用户网关的 IP 地址所在网段下的 IP 地址,因此,中央路由器会将该认证成功响应发送至用户网关。

[0058] 用户网关接收到该认证成功响应后,会向其所连接的所有 AP 广播包含该 STA 的 IP 地址的 ARP 请求,由于 AP 默认开启了下行的本地转发功能,因此,与该 STA 连接的 AP 接收到该 ARP 请求后,会代替 STA 进行 ARP 应答,告知该用户网关该 STA 的 MAC 地址,用户网关存储该 STA 的 IP 地址和 MAC 地址的 ARP 表项,并利用该表项进行后续的报文转发。用户网关利用该 ARP 表项将认证成功响应发送给 AP,由 AP 转发给 STA。

[0059] 需要说明的是,中央路由器为 AC 与 Portal 服务器之间的路由器或路由器网络的统称。

[0060] 步骤 409 :AC 获知认证成功后,向 AP 发送开启针对该 STA 的上行本地转发功能的配置消息,AP 接收到该配置消息后,开启针对该 STA 的上行本地转发功能。

[0061] AC 向 AP 发送的配置消息中可以包括该 STA 的 MAC 地址信息,AP 接收到该配置消息后,针对该 STA 的 MAC 地址使能上行本地转发。

[0062] AP 在接收到 STA 发送的报文后,可以首先判断是否针对该 STA 开启了上行本地转发功能,如果是,则对该报文进行本地转发,否则,通过 CAPWAP 隧道将该报文发送至 AC。

[0063] 也就是说,STA 认证成功后,AP 便会开启针对该 STA 的上行本地转发功能,且该 AP 已经具有下行本地转发功能,因此,后续针对该 STA 的报文,便可以通过 AP 的本地转发功能来进行转发,而不必集中发送至 AC 进行转发。

[0064] 如果认证失败,则 Portal 服务器会告知 AC 认证失败,并向 STA 发送认证失败响

应,该认证失败响应的转发路径与认证成功响应相同。AC 获知认证失败后,便不会向 AP 发送开启针对该 STA 的上行本地转发功能的配置消息,则针对该 STA 则不会实现上行数据的本地转发,从而达到 Portal 认证的目的。

[0065] Portal 认证过程,即步骤 407 至 409 的报文流向可以如图 6 所示。

[0066] 如果用户退出认证,则可以继续执行以下步骤:

[0067] 步骤 410:用户退出认证时,按照现有 Portal 退出认证流程执行,即 Portal 服务器向 AC 告知该用户的 STA 退出登录。AC 通过 CAPWAP 隧道向 AP 发送关闭针对该 STA 的上行本地转发功能的配置消息。

[0068] 用户退出认证可能存在两种情况:其一是,用户下线,STA 会向 Portal 服务器发送认证退出请求报文,Portal 服务器接收到该退出请求报文后,通知 AC 该 STA 退出认证,AC 删除存储的该 STA 的相关 ARP 表项;其二,STA 关机,Portal 服务器和 STA 之间会周期性地发送心跳报文,如果 Portal 服务器在设定时间内没有收到 STA 的心跳报文,则认为 STA 故障,Portal 服务器通知 AC 该 STA 退出认证,AC 删除存储的该 STA 的相关 ARP 表项。

[0069] 当用户退出认证后,AC 会相应地通知 AP 关闭针对该 STA 的上行本地转发功能。这样,该 STA 在下次上线时,仍按照图 4 所示流程执行完整的认证流程来开启 AP 针对该 STA 的本地转发。

[0070] 实施例一在认证报文的交互过程中采用的是不对称路径,这是通过在 AP 上默认开启针对 STA 的下行本地转发功能实现的。除此之外,还可以在认证报文的交互过程中始终采用对称路径,这样无需默认开启针对该 STA 的下行本地转发功能,而在认证成功后在同时开启针对该 STA 的上行和下行本地转发功能,下面在实施例二中对这种情况进行详细描述。

[0071] 实施例二:

[0072] 图 7 为本发明实施例二提供的详细方法流程图,同样,在该流程中仍使用如图 1 所示的现有认证架构来实现 AP 本地转发情况下的认证,如图 7 所示,该方法可以包括以下步骤:

[0073] 步骤 701-707 与步骤 401-407 相同,不再赘述。

[0074] 在该实施例中,AP 在初始时默认关闭 STA 的上行和下行本地转发功能。

[0075] 步骤 708:Portal 服务器接收到认证请求后,对该用户进行认证,认证通过后,向 STA 发送认证成功响应。

[0076] 该认证成功响应的目的 IP 地址为该 STA 的 IP 地址。

[0077] 在该实施例中,由于 AP 初始时关闭 STA 的下行本地转发功能,因此,认证成功响应仍然需要通过 AC 转发给 STA,而不能通过用户网关来进行认证成功响应的下行发送。此时,可以在 AC 上启动诸如开放式最短路径优先 (OSPF) 的动态路由协议,AC 将收集到的该 STA 的主机明细路由发送至中央路由器,使得该中央路由器在接收到 Portal 服务器的认证成功响应后,根据主机该 STA 的主机明细路由将该认证成功响应发送给 AC。

[0078] 假设 STA 和用户网关所在网段为 10.0.0.0,STA 具体的 IP 地址为 10.0.0.10,用户网关的 IP 地址为 10.0.0.1,如果 AC 不将主机明细路由发送至中央路由器,则中央路由器仅知晓 STA 在用户网关所在网段中,因此,会将认证成功响应发送至用户网关;如果 AC 将主机明细路由即 10.0.0.10 对应的路由发送至中央路由器,则中央路由器会选择将该认证成功

功响应按照主机明细路由进行发送,即发送给 AC。

[0079] 步骤 709 :AC 接收到认证成功响应后,将该认证成功响应通过 CAPWAP 隧道发送给 AP,并通过 CAPWAP 隧道向 AP 发送开启针对该 STA 的上行和下行本地转发功能的配置消息。

[0080] 步骤 710 :AP 将接收到的认证成功响应发送给 STA,并按照接收到的配置消息开启针对该 STA 的上行和下行本地转发功能。

[0081] 步骤 711 :用户退出认证时,按照现有 Portal 退出认证流程执行,AC 获知该用户的 STA 退出登录时,AC 通过 CAPWAP 隧道向 AP 发送关闭针对该 STA 的上行和下行本地转发功能的配置消息,并通知中央路由器删除该 STA 的主机明细路由。

[0082] 在该实施例二中,需要中央路由器及时更新来自 AC 的 STA 的主机路由,这相比较实施例一对组网中的路由器具有一定性能要求。

[0083] 以上是对本发明所提供的方法进行的详细描述,下面对本发明所提供的系统和装置进行详细描述。

[0084] 本发明所提供的 Portal 认证系统可以如图 1 所示的架构,只是某些设备的功能发生了变更,该系统可以包括 :AP、AC 和 Portal 服务器。

[0085] AP,用于接收到 STA 的认证请求后,通过 CAPWAP 隧道将该认证请求发送给 AC ;接收到第一配置消息后,开启针对 STA 的本地转发功能 ;接收到第二配置消息后,关闭针对 STA 的本地转发功能。

[0086] AC,用于将接收到的认证请求发送给 Portal 服务器,在获知 Portal 服务器针对 STA 的认证成功后,通过 CAPWAP 隧道向 AP 发送第一配置消息 ;获知 STA 退出认证后,通过 CAPWAP 隧道向 AP 发送第二配置消息。

[0087] Portal 服务器,用于接收到认证请求后,对 STA 进行认证。

[0088] 由于通常在 STA 与 AP 建立连接后且进行认证之前,需要进行 DHCP 过程,因此,该系统还可以包括 :DHCP 服务器。

[0089] AP,还用于接收 STA 在连接到该 AP 后发送的 DHCP 请求报文,并将该 DHCP 请求报文通过 CAPWAP 隧道发送给 AC ;将接收到的 STA 的 IP 地址和 STA 的用户网关 IP 地址转发给 STA,并存储 STA 的 IP 地址、STA 的 MAC 地址和用户网关 IP 地址之间的对应关系。

[0090] AC,还用于将接收到的 DHCP 报文发送给 DHCP 服务器 ;将 DHCP 服务器返回的 STA 的 IP 地址和 STA 的用户网关 IP 地址通过 CAPWAP 隧道发送给 AP。

[0091] DHCP 服务器,用于接收到 DHCP 报文后,为 STA 分配 IP 地址,并将分配的 STA 的 IP 地址和 STA 的用户网关 IP 地址返回给 AC。

[0092] 另外,AC 还可以用于利用预先配置的包含用户网关的 IP 地址和 MAC 地址的 ARP 表项,进行针对用户网关的 ARP 应答。

[0093] 该系统还可以包括 :用户网关以及在 Portal 服务器和 AC 之间的中央路由器。对于具体的认证成功响应回复过程,可以采用以下两种方式 :

[0094] 第一种方式 :

[0095] AP 初始默认开启针对 STA 的下行本地转发功能,关闭针对 STA 的上行本地转发功能 ;接收到第一配置消息后,开启针对 STA 的上行本地转发功能,接收到第二配置消息后,关闭针对 STA 的上行本地转发功能。

[0096] Portal 服务器,还可以用于在针对 STA 认证成功后,向 AC 发送认证成功消息,并发

送目的 IP 地址为 STA 的 IP 地址的认证成功响应。

[0097] AC 接收到认证成功消息后,获知 Portal 服务器针对 STA 的认证成功。

[0098] 中央路由器,用于接收到认证成功响应后,将认证成功响应发送给用户网关。

[0099] 用户网关,用于将接收到的认证成功响应经由 AP 发送给 STA。

[0100] 第二种方式:

[0101] AC 利用预先启动的动态路由协议,将收集到的 STA 的主机明细路由发送至中央路由器。

[0102] Portal 服务器,还可以用于在针对 STA 认证成功后,发送目的 IP 地址为 STA 的 IP 地址的认证成功响应。

[0103] 中央路由器,用于根据 STA 的主机明细路由,将 Portal 服务器发送的认证成功响应发送给 AC。

[0104] AC 接收到认证成功响应后获知 Portal 服务器针对 STA 的认证成功,并通过 CAPWAP 隧道将认证成功响应发送给 AP;获知 STA 退出认证后,通知中央路由器删除 STA 的主机明细路由。

[0105] AP,还用于将接收到的认证成功响应发送给 STA;接收到第一配置消息后,开启针对 STA 的上行和下行本地转发功能;接收到第二配置消息后,关闭针对 STA 的上行和下行本地转发功能。

[0106] 图 8 为本发明实施例提供的 AP 结构示意图,如图 8 所示,该 AP 可以包括:报文收发单元 801 和功能配置单元 802。

[0107] 报文收发单元 801,用于接收到 STA 的认证请求后,通过 CAPWAP 隧道将该认证请求发送给 AC;接收 AC 通过 CAPWAP 隧道发送的配置消息;在功能配置单元 802 开启了针对 STA 的本地转发功能后,采用本地转发的方式对 STA 进行报文转发。

[0108] 功能配置单元 802,用于在报文收发单元 801 接收到指示开启针对 STA 的本地转发功能的配置消息时,开启针对 STA 的本地转发功能;在报文收发单元 801 接收到指示关闭针对 STA 的本地转发功能的配置消息时,关闭针对 STA 的本地转发功能。

[0109] 另外,报文收发单元 801,还可以用于将接收到的 DHCP 请求报文通过 CAPWAP 隧道发送给 AC;通过 CAPWAP 隧道接收 AC 发送的 STA 的 IP 地址和 STA 的用户网关 IP 地址,将该 STA 的 IP 地址和用户网关 IP 地址转发给 STA,并存储 STA 的 IP 地址、STA 的 MAC 地址和用户网关 IP 地址之间的对应关系。

[0110] 针对上述的两种认证的方式,AP 也可以采用以下两种结构:

[0111] 其一、功能配置单元 802 初始默认开启针对 STA 的下行本地转发功能,关闭针对 STA 的上行本地转发功能;在报文收发单元 801 接收到指示开启针对 STA 的本地转发功能的配置消息时,开启针对 STA 的上行本地转发功能;在报文收发单元 801 接收到指示关闭针对 STA 的本地转发功能的配置消息时,关闭针对 STA 的上行本地转发功能。

[0112] 报文转发单元 801,还用于接收到 Portal 服务器经由中央路由器和用户网关发送来的认证成功响应后,将该认证成功响应发送给 STA。

[0113] 此时,该 AP 还可以包括:ARP 代答单元 803。

[0114] 报文收发单元 801,还用于接收到用户网关的 ARP 请求后,将该 ARP 请求发送给 ARP 代答单元 803;将 ARP 代答单元 803 提供的 ARP 响应发送给用户网关。

[0115] ARP 代答单元 803,用于判断 ARP 请求中包含的 IP 地址是否为自身所连接 STA 的 IP 地址,如果是,则将该 IP 地址对应的 STA 的 MAC 地址包含在 ARP 响应中提供给报文收发单元 801。

[0116] 其二、功能配置单元 802 在报文收发单元 801 接收到指示开启针对 STA 的本地转发功能的配置消息时,开启针对 STA 的上行和下行本地转发功能;在报文收发单元 801 接收到指示关闭针对 STA 的本地转发功能的配置消息时,关闭针对 STA 的上行和下行本地转发功能。

[0117] 报文转发单元 801,还用于接收到 Portal 服务器经由 AC 发送来的认证成功响应后,将该认证成功响应发送给 STA。

[0118] 图 9 为本发明实施例提供的 AC 结构示意图,如图 9 所示,该 AC 可以包括:报文收发单元 901、认证确定单元 902 和管理配置单元 903。

[0119] 报文收发单元 901,用于通过 CAPWAP 隧道接收到 AP 发送来的 STA 的认证请求后,将该认证请求发送给 Portal 服务器。

[0120] 认证确定单元 902,用于在获知 Portal 服务器针对 STA 的认证成功后,向管理配置单元 903 发送第一配置通知;在获知 STA 退出认证后,向管理配置单元 903 发送第二配置通知。

[0121] 管理配置单元 903,用于接收到第一配置通知后,通过 CAPWAP 隧道发送配置消息指示 AP 开启针对 STA 的本地转发功能;接收到第二配置通知后,通过 CAPWAP 隧道发送配置消息指示 AP 关闭针对 STA 的本地转发功能。

[0122] 另外,该 AC 还可以包括:ARP 代答单元 904,用于根据预先配置在该 AC 上的包含用户网关的 IP 地址和 MAC 地址的 ARP 表项,进行针对用户网关的 ARP 应答。

[0123] 同样针对上述的两种认证响应回复方式,AC 也可以存在以下两种结构:

[0124] 其一、当 AP 初始默认开启针对 STA 的下行本地转发功能,关闭针对 STA 的上行本地转发功能时,认证确定单元 902 在报文收发单元 901 接收到 Portal 服务器发送的认证成功消息后,获知 Portal 服务器针对 STA 的认证成功。

[0125] 其二、该 AC 还可以包括:路由发送单元 905,用于利用预先在该 AC 上启动的动态路由协议,将收集到的 STA 的主机明细路由发送至中央路由器;在认证确定单元 902 获知 STA 退出认证后,通知中央路由器删除 STA 的主机明细路由;其中,中央路由器为 Portal 服务器和 AC 之间的路由器或路由器网络。

[0126] 认证确定单元 902 在报文收发单元 901 接收到 Portal 服务器发送的认证成功响应后,获知 Portal 服务器针对 STA 的认证成功。

[0127] 报文收发单元 901,还用于接收到认证成功响应后,将认证成功响应通过 CAPWAP 隧道发送给 AP。

[0128] 由以上描述可以看出,本发明提供的方法、系统和装置中,AP 将 STA 的认证请求通过 CAPWAP 隧道发送给 AC,由 AC 转发给 Portal 服务器,并且 AC 在获知 Portal 服务器针对该 STA 认证成功后,通过 CAPWAP 隧道发送配置消息指示 AP 开启针对该 STA 的本地转发功能;在获知 STA 退出认证后,通过 CAPWAP 隧道发送配置消息指示 AP 关闭针对该 STA 的本地转发功能。也就是说,在认证通过之前,认证请求集中发送至 AC,在认证通过之后,由 AC 配置 AP 开启通过认证的 STA 的本地转发功能。通过本发明可以利用已有网络认证架构实现

AP 本地转发情况下的 Portal 认证, 无需额外增加认证设备, 节约组网成本。

[0129] 另外, 本发明中, AP 仅需要在认证之前和认证过程中, 将接收到的所有报文都转发到 AC 进行集中处理, 在认证成功完成之后, 便开启了本地转发功能, 在 AP 本地完成通过认证的 STA 的报文转发, 从而减轻了 AC 的性能负担。

[0130] 以上所述仅为本发明的较佳实施例而已, 并不用以限制本发明, 凡在本发明的精神和原则之内, 所做的任何修改、等同替换、改进等, 均应包含在本发明保护的范围之内。

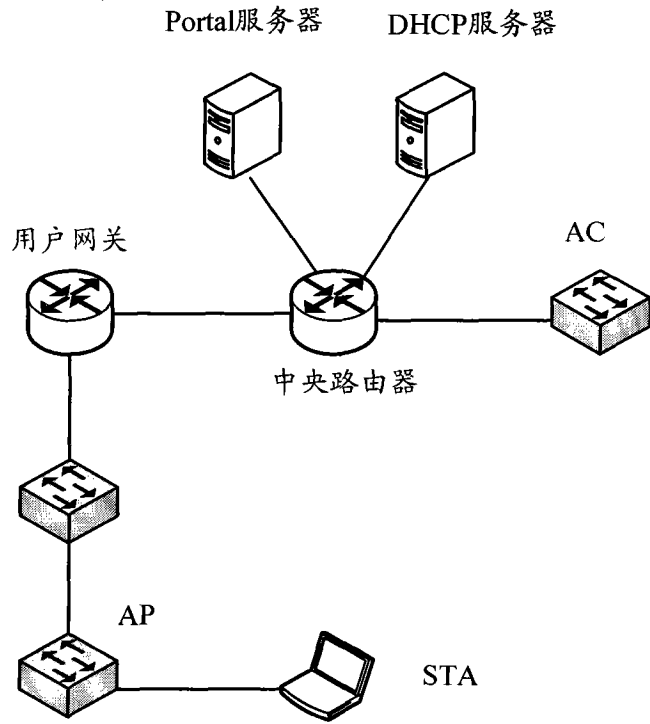


图 1

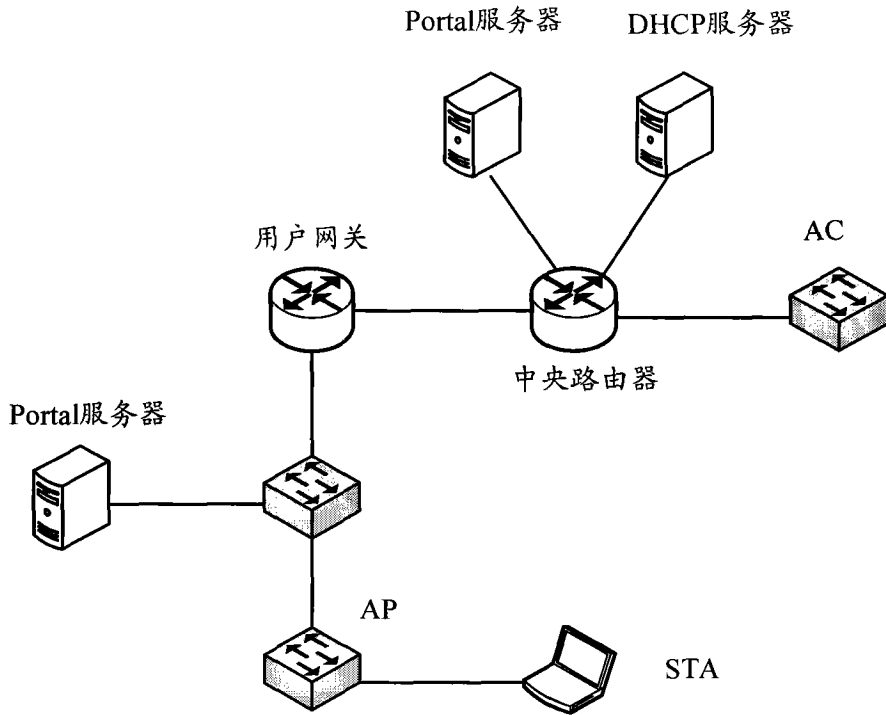


图 2

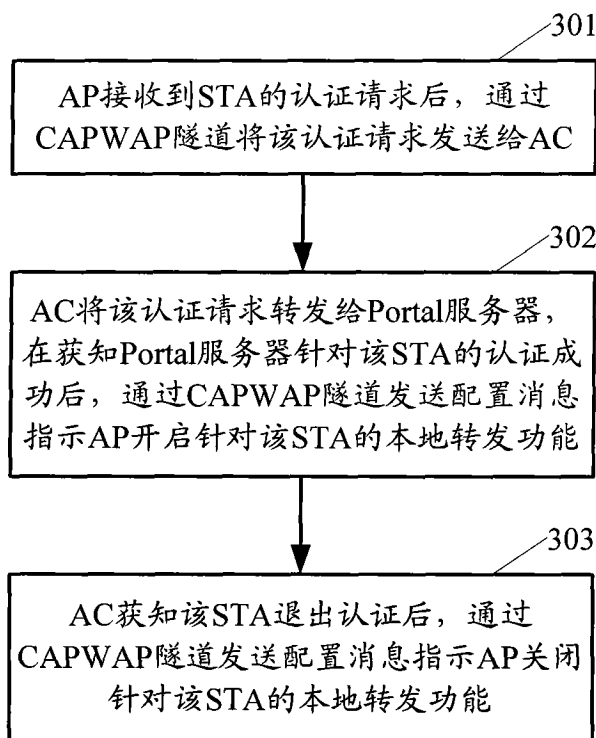


图 3

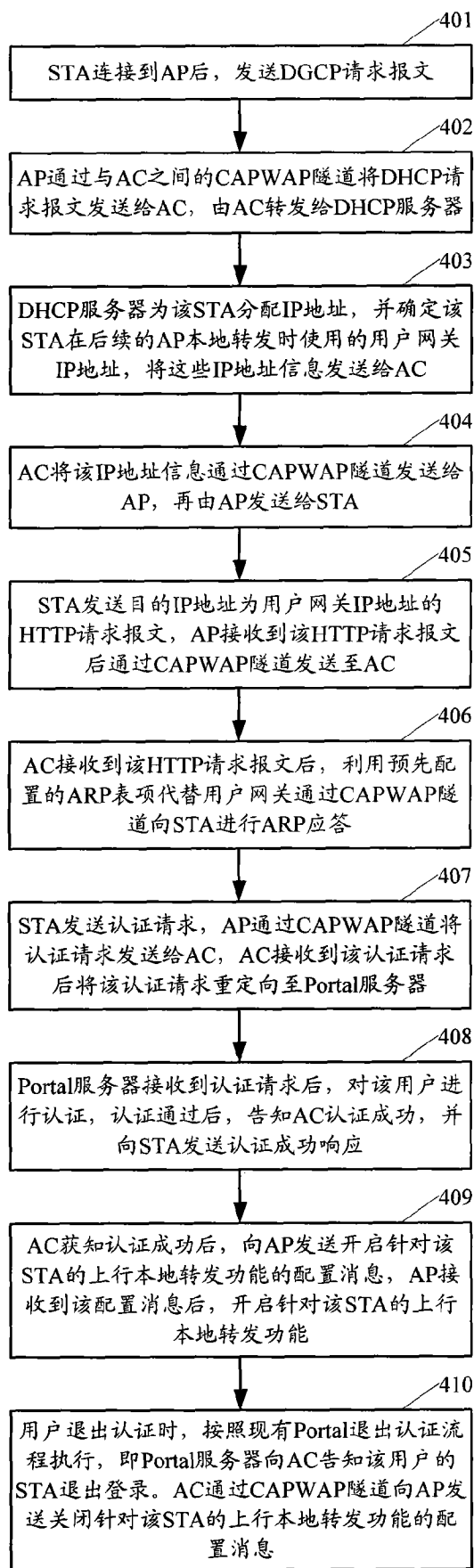


图 4

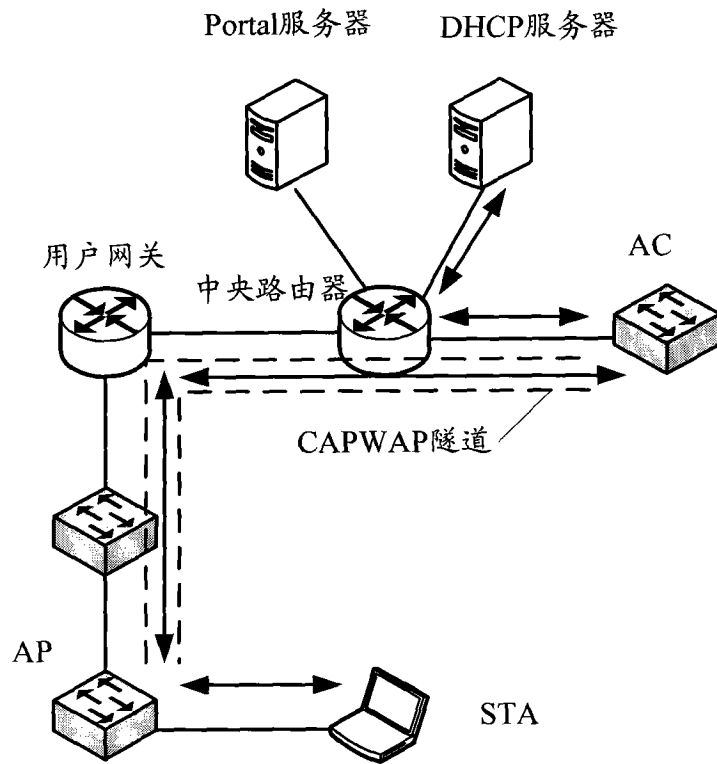


图 5

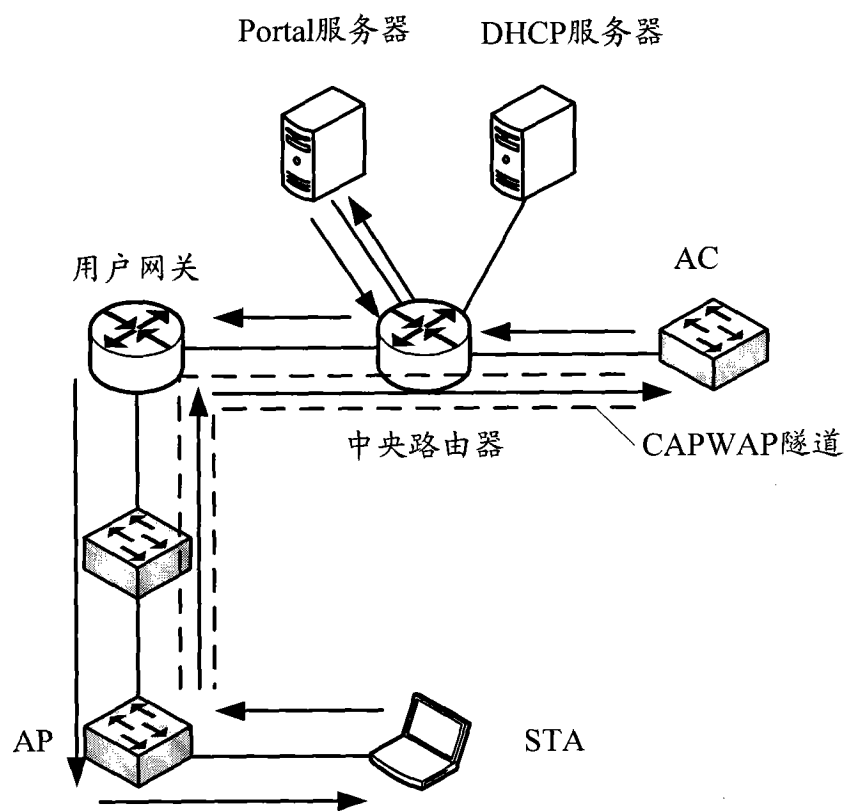


图 6

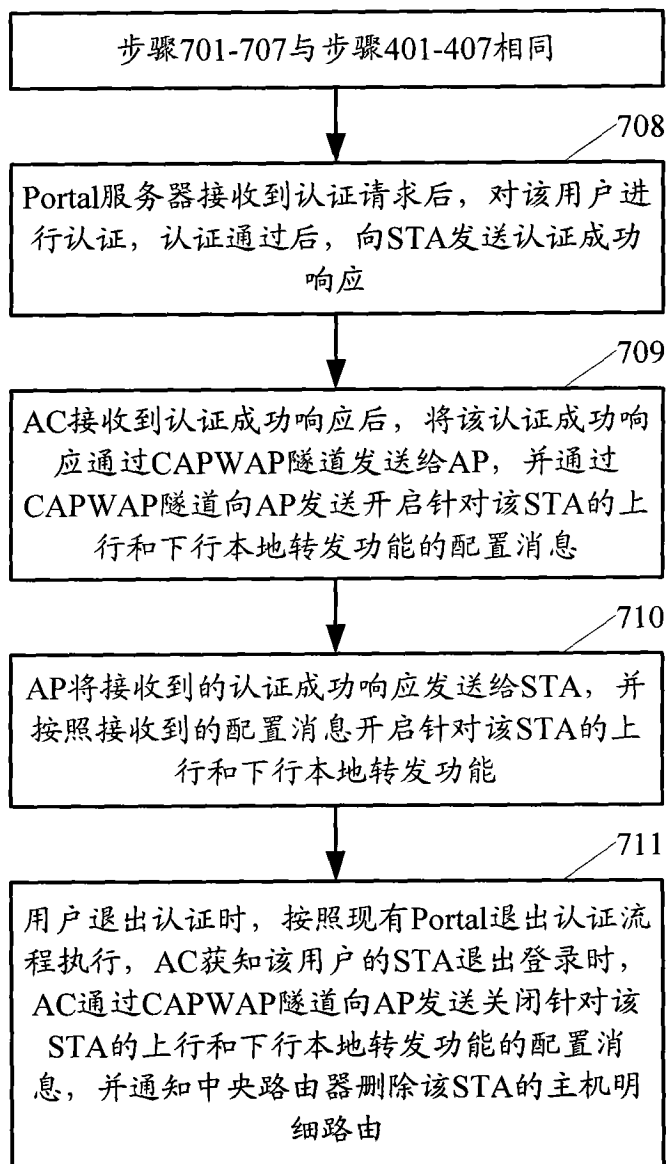


图 7

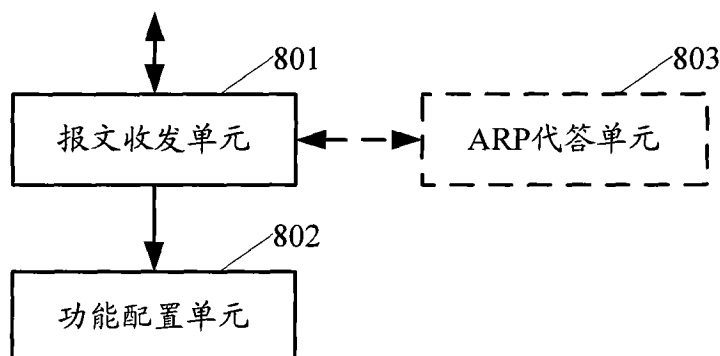


图 8

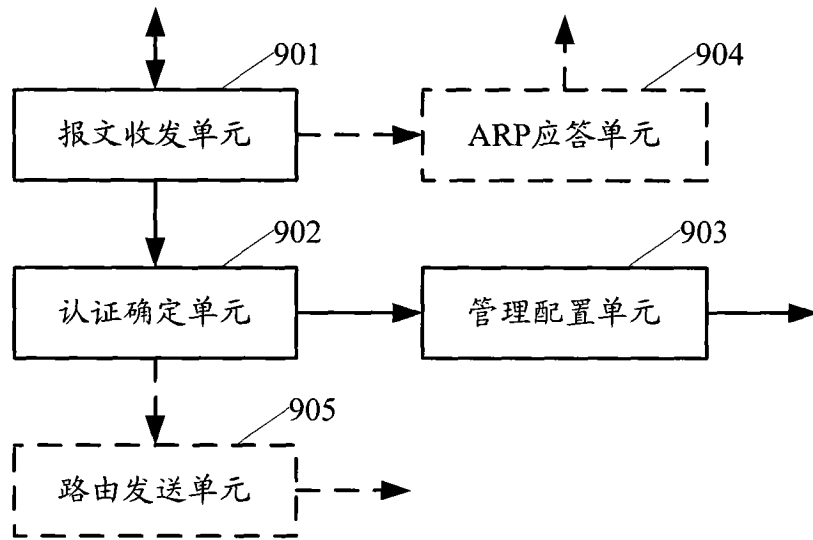


图 9