



(12) 发明专利

(10) 授权公告号 CN 101478576 B

(45) 授权公告日 2012. 02. 15

(21) 申请号 200810000123. X

CN 1271822 C, 2006. 08. 23,

(22) 申请日 2008. 01. 03

CN 1287738 A, 2001. 03. 14,

(73) 专利权人 华为技术有限公司

审查员 刘欣科

地址 518129 广东省深圳市龙岗区坂田华为
基地华电大楼 B1-3A

(72) 发明人 李宏宇

(74) 专利代理机构 北京中博世达专利商标代理
有限公司 11274

代理人 申健

(51) Int. Cl.

H04L 29/12 (2006. 01)

H04L 9/32 (2006. 01)

H04L 29/06 (2006. 01)

(56) 对比文件

EP 1643676 A4, 2006. 08. 02,

US 2006179310 A1, 2006. 08. 10,

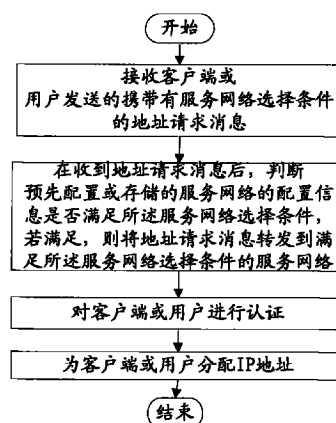
权利要求书 2 页 说明书 14 页 附图 6 页

(54) 发明名称

选择服务网络的方法、装置和系统

(57) 摘要

本发明实施例公开了一种选择服务网络的方法、装置和系统, 涉及网络通信技术, 为提高服务网络为客户服务的能力而发明。所述方法包括: 接收客户端或用户发送的携带有服务网络选择条件的地址请求消息; 在收到地址请求消息后, 判断预先配置或存储的服务网络的配置信息是否满足所述服务网络选择条件, 若满足, 则将地址请求消息转发到满足所述服务网络选择条件的服务网络。所述装置包括: 报文收发单元、配置单元以及服务网络选择单元。所述系统包括: 客户端或用户以及认证器/代理。本发明实施例可根据客户端或用户的要求为客户端或用户选择服务网络, 能够提高网络的服务能力。



1. 一种选择服务网络的方法,其特征在于包括以下步骤:

接收客户端或用户发送的携带有服务网络选择条件的地址请求消息;

在收到地址请求消息后,判断预先配置或存储的服务网络的配置信息是否满足所述服务网络选择条件,若满足,则将地址请求消息转发到满足所述服务网络选择条件的服务网络;

其中,所述服务网络选择条件至少包括:选择信息类型字段、选择信息长度字段及选择信息字段;

所述选择信息字段包括服务网络的网络接入标识、服务网络支持的认证方式、服务网络提供商信息、客户端或用户选择的认证协议信息、客户端或用户期望申请的地址信息、客户端或用户期望获得的服务等级协议信息中的至少一种。

2. 根据权利要求1所述的选择服务网络的方法,其特征在于,所述选择信息字段包括至少一个子选项字段,所述每个子选项字段至少包括:子选项类型字段、子选项长度字段、子选择信息字段。

3. 根据权利要求2所述的选择服务网络的方法,其特征在于,所述子选项类型字段为服务网络提供商信息、客户端或用户选择的认证协议信息、客户端或用户期望申请的地址信息、客户端或用户期望获得的服务等级协议信息中的至少一种。

4. 根据权利要求1所述的选择服务网络的方法,其特征在于,

所述服务网络选择条件由所述地址请求消息中的DHCP Option 82和/或DHCP Option 60携带。

5. 根据权利要求1所述的选择服务网络的方法,其特征在于还包括:

所述服务网络在收到所述地址请求消息后,对客户端或用户进行认证。

6. 根据权利要求5所述的选择服务网络的方法,其特征在于还包括:

所述服务网络为客户端或用户分配IP地址。

7. 一种选择服务网络的装置,其特征在于包括:

报文收发单元,用于收发报文;

配置单元,用于配置或存储服务网络选择单元所属服务网络的配置信息;和

服务网络选择单元,用于判断其所属服务网络的配置信息是否满足报文收发单元接收的报文中的服务网络选择条件,若满足,则将地址请求消息通过所述报文收发单元转发到满足所述服务网络选择条件的服务网络;

其中,所述服务网络选择条件至少包括:选择信息类型字段、选择信息长度字段及选择信息字段;

所述选择信息字段包括服务网络的网络接入标识、服务网络支持的认证方式、服务网络提供商信息、客户端或用户选择的认证协议信息、客户端或用户期望申请的地址信息、客户端或用户期望获得的服务等级协议信息中的至少一种。

8. 根据权利要求7所述的选择服务网络的装置,其特征在于,所述选择信息字段包括至少一个子选项字段,所述每个子选项字段至少包括:子选项类型字段、子选项长度字段、子选择信息字段。

9. 根据权利要求8所述的选择服务网络的装置,其特征在于,所述子选项类型字段为服务网络提供商信息、客户端或用户选择的认证协议信息、客户端或用户期望申请的地址

信息、客户端或用户期望获得的服务等级协议信息中的至少一种。

10. 根据权利要求 7 所述的选择服务网络的装置,其特征在于,所述服务网络选择条件由所述地址请求消息中的 DHCP Option 82 和 / 或 DHCP Option 60 携带。

11. 一种选择服务网络的系统,其特征在于,所述系统包括:

动态主机配置协议客户端,用于向认证器 / 代理发送携带有服务网络选择条件的地址请求消息;

认证器 / 代理,用于分别配置或存储其所属服务网络的配置信息,并判断其所属服务网络的配置信息,是否满足所述服务网络选择条件,若满足,则将地址请求消息转发到满足所述服务网络选择条件的服务网络;

其中,所述服务网络选择条件至少包括:选择信息类型字段、选择信息长度字段及选择信息字段;

所述选择信息字段包括服务网络的网络接入标识、服务网络支持的认证方式、服务网络提供商信息、客户端或用户选择的认证协议信息、客户端或用户期望申请的地址信息、客户端或用户期望获得的服务等级协议信息中的至少一种。

12. 根据权利要求 11 所述的选择服务网络的系统,其特征在于,所述系统还包括:

认证、授权和计费服务器,位于服务网络端,用于对客户端或用户进行认证。

13. 根据权利要求 12 所述的选择服务网络的系统,其特征在于,所述系统还包括:

动态主机配置协议服务器,位于服务网络端,用于为客户端或用户分配 IP 地址。

14. 根据权利要求 11 所述的选择服务网络的装置,其特征在于,所述选择信息字段包括至少一个子选项字段,所述每个子选项字段至少包括:子选项类型字段、子选项长度字段、子选择信息字段。

15. 根据权利要求 14 所述的选择服务网络的装置,其特征在于,所述子选项类型字段为服务网络提供商信息、客户端或用户选择的认证协议信息、客户端或用户期望申请的地址信息、客户端或用户期望获得的服务等级协议信息中的至少一种。

选择服务网络的方法、装置和系统

技术领域

[0001] 本发明涉及网络通信技术,尤其涉及一种在网络中为客户端或用户选择服务网络的方法、装置和系统。

背景技术

[0002] DHCP(Dynamic Host Configuration Protocol,动态主机配置协议),是一种简化主机 IP 配置管理的 TCP/IP 标准。它动态地为客户端指定 IP 地址和配置参数,如 IP 地址,子网掩码,缺省网关,域名服务器等。

[0003] 从组成上来看,DHCP 分为两个部分:DHCP 服务器(DHCP Server)和 DHCP 客户端(DHCP Client)。DHCP 服务器的主要功能是,根据 DHCP 客户端的请求,为客户端分配 IP 地址或者其他配置参数等。它一般存在于路由器,三层交换机中,或者以专门 DHCP 服务器的形式存在。DHCP 客户端,是利用 DHCP 协议获取配置参数的主机。

[0004] 由于 DHCP 服务器不仅能够为 DHCP 客户端分配 IP 地址,而且能够对 DHCP 客户端的 IP 地址进行租期管理,实现 IP 地址的分时复用等功能,因而,DHCP 协议得到了广泛的应用。

[0005] 图 1 为现有技术中 DHCP 认证过程的流程图。现有的 DHCPv4(DHCP 版本 4)的认证消息有两种:一种是 DHCP Auth-request(DHCP 认证请求)和 DHCPAuth-response(DHCP 认证响应),二者结合使用;另一种是 DHCP EAP。DHCP 认证过程可以采用其中任意一种。如图 1 所示,DHCP 的认证过程如下:

[0006] 1)DHCP 客户端接入到网络,发送 DHCP Discover(动态主机配置协议发现报文)给 DHCP 服务器。所述 DHCP Discover 携带有 DHCP 客户端支持的认证模式。所述认证模式可以为 DHCP 中的 CHAP(挑战握手认证协议)或 EAP(PPP 扩展认证协议)。

[0007] 2)DHCP 服务器收到所述 DHCP Discover 后,向 DHCP 客户端发出 DHCPAuth-request(动态主机配置协议认证请求)消息或 DHCP EAP 消息,两个消息都可以承载 EAP 消息。所述 EAP 消息中包括有 MD5 挑战字等信息。

[0008] 3)DHCP 客户端接收到 DHCP Auth-request 消息或 DHCP EAP 消息后,对 DHCP 服务器端发送的 EAP 消息中的 MD5 挑战字进行加密,得到经加密后的 EAP 消息,并通过 DHCP Auth-response(动态主机配置协议认证响应)承载所述加密后的 EAP 消息,然后发送给 DHCP 服务器。

[0009] 4)DHCP 服务器接收到 DHCP Auth-response 后,将 DHCP 客户端加密后的 EAP 消息重新封装在 AAA(认证、授权和计费)消息中,通过 Access-request 消息发送给认证服务器 AS。

[0010] 5)认证服务器 AS 通过所述 AAA 消息,对 DHCP 客户端进行认证;若认证成功,则将封装有 AAA 消息的 EAP success 消息,通过 Access-accept 消息发送给 DHCP 服务器;若认证不成功,则将封装有 AAA 消息的 EAP Failure 消息,发送给 DHCP 服务器。

[0011] 6)DHCP 服务器构造 DHCP Offer(地址分配服务确认)消息,该消息承载 EAP

success 消息后,发给 DHCP 客户端。在该消息中包含预分配给客户端的 IP 地址。

[0012] 7)DHCP 客户端发送 DHCP Request (地址分配请求) 响应 DHCP 服务器的 DHCP Offer 消息,表明 DHCP 客户端支持 DHCP 服务器的认证模式,并接受为其分配的 IP 地址。

[0013] 8)DHCP 服务器向 DHCP 客户端发送 DHCP Ack (地址分配回应) 消息。

[0014] 在实现本发明的过程中,发明人发现现有技术中存在有以下问题:DHCP 服务器在收到客户端的 DHCP Discover 后,会在与 DHCP 服务器连接的各个服务网络所能提供的 IP 地址中,查找空闲的 IP 地址,并为客户端分配。但,这种分配 IP 地址的方式,没有考虑到客户端对服务网络的要求。因而,DHCP 客户端收到的 IP 地址,很可能不是客户端所需要的 IP 地址。也就是说,通过上述的流程,当存在多个服务网络时,DHCP 客户端并不能主动选择符合自己需要的服务网络。

发明内容

[0015] 一方面,本发明的实施例提供了一种选择服务网络的方法,该方法能够提高网络为客户端或用户服务的能力。

[0016] 一种选择服务网络的方法,与所述服务网络对应的标识参数存储于相应的认证器/代理中,包括以下步骤:

[0017] 接收客户端或用户发送的携带有服务网络选择条件的地址请求消息;

[0018] 在收到地址请求消息后,判断预先配置或存储的服务网络的配置信息是否满足所述服务网络选择条件,若满足,则将地址请求消息转发到满足所述服务网络选择条件的服务网络。

[0019] 本发明的实施例选择服务网络的方法,在存在多个服务网络,多个认证、代理机构的情况下,通过在客户端或用户的地址分配请求中携带的服务网络选择条件,可以根据客户端或用户对服务网络的要求,为客户端或用户选择认证代理结构、服务网络,并为客户端或用户分配符合其网络服务要求的 IP 地址。因而,本发明的实施例避免了现有技术中,“盲目”的为客户端或用户分配 IP 地址的缺点,提高了网络为客户端或用户服务的能力。

[0020] 另一方面,本发明的实施例提供了一种选择服务网络的装置。利用所述装置,能够提高网络为客户端或用户服务的能力。

[0021] 一种选择服务网络的装置,包括:

[0022] 报文收发单元,用于收发报文;

[0023] 配置单元,用于配置或存储服务网络选择单元所属服务网络的配置信息;和

[0024] 服务网络选择单元,用于判断其所属服务网络的配置信息是否满足报文收发单元接收的报文中的服务网络选择条件,若满足,则将地址请求消息通过所述报文收发单元转发到满足所述服务网络选择条件的服务网络。

[0025] 本发明的实施例选择服务网络的装置,在多个服务网络,多个认证、代理机构的情况下,通过在客户端或用户的地址分配请求中携带的服务网络选择条件,使得服务网络选择单元可以根据客户端或用户对服务网络的要求,为客户端或用户选择服务网络,并为客户端或用户分配符合其网络服务要求的 IP 地址。从而避免了现有技术中,“盲目”的为客户端或用户分配 IP 地址的缺点,提高了网络为客户端或用户服务的能力。

[0026] 再一方面,本发明的实施例提供了一种选择服务网络的系统。利用所述系统,能够

提高网络为客户端或用户服务的能力。

[0027] 一种选择服务网络的系统,包括:

[0028] 动态主机配置协议客户端或用户,用于向认证器/代理发送携带有服务网络选择条件的地址请求消息;

[0029] 认证器/代理,用于分别配置和/或存储其所属服务网络的配置信息,并判断其所属服务网络的配置信息,是否满足所述服务网络选择条件,若满足,则将地址请求消息转发到满足所述服务网络选择条件的服务网络。

[0030] 本发明的实施例选择服务网络的系统,在多个服务网络,多个认证、代理机构的情况下,通过客户端或用户发送的地址分配请求消息中的服务网络选择条件,使得认证器/代理可以根据客户端或用户对服务网络的要求,为客户端或用户选择服务网络,并为客户端或用户分配符合其网络服务要求的 IP 地址。从而避免了现有技术中,“盲目”的为客户端或用户分配 IP 地址的缺点,提高了网络为客户端或用户服务的能力。

附图说明

[0031] 图 1 为现有技术中 DHCP 认证过程的流程图;

[0032] 图 2 为本发明的实施例选择服务网络的方法的流程图;

[0033] 图 3 为本发明的实施例选择服务网络的方法的具体流程图;

[0034] 图 4 为本发明的实施例选择服务网络的方法中实施例一的流程图;

[0035] 图 5 为本发明的实施例选择服务网络的方法中实施例二的流程图;

[0036] 图 6 为本发明的实施例选择服务网络的方法中实施例三的流程图;

[0037] 图 7 为本发明的实施例选择服务网络的方法中实施例四的流程图;

[0038] 图 8 为本发明的实施例选择服务网络的装置的原理图;

[0039] 图 9 为本发明的实施例选择服务网络的装置的实施例一的原理图;

[0040] 图 10 为本发明的实施例选择服务网络的装置的实施例二的原理图;

[0041] 图 11 为本发明的实施例选择服务网络的装置的实施例四的原理图;

[0042] 图 12 为本发明的实施例选择服务网络的系统的原理图。

具体实施方式

[0043] 为了能够为客户端或用户提供符合客户端或用户要求的服务网络,从而提高为客户端或用户服务的能力,本发明的实施例提供了一种选择服务网络的方法、装置和系统。在本发明的实施例中,所述服务网络是指各运营商(SP)提供的网络,例如中国电信的网络,中国网通的网络,中国移动的网络,但不限于上述网络。在本发明的实施例中,客户端指各种具备 DHCP 客户端功能的设备,至少包括各种终端设备,或用户驻地网中的设备,但不限于上述内容。

[0044] 如图 2 所示,本发明实施例选择服务网络的方法包括如下步骤:

[0045] T1:接收客户端或用户发送的携带有服务网络选择条件的地址请求消息;

[0046] T2:在收到地址请求消息后,判断预先配置和/或存储的服务网络的配置信息是否满足所述服务网络选择条件,若满足,则将地址请求消息转发到满足所述服务网络选择条件的服务网络。

[0047] 因此,各认证器/代理,可以根据客户端或用户的要求为客户端或用户选择服务网络,并为客户端或用户分配符合其服务网络要求的 IP 地址,从而提高了为客户端或用户服务的能力。

[0048] 为使本发明实施例的技术方案的优点更加清楚,下面结合附图对本发明的实施例作进一步的详细说明。

[0049] 如图 3 所示,本发明的实施例选择服务网络的方法,包括以下步骤:

[0050] S1:接收客户端或用户发送的携带有服务网络选择条件的地址请求消息;

[0051] S2:在收到地址请求消息后,判断预先配置和/或存储的服务网络的配置信息是否满足所述服务网络选择条件,若满足,则将地址请求消息转发到满足所述服务网络选择条件的服务网络。

[0052] 在将客户端或用户的地址请求消息发送到所述服务网络后,所述选择服务网络的方法还包括如下步骤:

[0053] S3:所述服务网络在收到所述地址请求后,对客户端或用户进行认证。

[0054] 根据运营商的设置,所述的认证过程是可选的,即运营商网络可以选择不对客户端或用户进行认证,也可以根据客户端或用户的位置信息(比如 Option 82 当中携带的信息)、客户端或用户的源 MAC 地址等进行隐式的认证。所述认证过程可以采用现有技术中的认证过程,如 DHCP 认证,或其它认证方式。

[0055] S4:在认证过程结束后,所述服务网络为客户端或用户分配 IP 地址。

[0056] 至此,服务网络为客户端或用户分配了满足客户端或用户要求的 IP 地址。

[0057] 其中,在步骤 S1 之前,还可以进一步包括:配置和/或存储服务网络的配置信息的步骤。

[0058] 其中,所述服务网络选择条件(DHCP Selection Option)的定义方式如表 1 所示。所述 DHCP Selection Option 可以包括三个组成部分:选择信息类型字段,选择信息长度字段和选择信息字段。当然,还可根据需要将服务网络选择条件进行扩展,使所述服务网络选择条件包含更多的信息。

[0059] 表 1

[0060]

选择信息类型	选择信息长度	选择信息字段					
345	N	i1	i2	i3	i4		iN

[0061] 在表 1 中,选择信息类型 345 表示这个消息是 DHCP Selection Option。需要注意的是,在此仅举例说明信息类型的取值,在实际应用中,可以根据 DHCP 协议定义信息类型或根据需要自定义。选择信息长度表示选择信息字段的长度。

[0062] 选择信息字段中写入有客户端或用户的具体选择信息,可以只包含单一的信息,例如:运营商的服务网络信息,或客户端或用户期望使用的认证协议,或客户端或用户期望申请的 IP 地址等信息,或客户端或用户期望获得的 SLA(服务等级协议)等。

[0063] 另外,上述信息也可以以子选项的形式表示,也即将这些信息写入到子选项字段中,此时所述的子选项字段作为选择信息字段的内容。表 2 中定义了子选项字段的内容。这

样,选择信息字段中既可以写入某种单一的信息,也可写入子选项字段,或者可以存在上述两种信息的表示形式。

[0064] 表 2

[0065]

子选项 类型字段	子选项 长度字段	子选择信息值字段
-------------	-------------	----------

[0066]

1	N	i1	i2	i3	i4		iN
2	N	i1	i2	i3	i4		iN
3	N	i1	i2	i3	i4		iN
4	N	i1	i2	i3	i4		iN

[0067] 在表 2 中,子选项类型字段 1 表示运营商的服务网络信息,如 NAI (NetworkAccess Identifier,网络接入标识)、带域的客户端或用户名或其它代表运营商的服务网络信息。

[0068] 子选项类型字段 2 表示客户端或用户期望使用的认证协议,比如 DHCP 认证协议等;也可以是某种认证协议中具体的认证方法,如 DHCP 认证中的 EAP 或者 CHAP 认证协议(挑战握手认证协议)。

[0069] 子选项类型字段 3 表示客户端或用户期望申请的 IP 地址等信息,如服务网络的某个 IP 网段的地址,或者长期固定的 IP 地址等。

[0070] 子选项类型字段 4 表示客户端或用户期望获得的 SLA(服务等级协议),比如客户端或用户期望获得的带宽、QoS(服务质量)等内容。

[0071] 需要注意的是,上述子选项字段仅为举例。在具体应用中,还可根据需要扩展更多的子选项字段。

[0072] 下面举例说明 DHCP Selection Option 在具体应用中的数据填写格式。

[0073] 如果网络中同时存在中国电信和中国网通两家运营商的服务网络,则服务网络的 NAI 可分别定义为 ChinaTelecom(中国电信)和 ChinaNetcom(中国网通)。如果客户端或用户希望接入的服务网络是中国电信提供的服务网络,且希望采用 EAP 封装的 DHCP 认证方法,则客户端或用户对服务网络的要求以子选项字段的形式填充在 DHCP Selection Option 的选择信息字段中。那么,将设置子选项字段 1 的子选择信息值字段为 ChinaTelecom,子选项字段 2 的子选项信息值字段为 DHCP+EAP。那么,由上述信息可定义出 DHCP Selection Option 的格式如表 3 所示:

[0074] 表 3

[0075]

选择信息类型	选择信息长度	选择信息字段					
		子选项字段 1			子选项字段 2		
345	24	1	12	ChinaTelecom	2	8	DHCP+EAP

[0076] 同时,服务网络的配置信息可以包括但不限于如下内容:服务网络支持的认证方式、服务网络的网络接入标识、服务网络提供的带宽等等,且可由认证器/代理根据需要自由配置。

[0077] 因此,在所述步骤 S3 中,各认证器/代理判断其所属服务网络的配置信息,是否满足客户端或用户的服务网络选择条件的情况至少存在以下三种:

[0078] 第一种:服务网络的配置信息,与客户端或用户的服务网络选择条件的内容全部相同。

[0079] 例如,客户端或用户的服务网络选择条件包括:客户端或用户希望接入的服务网络为中国电信(ChinaTelecom),且希望服务网络支持的认证方式为 DHCP 认证方式。若某个认证器/代理在其存储的服务网络的配置信息中发现,其所属服务网络的配置信息包括:网络接入标识为 ChinaTelecom,支持的认证方式为 DHCP 认证方式。那么,在比较所述客户端或用户的服务网络选择条件,与服务网络的配置信息后,发现二者一致,那么该认证器/代理则将客户端或用户的地址请求消息发送给其所属的 ChinaTelecom 的网络。

[0080] 第二种:服务网络的配置信息,与客户端或用户的服务网络选择条件的内容部分相同。

[0081] 例如,客户端或用户的服务网络选择条件包括:客户端或用户希望接入的服务网络为 ChinaTelecom。若某个认证器/代理在其存储的服务网络的配置信息中发现,其所属的一个服务网络的配置信息包括:网络接入标识为 ChinaTelecom,支持的认证方式为 DHCP 认证方式。那么,在比较所述客户端或用户的服务网络选择条件,与服务网络的配置信息后,该认证器/代理发现其所属的一个服务网络的网络接入标识为 ChinaTelecom,那么该认证器/代理同样会将客户端或用户的地址请求消息发送给其所属的 ChinaTelecom 的网络。

[0082] 又例如,如果客户端或用户希望接入的服务网络为 ChinaTelecom.sz,某个认证器/代理在其存储的服务网络的配置信息中,所述服务网络的网络接入标识为 ChinaTelecom,若认证器/代理配置的满足条件是部分匹配,也可以认为是满足条件。当然,若客户端或用户希望接入的服务网络为 ChinaTelecom,而某个认证器/代理在其存储的服务网络的配置信息中,所述服务网络的网络接入标识为 ChinaTelecom.sz,若认证器/代理配置的满足条件是部分匹配,也可以认为是满足条件。

[0083] 第三种:服务网络选择条件中,某个或某些参数的取值,落在了服务网络的配置参数中同一参数的取值范围内。

[0084] 例如,客户端或用户的服务网络选择条件包括:客户端或用户希望服务网络为其提供 5M 的带宽。若某个认证器/代理在其存储的服务网络的配置信息中发现,其所属的一个服务网络的配置信息中显示,该服务网络能够提供 10M 的带宽。那么,该服务网络能够满足客户端或用户对带宽的需求。那么该认证器/代理则将客户端或用户的地址请求消息发送给所述的服务网络。

[0085] 需要说明的是,上面仅列举了“服务网络选择条件”与“服务网络配置信息”之间的三种匹配关系。但转发出发条件的设置并不局限于在此所列举的。在实际使用中可以在认证器/代理上根据需要配置转发的触发条件,即对“满足”进行定义。比如当服务网络的配置信息,与客户端或用户的服务网络选择条件的内容需要完全匹配时,才认为是“满足”;或者当服务网络的配置信息,与客户端或用户的服务网络选择条件的内容达到部分匹配时,就认为是“满足”,也可以定义其它的认为是“满足”的条件。

[0086] 下面分别结合本实施例的不同应用场景,详细描述一下本实施例的具体实现过程。

[0087] 实施例一:

[0088] 如图 4 所示,在此实施例中,客户端或用户通过接入汇聚网与多个认证器/代理连接,各认证器/代理分别通过各自的 IP 网络连接到所属的服务网络,即运营商网络 SP。其中,客户端或用户可以是各种有线、无线终端,且具备 DHCP 客户端或用户功能。认证器/代理可以具备 DHCP 中继代理功能(DHCP Proxy 或 DHCP Relay),还可具备认证器(Authenticator)/AAA 客户端或用户功能,且其上配置有其所属运营商网络的配置信息。各认证器/代理中的服务网络的配置信息可以通过动态或静态的方式配置。若采用动态方式配置,可以采用 DIAMETER 协议或其它协议,由运营商的策略服务器或其它控制设备来动态对认证器/代理进行配置,对服务网络的配置信息进行动态修改。

[0089] 运营商网络 SP 中分别包含各自的 AAA 服务器(认证、授权和计费服务器)(如 Radius 服务器)和 DHCP 服务器。

[0090] 在此实施例中,运营商网络 SP1 为 ChinaNetcom,只支持 DHCP+CHAP 认证;运营商网络 SP2 为 ChinaTelecom,支持 DHCP+EAP 认证。客户端或用户发出的 DHCP Selection Option 中携带的 NAI 为 ChinaTelecom,且希望使用 DHCP+EAP 认证方法进行认证。那么,本发明的实施例选择服务网络的方法的步骤如下:

[0091] S11:DHCP 客户端或用户以广播形式向各认证器/代理发送 DHCP Discover,并携带 DHCP Selection Option 信息,在所述 DHCP Selection Option 信息中包含运营商的服务网络信息,如 NAI(Network Access Identifier,网络接入标识)等,客户端或用户期望使用的认证协议,客户端或用户期望申请的 IP 地址等信息,客户端或用户期望获得的 SLA(服务等级协议)等信息;

[0092] S12:各认证器/代理收到所述 DHCP Discover 后,分别根据 DHCP SelectionOption 中的信息判断其所属的网络是否能够满足客户端或用户的要求;

[0093] 在本实施例中,认证器/代理 2 根据 DHCP Selection Option 中的 NAI 以及自身存储的服务网络的配置信息,判断出客户端或用户所要求的服务网络为其所属的运营商网络 SP2。因此,认证器/代理 2 将 DHCP Discover 消息转发到运营商网络 SP2 的 DHCP 服务器上;

[0094] S13 :运营商网络 SP2 对客户端或用户进行认证。

[0095] 根据运营商的设置,所述的认证过程是可选的,即运营商网络可以选择不对客户端或用户进行认证,也可以客户端或用户的根据位置信息(比如 Option 82 当中携带的信息)、客户端或用户的源 MAC 地址等进行隐式的认证。所述认证过程可以采用现有技术中的认证过程,或其它认证方式。

[0096] 在此实施例中,假设需要对客户端或用户进行认证。若采用现有技术中的认证过程时,所述认证的具体过程可以包括如下步骤:

[0097] S131 :DHCP 服务器检查 DHCP Discover 中的参数,回应 DHCP Offer(地址分配服务确认)消息给认证器/代理 2,为 DHCP 客户端或用户提供一个未租借的 IP 地址和其它 DHCP 配置信息,比如子网掩码和缺省网关等;

[0098] S132 :认证器/代理 2 收到 DHCP Offer 消息后,添加认证选项表明认证器/代理 2 支持的认证模式,记录下 DHCP 服务器为 DHCP 客户端或用户提供的未租借的 IP 地址,并可将所述未租借的 IP 地址替换为一个供 DHCP 客户端或用户本地使用的局部 IP 地址,然后向 DHCP 客户端或用户转发 DHCP Offer 消息;

[0099] S133 :DHCP 客户端或用户发送 DHCP Request(地址分配请求)消息来响应认证器/代理 2 的 DHCP Offer,在所述 DHCP Offer 消息中包含认证器/代理 2 支持的认证模式 DHCP+CHAP 及其所提供的 IP 地址等,表明 DHCP 客户端或用户已经选择支持相应认证模式的认证器/代理 2,并接受了认证器/代理 2 提供的 IP 地址;

[0100] S134 :认证器/代理 2 接收到 DHCP Request 消息后,向 DHCP 客户端或用户发出 EAP-Request/Identity 身份查询请求(该报文由 DHCP Ack(地址分配回应)消息承载),并通过 DHCP Ack 消息下发一个仅供 DHCP 客户端或用户认证使用的“假”租期(lease time);该租期应设置为使 DHCP 客户端或用户能迅速响应 EAP 认证消息,并且预留足够的时间用于认证器/代理 2 回复 EAP 认证消息给 DHCP 客户端或用户;

[0101] S134 :DHCP 客户端或用户接收到 DHCP Ack 消息后,根据 lease time 设置定时器 T1 和 T2;当 T1 到时,触发 DHCP Request 消息更新租期,并承载 EAP-Response/Identity 应答消息给认证器/代理 2;

[0102] S135 :认证器/代理 2 将 DHCP 客户端或用户的 EAP-Response/Identity 应答消息重新封装在 AAA 消息中发送给 AAA 服务器;

[0103] S136 :DHCP 客户端或用户、认证器/代理 2 以及 AAA 服务器之间进行 EAP 的认证方法(EAP Method)协商,以及认证方法交换的过程;

[0104] 在上述过程中,DHCP 客户端或用户和认证器/代理 2 之间均采用 DHCPRequest/Ack 消息承载 EAP 消息进行交互;在认证器/代理 2 和 AAA 服务器之间均采用 AAA 消息承载 EAP 消息进行交互;直到 EAP 认证过程结束;

[0105] 其中,认证器/代理 2 每收到 DHCP Request 消息后,会通过 DHCP Ack 消息承载 EAP 消息并下发一个仅供 DHCP 客户端或用户认证使用的“假”租期(leasetime);DHCP 客户端或用户每收到 DHCP Ack 消息后,会根据 lease time 重新设置定时器 T1 和 T2;当 T1 或 T2 到时,触发 DHCP Request 消息更新租期以承载 EAP 消息;

[0106] S137 :AAA 服务器最终通知认证器/代理 2 认证结果;

[0107] 若认证不成功,则 EAP failure 消息封装在 AAA 消息中发送给认证器/代理 2;

[0108] 若认证成功,则将 EAP success 消息和相应的 EAP 衍生密钥封装在 AAA 消息中发送给认证器 / 代理 2 ;

[0109] S14 :认证过程结束后, DHCP 服务器为客户端或用户分配 IP 地址。

[0110] 在上述的过程中,各认证器 / 代理可对其自身的判断条件进行设置。例如,对客户端或用户的 DHCP Discover 中所携带 DHCP Selection Option 条件,各认证器 / 代理可以设置成部分满足客户端或用户的条件即可转发所述 DHCP Discover,也可以设置成全部满足客户端或用户的条件才能转发所述 DHCP Discover。

[0111] 例如,如果运营商网络 SP2 不支持 DHCP+EAP,但在认证器 / 代理 2 中设置为认证器 / 代理 2 满足 DHCP 客户端要求的 NAI 即可转发 DHCP Discover。那么,当认证器 / 代理 2 收到该 DHCP Discover 报文时,判断 DHCP Selection Option 中的 NAI 与自己所属的服务网络的 NAI 相同,则仍可转发 DHCP Discover 报文。

[0112] 同时,如果 DHCP 客户端发出 DHCP Discover 后,长时间没有收到回应(回应可以是 DHCP OFFER ;在采用不同认证方法的时候,回应也可能是其它的报文),客户端可以修改 DHCP Selection Option 中的参数重新进行发送。比如 DHCP 客户端可将 DHCP Selection Option 中的 NAI 由 ChinaTelecom 改为 ChinaNetcom 后重新发送给各认证器 / 代理。在修改 DHCP Selection Option 中的参数重新进行发送之前, DHCP 客户端可以将发送多次,在多次尝试都失败后可再修改相应参数,重新发送携带有 DHCP Selection Option 的 DHCP Discover 报文。

[0113] 另外,若有多个服务网络满足客户端或用户的要求,那么满足要求的服务网络均能收到客户端的地址分配请求消息,并为客户端或用户分配 IP 地址。而客户端或用户则会选择最先到达客户端或用户端的 IP 地址。此过程和现有技术中利用 DHCP 协议进行 IP 地址分配的过程相同。

[0114] 本实施例中认证器 / 代理、AAA 服务器和 DHCP 服务器为逻辑功能体,实际使用中可以是分开的物理节点,也可以任意组合合并到一个物理节点中,甚至可以内置到其它网络设备中。当三者合并到一个物理实体中时, IP 网络可以用于该物理实体与运营商网络其它部分或接入网连接。

[0115] 实施例二 :

[0116] 在此实施例中,如图 5 所示, DHCP 客户端或用户通过接入汇聚网与认证器 / 代理相连接,多个运营商网络 SP 共用一个认证器 / 代理。认证器 / 代理通过 IP 网络连接到多个运营商网络 SP。 DHCP 客户端或用户可以是各种有线、无线终端,具备 DHCP 客户端或用户功能。认证器 / 代理具备 DHCP 中继代理功能 (DHCP Proxy 或 DHCP Relay),还可具备认证器 (Authenticator)/AAA 客户端或用户功能,且配置有与之相连的各运营商网络的配置信息,如 NAI、具备的能力等信息。同样,各认证器 / 代理中的网络标识参数可以通过动态或静态的方式配置。配置的方式和在实施例一中所述的相同。

[0117] 运营商网络 SP1 和 SP2 中分别包含有 AAA 服务器 (如 Radius Server) 和 DHCP 服务器。 IP 网可以是多个独立的 IP 网络,也可以是一张网。

[0118] 在此实施例中,若运营商网络 SP1 为 ChinaTelecom,只支持 DHCP+CHAP 认证 ;运营商网络 SP2 为 ChinaNetcom,支持 DHCP+EAP 认证。客户端或用户发出的 DHCP Selection Option 中携带的 NAI 为 ChinaNetcom,且希望使用 DHCP+EAP 认证方法进行认证。具体过程

如下：

[0119] S21:DHCP 客户端或用户发送带 DHCP Selection Option 的 DHCP Discover 报文；在所述 DHCP Selection Option 信息中包含运营商的服务网络信息，如 NAI(Network Access Identifier,网络接入标识)等，客户端或用户期望使用的认证协议，客户端或用户期望申请的 IP 地址等信息，客户端或用户期望获得的 SLA(服务等级协议)等信息；

[0120] S22:认证器/代理收到该报文后，根据 DHCP Selection Option 中的 NAI 以及自身存储的服务网络的配置信息，判断出其所属的运营商网络 SP2 符合客户端或用户的要求，因此所述认证器/代理将包含 DHCP Selection Option 的 DHCP Discover 报文转发到 SP2 的 DHCP 服务器；

[0121] S23:所述运营商网络 SP2 开始对 DHCP 客户端或用户进行认证和地址分配过程。

[0122] 同样，在此实施例中，所述的认证过程是可选的，根据运营商的设置，可以选择不对客户端或用户进行认证，也可以客户端或用户的根据位置信息（比如 Option 82 当中携带的信息）、客户端或用户的源 MAC 地址等进行隐式的认证。所述认证过程可以采用现有技术中的认证过程，或其它认证方式。若进行认证，此实施例中的认证和地址分配的过程和实施例中 1 中的认证、地址分配过程相同，在此不再赘述。同样，在本实施例中，认证的方法也不局限于在背景技术中所列举的认证方法。

[0123] 实际应用中，根据不同的认证方法，认证器/代理可以对自己的转发条件进行设置，从而根据需要将 DHCP 客户端或用户发送的带 DHCP Selection Option 的 DHCP Discover 报文，完整的转发给运营商网络中的 DHCP 服务器，或者将其中的部分信息转发到对应运营商网络中的 DHCP 服务器，或者将 DHCP SelectionOption 中的信息提取出来放到认证协议中送到对应的 AAA 服务器。

[0124] 如果认证器/代理在其所属的运营商网络中找不到可以满足 DHCP SelectionOption 的要求的运营商网络，则将丢弃 DHCP Discover 报文，或者将该报文向所有运营商广播。

[0125] DHCP 客户端或用户发出 DHCP Discover 后长时间没有收到回应的处理方法与实施例一相同。

[0126] 实施例三：

[0127] 在实施例 1 和 2 中，认证器/代理实际上可以由多个子认证器/代理设备构成。如图 6 所示，认证器/代理 1 由子认证器/代理 A 和子认证器/代理 B 构成。

[0128] 当子认证器/代理 A 和子认证器/代理 B 都有效，或处于负荷分担或主备用关系的情况下，当认证器/代理收 1 收到带 DHCP Selection Option 报文的 DHCPDiscover 报文时，除了按实施例 1 或 2 中所述的可由认证器/代理收 1 根据 DHCPSelection Option 中的参数进行判断、选择运营商网络外，还可以由认证器/代理收 1 进一步根据自身目前的负荷，网络资源状况，流量分担策略，客户端或用户分担策略等决定由哪个子认证器/代理对该报文进行转发和后续客户端或用户数据的处理。同时，子认证器/代理之间可以通过预先设置的算法进行判断，也可以在它们之间通过协议进行协商。

[0129] 在此实施例中，通过自子认证器/代理 A 和 B 之间进行协商，由子认证器/代理 B 转发 DHCP 客户端或用户的 DHCP Discover 报文。

[0130] 之后，进行运营商网络与 DHCP 客户端或用户的认证和地址分配过程。所述的认证

过程是可选的,根据运营商的设置,可以选择不对客户端或用户进行认证,也可以客户端或用户的根据位置信息(比如 Option 82 当中携带的信息)、客户端或用户的源 MAC 地址等进行隐式的认证。所述认证过程可以采用现有技术中的认证过程,或其它认证方式。若进行认证,在本实施例中,认证和地址分配过程和实施例 1 中的认证和地址分配过程相同,在此不再赘述。

[0131] 当然,在本发明的实施例 1-3 中的 DHCP Selection Option,也可通过利用现有的 DHCP Option 实现。

[0132] 在 DHCP Option 中, DHCP Option 60 中带有 Vendor 和 Service Option(服务选项)信息,是由客户端或用户发起 DHCP 请求时携带的信息。在应用中, DHCP Option 60 的作用是用来标识客户端或用户类型,从而由 DHCP 服务器识别用户业务类型,并借此为客户端或用户分配不同的 IP 地址。而 DHCP Option 82 是由网络设备插入在客户端或用户发出的 DHCP 报文中,主要用来标识客户端或用户的接入位置。在 DHCP Option 82 中携带客户端或用户的位置信息、物理或逻辑端口信息等。其中,位置信息、物理或逻辑端口信息可以是客户端或用户所接入的设备的框、槽、端口、PVC、VLAN、信道等,设备类型,或所用于的业务类型可以是 STB、PC、IPTV、RG、家庭网关(HG、Home Gateway)、生产厂家代码、或其它约定的信息等。

[0133] 以 DHCP Option 82 为例,当一个客户端或用户的接入设备传输 DHCP 客户端或用户发起的 DHCP 请求时, DHCP Option 82 被嵌入到客户端或用户的 DHCP 请求中。当 DHCP 服务器识别到认证器/代理转发的 DHCP 请求后,就会根据请求中的信息执行相应的 IP 地址分配过程。

[0134] 在本实施例中以 DHCP Option 60 为例进行说明,实际应用中也可以采用其它的 DHCP Option,也可以采用 DHCP Option 82 和 DHCP Option 60 相结合的方式。

[0135] 那么,当用 DHCP Option 82 或 DHCP Option 60 代替实施例 1-3 中的 DHCP Selection Option 时,各认证器/代理将根据 DHCP Option 82 或 DHCP Option 60 中携带的客户端或用户对服务网络要求的相关信息,选择能够满足客户端或用户要求的服务网络为客户端或用户分配 IP 地址等信息。

[0136] 实施例四:

[0137] 在此,以实施例 1 中的网络架构,来说明采用 DHCP Option 82 或 DHCP Option 60 携带客户端或用户对服务网络的需求等信息时的流程图。

[0138] 在此实施例中,假设运营商网络为 IPTV 网络,运营商网络为 Internet 网络。客户端或用户发出的 DHCP Option 60 中携带的信息为 PC。

[0139] 如图 7 所示,具体过程如下:

[0140] S41: DHCP 客户端或用户以广播形式向各认证器/代理发送 DHCP Discover,并携带 DHCP Option 60 信息;

[0141] S42: 各认证器/代理收到所述 DHCP Discover 后,分别根据 DHCP Option 60 中的信息判断其所属的网络是否能够满足客户端或用户的要求;

[0142] 在此实施例中,认证器/代理 2 根据 DHCP Selection Option 中的 DHCP Option 60,判断出客户端或用户所要求的服务网络为自己所属的运营商网络 SP2。因此,认证器/代理 2 将 DHCP Discover 消息转发到运营商网络 SP2 的 DHCP 服务器上;

- [0143] S43 :运营商网络 SP2 对客户端或用户进行认证,并为客户端或用户分配 IP 地址。
- [0144] 此认证过程,可以根据运营商的设置,自由选择,即可以选择对客户端或用户不进行认证,也可以选择认证。若进行认证,认证和分配 IP 地址的过程和实施例一中的相同,在此不再赘述。
- [0145] 当接入设备在客户端或用户发送的 DHCP Discover 报文中插入 DHCP Option82 后,利用所述 DHCP Option 82 携带服务网络选择条件的过程,和上述以 DHCP Option 60 为例进行说明时的过程相同。
- [0146] 通过上述的实施例,可以根据客户端或用户的要求为客户端或用户选择符合客户端或用户要求的服务网络,提高了网络的服务质量。
- [0147] 与本发明的选择服务网络的方法相对应,本发明的实施例还提供了一种选择服务网络的装置。
- [0148] 如图 8 所示,本发明的实施例选择服务网络的装置包括 :
- [0149] 报文收发单元,用于收发报文 ;
- [0150] 配置单元,用于配置和 / 或存储服务网络选择单元所属服务网络的配置信息 ;和
- [0151] 服务网络选择单元,用于判断其所属服务网络的配置信息,是否满足报文收发单元接收的报文中的服务网络选择条件,若满足,则将地址请求消息通过所述报文收发单元转发到所述服务网络。
- [0152] 那么,服务网络选择收发单元在收到地址请求消息后,逐一的读取或采用其他方式读取配置单元中存储的服务网络的配置信息,并与所述地址请求消息中的服务网络选择条件进行比较,若满足则将所述地址请求消息通过所述报文收发单元转发到符合要求的服务网络中。
- [0153] 这样,服务网络选择单元就可根据客户端或用户的服务网络选择条件,为客户端或用户选择出符合客户端或用户要求的服务网络,并为客户端或用户分配符合其网络服务要求的 IP 地址,从而提高了为客户端或用户服务的能力。
- [0154] 在实际应用中,本发明实施例所述的选择服务网络的装置至少存在以下三种情形 :
- [0155] 情形 1 :如图 9 所示,所述选择服务网络的包括多个报文收发单元、配置单元和服务网络选择单元,且所述的报文收发单元、配置单元和服务网络选择单元存在一一对应关系。那么这样,每个报文收发单元,负责为与其相对应的服务网络选择单元收发客户端或用户的地址请求消息,配置单元中存储的只是与其相对应的服务网络选择单元所属的服务网络的配置信息。
- [0156] 各服务网络选择单元根据所述服务网络选择条件,分别读取其对应的配置单元中存储的服务网络的配置信息,判断所属的服务网络是否满足客户端或用户的要求。若满足,则将地址请求消息通过所述报文收发单元转发到所述服务网络。由所述服务网络的认证单元与服务网络选择单元、报文发送单元之间进行认证,协商认证方法等。在认证过程结束后,由地址分配单元为客户端或用户分配 IP 地址。其中,认证过程可根据运营商的设置为可选的。若不进行认证,则直接由地址分配单元为客户端或用户分配 IP 地址。
- [0157] 情形 2 :如图 10 所示,所述选择服务网络的装置包括一个报文收发单元,多个配置单元与多个服务网络选择单元,且所述配置单元与服务网络选择单元为多对一的关系。所

述的服务网络选择单元与多个服务网络连接,配置单元分别存储至少一个服务网络选择单元所属服务网络的配置信息。所述报文收发单元,分别为各服务网络选择单元收发客户端或用户的地址请求消息。

[0158] 服务网络选择单元根据所述服务网络选择条件,分别读取各配置单元中存储的服务网络的配置信息,并判断由各配置单元读取的配置参数,是否满足客户端或服务网络选择条件。若满足,则将地址请求消息通过所述报文收发单元转发到所述服务网络。由所述服务网络的认证单元与服务网络选择单元、报文发送单元之间进行认证,协商认证方法等。在认证过程结束后,由地址分配单元为客户端或用户分配 IP 地址。同样,在情形 2 中认证过程也是可选的。处理过程与情形 1 中的相同。

[0159] 情形 3:如图 11 所示,所述选择服务网络的装置包括一个报文收发单元、多个配置单元和服务网络选择单元,且所述的配置单元和服务网络选择单元存在一一对应关系。那么这样,每个配置单元中存储的只是与其相对应的服务网络选择单元所属的服务网络的配置信息。

[0160] 报文收发单元,将接收到的报文分别发送给各服务网络选择单元。各服务网络选择单元根据所述服务网络选择条件,分别读取其对应的配置单元中存储的服务网络的配置信息,判断所属的服务网络是否满足客户端或用户的要求。若满足,则将地址请求消息通过所述报文收发单元转发到所述服务网络。接下来的处理过程与情形 1 或情形 2 中的相同,在此不再赘述。

[0161] 在本发明实施例所述的装置中,服务网络选择单元判断所述服务网络的配置参数是否满足客户端或服务网络选择条件的标准,与本发明方法实施例中的相同,在此不再赘述。

[0162] 当然,配置单元与服务网络选择单元的对应关系并不局限于在此列举的几种,可根据实际需要自由配置。

[0163] 在此实施例中,所述服务网络选择条件为 DHCP Selection Option,其定义方式和组成部分与实施例 1 中所述 DHCP Selection Option 相同。

[0164] 当然,所述服务网络选择条件也可利用现有技术中的 DHCP Option 82/Option 60 来实现,也可采用其他的 Option 来实现。

[0165] 当服务网络选择条件采用不同的实现方式时,服务网络选择单元会根据具体的服务网络选择条件来进行判断,并为客户端或用户选择符合客户端或用户要求的服务网络,从而提高了服务的质量。

[0166] 此外,本发明的实施例还提供了一种选择服务网络的系统。

[0167] 如图 12 所示,所述选择服务网络的系统包括:动态主机配置协议客户端或用户,用于向认证器/代理发送携带有服务网络选择条件的地址请求消息;

[0168] 认证器/代理,用于分别配置和/或存储其所属服务网络的配置信息,并判断其所属服务网络的配置信息,是否满足所述服务网络选择条件,若满足,则将地址请求消息转发到所述服务网络;

[0169] AAA 服务器,位于服务网络端,用于根据所述地址请求消息,对客户端或用户进行认证;

[0170] 动态主机配置协议服务器(DHCP 服务器),位于服务网络端,用于为客户端或用户

分配 IP 地址。

[0171] DHCP 客户端或用户向各认证器 / 代理发送地址请求消息,并在所述地址请求消息中携带服务网络选择条件。所述认证器 / 代理根据所述服务网络选择条件,判断其所属的服务网络是否满足客户端或用户的要求。若满足,则由认证器 / 代理、AAA 服务器、DHCP 服务器之间进行认证协商,协商认证方法等。在认证通过后,由 DHCP 服务器为客户端或用户分配 IP 地址。

[0172] 在此实施例中,所述服务网络选择条件为 DHCP Selection Option,其定义方式和组成部分与方法实施例 1 中所述 DHCP Selection Option 相同。

[0173] 当然,所述服务网络选择条件也可利用现有技术中的 DHCP Option 82/Option 60 来实现。

[0174] 当服务网络选择条件采用不同的实现方式时,各认证器 / 代理会根据具体的服务网络选择条件来选择出与客户端或用户的要求相应的服务网络,并由所属服务网络为客户端或用户分配 IP 地址等。具体过程可参照网络选择方法的实施例。

[0175] 本发明的实施例选择服务网络的系统,通过 DHCP 客户端或用户发送的地址分配请求消息中所携带的服务网络选择条件,使得认证器 / 代理可以根据客户端或用户对服务网络的要求,为客户端或用户选择服务网络,并为客户端或用户分配符合其网络服务要求的 IP 地址。从而避免了现有技术中,“盲目”的为客户端或用户分配 IP 地址的缺点,提高了网络为客户端或用户服务的能力。通过本实施例所述系统,可以在多个服务网络,多个认证机构、多个代理机构的情况下,由网络选择符合客户端或用户需求的服务网络。

[0176] 当然,本发明的实施例还可有很多种,在不背离本发明的实施例精神及其实质的情况下,本领域技术人员当可根据本发明的实施例做出各种相应的改变和变形,但这些相应的改变和变形都应属于本发明的实施例所附的权利要求的保护范围。

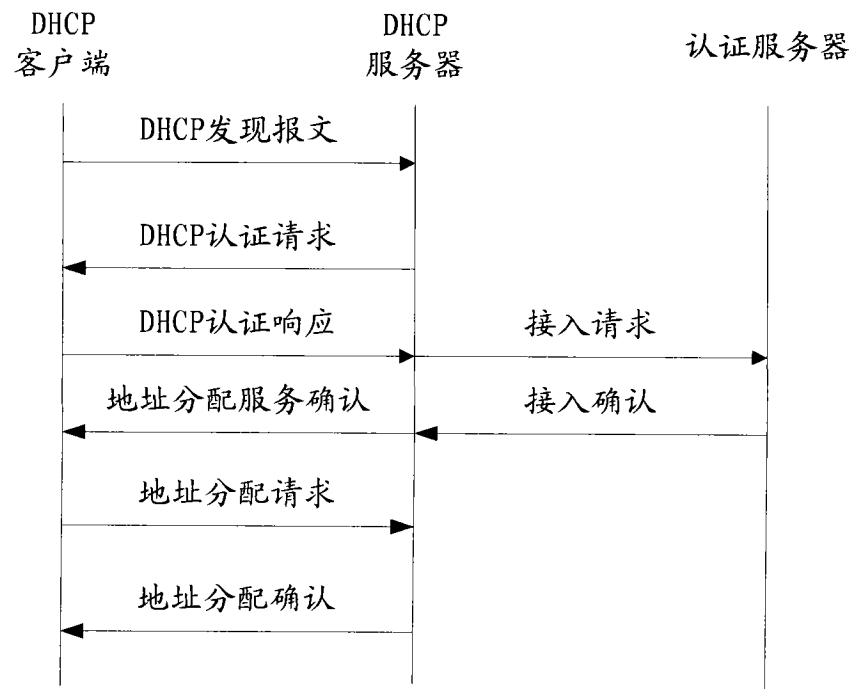


图 1

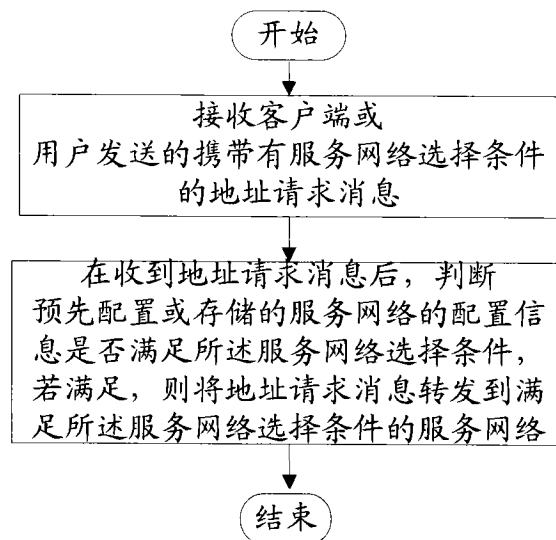


图 2

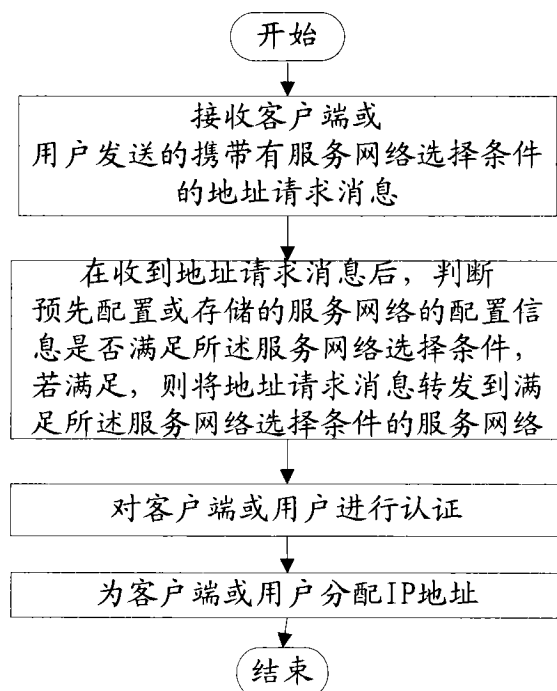


图 3

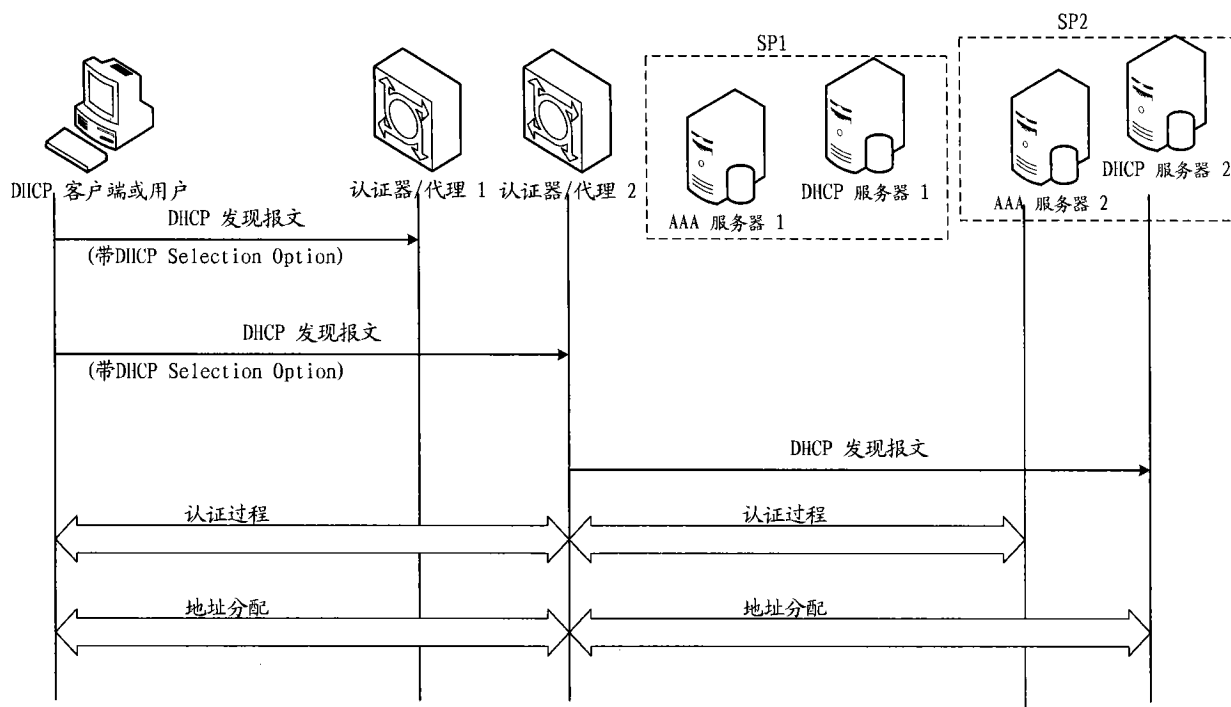


图 4

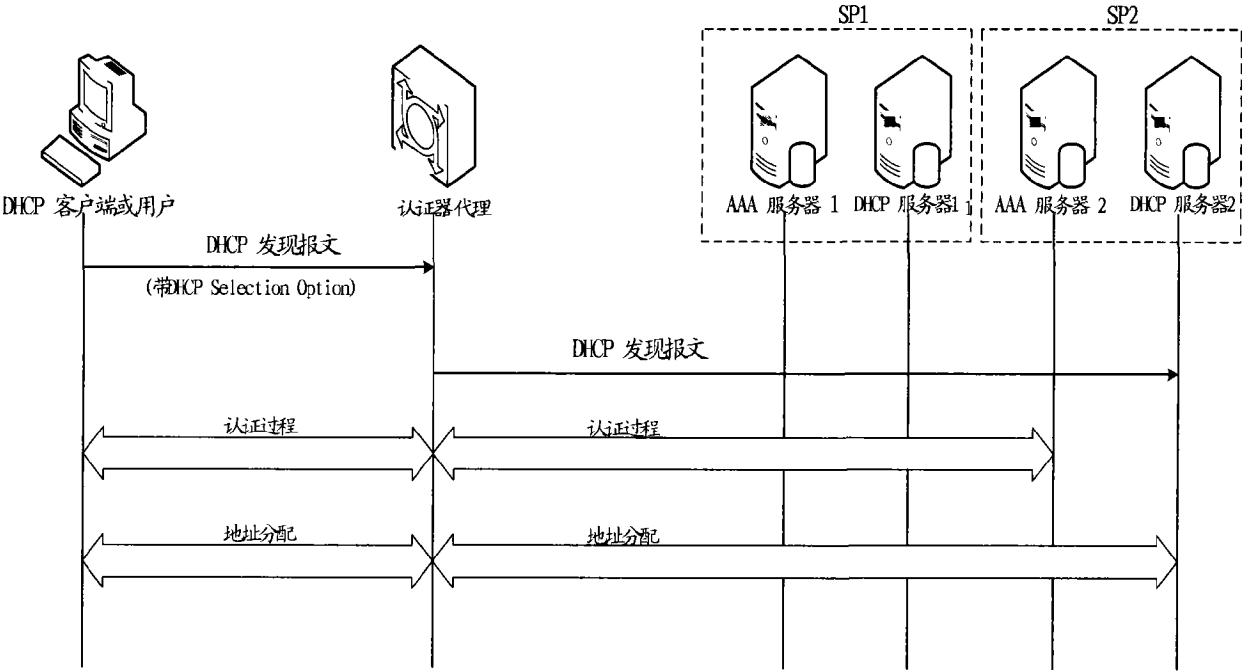


图 5

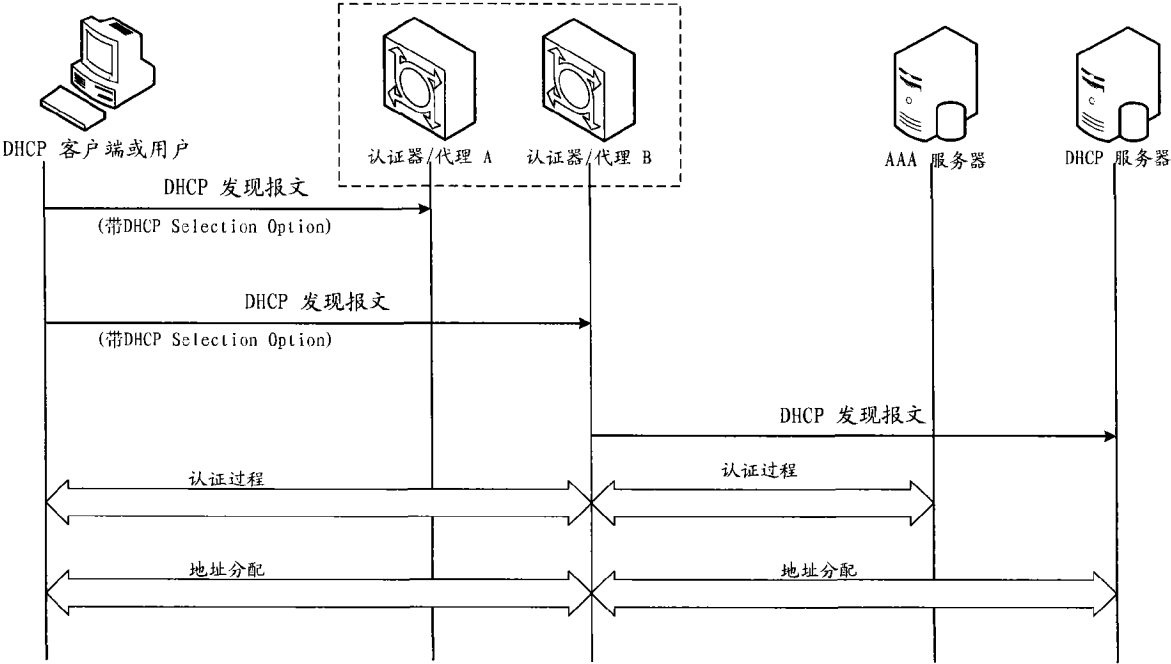


图 6

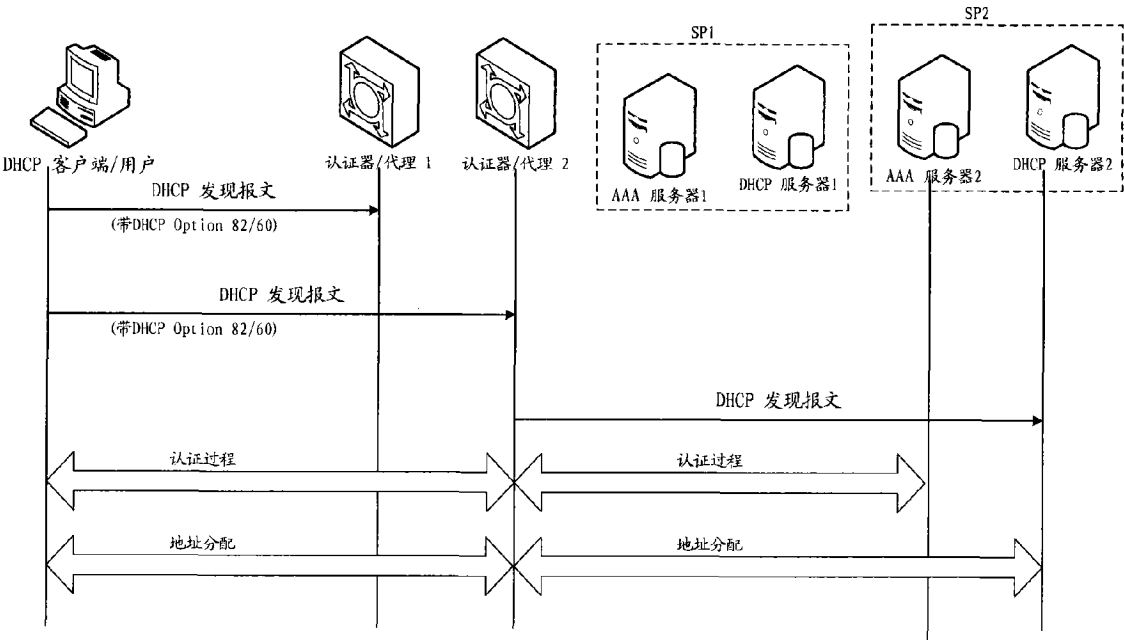


图 7

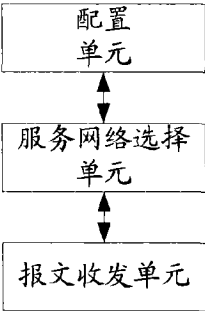


图 8

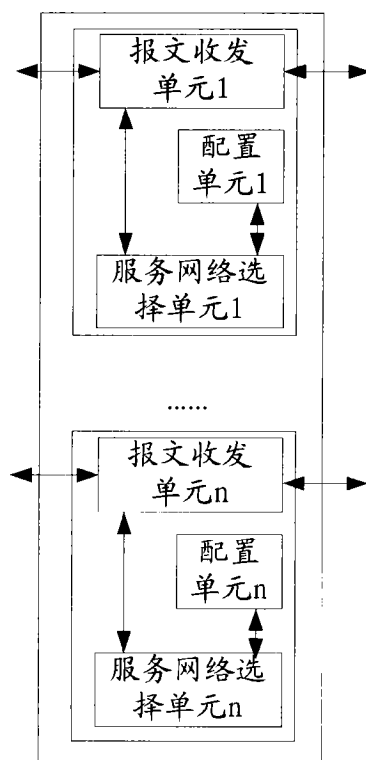


图 9

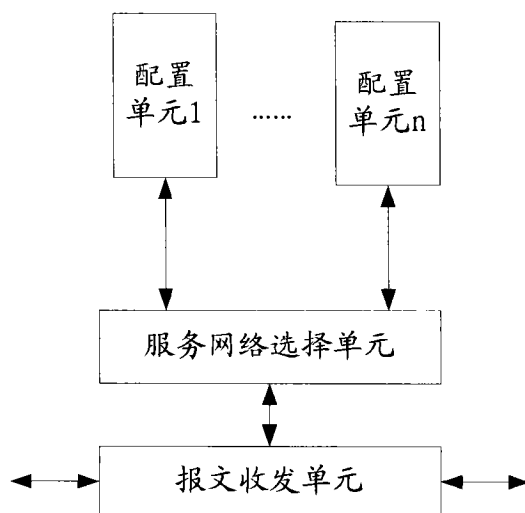


图 10

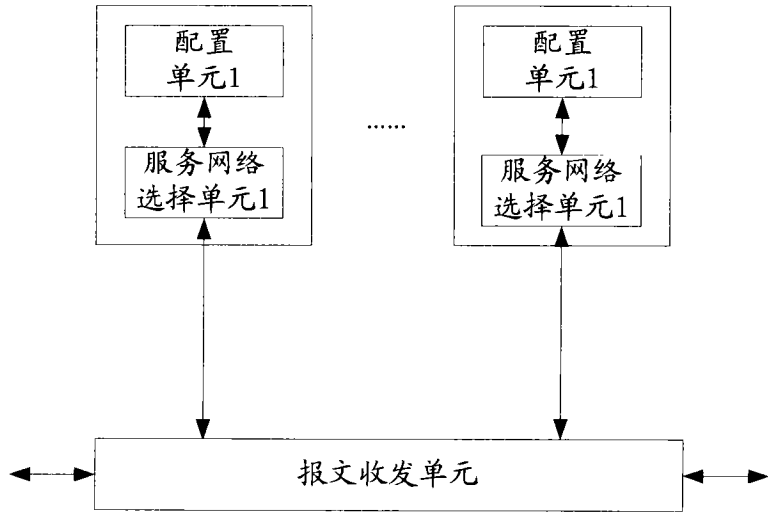


图 11

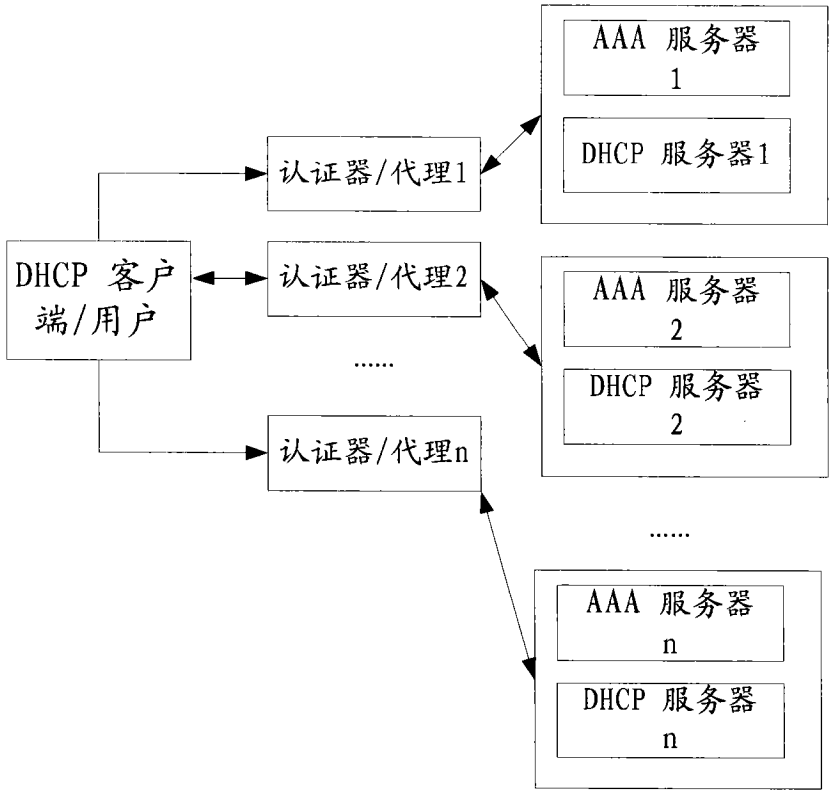


图 12