



## (12) 发明专利

(10) 授权公告号 CN 101442516 B

(45) 授权公告日 2012. 04. 25

(21) 申请号 200710169784. 0

(22) 申请日 2007. 11. 20

(73) 专利权人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为  
总部办公楼

(72) 发明人 郑若滨

(74) 专利代理机构 北京挺立专利事务所 11265

代理人 皋吉甫

(51) Int. Cl.

H04L 29/06 (2006. 01)

H04L 9/00 (2006. 01)

(56) 对比文件

CN 1549546 A, 2004. 11. 24,

JP 特開 2001-189761 A, 2001. 07. 10,

CA 2337414 A1, 2001. 08. 19,

审查员 李晓利

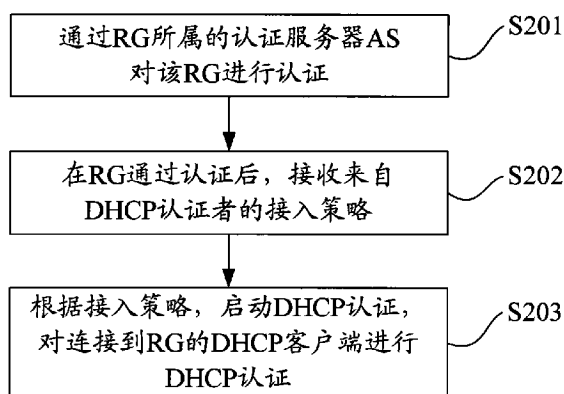
权利要求书 2 页 说明书 10 页 附图 6 页

(54) 发明名称

一种 DHCP 认证的方法、系统和装置

(57) 摘要

本发明实施例公开了一种动态主机配置协议 DHCP 认证的方法, 包括以下步骤: 通过路由网关 RG 所属的认证服务器 AS 对所述 RG 进行认证; 在所述 RG 通过认证后, 接收来自 DHCP 认证者的接入策略; 根据所述接入策略, 启动 DHCP 认证, 对连接到所述 RG 的 DHCP 客户端进行 DHCP 认证。通过本发明实施例, 启动 RG 上的 DHCP 认证, 对连接到 RG 的 DHCP 客户端进行 DHCP 认证, 从而使与 RG 连接的 DHCP 客户端能够通过 RG 进行 DHCP 认证, 以接入网络。



1. 一种动态主机配置协议 DHCP 认证的方法,其特征在于,包括以下步骤:  
通过路由网关 RG 所属的认证服务器 AS 对所述 RG 进行认证;  
在所述 RG 通过认证后,接收来自 DHCP 认证者的接入策略;  
根据所述接入策略,启动 DHCP 认证,对连接到所述 RG 的 DHCP 客户端进行 DHCP 认证。
2. 如权利要求 1 所述 DHCP 认证的方法,其特征在于,所述启动 DHCP 认证具体包括:  
如果启动所述 DHCP 认证为启动 DHCP 认证代理功能对所述 DHCP 客户端进行 DHCP 认证;  
DHCP 认证代理将所述 DHCP 客户端发送的 DHCP Discover 消息按广播或单播的方式转发;  
所述 DHCP 认证代理将承载所述 DHCP Discover 消息的报文源地址改为所述 DHCP 认证代理的地址,并将承载所述 DHCP Discover 消息的报文目的地址改为由所述 RG 通过认证协议下载的下一跳 IP 节点的地址。
3. 如权利要求 2 所述 DHCP 认证的方法,其特征在于,所述下一跳 IP 节点的地址包括:支持 DHCP 认证代理功能的 IP 节点的地址。
4. 如权利要求 2 所述 DHCP 认证的方法,其特征在于,进一步包括:  
当所述下一跳 IP 节点为 IP 边缘节点时,所述 IP 边缘节点接收所述承载 DHCP Discover 消息的报文;  
所述 IP 边缘节点根据不同的虚拟局域网 VLAN 标签决定所述承载 DHCP Discover 消息的报文的转发地址,所述 VLAN 标签是由所述 RG 为不同重的认证分配的。
5. 如权利要求 1 所述 DHCP 认证的方法,其特征在于,所述对连接到 RG 的 DHCP 客户端进行 DHCP 认证进一步包括:  
发送 DHCP 强制更新消息给所述 DHCP 客户端,所述 DHCP 强制更新消息携带认证选项;  
接收所述 DHCP 客户端回复的 DHCP 请求消息,所述 DHCP 请求消息携带所述 DHCP 客户端设置好的认证选项;  
将携带所述认证选项的 DHCP 请求消息转发给 DHCP 认证代理。
6. 一种路由网关 RG,其特征在于,包括:申请认证模块、策略保存模块和执行点 EP 功能模块,还包括动态主机配置协议 DHCP 认证服务器功能模块或 DHCP 认证代理功能模块,  
所述申请认证模块,用于通过所述 RG 所属的认证服务器 AS 对所述 RG 进行认证;  
所述策略保存模块,与所述申请认证模块连接,用于在所述 RG 通过认证后,将来自 DHCP 认证者的接入策略保存到所述 EP 功能模块;  
所述 EP 功能模块,用于保存并执行所述来自 DHCP 认证者的接入策略;  
所述 DHCP 认证服务器功能模块,用于对连接到所述 RG 的 DHCP 客户端进行 DHCP 认证;  
所述 DHCP 认证代理功能模块,用于将接收 DHCP 客户端的 DHCP Discover 消息按广播或单播的方式转发,将承载所述 DHCP Discover 消息的报文源地址改为所述 DHCP 认证代理的地址,并将承载所述 DHCP Discover 消息的报文目的地址改为由所述 RG 通过认证协议下载的下一跳 IP 节点的地址。
7. 如权利要求 6 所述 RG,其特征在于,进一步包括:标签分配模块,用于为不同重的认证分配不同的 VLAN 标签。
8. 一种 IP 边缘节点,其特征在于,包括:

动态主机配置协议 DHCP 认证代理功能模块,用于对 DHCP 认证消息进行中转,将接收自路由网关 RG 的承载 DHCP Discover 消息的报文按广播或单播的方式转发;

DHCP 认证者模块,用于向 DHCP 客户端发送 DHCP 强制更新消息,以及向 RG 下发接入策略。

9. 如权利要求 8 所述 IP 边缘节点,其特征在于,进一步包括:

报文接收模块,用于接收所述 RG 发送的承载 DHCP Discover 消息的报文;

认证区分模块,与所述报文接收模块连接,用于根据不同的虚拟局域网 VLAN 标签决定所述报文接收模块接收的承载 DHCP Discover 消息的报文的 转发地址。

10. 一种动态主机配置协议 DHCP 认证的系统,其特征在于,包括路由网关 RG、IP 边缘节点和认证服务器;

所述 RG,用于通过所述 RG 所属的认证服务器对所述 RG 进行认证,在所述 RG 通过认证后,接收来自 DHCP 认证者的接入策略,并根据所述接入策略,启动 DHCP 认证,对连接到所述 RG 的 DHCP 客户端进行 DHCP 认证;

所述 IP 边缘节点,用于对 DHCP 认证消息进行中转,将接收自所述 RG 的承载 DHCP Discover 消息的报文按广播或单播的方式转发,并向所述 DHCP 客户端转发 DHCP 强制更新消息,以及向所述 RG 下发接入策略;

所述认证服务器,用于对所述认证服务器服务的 RG 进行认证。

11. 如权利要求 10 所述 DHCP 认证的系统,其特征在于,所述 RG 具体包括:申请认证模块、策略保存模块、执行点 EP 功能模块和 DHCP 认证代理功能模块,

所述申请认证模块,用于通过所述 RG 所属的认证服务器对所述 RG 进行认证;

所述策略保存模块,与所述申请认证模块连接,用于在所述 RG 通过认证后,将所述来自 DHCP 认证者的接入策略保存到所述 EP 功能模块;

所述 EP 功能模块,用于保存并执行所述来自 DHCP 认证者的接入策略;

所述 DHCP 认证代理功能模块,用于将接收所述 DHCP 客户端的 DHCP Discover 消息按广播或单播的方式转发,将承载所述 DHCP Discover 消息的报文源地址改为所述 DHCP 认证代理的地址,并将承载所述 DHCP Discover 消息的报文目的地址改为由所述 RG 通过认证协议下载的下一跳 IP 节点的地址。

12. 如权利要求 10 所述 DHCP 认证的系统,其特征在于,所述 IP 边缘节点包括 DHCP 认证代理功能模块和 DHCP 认证者模块,

所述 DHCP 认证代理功能模块,用于对所述 DHCP 认证消息进行中转,将接收自所述 RG 的承载 DHCP Discover 消息的报文按广播或单播的方式转发;

所述 DHCP 认证者模块,用于向所述 DHCP 客户端发送 DHCP 强制更新 消息,以及向所述 RG 下发接入策略。

## 一种 DHCP 认证的方法、系统和装置

### 技术领域

[0001] 本发明涉及网络通信技术领域,特别涉及一种 DHCP 认证的方法、系统和装置。

### 背景技术

[0002] DHCP(Dynamic Host Configuration Protocol,动态主机配置协议)提供了一种动态指定 IP(Internet Protocol,因特网协议)地址和配置参数的机制,该配置参数包括分配的 IP 地址、子网掩码、缺省网关等参数,主要用于大型网络环境和配置比较困难的地方。DHCP 服务器自动为客户机指定 IP 地址,指定的配置参数有些和 IP 协议并不相关,它的配置参数使得网络上的计算机通信变得方便而容易实现了。由于 DHCP 具有配置过程自动实现,所有配置信息都可以由 DHCP 服务器统一管理,不仅能够分配 IP 地址,而且还能够配置其他大量的信息,以及对 IP 地址进行租期管理,实现 IP 地址的分时复用等诸多优点,现在已经得到广泛的应用。

[0003] 在 DHCP 协议中定义的成员包括:DHCP Server、DHCP Relay 和 DHCPClient。其中,DHCP Server 用于提供 DHCP 服务,根据客户端的请求,为客户端分配 IP 地址或其他网络参数,一般存在于路由器、三层交换机或者专门的 DHCP 服务器中;

[0004] DHCP Relay 是在 DHCP Server 和 DHCP Client 间传输 DHCP 报文的设备,能够为不同网段内的 Server 和 Client 传递 DHCP 报文,同时它还提供了安全选项;DHCP Relay 还提供了一种广播报文的透传机制,为不能通过交换机的 DHCP 广播报文提供转发功能,使得 DHCP 服务器可以为不在其本网段的 DHCP 客户端提供服务,Relay 在收到客户端发来的 DHCP 请求报文后,将收到该报文的接口地址填入报文,然后转发,这样 DHCP 服务器根据收到的报文中的接口地址就可以确定需要分配哪个子网的 IP 地址;

[0005] DHCP Client 是网络中利用 DHCP 协议来获取配置参数(如:IP 地址)的主机,即客户主机或者其他能够获取 IP 地址的三层设备。

[0006] 在 DHCP 协议中,DHCP 的报文类型包括以下几种:

[0007] DHCP DISCOVER:由客户端广播来查找可用的服务器。

[0008] DHCP OFFER:服务器用来响应客户端的 DHCP DISCOVER 报文,并指定相应的配置参数。

[0009] DHCP REQUEST:由客户端发送给服务器来请求配置参数或者请求配置确认或者续借租期。

[0010] DHCP ACK:由服务器到客户端,含有配置参数包括 ip 地址。

[0011] DHCP DELINE:当客户端发现地址已经被使用时,用来通知服务器。

[0012] DHCP NAK:由服务器发送给客户端来表明客户端的地址请求不正确或者租期已过期。

[0013] DHCP INFORM:客户端已经有 IP 地址时用它来向服务器请求其他的配置参数。

[0014] DHCP RELEASE:客户端要释放地址时用来通知服务器。

[0015] 租期是整个 DHCP 工作过程的基础。DHCP 服务器提供的每个 IP 地址都有相应的租

用期。“租期”是一个精确的术语,因为 DHCP 服务器允许客户在某个指定的时间内使用某个 IP 地址。当然无论是服务器还是客户端都可以在任何时刻中止租用。

[0016] 当客户端注意到它的租用期到了 50%以上时,就要更新该租用期。这时它直接发送一个 UDP(User Datagram Protocol,用户数据报协议)信息包给获得它的原始信息的服务器。该信息包是一个 DHCP Request 信息包,用以询问是否能保持 TCP(Transmission Control Protocol,传输控制协议)/IP 配置信息并更新它的租用期。如果服务器是可用的,通常会发送一个 DHCP Ack 信息包给客户端,同意客户端的请求。

[0017] 当租用期达到期满时间的近 87.5%时,客户端如果在前一次请求,即 50%后的请求中没能更新租用期的话,则会再次试图更新租用期。如果这次更新失败的话,客户端就会试着与任何一个 DHCP 服务器联系以获得一个有效的 IP 地址。如果另外的一个 DHCP 服务器能够分配一个新的 IP 地址,则该客户端再次进入捆绑状态。如果客户端当前的 IP 地址租用期满,则客户端必须放弃该 IP 地址,重新进入初始化状态,然后重复整个过程。

[0018] 现有的 DHCP 认证采用两个 DHCPv4(DHCP 版本 4)消息:DHCPAuth-request 和 DHCP Auth-response,或者采用一个 DHCPv4 消息:DHCP EAP(Extensible Authentication Protocol,可扩展认证协议);以及两个新的 DHCP Option(选项):auth-proto Option 和 EAP-Message Option。现有的 DHCP 认证流程如图 1 所示:

[0019] S101,当 RG(Routing Gateway,路由网关)接入到网络时,发送 DHCPDiscover(动态主机配置协议的发现报文)给 BNG(Broadband NetworkGateway,宽带网络网关),并通过认证选项表明 DHCP Client 支持的认证模式;

[0020] S102, BNG 直接在 DHCP Auth-request 消息或 DHCP EAP 消息中承载向 RG 发出的 EAP 消息,进入认证过程;

[0021] S103, RG 接收到 DHCP Auth-request 消息或 DHCP EAP 消息后, RG 发送 DHCP Auth-response 承载 EAP 消息给 BNG;

[0022] S104, BNG 将 RG 的 EAP 消息重新封装在 AAA(Authentication Authorization and Accounting,认证、授权和计费)消息中发送给 AS(Authentication Server,认证服务器);

[0023] S105, AS 最终将 DHCP 服务器的认证结果通知 BNG 或 ISP(Internet Service Provider,因特网服务提供商);若认证成功,则将 EAP success 消息封装在 AAA 消息中发送给 BNG;

[0024] S106, BNG 构造 DHCP Offer 消息承载 EAP success 消息发送给 RG,其中 yiaddr 项包含预分配给用户的 IP 地址;

[0025] S107, RG 向 BNG 发送 DHCP Request 信息包,以请求配置参数;

[0026] S108, BNG 向 RG 回复 DHCP Ack 信息包,该信息包中含有配置参数,包括 IP 地址。

[0027] 在实现本发明的过程中,发明人发现现有技术至少存在以下问题:

[0028] 当 RG 为路由网关,即 RG 为三层设备时,现有的 DHCP 认证广播消息(如 DHCP Discover)无法穿越 RG,从而导致 RG 之后的用户无法进行 DHCP 认证。

[0029] 发明内容

[0030] 本发明实施例提供一种 DHCP 认证的方法、系统和装置,以实现与 RG 连接的 DHCP 客户端能够通过 RG 进行 DHCP 认证,以接入网络。

[0031] 为达到上述目的,本发明实施例一方面提供一种动态主机配置协议 DHCP 认证的

方法,包括以下步骤:通过路由网关 RG 所属的认证服务器 AS 对所述 RG 进行认证;在所述 RG 通过认证后,接收来自 DHCP 认证者的接入策略;根据所述接入策略,启动 DHCP 认证,对连接到所述 RG 的 DHCP 客户端进行 DHCP 认证。

[0032] 另一方面,本发明实施例还提供一种路由网关 RG,包括:申请认证模块、策略保存模块和执行点 EP 功能模块,还包括动态主机配置协议 DHCP 认证服务器功能模块或 DHCP 认证代理功能模块,所述申请认证模块,用于通过所述 RG 所属的认证服务器 AS 对所述 RG 进行认证;所述策略保存模块,与所述申请认证模块连接,用于在所述 RG 通过认证后,将来自 DHCP 认证者的接入策略保存到所述 EP 功能模块;所述 EP 功能模块,用于保存并执行所述来自 DHCP 认证者的接入策略;所述 DHCP 认证服务器功能模块,用于对连接到所述 RG 的 DHCP 客户端进行 DHCP 认证;所述 DHCP 认证代理功能模块,用于将接收 DHCP 客户端的 DHCP Discover 消息按广播或单播的方式转发,将承载所述 DHCP Discover 消息的报文源地址改为所述 DHCP 认证代理的地址,并将承载所述 DHCP Discover 消息的报文目的地址改为由所述 RG 通过认证协议下载的下一跳 IP 节点的地址。

[0033] 再一方面,本发明实施例还提供一种 IP 边缘节点,包括:DHCP 认证代理功能模块,用于对 DHCP 认证消息进行中转,将接收自路由器网关 RG 的承载 DHCP Discover 消息的报文按广播或单播的方式转发;DHCP 认证者模块,用于向 DHCP 客户端发送 DHCP 强制更新消息。

[0034] 再一方面,本发明实施例还提供一种 DHCP 认证的系统,包括 RG、IP 边缘节点和认证服务器,所述 RG,用于通过所述 RG 所属的认证服务器对所述 RG 进行认证,在所述 RG 通过认证后,接收来自 DHCP 认证者的接入策略,并根据所述接入策略,启动 DHCP 认证,对连接到所述 RG 的 DHCP 客户端进行 DHCP 认证;所述 IP 边缘节点,用于对 DHCP 认证消息进行中转,将接收自所述 RG 的承载 DHCP Discover 消息的报文按广播或单播的方式转发,并向所述 DHCP 客户端转发 DHCP 强制更新消息,以及向所述 RG 下发接入策略;所述认证服务器,用于对所述认证服务器服务的 RG 进行认证。

[0035] 与现有技术相比,本发明实施例具有以下优点:通过本发明实施例,启动 RG 上的 DHCP 认证,对连接到该 RG 的 DHCP 客户端进行 DHCP 认证。从而使与 RG 连接的 DHCP 客户端能够通过 RG 进行 DHCP 认证,以接入网络。

[0036] 附图说明

[0037] 图 1 为现有技术 DHCP 认证的流程图;

[0038] 图 2 为本发明实施例 DHCP 认证的方法的流程图;

[0039] 图 3 为本发明 DHCP 认证的方法实施例一的流程图;

[0040] 图 4 为本发明实施例支持 DHCP 认证服务器功能的路由网关的示意图;

[0041] 图 5 为本发明 DHCP 认证的方法实施例二的流程图;

[0042] 图 6 为本发明实施例支持 DHCP 认证代理功能的路由网关的示意图;

[0043] 图 7 为本发明 DHCP 认证的方法实施例三的流程图;

[0044] 图 8 为本发明 DHCP 认证的方法实施例四的流程图;

[0045] 图 9 为本发明 DHCP 认证的方法实施例五的流程图;

[0046] 图 10 为本发明 DHCP 认证的方法实施例六的流程图;

[0047] 图 11 为本发明实施例 DHCP 认证的系统的结构图。

[0048] 具体实施方式

[0049] 本发明实施例提供一种 DHCP 认证的方法,通过启动 RG 上的 DHCP 认证,对连接到该 RG 的 DHCP 客户端进行 DHCP 认证。从而使与 RG 连接的 DHCP 客户端能够通过 RG 进行 DHCP 认证,以接入网络。在 RG 上配置 DHCP 认证服务器功能或 DHCP 认证代理功能之后,DHCP 认证消息能够穿越 IP 节点,实现了 DHCP 认证消息跨越不同的 IP 域,使 IP Wholesale(批发)的跨 IP 域批发业务成为可能,为下一代基于 IP 的接入网奠定了技术基础。

[0050] 如图 2 所示,为本发明实施例 DHCP 认证的方法的流程图,具体包括以下步骤:

[0051] 步骤 S201,通过 RG 所属的认证服务器 AS 对该 RG 进行认证。RG 支持双重认证和 EP(Enforcement Point,执行点)功能, RG 作为 Suppliant(认证申请者)通过 RG 所属的 AS 对该 RG 进行认证。

[0052] 步骤 S202,在 RG 通过认证后,接收来自 DHCP 认证者的接入策略。在 RG 通过认证后,通过 DHCP 认证者下载接入策略到 RG 的 EP 功能模块,完成 RG 上的 DHCP 认证服务器功能或 DHCP 认证代理功能的配置。当然也可以静态配置 RG 上的 DHCP 认证服务器功能或 DHCP 认证代理功能。

[0053] 步骤 S203,根据接入策略,启动 DHCP 认证,对连接到 RG 的 DHCP 客户端进行 DHCP 认证,从而使与 RG 之后的 DHCP 客户端能够通过 RG 进行 DHCP 认证,以接入网络。RG 的 EP 功能模块执行 RG 下载的或静态配置到 RG 上的接入策略,启动 RG 的 DHCP 认证,即启动 RG 的 DHCP 认证服务器功能或 DHCP 认证代理功能,对连接到 RG 的 DHCP 客户端进行 DHCP 认证。

[0054] RG 为不同重的认证打不同的 VLAN(Virtual Local Area Network,虚拟局域网),例如第一重认证报文打 VLAN1,第二重认证报文打 VLAN2, IP 边缘节点通过不同的 VLAN 区分不同的认证,以决定将认证报文送往 DHCP 认证代理功能模块,还是将认证报文送往 DHCP 认证者功能模块,例如:对于 VLAN1 的认证报文将被送往 DHCP 认证者功能模块处理,对于 VLAN2 的认证报文将被送往 DHCP 认证代理功能模块处理。

[0055] 在对连接到 RG 的 DHCP 客户端进行 DHCP 认证之后,还可由网络侧或 DHCP 客户端触发重认证过程,这时 DHCP 认证代理为 DHCP 客户端和 DHCP 认证者 /DHCP 服务器中转 DHCP 认证消息。

[0056] 上述 DHCP 认证的方法,在 RG 上配置 DHCP 认证服务器功能或 DHCP 认证代理功能,从而使与 RG 连接的 DHCP 客户端能够通过 RG 进行 DHCP 认证,以接入网络。另外,在 RG 上配置 DHCP 认证服务器功能或 DHCP 认证代理功能之后,DHCP 认证消息能够穿越 IP 节点,从而实现了 DHCP 认证消息跨越不同的 IP 域,使跨 IP 域的批发业务成为可能,为下一代基于 IP 的接入网奠定了技术基础。

[0057] 如图 3 所示,为本发明 DHCP 认证的方法实施例一的流程图,本发明实施例提出一种支持 DHCP 认证服务器功能的路由网关 RG,该 RG 与接入网和 IP 边缘节点以及认证服务器的连接示意图,如图 4 所示,从而使与 RG 连接的 DHCP 客户端能够通过 RG 上的 DHCP 认证服务器进行 DHCP 认证,以接入网络。

[0058] 优选地, RG 支持双重认证和 EP 功能, RG 作为认证申请者通过 RG 所属的 AS 进行 RG 认证;RG 认证通过后,通过认证者下载接入策略到 RG 的 EP;EP 执行接入策略,启动 RG 的 DHCP 认证服务器功能,对 RG 之后的用户进行 DHCP 认证。具体包括以下步骤:

[0059] 步骤 S301, RG 作为认证申请者通过 RG 所属的 AS 进行 RG 认证,该 RG 认证可采用

DHCP 认证；

[0060] 步骤 S302, RG 认证通过后,通过认证者下载接入策略到 RG 的 EP；

[0061] 步骤 S303, EP 执行接入策略,启动 RG 的 DHCP 认证服务器功能；

[0062] 步骤 S304, 连接到 RG 的 DHCP 客户端向 RG 发送 DHCP Discover 消息包,该 DHCP Discover 消息包携带认证选项(auth-proto Option)。

[0063] 步骤 S305, RG 在 DHCP 认证请求消息中承载向 DHCP 客户端发出的 EAP 信息,进入认证过程。

[0064] 步骤 S306, DHCP 客户端接收到 DHCP 认证请求消息后,发送携带 EAP 信息的 DHCP 认证响应消息给 RG。

[0065] 步骤 S307, RG 向 AS 发送携带 EAP 信息的接入请求(Access-Request)消息。

[0066] 步骤 S308, AS 向 RG 发送携带 EAP 信息的允许接入(Access-Accept)消息。

[0067] 步骤 S309, RG 构造携带 EAP success 消息的 DHCP Offer 消息,发送给 DHCP 客户端,其中 yiaddr 项包含预分配给用户的 IP 地址。

[0068] 步骤 S310, DHCP 客户端向 RG 发送 DHCP 请求信息包,以请求配置参数；

[0069] 步骤 S311, RG 向 DHCP 客户端回复 DHCP Ack 信息包,该信息包中含有配置参数,包括 IP 地址。

[0070] 其中,还可以在 RG 上静态配置 DHCP 认证服务器功能,则步骤 S301 和步骤 S302 可省略。

[0071] 如图 5 所示,为本发明 DHCP 认证的方法实施例二的流程图,本发明实施例提出一种支持 DHCP 认证代理功能的路由网关,如图 6 所示,从而使连接到 RG 的 DHCP 客户端能够通过 RG 上的 DHCP 认证代理进行 DHCP 认证,以接入网络。

[0072] 另外,如图 6(b),如果 DHCP 客户端和 DHCP 认证者或 DHCP 服务器之间有任何 IP 节点,不是 DHCP 认证者或 DHCP 服务器,则该 IP 节点也必须支持 DHCP 认证代理功能;本发明实施例提出一种支持 DHCP 认证代理功能和 DHCP 认证者功能的 IP 边缘节点,用于 DHCP 认证消息的中转,能够实现 DHCP 认证消息穿越 IP 节点的功能。RG 为不同重的认证分配不同的 VLAN 标签,例如第一重认证报文打 VLAN1,第二重认证报文打 VLAN2。这样,IP 边缘节点通过不同的 VLAN 标签就可区分不同的认证,以决定是将认证报文送往 DHCP 认证代理功能模块,还是将认证报文送往 DHCP 认证者功能模块。例如:标签为 VLAN1 的认证报文将被送往 DHCP 认证者功能模块处理,标签为 VLAN2 的认证报文将被送往 DHCP 认证代理功能模块处理。

[0073] 在进入认证之前,优选地, RG 支持双重认证和 EP 功能, RG 作为认证申请者通过 RG 所属的 AS 进行 RG 认证; RG 认证通过后,通过认证者下载接入策略到 RG 的 EP; EP 执行接入策略,启动 RG 的 DHCP 认证代理功能,对连接到 RG 的 DHCP 客户端进行 DHCP 认证。

[0074] 步骤 S501, 连接到 RG 的 DHCP 客户端向 DHCP 认证代理发送 DHCP Discover 广播报文,该 DHCP Discover 广播报文携带认证选项。

[0075] 步骤 S502, DHCP 认证代理收到 DHCP Discover 消息后,仍将 DHCP Discover 消息按广播方式转发,将承载 DHCP Discover 消息的报文源地址改为 DHCP 认证代理的地址;或者,

[0076] DHCP 认证代理收到 DHCP Discover 消息后,将 DHCP Discover 消息按单播方式转发,将承载 DHCP Discover 消息的报文源地址改为 DHCP 认证代理的地址,将承载 DHCP

Discover 消息的报文目的地址改为下一跳 IP 节点的地址,通常为 DHCP 认证者或 DHCP 服务器的地址;如果下一跳 IP 节点不是 DHCP 认证者或 DHCP 服务器,下一跳 IP 节点也必须支持 DHCP 认证代理功能,如图 6(b) 所示的 IP 边缘节点。

[0077] 其中,下一跳 IP 节点的地址是在 RG 认证通过后,通过认证协议下载到 RG 获得的,以供广播转单播时使用。

[0078] 步骤 S503,DHCP 认证者或 DHCP 服务器向 DHCP 认证代理发送携带 EAP 请求 / 身份的 DHCP 认证请求消息。

[0079] 步骤 S504,DHCP 认证代理将携带 EAP 请求 / 身份的 DHCP 认证请求消息向 DHCP 客户端转发。

[0080] 步骤 S505,DHCP 客户端向 DHCP 认证代理回复 DHCP 认证响应消息,该 DHCP 认证响应消息携带 EAP 响应 / 身份消息。

[0081] 步骤 S506,DHCP 认证代理将携带 EAP 响应 / 身份消息的 DHCP 认证响应消息向 DHCP 认证者或 DHCP 服务器转发。

[0082] 步骤 S507, DHCP 认证代理与 DHCP 客户端交互携带 EAP Method 的 DHCP 认证请求 / 响应消息。

[0083] 步骤 S508, DHCP 认证代理与 DHCP 认证者或 DHCP 服务器交互携带 EAP Method 的 DHCP 认证请求 / 响应消息。

[0084] 步骤 S509, DHCP 认证者或 DHCP 服务器构造 DHCP Offer 消息承载 EAPSuccess/Failure 消息发送给 DHCP 认证代理。

[0085] 步骤 S510, DHCP 认证代理将承载 EAP Success/Failure 消息的 DHCP Offer 消息发送给 DHCP 客户端。

[0086] 步骤 S511, DHCP 客户端向 DHCP 认证代理发送 DHCP Request 信息包,以请求配置参数。

[0087] 步骤 S512, DHCP 认证代理向 DHCP 认证者或 DHCP 服务器转发 DHCPRequest 信息包。

[0088] 步骤 S513,DHCP 认证者或 DHCP 服务器向 DHCP 认证代理回复 DHCP Ack 信息包,该信息包中含有配置参数,包括 IP 地址。

[0089] 步骤 S514, DHCP 认证代理向 DHCP 客户端转发 DHCP Ack 信息包,该信息包中含有配置参数,包括 IP 地址。

[0090] 上述 DHCP 认证的方法与现有技术不同的是:现有技术中 DHCP 认证广播消息无法穿越 RG,而本发明实施例引入 DHCP 认证代理做 DHCP 认证消息的中转,特别是对 DHCP 认证广播消息,例如认证用的 DHCP Discover 消息进行转发。

[0091] 如图 7 所示,为本发明 DHCP 认证的方法实施例三流程图,当网络侧重认证定时器到时触发重认证,或网络侧其它事件触发重认证时,进入重认证过程,具体包括以下步骤:

[0092] 步骤 S701,DHCP 认证代理直接向 DHCP 客户端发送 DHCP 认证请求消息或 DHCP EAP 消息,承载向 DHCP 客户端发出的 EAP 请求 / 身份消息,进入重认证过程;或者,DHCP 认证者或 DHCP 服务器通过 DHCP 认证代理向 DHCP 客户端转发 DHCP 认证请求消息或 DHCP EAP 消息,承载向 DHCP 客户端发出的 EAP 请求 / 身份消息,进入重认证过程,即 IP 会话进入重建

立过程。

[0093] 步骤 S702, DHCP 客户端向 DHCP 认证代理回复 DHCP 认证响应消息, 该 DHCP 认证响应消息携带 EAP 响应 / 身份消息。

[0094] 步骤 S703, DHCP 认证代理将携带 EAP 响应 / 身份消息的 DHCP 认证响应消息向 DHCP 认证者或 DHCP 服务器转发。

[0095] 步骤 S704, DHCP 认证代理与 DHCP 客户端交互携带 EAP Method 的 DHCP 认证请求 / 响应消息。

[0096] 步骤 S705, DHCP 认证代理与 DHCP 认证者或 DHCP 服务器交互携带 EAP Method 的 DHCP 认证请求 / 响应消息。

[0097] 步骤 S706, DHCP 认证者或 DHCP 服务器构造 DHCP Offer 消息承载 EAP Success / Failure 消息发送给 DHCP 认证代理。

[0098] 步骤 S707, DHCP 认证代理将承载 EAP Success / Failure 消息的 DHCP Offer 消息发送给 DHCP 客户端。

[0099] 如图 8 所示, 为本发明 DHCP 认证的方法实施例四的流程图, 当网络侧重认证定时器到时触发重认证, 或网络侧其它事件触发重认证时, 进入重认证过程, 具体包括以下步骤:

[0100] 步骤 S801, DHCP 认证代理直接向 DHCP 客户端发送 DHCP 强制更新消息, 消息携带认证选项 (auth-proto Option), 以要求 DHCP 客户端进行重认证; 或者, DHCP 认证者或 DHCP 服务器通过 DHCP 认证代理向 DHCP 客户端转发 DHCP 强制更新消息, 消息携带认证选项 (auth-proto Option), 以要求 DHCP 客户端进行重认证, 即 IP 会话进入重建过程;

[0101] 步骤 S802, DHCP 客户端回复 DHCP 请求消息, 该 DHCP 请求消息携带认证选项 (auth-proto Option), 表明 DHCP 客户端已准备好进行重认证, DHCP 认证者或 DHCP 服务器可以发起重认证。

[0102] 步骤 S803, DHCP 认证代理将携带认证选项的 DHCP 请求消息转发给 DHCP 认证者或 DHCP 服务器。

[0103] 步骤 S804, DHCP 认证者或 DHCP 服务器向 DHCP 认证代理发送 DHCP 认证请求消息, 该 DHCP 认证请求消息携带 EAP 请求 / 身份消息。

[0104] 步骤 S805, DHCP 认证代理向 DHCP 客户端转发 DHCP 认证请求消息, 该 DHCP 认证请求消息携带 EAP 请求 / 身份消息。

[0105] 步骤 S806, DHCP 客户端向 DHCP 认证代理回复 DHCP 认证响应消息, 该 DHCP 认证响应消息携带 EAP 响应 / 身份消息。

[0106] 步骤 S807, DHCP 认证代理将携带 EAP 响应 / 身份消息的 DHCP 认证响应消息向 DHCP 认证者或 DHCP 服务器转发。

[0107] 步骤 S808, DHCP 认证代理与 DHCP 客户端交互携带 EAP Method 的 DHCP 认证请求 / 响应消息。

[0108] 步骤 S809, DHCP 认证代理与 DHCP 认证者或 DHCP 服务器交互携带 EAP Method 的 DHCP 认证请求 / 响应消息。

[0109] 步骤 S810, DHCP 认证者或 DHCP 服务器向 DHCP 认证代理回复认证结果, 其中 EAP Success 消息由 DHCP Ack 消息携带, EAP Failure 消息由 DHCP Nack 消息携带。该 DHCP

Ack 消息携带 IP 地址,该 IP 地址可以为 DHCP 认证者或 DHCP 服务器为 DHCP 客户端重新分配的 IP 地址,也可以为 DHCP 客户端通过第一次认证获得的 IP 地址。

[0110] 步骤 S811, DHCP 认证代理将认证结果向 DHCP 客户端转发,其中 EAPSuccess 消息由 DHCP Ack 消息携带, EAP Failure 消息由 DHCP Nack 消息携带。该 DHCP Ack 消息携带 IP 地址,该 IP 地址可以为 DHCP 认证者或 DHCP 服务器为 DHCP 客户端重新分配的 IP 地址,也可以为 DHCP 客户端通过第一次认证获得的 IP 地址。

[0111] 如图 9 所示,为本发明 DHCP 认证的方法实施例五的流程图,当网络侧重认证定时器到时触发重认证,或网络侧其它事件触发重认证时,进入重认证过程,具体包括以下步骤:

[0112] 步骤 S901, DHCP 认证代理直接向 DHCP 客户端发送 DHCP 强制更新 (DHCP Forcerenew) 消息,消息携带认证选项 (auth-proto Option),以要求 DHCP 客户端进行重认证;或者, DHCP 认证者或 DHCP 服务器通过 DHCP 认证代理向 DHCP 客户端转发 DHCP 强制更新消息,消息携带认证选项 (auth-protoOption),以要求 DHCP 客户端进行重认证,即 IP 会话进入重建过程;

[0113] 步骤 S902, DHCP 客户端回复 DHCP 请求消息,该 DHCP 请求消息携带认证选项 (auth-proto Option),表明 DHCP 客户端已准备好进行重认证, DHCP 认证者或 DHCP 服务器可以发起重认证。

[0114] 步骤 S903, DHCP 认证代理将携带认证选项的 DHCP 请求消息转发给 DHCP 认证者或 DHCP 服务器。

[0115] 步骤 S904, DHCP 认证者或 DHCP 服务器向 DHCP 认证代理发送 DHCP Ack 消息,该 DHCP Ack 消息携带 EAP 请求 / 身份消息。

[0116] 步骤 S905, DHCP 认证代理将携带 EAP 请求 / 身份消息的 DHCP Ack 消息向 DHCP 客户端转发。

[0117] 步骤 S906, DHCP 客户端向 DHCP 认证代理回复 DHCP 认证响应消息,该 DHCP 认证响应消息携带 EAP 响应 / 身份消息。

[0118] 步骤 S907, DHCP 认证代理将携带 EAP 响应 / 身份消息的 DHCP 认证响应消息向 DHCP 认证者或 DHCP 服务器转发。

[0119] 步骤 S908, DHCP 认证代理与 DHCP 客户端交互携带 EAP Method 的 DHCP Request/Ack 消息。

[0120] 步骤 S909, DHCP 认证代理与 DHCP 认证者或 DHCP 服务器交互携带 EAPMethod 的 DHCP Request/Ack 消息。

[0121] 步骤 S910, DHCP 认证者或 DHCP 服务器向 DHCP 认证代理回复认证结果,其中 EAP Success 消息由 DHCP Ack 消息携带, EAP Failure 消息由 DHCP Nack 消息携带。该 DHCP Ack 消息携带 IP 地址,该 IP 地址可以为 DHCP 认证者或 DHCP 服务器为 DHCP 客户端重新分配的 IP 地址,也可以为 DHCP 客户端通过第一次认证获得的 IP 地址。

[0122] 步骤 S911, DHCP 认证代理将认证结果向 DHCP 客户端转发,其中 EAPSuccess 消息由 DHCP Ack 消息携带, EAP Failure 消息由 DHCP Nack 消息携带。该 DHCP Ack 消息携带 IP 地址,该 IP 地址可以为 DHCP 认证者或 DHCP 服务器为 DHCP 客户端重新分配的 IP 地址,也可以为 DHCP 客户端通过第一次认证获得的 IP 地址。

[0123] 如图 10 所示,为本发明 DHCP 认证的方法实施例六的流程图,当用户侧重认证定时器到时触发重认证,或用户侧其它事件触发重认证时,进入重认证过程,具体包括以下步骤:

[0124] 步骤 S1001, DHCP 客户端向 DHCP 认证代理发送 DHCP 请求消息,携带认证选项(auth-proto Option),表明用户要求进行重认证,该报文可以为单播报文或广播报文。

[0125] 步骤 S1002, DHCP 认证代理将携带认证选项的 DHCP 请求消息转发给 DHCP 认证者或 DHCP 服务器,如果 DHCP 客户端发送的 DHCP 请求消息为广播报文,则需转换为广播/单播报文。

[0126] 步骤 S1003, DHCP 认证者或 DHCP 服务器向 DHCP 认证代理发送 DHCP 认证请求消息,该 DHCP 认证请求消息携带 EAP 请求/身份消息。

[0127] 步骤 S1004, DHCP 认证代理向 DHCP 客户端转发 DHCP 认证请求消息,该 DHCP 认证请求消息携带 EAP 请求/身份消息。

[0128] 步骤 S1005, DHCP 客户端向 DHCP 认证代理回复 DHCP 认证响应消息,该 DHCP 认证响应消息携带 EAP 响应/身份消息。

[0129] 步骤 S1006, DHCP 认证代理将携带 EAP 响应/身份消息的 DHCP 认证响应消息向 DHCP 认证者或 DHCP 服务器转发。

[0130] 步骤 S1007, DHCP 认证代理与 DHCP 客户端交互携带 EAP Method 的 DHCP 认证请求/响应消息。

[0131] 步骤 S1008, DHCP 认证代理与 DHCP 认证者或 DHCP 服务器交互携带 EAPMethod 的 DHCP 认证请求/响应消息。

[0132] 步骤 S1009, DHCP 认证者或 DHCP 服务器向 DHCP 认证代理回复认证结果,其中 EAP Success 消息由 DHCP Ack 消息携带, EAP Failure 消息由 DHCPNack 消息携带。该 DHCP Ack 消息携带 IP 地址,该 IP 地址可以为 DHCP 认证者或 DHCP 服务器为 DHCP 客户端重新分配的 IP 地址,也可以为 DHCP 客户端通过第一次认证获得的 IP 地址。

[0133] 步骤 S1011, DHCP 认证代理将认证结果向 DHCP 客户端转发,其中 EAPSuccess 消息由 DHCP Ack 消息携带, EAP Failure 消息由 DHCP Nack 消息携带。该 DHCP Ack 消息携带 IP 地址,该 IP 地址可以为 DHCP 认证者或 DHCP 服务器为 DHCP 客户端重新分配的 IP 地址,也可以为 DHCP 客户端通过第一次认证获得的 IP 地址。

[0134] 上述 DHCP 认证的方法与现有的 DHCP 认证过程相比,不同之处在于:本发明实施例由 DHCP 认证代理实现 DHCP 客户端和 DHCP 认证者或 DHCP 服务器之间的 DHCP 认证消息的中转。

[0135] 如图 11 所示,为本发明实施例 DHCP 认证的系统的结构图,包括:RG1、IP 边缘节点 2 和认证服务器 3,

[0136] RG1,用于通过 RG1 所属的认证服务器 3 对 RG1 进行认证,在 RG1 通过认证后,接收来自 DHCP 认证者的接入策略,并根据接入策略,启动 DHCP 认证,对连接到 RG1 的 DHCP 客户端进行 DHCP 认证;

[0137] IP 边缘节点 2,用于对 DHCP 认证消息进行中转,将接收自 RG1 的承载 DHCP Discover 消息的报文按广播或单播的方式转发,并向 DHCP 客户端转发 DHCP 强制更新消息,以及向 RG1 下发接入策略;

- [0138] 认证服务器 3,用于对认证服务器 3 服务的 RG1 进行认证。
- [0139] 其中, RG1 具体包括 :申请认证模块 11、策略保存模块 12 和 EP 功能模块 13,
- [0140] 申请认证模块 11,用于通过 RG1 所属的认证服务器 3 对 RG1 进行认证 ;
- [0141] 策略保存模块 12,与申请认证模块 11 连接,用于在 RG1 通过认证后,将来自 DHCP 认证者的接入策略保存到 EP 功能模块 13 ;
- [0142] EP 功能模块 13,用于保存并执行来自 DHCP 认证者的接入策略。
- [0143] 其中, IP 边缘节点 2 包括 DHCP 认证代理功能模块 21 和 DHCP 认证者模块 22,
- [0144] DHCP 认证代理功能模块 21,用于对 DHCP 认证消息进行中转,将接收自 RG1 的承载 DHCP Discover 消息的报文按广播或单播的方式转发 ;
- [0145] DHCP 认证者模块 22,用于向 DHCP 客户端发送 DHCP 强制更新消息,以及向 RG1 下发接入策略。
- [0146] 其中, RG1 进一步包括 :DHCP 认证服务器功能模块 14,用于对连接到 RG1 的 DHCP 客户端进行 DHCP 认证。
- [0147] 其中, RG1 进一步包括 :DHCP 认证代理功能模块 15,用于将接收自 DHCP 客户端的 DHCP Discover 消息按广播或单播的方式转发,将承载 DHCPDiscover 消息的报文源地址改为该 DHCP 认证代理的地址,并将承载 DHCPDiscover 消息的报文目的地址改为由 RG1 通过认证协议下载的下一跳 IP 节点的地址。
- [0148] 其中, RG1 进一步包括 :标签分配模块 16,用于为不同重的认证分配不同的 VLAN 标签。
- [0149] 其中, IP 边缘节点 2 进一步包括 :报文接收模块 23,用于接收 RG1 发送的承载 DHCP Discover 消息的报文 ;
- [0150] 认证区分模块 24,与报文接收模块 23 连接,用于根据不同的虚拟局域网 VLAN 标签决定所述报文接收模块接收的承载 DHCP Discover 消息的报文的转发地址。
- [0151] 上述 DHCP 认证的系统, RG1 通过 RG1 所属的认证服务器 3 对 RG1 进行认证,在 RG1 通过认证后,接收来自 DHCP 认证者的接入策略,并根据接入策略,启动 DHCP 认证,对连接到 RG1 的 DHCP 客户端进行 DHCP 认证。另外,在 RG1 上配置了 DHCP 认证服务器功能模块 14 或 DHCP 认证代理功能模块 15,以及在 IP 边缘节点 2 上配置了 DHCP 认证代理模块 21 和 DHCP 认证者模块 22 之后, DHCP 认证消息能够穿越 IP 节点,从而实现了 DHCP 认证消息跨越不同的 IP 域,使跨 IP 域的批发业务成为可能,为下一代基于 IP 的接入网奠定了技术基础。
- [0152] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本发明各个实施例所述的方法。
- [0153] 以上公开的仅为本发明的几个具体实施例,但是,本发明并非局限于此,任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

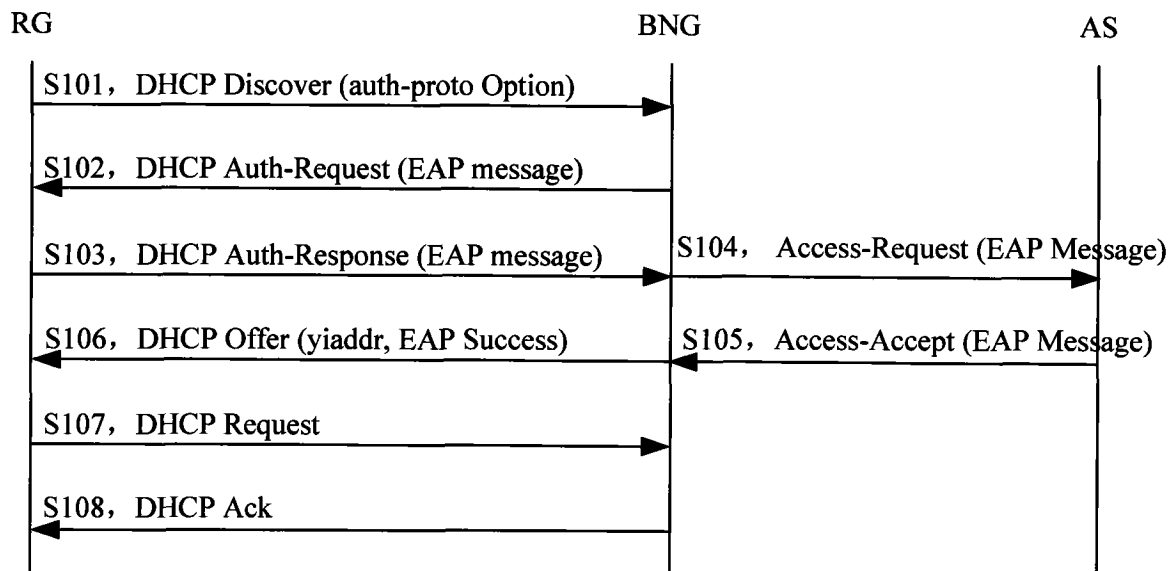


图 1

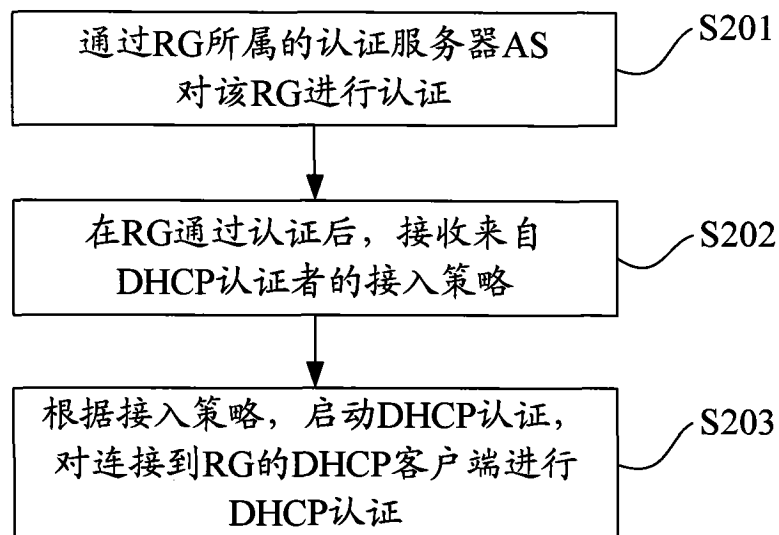


图 2

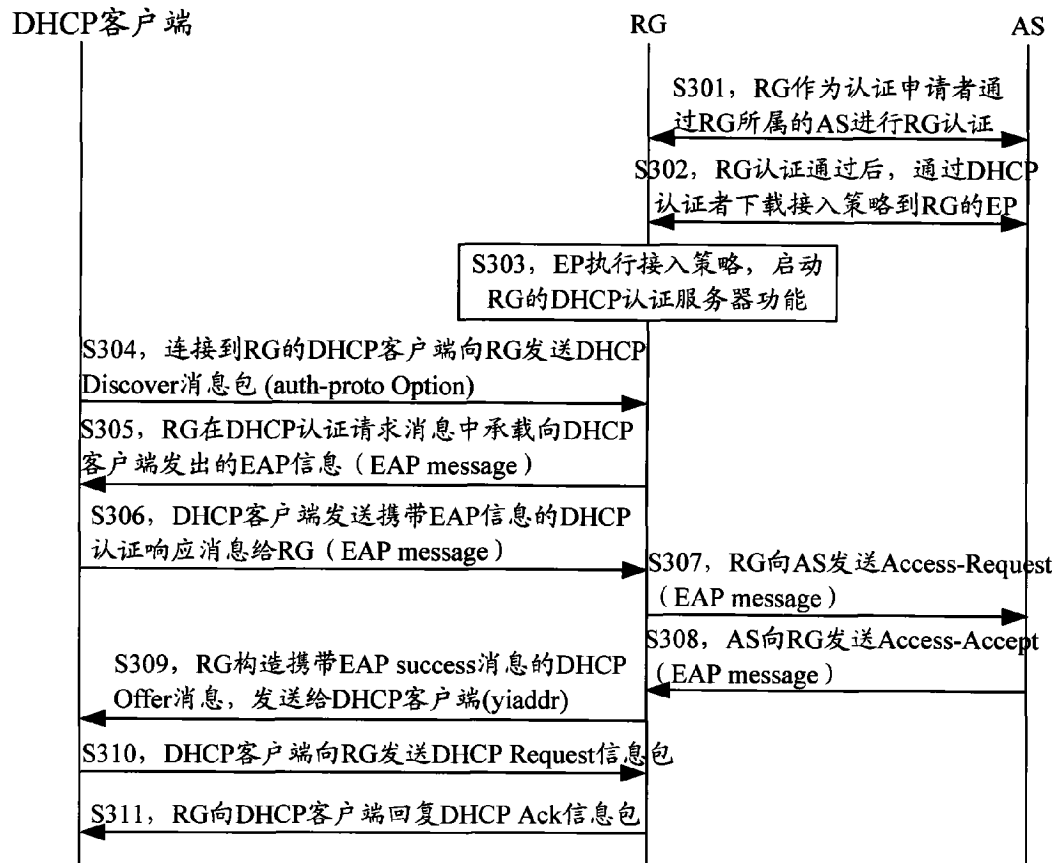


图 3

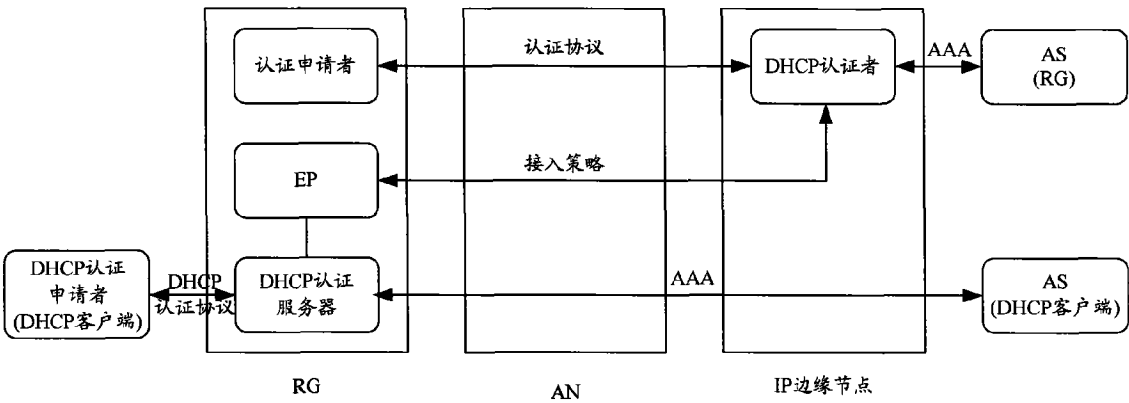


图 4

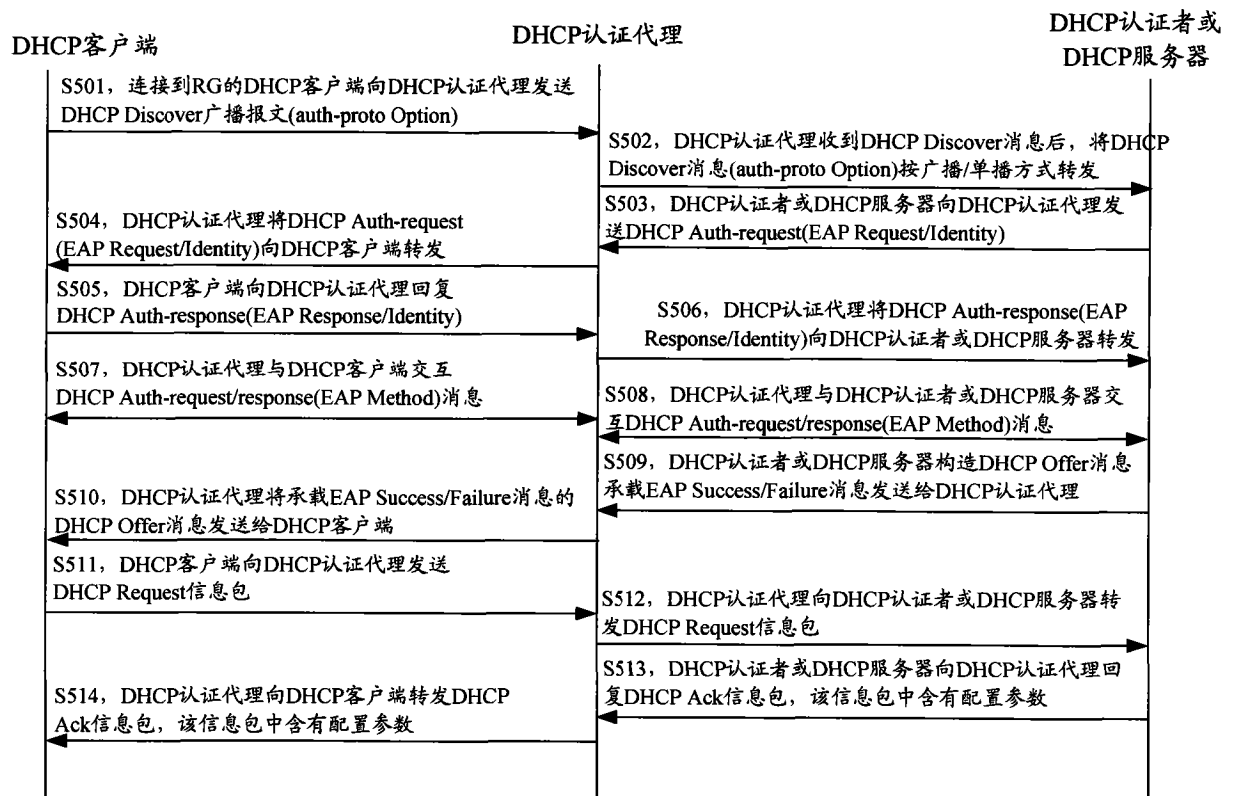
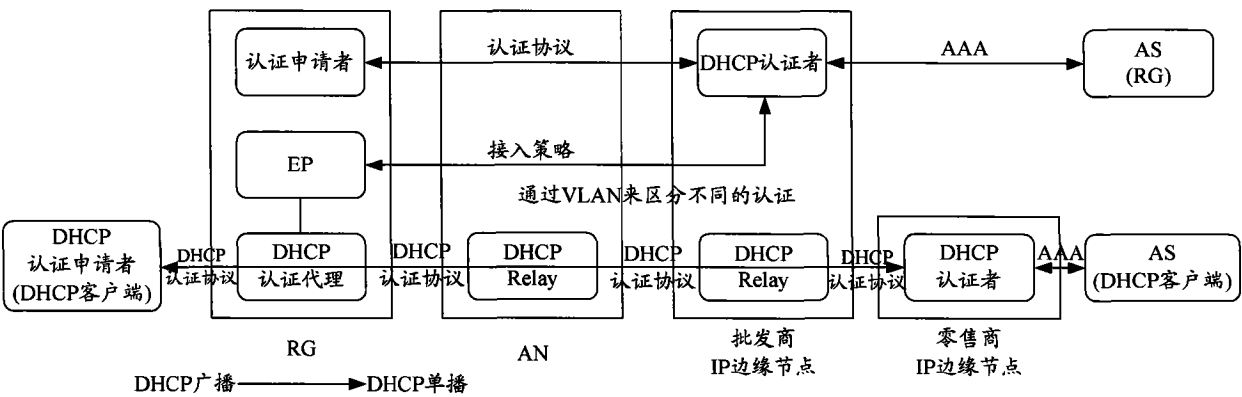
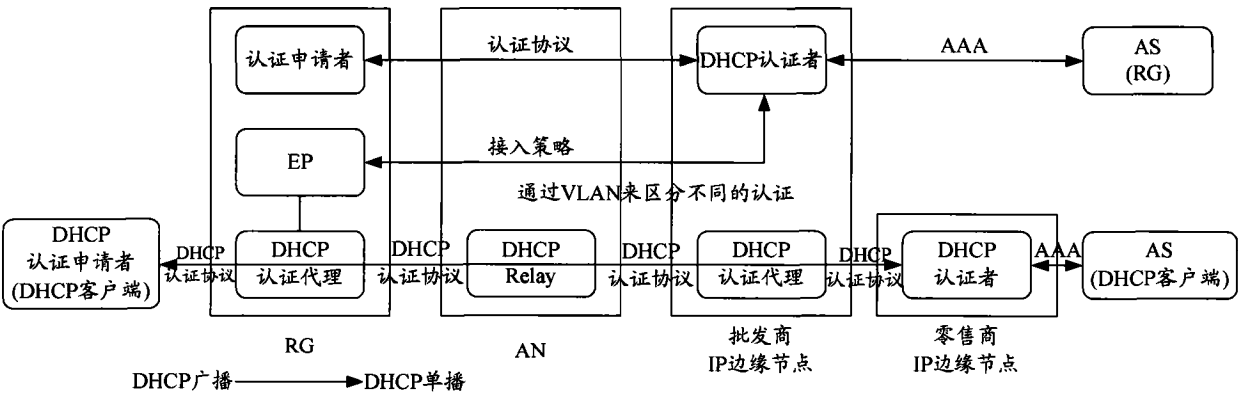


图 5



(a)



(b)

图 6

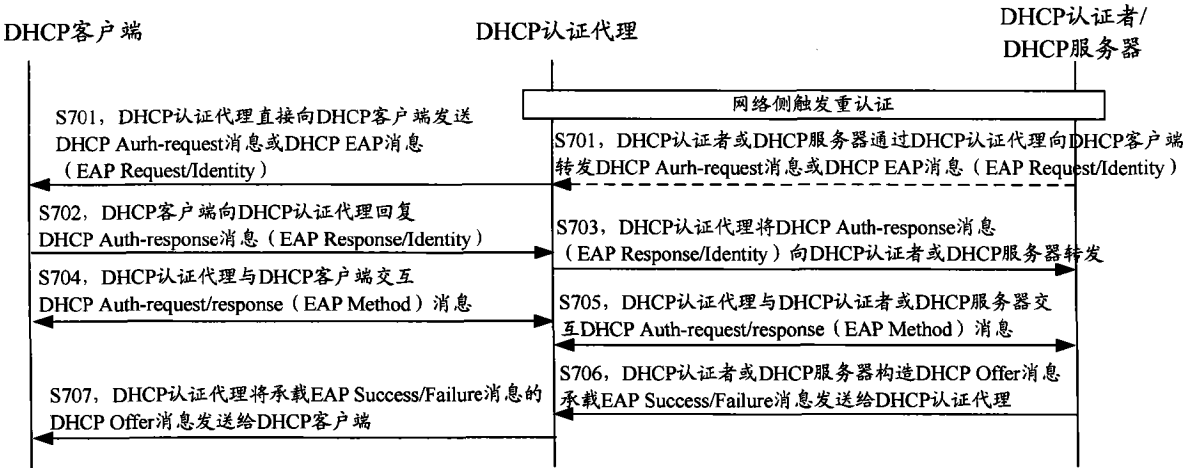


图 7

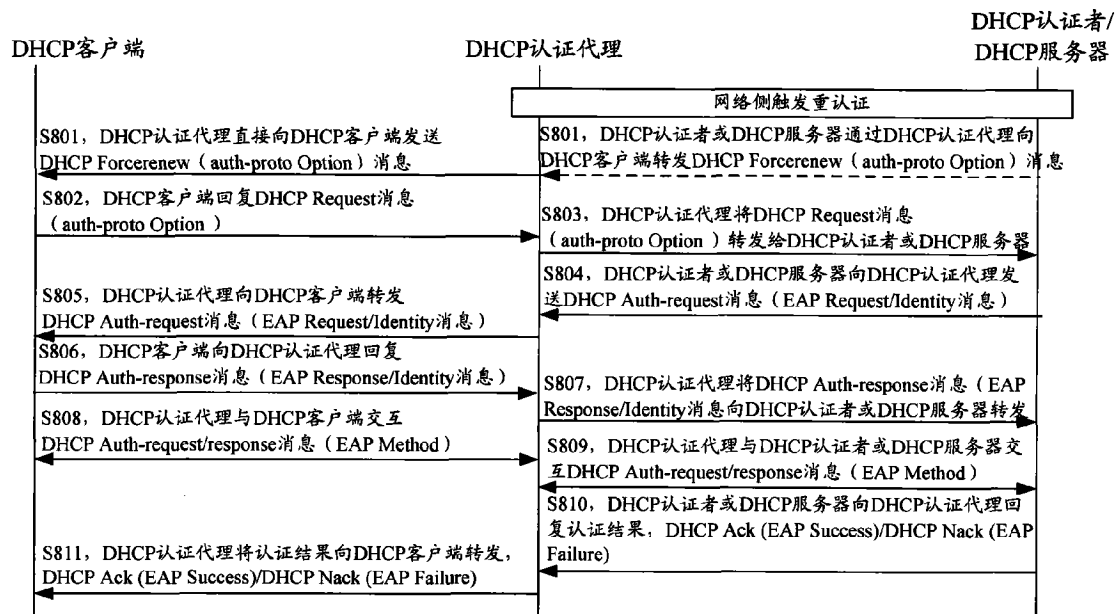


图 8

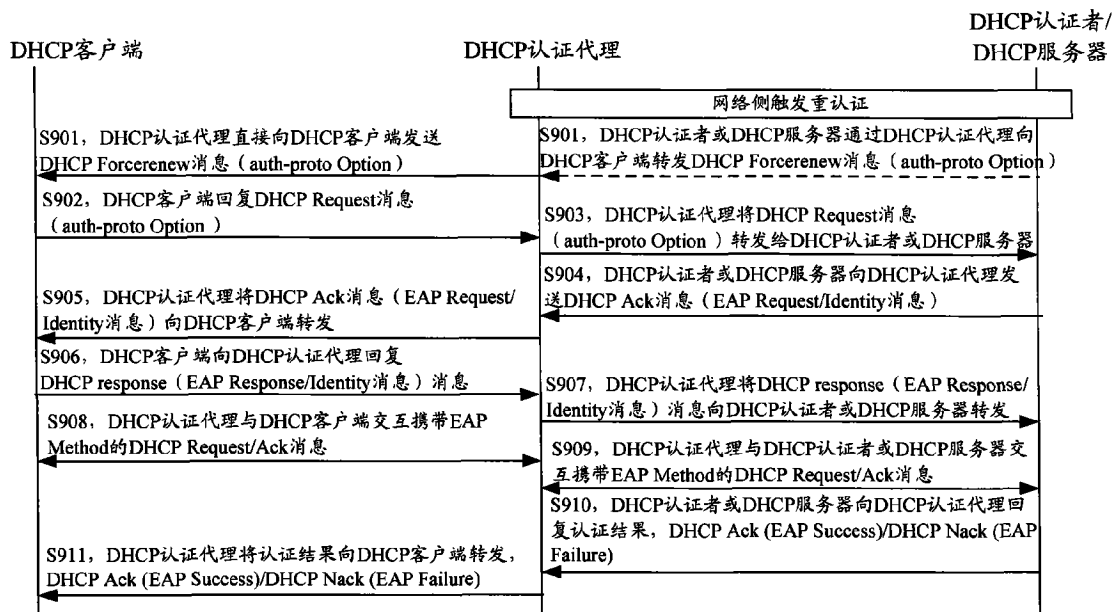


图 9

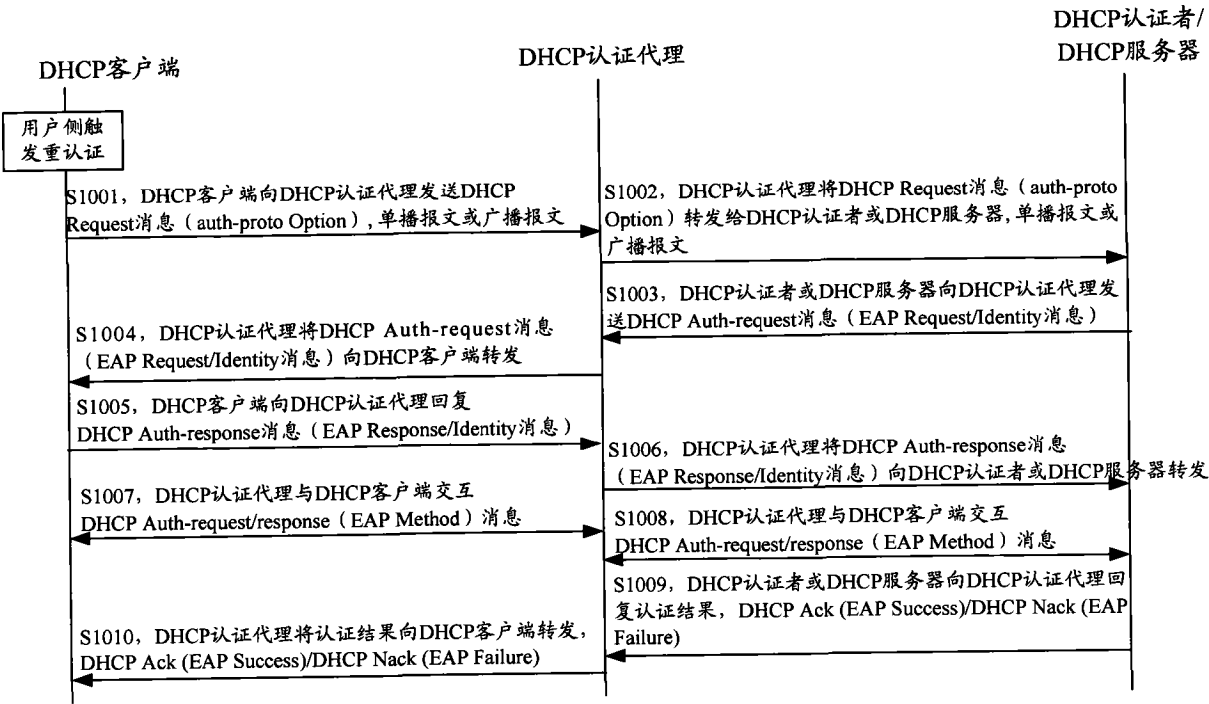


图 10

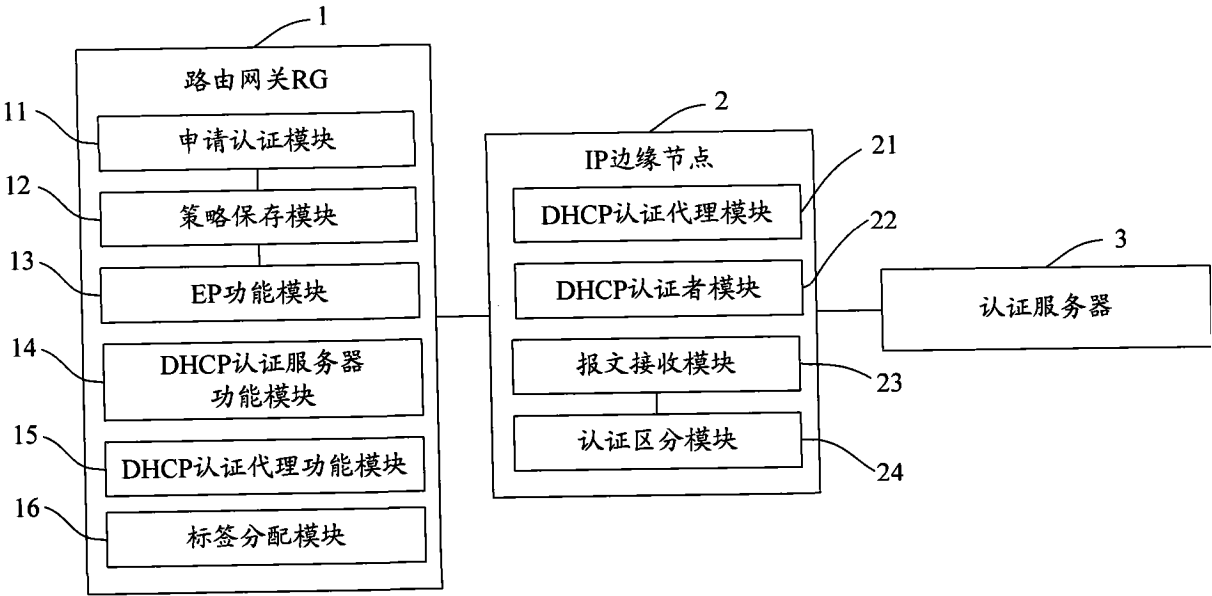


图 11