(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114258667 B
(45)授权公告日 2024.07.02

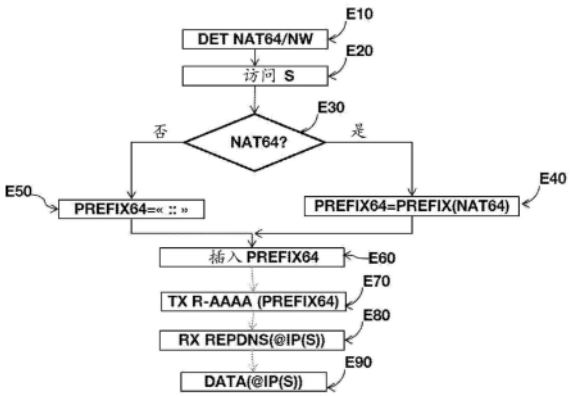
(21)申请号 202080057856.6
(22)申请日 2020.06.18
(65)同一申请的已公布的文献号
申请公布号 CN 114258667 A
(43)申请公布日 2022.03.29
(30)优先权数据
FR1906673 2019.06.20 FR
(85)PCT国际申请进入国家阶段日
2022.02.16
(86)PCT国际申请的申请数据
PCT/FR2020/051057 2020.06.18
(87)PCT国际申请的公布数据
WO2020/254766 FR 2020.12.24
(73)专利权人 奥兰治
地址 法国伊西莱穆利欧
(72)发明人 M.布卡戴尔 C.雅克内特
(74)专利代理机构 北京市柳沈律师事务所 11105
专利代理师 李芳华
(51)Int.Cl.
*H04L 61/4511*(2022.01)
*H04L 45/74*(2022.01)
*H04L 61/251*(2022.01)
(56)对比文件
FR 3023098 A1,2016.01.01
KORHONEN J等.Analysis of solution proposals for hosts to learn NAT64 prefix draft-korhonen-behave-nat64-learn-analysis-00.txt.《IETF》.2010,全文.
审查员 何丹霞
权利要求书3页 说明书23页 附图5页

(54)发明名称

# 用于获得IP地址的方法和装置

(57)摘要

本发明涉及一种用于使客户端装置获得IP地址以便经由至少一个IP网络来访问网络资源的方法,该方法包括:-在该网络资源具有IPv4连接时,将表示由该DNS服务器的客户端装置响应于用于获得IPv6地址以便访问所述网络资源的针对DNS服务器的请求而预期的IP地址类型的信息插入到该获得请求中的步骤(E60);以及-向该DNS服务器发送该获得请求的步骤(E70)。



1.一种用于使客户端装置(T)获得互联网协议IP地址以便经由向所述客户端装置提供IP连接服务的至少一个网络(NW1,NW2)来访问网络资源(S)的获得方法,所述客户端装置仅具有IPv6连接,所述方法包括:

-在所述网络资源具有IPv4连接时,将表示由所述客户端装置响应于用于获得IPv6地址以便访问所述网络资源的针对DNS服务器的请求(R-AAAA)而从所述DNS服务器预期的IP地址类型的信息插入(E60)到所述获得请求中的步骤,所述预期的IP地址类型能够是IPv4地址或伪IPv6地址;以及

-向所述DNS服务器发送(E70)所述获得请求的步骤。

2.如权利要求1所述的获得方法,其中,如果所述预期的IP地址类型是由该DNS服务器从至少一个IPv6前缀和所述网络资源(S)的IPv4地址形成的IPv6地址,则插入到该获得请求中的所述信息包括所述至少一个IPv6前缀或包括至少一个IPv6前缀的至少一个IPv6地址。

3.如权利要求2所述的获得方法,其中,所述至少一个IPv6前缀是由所述网络实施的用于将IPv4分组转换成IPv6分组的功能所使用的至少一个IPv6前缀。

4.如权利要求2所述的获得方法,其中,该获得请求进一步包括:

-用于仅当该网络资源仅具有IPv4连接时形成所述IPv6地址的指令;或者

-用于在该网络资源具有IPv4连接时形成所述IPv6地址的指令,即使该网络资源也具有IPv6连接。

5.如权利要求1所述的获得方法,其中,如果所述预期的IP地址类型是所述网络资源的IPv4地址,则插入到该获得请求中的所述信息是该DNS服务器已知的预定义值。

6.如权利要求1至5中任一项所述的获得方法,其中,该获得请求进一步包括:

-用于执行确定的算法以从该网络资源的IPv4地址形成IPv6地址的指令;和/或

-用于使用众所周知的前缀WKP前缀从该网络资源的IPv4地址形成IPv6地址的指令;和/或

-用于使用后缀的指令,该后缀保证用于检查传输层的伪报头的完整性的机制的中立性;和/或

-用于将IPv4地址插入到对该获得请求的响应的附加部分中的指令。

7.如权利要求1至5中任一项所述的获得方法,进一步包括确定所述网络是否实施用于将IPv4分组转换成IPv6分组的功能的确定步骤(E10)。

8.如权利要求7所述的获得方法,进一步包括,在所述网络实施用于将IPv4分组转换成IPv6分组的功能时,获得由所述分组转换功能使用的至少一个IPv6前缀的步骤。

9.如权利要求7所述的获得方法,其中:

-该DNS服务器是与“名义上的”DNS服务器不同的服务器,该网络的运营商已经用该服务器配置了该客户端装置;

-该确定步骤包括向该名义上的DNS服务器发送用于获得IPv6地址以便访问已知仅具有IPv4连接的给定网络资源的请求的步骤;并且

-如果从该名义上的DNS服务器接收到包括所述给定网络资源的IPv6地址的肯定响应,则该客户端装置确定该网络实施用于将IPv4分组转换成IPv6分组的功能。

10.如权利要求9所述的获得方法,包括从包含在从该名义上的DNS服务器接收的该肯

定响应中的该IPv6地址获得由用于将IPv4分组转换成IPv6分组的所述功能使用的IPv6前缀的步骤。

11.一种处理方法,由与向仅具有IPv6连接的至少一个客户端装置(T)供应IP连接服务的网络相关联的DNS服务器(DNS#2)进行,所述方法包括:

-在网络资源具有IPv4连接时,从所述客户端装置(T)接收(F10)用于获得IPv6地址以便访问所述网络资源的请求的步骤,并且在该请求中插入了表示由所述客户端装置响应于所述获得请求而从所述DNS服务器预期的IP地址类型的信息,所述预期的IP地址类型能够是IPv4地址或伪IPv6地址;

-在所述网络资源具有IPv6连接时,响应于所述获得请求而向该客户端装置发送(F70)所述网络资源的IPv6地址的步骤;

-在所述网络资源具有IPv4连接时:

获得(F50)所述网络资源的IPv4地址的步骤;以及

发送(F90,F110)对所述获得请求的响应的步骤,该响应包含由该DNS服务器从所述获得的IPv4地址中确定的并且与由该客户端装置预期的IP地址类型相对应的至少一个IP地址。

12.如权利要求11所述的处理方法,其中,插入到该获得请求中的所述信息包括至少一个IPv6前缀或包括至少一个IPv6前缀的至少一个IPv6地址,并且由该DNS服务器确定的所述至少一个IP地址包括由该DNS服务器从所述至少一个IPv6前缀和从该获得的网络资源的所述IPv4地址形成的至少一个IPv6地址。

13.如权利要求11所述的处理方法,其中,插入到该获得请求中的所述信息具有该DNS服务器已知的预定义值,并且由该DNS服务器确定的所述至少一个IP地址是该获得的网络资源的IPv4地址。

14.如权利要求13所述的处理方法,其中,所述IPv4地址由该DNS服务器在该响应的正文中发送给该客户端装置,该响应通过使用前缀“::ffff:0:0/96”根据IPv6格式进行编码。

15.如权利要求11至14中任一项所述的处理方法,其中,仅当该网络资源仅具有IPv4连接时,该发送步骤(F90,F110)和该获得步骤(F50)才由该DNS服务器实施。

16.一种客户端装置(T),该客户端装置连接到向该客户端装置供应IP连接服务的至少一个网络,所述客户端装置仅具有IPv6连接并且包括:

-插入模块(M1),该插入模块被配置成在网络资源具有IPv4连接时,将表示由所述客户端装置响应于用于获得IPv6地址以便经由所述网络来访问该网络资源的针对DNS服务器的请求而从所述DNS服务器预期的IP地址类型的信息插入到所述获得请求中,所述预期的IP地址类型能够是IPv4地址或伪IPv6地址;以及

-发送模块(M2),该发送模块被配置成向该DNS服务器发送所述获得请求。

17.如权利要求16所述的客户端装置,进一步包括用于将IPv4地址转换成IPv6地址的模块,该模块在从该DNS服务器接收到对所述获得请求的响应时被激活,该响应包括所述网络资源的IPv4地址,所述转换模块被配置成通过使用所述IPv4地址和由该网络实施的用于将IPv4分组转换成IPv6分组的功能使用的IPv6前缀来将所述IPv4地址转换成IPv6地址。

18.一种DNS服务器(DNS#2),包括:

-接收模块(M4),该接收模块能够从连接到向客户端装置供应IP连接服务的网络的所

述客户端装置接收用于获得IPv6地址以便经由所述网络来访问网络资源的请求,所述客户端装置仅具有IPv6连接;

-检测模块(M5),该检测模块被配置成在所述网络资源具有IPv4连接时,在所述请求中检测表示由所述客户端装置响应于所述获得请求而从所述DNS服务器预期的IP地址类型的信息,所述预期的IP地址类型能够是IPv4地址或伪IPv6地址;

-发送模块(M7),该发送模块在所述网络资源具有IPv6连接时被激活,并且被配置成响应于所述获得请求而向该客户端装置发送所述网络资源的IPv6地址;

-获得模块(M6),该获得模块在所述网络资源具有IPv4连接时被激活,并被配置成获得该网络资源的IPv4地址,

所述发送模块(M7)进一步在所述网络资源具有IPv4连接时被激活,并被配置成发送对所述获得请求的响应,该响应包含至少一个IP地址以便访问所述网络资源,该至少一个IP地址由该DNS服务器从所述获得的IPv4地址确定并且与插入到所述获得请求中的所述信息所指示的由该客户端装置预期的该IP地址类型相对应。

19.一种通信系统(1),包括:

-如权利要求16或17所述的客户端装置(T),该客户端装置连接到向所述客户端装置供应IP连接服务的至少一个网络,所述客户端装置仅具有IPv6连接;以及

-如权利要求18所述的DNS服务器(DNS#22),该DNS服务器旨在由该客户端装置用来经由所述网络访问网络资源。

20.如权利要求19所述的系统(1),其中,所述DNS服务器是与名义上的DNS服务器(DNS#11,DNS#21)不同的公共DNS服务器(DNS#2),所述网络的运营商已经用该公共DNS服务器配置了该客户端装置。

# 用于获得IP地址的方法和装置

## 技术领域

[0001] 本发明涉及一般电信领域,并且更具体地涉及增值IP(互联网协议)服务。

## 背景技术

[0002] IP网络已经成为用于众多服务和应用的联合网络。为了预测IP地址方面日益增长的需求,运营商、网络设备制造商和大学已经合作指定了IP协议的新版本,称为IPv6(互联网协议版本6)。IPv6规范现在已经足够成熟。因此,在运营商运营的大多数网络中,IPv6是运营部署的主题。然而,该IP协议的新版本的引入带来了由于构造而与IPv4版本的互操作性和互通的问题。

[0003] IPv4仍然主要用于互联网(大约占流量的75%),但是IPv4地址库现在已经枯竭。不应忘记IPv4地址以32位编码(相比而言IPv6地址以128位编码)。因此,IPv4地址的耗竭使得IPv6的部署成为运营商和IP服务提供商的主要问题。

[0004] 然而,两个主要限制因素使迁移策略的实施变得复杂:

[0005] -需要在过渡期间保证IPv4服务的连续性,尽管无法向每个客户端提供公共IPv4地址;以及

[0006] -IPv4协议与IPv6协议之间的不兼容性,这使两个世界的互连变得复杂。

[0007] 此外,运营商和服务提供商还必须考虑在网络和服务基础设施中引入IPv6的各种限制,还要设计利用IPv6的新固有功能的新架构。

[0008] 因此,IPv6的激活不应被视为与IPv4互联网网络并行的互联网网络的实施,而应被视为当前互联网网络的演进。现在,在IPv4协议和IPv6协议两者共存的背景下,必须特别支持仅具有单个IP栈(即IPv4栈或IPv6栈)并且因此具有单一类型的IPv4连接或IPv6连接的异构节点之间的通信。此外,用于建立给定会话的协议版本在理想情况下必须对最终用户透明。应当注意,仅具有单个IP栈,即仅具有IPv4栈(节点于是被称为仅IPv4)或仅具有IPv6栈(节点于是被称为仅IPv6)的节点能够发送、接收或处理仅符合由该IP栈实施的协议版本的分组,换句话说,对于仅IPv4节点,仅符合IPv4协议的分组,或者对于仅IPv6节点,仅符合IPv6协议的分组。

[0009] 因此,必须部署IPv4-IPv6互连机制,以确保全球连接。整体可访问性不仅涉及地址与源地址属于同一地址家族(IPv4或IPv6)的目的地,还涉及属于异构域的目的地(即具有IPv4地址或IPv6地址的任何目的地)。

[0010] 在已知IPv6协议与IPv4协议不兼容的情况下,已经选择仅基于IPv6协议(即“仅IPv6”)的部署的网络运营商使用了用于将IPv6分组转换成IPv4分组的功能,并且反之亦然,包括用于将IPv4地址转换成IPv6地址(并且反之亦然)的功能,以确保IPv4服务的连续性。通常称为NAT64的该功能(也称为用于将IPv4分组转换成IPv6分组的功能)在IETF(互联网工程任务组)于2011年4月发布的且名称为“Stateful NAT64:Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers[有状态NAT64:从IPv6客户端到IPv4服务器的网络地址和协议转换]”的文档RFC 6146中进行了描述。

[0011] 参考图1,考虑:

[0012] -仅IPv6网络N1,其中仅激活IPv6连接服务用于传递IP分组,并且仅具有IPv6栈的终端TERM连接到该网络;以及

[0013] -仅IPv4网络N2,其中仅激活IPv4连接服务用于传递IP分组,并且因此仅可在IPv4模式下访问的远程服务器SERV连接到该网络。

[0014] 为了允许终端TERM访问远程服务器SERV,调用NAT64功能,以便一方面使用外部IPv4地址(和外部端口号),这使得可以建立与远程服务器SERV的通信,并且另一方面维护该外部IPv4地址与终端TERM使用的IPv6源地址(以及源端口号)之间的关联。为此,NAT64功能使用包含IPv4地址的特定IPv6地址,并且如IETF在2010年10月名称为“IPv6 Addressing of IPv4/IPv6 Translators[IPv4/IPv6转换器的IPv6寻址]”的RFC 6052文档中所定义的。这种IPv6地址可以具有不同的类型,并且更具体地具有以下类型:

[0015] -“IPv4嵌入的IPv6”类型,该类型指定在其128位中包括与IPv4地址相对应的32位的IPv6地址;

[0016] -“IPv4转换的IPv6”类型(“IPv4嵌入的IPv6”类型地址的变体),该类型指定表示IPv6网络中的IPv4节点的IPv6地址(换句话说,IPv4节点将可以从仅IPv6节点使用该地址进行访问);以及

[0017] -“IPv4可转换IPv6”类型,该类型指定分配给IPv6节点的允许无状态IPv6-IPv4互连的IPv6地址。

[0018] 为了将IPv4地址转换成“IPv4嵌入的IPv6”地址(并且反之亦然),运营商可以使用形成其整体IPv6前缀的一部分的称为NSP(“网络特定前缀”)的前缀,或者使用由IETF分配的称为WKP(“众所周知的前缀”)的前缀,例如前缀“64:ff9b::/96”(其他WKP前缀已经由IETF保留,如前缀“64:ff9b::/48”)。应当注意,当所使用的前缀长度小于96时,优选十六进制表示法,以便表示适当构造的IPv6地址(换句话说,所包括的IPv4地址不会以十进制表示)。因此,作为说明,“2001:db8:122:344:c0:2:2100::”是使用NSP前缀“2001:db8:122:344::/64”从地址“192.0.2.33”构造“伪”(虚拟)IPv6地址的结果;“64:ff9b::192.0.2.33”是使用WKP前缀64:ff9b::/96从地址192.0.2.33构造“伪”IPv6地址的结果。NAT64功能根据不同的工程被配置有NSP或WKP前缀,以在IPv4地址的基础上构造IPv6地址,并且反之亦然。此处的术语“伪”指定IPv4地址由DNS服务器转换为IPv6地址,而不是授予具有IPv6连接的资源的“本地”IPv6地址。

[0019] 如本身已知的,DNS(“域名系统”)服务允许连接到IP网络的用户终端(或嵌入到该终端中的应用程序)从域名中获得IP(IPv4和/或IPv6)地址或由该域名指定的网络资源的地址。网络资源被理解为受益于IP连接并且可以经由IP地址到达的任何类型的装置或设备,例如服务器。可以设想几种传输模式用于交换DNS消息,这些消息包括IETF最近定义的那些消息,如DNS-over-TLS、DNS-over-DTLS或DoH(DNS-over-HTTP)。

[0020] 具有IPv4连接并且因此可以经由IPv4地址到达的网络资源可以与DNS服务一起发布类型A的DNS记录(或A RR(资源记录)),从而建立与该网络资源相关联的域名与其IPv4地址之间的对应关系。具有IPv6连接并且因此可以在IPv6模式下到达的网络资源可以发布AAAA类型的记录(或AAAA RR)。受益于IPv4连接和IPv6连接并且因此可以经由IPv4地址和IPv6地址到达的网络资源可以分别发布类型A和类型AAAA的两个记录。在IETF文档RFC1035

和RFC3596中分别描述了类型A和AAAA的RR记录。DNS记录的发布由网络资源(例如,通过“动态DNS”机制)或另一个实体(例如,管理员)执行。在下文中,没有对用于发布这种记录的方法进行假设。

[0021] 根据DNS服务的当前操作模式,当终端希望到达如服务器等网络资源时,该终端向DNS服务发送对该其拥有的域名的解析请求,以便访问服务器。在该域名解析请求中,终端必须指定该终端响应于其请求而想要的记录类型(A或AAAA)。因此,支持IPv4协议和IPv6协议两者的终端必须向DNS服务发送两个请求:指示类型A的记录并且旨在获得网络资源的一个或多个IPv4地址的第一请求(在下文的描述中也称为“用于获得IPv4地址的DNS请求”或更简单地指定为“类型A的DNS请求”),以及指示类型AAAA的记录并且旨在获得网络资源的一个或多个IPv6地址的第二请求(在下文的描述中也称为“用于获得IPv6地址的DNS请求”或更简单地指定为“类型AAAA的DNS请求”)。因此,网络中IPv6的激活会影响DNS服务器的规模,因为可以为同一个网络资源传输两个域名解析请求。如果必须同时(而非顺序地)发送这两个请求以便优化通信建立延迟,则这些影响就更大了。

[0022] 选择在其网络中部署NAT64功能的IP连接提供商几乎系统地部署了DNS64功能,其配置有与NAT64功能使用的前缀相同的前缀,以便基于仅IPv4服务器的IPv4地址构造“IPv4转换的IPv6”类型的IPv6地址。依赖于NAT64和DNS64功能的使用的该工程理论上假设IPv6终端仅向DNS服务传输类型AAAA(IPv6)的DNS请求,而不传输类型A(IPv4)的DNS请求。然而,在实践中,当前部署揭示了终端的非最佳行为,这些终端针对相同的网络资源系统地发送类型A和类型AAAA的两个DNS请求。如先前所指示的,终端的该行为对DNS服务器的规模产生重大影响(由于为每个解析传输了两个请求,处理负荷加倍,对DNS流量产生影响),而且对建立用户连接时引起的延迟也产生重大影响,这可能导致终端用户感知到的连接服务质量下降。

[0023] 该问题的一种解决方案可以包括通过配置来限制由连接到仅IPv6网络的终端传输的DNS请求的类型。然而,这并不构成可行的解决方案。

[0024] 事实上,如今越来越多的第三方运营商(不同于提供IP连接服务的运营商)向终端的用户提供公共DNS服务。根据这些第三方运营商,与IP连接服务运营商运行的DNS服务器相比,这些公共DNS服务提高了用户的体验质量,和/或提供了高级安全性和保密功能。因此,一些第三方运营商指示在11ms内提供对DNS请求的响应,而在IP连接服务的运营商中观察到的平均值为68ms。面对这种争论,越来越多的用户正在他们的终端(无论是固定的还是移动的)上用涉及公共DNS服务器的配置来替换由其IP连接运营商供应的名义上的DNS服务配置。

[0025] 在这种情况下,将连接到仅IPv6网络的终端传输的DNS请求限制为单一类型的请求(在这种情况下为AAAA)可能导致禁止这些终端访问仅IPv4服务器,这既不可取也不可接受。

## 发明内容

[0026] 本发明使得尤其可以通过提出一种用于使客户端装置获得IP地址以便经由向该客户端装置提供IP连接服务的至少一个网络来访问网络资源(例如,与域名相关联的网络资源)的方法来克服现有技术的缺点,该方法由该客户端装置实施并且包括:

[0027] -在该网络资源具有IPv4连接时,将表示由该客户端装置响应于用于获得IPv6地址以便访问该网络资源的针对该DNS服务器的请求(换句话说,在如先前提及的类型AAAA的DNS请求中)而从该DNS服务器预期的IP地址类型的信息插入到该获得请求中的步骤;以及

[0028] -向该DNS服务器发送该请求的步骤。

[0029] 相关地,本发明还涉及一种客户端装置,该客户端装置连接到向该客户端装置供应IP连接服务的至少一个网络,该客户端装置包括:

[0030] -插入模块,该插入模块被配置成在网络资源具有IPv4连接时,将表示由该客户端装置响应于用于获得IPv6地址以便经由该网络来访问该网络资源的针对DNS服务器的请求而从该DNS服务器预期的IP地址类型的信息插入到该获得请求中;以及

[0031] -发送模块,该发送模块被配置成向该DNS服务器发送该获得请求。

[0032] 例如,在特定实施例中,如果预期的IP地址类型是由该DNS服务器从所述至少一个IPv6前缀和目标网络资源的IPv4地址形成的伪IPv6地址,则表示预期的IP地址类型并且如插入到该DNS请求中的该信息可以是至少一个IPv6前缀或者包括至少一个IPv6前缀的至少一个IPv6地址。该IPv6前缀尤其可以是由该客户端装置设想用来访问该网络资源的网络实施的用于将IPv4(数据)分组转换成IPv6(数据)分组(反之亦然)的功能(例如NAT64)使用的前缀,或包括这种前缀的IP地址。

[0033] 作为变体,如果预期的IP地址类型是该网络资源的IPv4地址,则插入的该信息可以是该DNS服务器已知的预定义值(例如零值或专用于该用途的另一个前缀)。

[0034] 相关地,根据本发明的客户端装置可以进一步包括用于将IPv4地址转换成IPv6地址的模块,该模块在从该DNS服务器接收到对所述获得请求的响应时被激活,并且该响应包括所述网络资源的IPv4地址,所述转换模块被配置成通过使用所述IPv4地址和由该网络实施的用于将IPv4分组转换成IPv6分组的功能使用的IPv6前缀来将所述IPv4地址转换成IPv6地址。

[0035] 当该网络资源具有IPv4连接时,由该客户端装置插入到用于获得IPv6地址的请求中的该信息因此允许该客户端装置指定其响应于用于获得IPv6地址的该请求(换句话说,在对用于获得IPv6地址的该请求的响应中,即如果该获得请求是DNS AAAA请求,则在AAAA类型的响应的“应答部分”部分中)而预期伪IPv6地址还是IPv4地址。

[0036] 注意,无论该客户端装置配置的该DNS服务器如何,本发明都有利地适用于:该服务器可以是在此称为“名义上”的DNS服务器,该DNS服务器由向该客户端装置提供该IP连接服务的运营商供应,例如在其附接到网络时或者在先前的配置中(例如,“工厂”配置),或者是替代性DNS服务器,例如该客户端装置的用户已经选择使用的公共DNS服务器,而不是其运营商提供的名义上的DNS服务器。这是由于该客户端装置在询问DNS服务器以便获得该客户端装置希望访问的该网络资源的IP地址时向该服务器供应的该信息。

[0037] 此外,参考向该客户端装置提供IP连接服务的网络来描述本发明。应当注意,该客户端装置可以同时具有几个活动连接接口,这些活动连接接口允许访问不同的网络,这些网络中的每一个都为该客户端装置提供了IP连接;然后,本发明适用于为这些活动连接接口中的每一个配置的每个DNS服务器。同一个DNS服务器可以用于若干个活动连接接口,或者每个活动连接接口可以使用不同的DNS服务器。

[0038] 本发明提供了一种机制,该机制使得可以协调这些服务提供商(IP连接的提供商

和公共DNS提供商)的需求、用户的需求以及终端制造商的需求。

[0039] 事实上,本发明提供的机制允许客户端装置根据该客户端装置的设置该客户端装置在网络资源具有IPv4连接时希望接收的IP地址类型的能力通过类型AAAA的单个请求(用于获得IPv6地址以便访问本发明意义内的网络资源的请求)来获得不同类型的IP地址,这取决于该客户端装置寻求访问的该网络资源是受益于IPv4连接、IPv6连接还是两者。因此,本发明允许仅IPv6客户端装置访问仅IPv4、仅IPv6或IPv4/IPv6网络资源,而不会不必要地使该客户端装置调用的该DNS服务器过载,并且同时节省了该客户端装置的资源(如果是移动装置,尤其是其电池)。由接入网路由的流量、并且更具体地DNS流量的体积密度被优化,并且因此,通信建立延迟也被优化。其结果是如该客户端装置的用户感知到的体验质量提高。

[0040] 此外,本发明为该客户端装置的用户提供了自由,该用户可以无偏好地使用他的或她的IP连接运营商的名义上的DNS服务器,或者用第三方运营商提供的DNS服务器(例如,如先前提及的公共DNS服务器)配置他的或她的客户端装置。借助于本发明,因此在使用由客户端装置的IP连接提供商提供的名义上的DNS服务器的这些客户端装置与决定使用由第三方服务提供商提供的替代性DNS服务的这些客户端装置之间存在一种功能对等形式。

[0041] 本发明还使得可以管理网络的不同可能配置,并且尤其是用于该网络的DNS服务器的不同可能配置,该服务器可以或可以不嵌入用于将IPv4地址转换成IPv6地址的DNS64以促进服务连续性的功能。

[0042] 应当注意,一些客户端装置本身可以嵌入地址转换模块,也称为CLAT(“客户侧(地址)转换器”)或BIH(主机中的块(Bump-in-the-Host))模块或功能,例如以允许安装在该客户端装置上并且仅在IPv4栈上运行的应用程序将包括客户端装置何时仅具有IPv6连接的消息传输到IPv4地址。这种模块于2013年4月在名称为“464XLAT:Combination of stateful and stateless translation[464XLAT:有状态和无状态转换的结合]”的IETF文档RFC 6877中进行了描述。当DNS64功能由该客户端装置咨询以访问资源的DNS服务器实施时,如果同时激活该DNS64功能和该客户端装置的CLAT模块,则两者是冗余的。本发明使得可以避免这种冗余,并且显著地最小化对CLAT模块的依赖。

[0043] 具体地,在可以被插入到上文提供的获得请求中的信息的示例中,预定义值使得可以管理由该客户端装置咨询的DNS服务器没有实施DNS64功能的情况,或者解除对由该DNS服务器支持的DNS64功能的依赖。在这种情况下,如果该客户端装置实施了CLAT模块,则该客户端装置可以使用返回给该客户端装置的IPv4地址来继续自己将该IPv4地址转换成IPv6地址。

[0044] 因此,本发明提供了在也由该DNS服务器支持DNS64功能的情况下避免冗余,而且还允许该客户端装置直接管理IPv6地址的构造的可能性。

[0045] 如果该DNS服务器实施了DNS64功能,则该客户端装置可以向该DNS服务器供应前缀,该前缀用于从该客户端装置的IPv4地址生成仅IPv4或双栈(IPv4-IPv6)网络资源的伪IPv6地址。然后,在来自DNS64服务器的响应中,由DNS64服务器如此形成的IPv6地址被返回到该客户端装置。供应的前缀通常是由网络中存在的用于将IPv4分组转换成IPv6分组的NAT64功能使用的前缀,该客户端装置希望经由该功能来访问网络资源。

[0046] 因此,本发明也适用于不实施DNS64功能并且依赖于由该客户端装置自身实施这

种功能的网络的情况。

[0047] 因此,本发明在先前描述的当前IPv4到IPv6迁移的背景下特别有利。

[0048] 在特定实施例中,该获得请求可以进一步包括:

[0049] -用于仅当该网络资源仅具有IPv4连接时生成IPv6格式的所述地址的指令;或者

[0050] -用于在该网络资源具有IPv4连接时生成IPv6格式的所述地址的指令,即使该网络资源也具有IPv6连接。

[0051] 借助于当客户端装置预期IPv6格式的地址时由该客户端装置插入到该获得请求中的该附加指令,可以更优化地管理被配置成与IPv4-IPv6网络资源通信的仅IPv4应用程序被嵌入到仅IPv6客户端装置上的情况(该客户端装置然后也嵌入CLAT模块)。事实上,该客户端装置在这种情况下可以请求该DNS服务器响应于该客户端的请求而不仅向该客户端装置发送网络资源的本地IPv6地址(当网络资源具有IPv6连接时,该DNS服务器在默认情况下在接收到AAAA类型的请求时将做什么),而且还发送该客户端装置然后可以直接向应用程序供应的IPv4地址,而无需激活NAT46功能以便将网络资源的本地IPv6地址转换成应用程序能够使用的IPv4地址。注意,在双连接网络资源的情况下,该客户端装置能够将由该DNS服务器为网络资源生成(即形成)的伪IPv6地址与该网络资源的本地IPv6地址区分开,因为该客户端装置具有用于形成伪IPv6地址的前缀。

[0052] 在另一个实施例中,该获得请求还可以包括针对该DNS服务器的其他指示,例如:

[0053] -用于执行确定的算法以从该网络资源的IPv4地址形成IPv6地址的指令(例如在IETF文档RFC 6052中定义的算法);和/或

[0054] -用于使用已知前缀(WKP,众所周知的前缀)从该网络资源的IPv4地址形成IPv6地址的指令;和/或

[0055] -用于使用后缀的指令,该后缀保证传输层的伪报头的“校验和”(完整性检查机制)的中立性;和/或

[0056] -用于将一个或多个IPv4地址返回到对该获得请求的响应的附加部分的指令。

[0057] 用于使用该WKP前缀的指令在希望在适当的情况下在来自该DNS服务器的响应的正文中将网络资源的IPv4地址传输到该客户端装置的实施例中可以证明是特别有用的。在该实施例中,然后可以通过使用该WKP前缀根据IPv6格式对IPv4地址进行编码。

[0058] 不应忘记TCP伪报头还覆盖了IP层的源地址和目的地址。因此,对这些地址的任何修改都会使基于伪报头(称为“校验和”)的检查验证过时。用于使用后缀的指令使得可以在通过NAT64(或CLAT)功能将IPv4分组转换成IPv6分组(反之亦然)时避免重新计算TCP该“校验和”。如果不使用该指令,则该NAT64功能必须基于新的伪报头重新计算该“校验和”。

[0059] 在特定实施例中,该方法进一步包括确定该网络是否实施用于将IPv4分组转换成IPv6分组的功能(反之亦然)(即,NAT64功能)的步骤。

[0060] 在适当的情况下,该方法可以进一步包括获得由所述转换功能(即,NAT64)使用的至少一个IPv6前缀的步骤。

[0061] 这允许该客户端装置自己动态地发现其连接到的网络以及其为了访问网络资源而设想使用的网络是否实施了NAT64功能。当该客户端装置具有几个活动网络接口或者当该客户端装置改变网络接口时,该实施例提供了特别的优势。注意,实施NAT64功能的网络的一部分没有限制:该功能可以位于接入网、核心网或互连网络等中。

[0062] 作为变体,例如在“工厂”配置的背景下,该客户端装置可以独立于实施根据本发明的方法而配置有该信息。该变体特别适用于客户端装置,如CPE(“客户驻地设备”)。

[0063] 为了发现网络是否实施了用于将IPv4分组转换成IPv6分组的功能,可以设想各种技术。

[0064] 因此,在特定实施例中,该客户端装置向其发送该获得请求的DNS服务器是与所谓的“名义上的”DNS服务器不同的服务器,该网络的运营商已经用该服务器配置了该客户端装置,并且:

[0065] -该确定步骤包括向名义上的DNS服务器发送用于获得IPv6地址以便访问已知仅具有IPv4连接的给定网络资源的请求的步骤;并且

[0066] -如果从名义上的DNS服务器接收到包括要用于访问给定网络资源的IPv6地址的肯定响应,则该客户端装置确定该IP网络实施了用于将IPv4分组转换成IPv6分组的功能(NAT64功能)。

[0067] 在该实施例中,该方法可以进一步包括从在从名义上的DNS服务器接收到的肯定响应中包含的IPv6地址获得由用于将IPv4分组转换成IPv6分组的功能使用的IPv6前缀的步骤。

[0068] 该实施例要求在该客户端装置上存储与由网络运营商供应的名义上的DNS配置相关的信息,该网络运营商向该客户端装置提供其IP连接,以便在该客户端装置随后用替代性DNS服务器配置时访问该网络资源。然而,它确实提供了一种很容易由该客户端装置实施的解决方案,以便动态地发现该IP网络是否包括NAT64功能,并且这样做不涉及所述NAT64功能。

[0069] 在另一个实施例中,确定步骤可以使用端口控制协议(PCP)来实施。

[0070] PCP协议本身是已知的,并且于2014年5月在名称为“Discovering NAT64 IPv6 Prefixes Using the Port Control Protocol(PCP)[使用端口控制协议(PCP)发现NAT64 IPv6前缀]”的IETF文档RFC 7225中进行了具体描述。

[0071] 该实施例呈现出可靠和确定性的优势,因为关于NAT64功能的存在以及由该功能使用的这些前缀的信息在必要时由位于由该客户端装置传输的消息的路径上的该NAT64功能本身提供。此外,这使得可以管理由网络运营商实施若干个NAT64功能的情况。

[0072] 在又一实施例中,根据本发明的获得方法包括:

[0073] -接收源自网络的广告消息的步骤,该广告消息包括由网络实施的用于将IPv4分组转换成IPv6分组的功能所使用的至少一个IPv6前缀;以及

[0074] -存储包含在该广告消息中的所述至少一个IPv6前缀的步骤。

[0075] 在该实施例中,该客户端装置使用由网络本身通告的信息来从中推断该网络是否使用NAT64功能,并且在适当的情况下,获得该功能使用的一个或多个前缀。

[0076] 此外,该实施例在发现过程中不涉及该NAT64功能,并且基于本身已知的配置机制。

[0077] 在特定实施例中,在检测到影响该客户端装置针对所述网络的网络配置的变化时,针对网络重复确定步骤。

[0078] 这种改变例如是由该客户端装置询问的该DNS服务器的改变,以便经由该网络或到新网络的连接来访问资源。因此,本发明使得可以针对该客户端装置的用户动态且透明

地适应该客户端装置的配置变化,并且尤其是DNS配置的变化(例如,当用户决定使用替代性DNS服务器而不是其名义上的DNS服务器时,或者如果DNS配置的变化由网络运营商决定)。

[0079] 鉴于以上情况,本发明基于该客户端装置及其实施的获得方法,还基于处理源自该客户端装置的DNS请求的DNS服务器以及由该客户端装置执行的处理方法。

[0080] 因此,本发明还针对一种处理方法,由与向至少一个客户端装置提供IP连接服务的网络相关联的DNS服务器进行,该方法包括:

[0081] -在网络资源具有IPv4连接时,从客户端装置接收用于获得IPv6地址以便访问该网络资源的请求的步骤,在该请求中插入了表示由该客户端装置响应于该获得请求而从该DNS服务器预期的IP地址类型的信息;

[0082] -在该网络资源具有IPv6连接时,响应于该获得请求而向该客户端装置发送所述网络资源的IPv6地址的步骤;

[0083] -在该网络资源具有IPv4连接时:

[0084] 获得该网络资源的IPv4地址的步骤;以及

[0085] 发送对该获得请求的响应的步骤,该响应包含由该DNS服务器从该获得的IPv4地址中确定的并且与由该客户端装置预期的IP地址相对应的至少一个IP地址,以便访问该网络资源。

[0086] 相关地,本发明涉及一种DNS服务器,包括:

[0087] -接收模块,该接收模块能够从连接到向客户端装置供应IP连接服务的网络的所述客户端装置接收用于获得IPv6地址以便经由所述IP网络来访问网络资源的请求;

[0088] -检测模块,该检测模块被配置成在该网络资源具有IPv4连接时,在该获得请求中检测表示由该客户端装置响应于该获得请求而从该DNS服务器预期的IP地址类型的信息;

[0089] -发送模块,该发送模块在该网络资源具有IPv6连接时被激活,并且被配置成响应于该获得请求而向该客户端装置发送该网络资源的IPv6地址;

[0090] -在该网络资源具有IPv4连接时被激活的模块,这些模块包括:

[0091] 获得模块,该获得模块被配置成获得该资源的IPv4地址;以及

[0092] 发送模块,该发送模块被配置成发送对该获得请求的响应,该响应包含至少一个IP地址以便访问所述网络资源,该至少一个IP地址由该DNS服务器从获得的IPv4地址确定并且与插入到该获得请求中的该信息所指示的由该客户端装置预期的该IP地址类型相对应。

[0093] 根据本发明的该处理方法和该DNS服务器受益于与根据本发明的获得方法和该客户端装置相同的先前引用的优势。

[0094] 本发明还提供了这样的可能性,即当该客户端装置试图获得地址的该网络资源具有IPv4连接,并且该客户端装置指示其响应于其用于获得IPv6地址的请求而预期IPv4地址时,DNS服务器响应于具有IPv4地址的用于获得IPv6地址的请求。

[0095] 在特定实施例中,插入到该获得请求中的该信息包括至少一个IPv6前缀或包括至少一个IPv6前缀的至少一个IPv6地址,并且由该DNS服务器确定的所述至少一个IP地址包括由该DNS服务器从所述至少一个IPv6前缀和从获得的网络资源的该IPv4地址形成的至少一个IPv6地址。

[0096] 作为变体,插入到该获得请求中的该信息可以具有该DNS服务器已知的预定义值,并且由该DNS服务器确定的所述至少一个IP地址然后是获得的网络资源的该IPv4地址。

[0097] 应当注意,该网络资源的IPv4地址可以在来自该DNS服务器的响应中发送,该响应的附加部分根据IPv4格式进行编码。

[0098] 作为变体,该IPv4地址可以在来自该DNS服务器的响应的正文中传输,该响应例如通过使用前缀“::ffff:0:0/96”根据IPv6格式进行编码。

[0099] 在特定实施例中,仅当该网络资源仅具有IPv4连接时,发送步骤和获得步骤才由该DNS服务器实施。换句话说,如果该网络资源除了具有IPv4连接之外还具有IPv6连接,则响应于类型AAAA的获得请求默认地向该客户端装置发送的是该网络资源的IPv6地址。

[0100] 在另一个实施例中,当该网络资源具有IPv4连接时实施发送步骤和获得步骤,即使该网络资源也具有IPv6连接。该实施例的优势先前已经描述过,并且这里不再赘述。

[0101] 在特定实施例中,该获得方法和/或该处理方法由计算机实施。

[0102] 本发明还针对存储介质上的第一计算机程序,该程序能够在计算机中或者更一般地在符合本发明的客户端装置中实施,并且包括适于实施如上文描述的获得方法的指令。

[0103] 本发明还针对存储介质上的第二计算机程序,该程序能够在计算机中或者更一般地在符合本发明的DNS服务器中实施,并且包括适于实施如上文描述的处理方法的指令。

[0104] 这些程序中的每个程序可以使用任何编程语言,并且可以是源代码、目标代码、或在源代码与目标代码之间的中间代码的形式,如呈部分编译的形式、或呈任何其他期望的形式。

[0105] 本发明还针对可以被计算机读取并且包括上述第一或第二计算机程序的指令的信息介质或存储介质。

[0106] 该信息或存储介质可以是能够存储程序的任何实体或装置。例如,该介质可以包括存储装置,如ROM(例如,CD ROM或微电子电路ROM),或者甚至磁性存储装置(例如,硬盘或闪速存储器)。

[0107] 此外,该信息或存储介质可以是如电信号或光信号等可传输介质,其可以经由电缆或光缆、通过无线电链路、通过无线光链路或通过其他装置被传输。

[0108] 根据本发明的程序可以具体地通过互联网类型的网络进行下载。

[0109] 可替换地,每个信息或存储介质可以是并入了程序的集成电路,该电路被适配成执行或用于执行根据本发明的获得方法或根据本发明的处理方法。

[0110] 根据另一方面,本发明针对一种通信系统,包括:

[0111] -根据本发明的至少一个客户端装置,该至少一个客户端装置经由连接接口连接到至少一个IP网络;以及

[0112] -根据本发明的至少一个DNS服务器,该至少一个DNS服务器由该客户端装置结合所述连接接口使用。

[0113] 在特定实施例中,该DNS服务器是与所谓的名义上的DNS服务器不同的公共服务器,该IP网络的运营商已经用该服务器配置了该客户端装置。

[0114] 根据本发明的通信系统受益于与根据本发明的该获得方法、该处理方法、该客户端装置和该DNS服务器相同的先前引用的优势。

[0115] 在其他实施例中,还可以设想根据本发明的该获得方法、该处理方法、该客户端装

置、该DNS服务器和该通信系统组合具有上述特性的全部或部分的可能性。

## 附图说明

[0116] 本发明的其他特征和优点将在以下参考附图所给出的描述中显现出来,这些附图展示了本发明的完全非限制性的示例性实施例。在附图中:

[0117] [图1]已经描述的图1在其环境中表示现有技术的通信系统,其中在仅IPv6网络与仅IPv4网络之间实施NAT64功能;

[0118] [图2]图2在其环境中表示了根据本发明的通信系统,在具体实施例中,该系统包括符合本发明的客户端装置和DNS服务器;

[0119] [图3]图3示意性地展示了在具体实施例中图2的客户端装置的硬件架构;

[0120] [图4]图4示意性地展示了在具体实施例中图2的DNS服务器的硬件架构;

[0121] [图5]图5以流程图的形式表示如在具体实施例中由图2的客户端装置实施的根据本发明的获得方法的主要步骤;

[0122] [图6]图6表示根据本发明由图2的客户端装置在其DNS请求中插入的信息的第一可能格式;

[0123] [图7]图7表示根据本发明由图2的客户端装置在其DNS请求中插入的信息的第二可能格式;

[0124] [图8]图8以流程图的形式表示如在具体实施例中由图2的DNS服务器实施的根据本发明的处理方法的主要步骤;

[0125] [图9]图9展示了使用网络资源的IPv6地址(该地址由DNS服务器返回并且不与为其生成该IPv6地址的网络连接接口相对应)对客户端装置与网络资源之间的通信体验质量的影响;以及

[0126] [图10]图10展示了使用网络资源的IPv6地址(该地址由DNS服务器返回并且不与为其生成该IPv6地址的网络连接接口相对应)对客户端装置与网络资源之间的通信体验质量的影响的另一个示例。

## 具体实施方式

[0127] 图2在其环境中表示在具体实施例中的符合本发明的通信系统1。

[0128] 通信系统1包括符合本发明的至少一个客户端装置T。在此处设想的示例中,客户端装置T是用户的终端,例如智能电话、数字平板计算机、便携式计算机等。注意,客户端装置T的性质没有限制。作为变体,该客户端装置可以是连接到局域网的路由器或CPE(“客户驻地设备”)、附接到用户设备的USB密钥或加密狗等。

[0129] 根据本发明,客户端装置T具有至少一个活动连接接口,经由该接口,该客户端装置连接到为其提供IP连接服务的至少一个网络(为了简单起见,在下文中称为“IP网络”)。在图2的示例中,客户端装置T具有两个活动连接接口I1和I2,经由这两个接口,该客户端装置分别连接到IP网络NW1和IP网络NW2。网络NW1和NW2两者向客户端装置T提供IP服务,具体地允许客户端装置T连接到公共互联网网络的IP连接。对由网络NW1和NW2向客户端装置提供的IP服务的性质(IP连接、IP语音服务等)或网络NW1和NW2的性质没有限制。这些网络可以是符合3GPP标准(版本15、16和后续版本)、WLAN(无线本地接入网)等任何一个版本的固

定或移动网络,例如3G、4G或5G网络。

[0130] 如先前提及的,本发明使得可以简化IP网络的迁移,针对该迁移,这些网络支持根据IPv6协议建立的通信。为了简化起见,在此假设网络NW1和NW2仅向客户端装置T提供IPv6连接。换句话说,网络NW1和NW2在此被假设为仅IPv6。作为变体,可以设想网络NW1和NW2的另一种配置,例如双栈IPv4-IPv6配置。此外,为了简化起见,还假设客户端装置T是仅IPv6的,换句话说,该客户端装置仅具有IPv6连接,而不具有IPv4连接。

[0131] 在图2的示例中,网络NW1和NW2各自托管一个DNS服务器,使得可以解析域名,该服务器分别为针对网络NW1引用DNS#11并且针对网络NW2引用DNS#21,并且该服务器符合本发明。这些DNS服务器在下文的描述中被定性为“名义上的”,因为它们是由网络NW1和NW2提供的DNS服务器,并且这些网络的运营商已经用这些DNS服务器初始地配置了客户端装置T,以允许该客户端装置经由这些运营商的网络访问网络资源S,例如远程服务器。客户端装置希望访问的网络资源(服务器、终端、应用程序等)的性质没有限制。在此假设远程服务器S经由IP网络NW3连接到互联网网络。IP网络NW3可以是仅IPv6、仅IPv4或双栈IPv4-IPv6。

[0132] 该配置是由网络NW1和NW2的运营商例如在客户端装置T附接到网络NW1和NW2时或者在先前步骤中(例如在“工厂”配置的背景下)建立的。如本身已知的,该配置可以由网络NW1和NW2的运营商通过使用用于3GPP网络的PCO(协议配置选项)协议或者用于固定网络的DHCPv6(用于IPv6的动态主机配置协议)协议的选项来执行。

[0133] 在该配置期间,网络NW1的运营商(依次地网络NW2的运营商)向客户端装置T提供关于名义上的DNS服务器DNS#11(依次地名义上的DNS服务器DNS#21)的可访问性的信息(也就是说,允许访问服务器DNS#11的信息)。这样的可访问性信息可以是名义上的DNS服务器的IP地址。这种配置的结果是,当客户端装置T希望经由网络NW1(依次地NW2)访问网络资源(例如服务器S)时,该客户端装置使用其连接接口I1(依次地I2)通过使用传送到名义上的DNS服务器DNS#11(依次地DNS#21)的可访问性信息来访问该名义上的DNS服务器而将DNS请求发送到该服务器。客户端装置因此联系DNS服务器,以便获得允许该客户端装置访问该网络资源的IP请求。

[0134] 下面的表1通过说明的方式提供了来自DNS配置的摘录,该摘录反映了客户端装置(如客户端装置T)通过使用PCO协议从3GPP网络接收的信息。

[0135] [表1]

[0136]

```
...
接入点名称
  长度: 4
  APN: myipv6onlyapn
PDN 地址
  长度: 9
  0000 0... = (多个) 备用位: 0x00
  PDN类型: IPv6 (2)
  PDN IPv6, id: 0000000000000011
ESM 原因
  元素 ID: 0x58
  原因: 仅允许PDN类型 IPv6 (51)
协议配置选项
  ...
    协议或容器ID: DNS服务器 IPv6 地址 (0x0003)
    长度: 0x10 (16)
    IPv6: 2001:db8::1
```

[0137] 表1中报告的由3GPP网络供应的信息向客户端装置T指示网络仅支持IPv6连接(ESM原因51“仅允许PDN类型IPv6”),并且由IPv6地址为“2001:db8::1”的网络提供DNS服务器。

[0138] 客户端装置T检索与其每个活动连接接口(在这种特定情况下,该客户端装置到网络NW1的连接接口I1和其到网络NW2的连接接口I2)相关联的名义上的DNS配置信息(换句话说,对于该客户端装置经由连接接口连接到的每个IP网络)。该客户端装置将检索到的信息存储在称为CONFIG-DNS的本地配置文件中。注意,可以为到不同IP网络的连接接口定义同一个名义上的DNS服务器。

[0139] 在此处描述的实施例中,每个名义上的DNS服务器(即由IP网络的运营商为其用户选择的服务器)在本地配置文件CONFIG-DNS中与在此称为NOMINAL-RESOLVER的参数相关联,并且设置为1以指示它是名义上的DNS服务器。每个名义上的DNS服务器还与在此称为NETWORK-ID的参数相关联,该参数允许该名义上的DNS服务器明确地链接到IP网络,经由该IP网络配置所述DNS服务器,或者等效地,链接到客户端装置T用来访问IP网络的连接接口。NETWORK-ID参数的结构对于每个客户端装置都是本地的。例如,NETWORK-ID参数可以用连接接口的标识符来设置,该连接接口用于连接到支持名义上的DNS服务器(并且在此处托管该名义上的DNS服务器)的IP网络,或者用支持名义上的DNS服务器的IP网络的标识符来设置。在此处考虑的示例中,作为说明,对于服务器DNS#11,NETWORK-ID参数被设置在NW1,并且对于服务器DNS#21,NETWORK-ID参数被设置在NW2。

[0140] 注意,保存在本地配置文件CONFIG-DNS中的名义上的DNS服务器的列表可以经历由客户端装置T连接到的IP网络发起的修改,并且根据从这些IP网络接收的指令进行更新。尤其是当客户端装置T连接到的IP网络之一希望客户端装置T为了解析其DNS请求而使用新的名义上的DNS服务器(例如,对于IP网络NW1,为服务器DNS#12而不是服务器DNS#11)时,或者在客户端装置T在几个IP网络之间漫游(“切换”)时,情况更是如此。在这种情况下,在本地配置文件CONFIG-DNS中,客户端装置T用其运营商供应的新的名义上的服务器替换现在过时的名义上的DNS服务器。

[0141] 在此处考虑的示例中,通信系统1进一步包括替代性DNS服务器,引用为DNS#2,该替代性DNS服务器符合本发明(也更通常地被称为公共DNS服务器)并且位于公共互联网网络中。假设该替代性DNS服务器可以独立于由客户端装置T选择的用于路由其DNS请求的连接接口来使用。替代性DNS服务器在此被理解为不是由网络NW1和NW2托管,而是由第三方网络托管。这种DNS服务器随后被定性为是公共的。谷歌公共DNS、Cloudflare以及甚至QUAD9服务器都是这种公共DNS服务器的示例。

[0142] 在此假设客户端装置T设置有应用程序模块,该应用程序模块允许其用户手动地或经由信任应用程序来配置一个(或几个)如上所描述的替代性DNS服务器的使用,而不是由客户端装置T连接到的网络的运营商向该客户端装置提供的名义上的DNS服务器的使用。在考虑的示例中,客户端装置T因此被配置有替代性公共DNS服务器DNS#2;在此假设服务器DNS#2可以被使用,而不管客户端装置T使用的连接接口如何(即其到网络NW1的连接接口I1或者其到网络NW2的连接接口I2),并且客户端装置T被配置成使用该替代性DNS服务器DNS#2而不是服务器DNS#11和DNS#21。换句话说,客户端装置T经由应用程序模块被配置成当该客户端装置希望通过使用其连接接口I1或其连接接口I2来访问网络资源(例如服务器S)

时,现在将其DNS请求寻址到公共DNS服务器DNS#2。

[0143] 作为变体,可以为客户端装置T的每个活动连接接口使用不同的替代性DNS服务器。

[0144] 至于名义上的DNS服务器,具有替代性服务器DNS#2的客户端装置T的配置尤其包括在客户端装置T上存储关于替代性DNS服务器DNS#2(例如其IP地址)的可访问性信息。该配置在此存储在客户端装置T的本地配置文件CONFIG-DNS中。在此处描述的实施例中,尽管替代性DNS服务器旨在用于代替名义上的DNS服务器DNS#11和DNS#21,但是名义上的DNS服务器的可访问性信息被保存在配置文件中。

[0145] 在配置文件CONFIG-DNS中,为了将由客户端装置T用来解析其DNS请求的替代性DNS服务器DNS#2与最初由网络NW1和NW2的运营商提供的名义上的DNS服务器DNS#11和DNS#21进行区分,替代性服务器DNS#2与设置为0的参数NOMINAL-RESOLVER相关联。

[0146] 此外,由于服务器DNS#2可以由客户端装置T独立于该客户端装置所采用的活动连接接口(即I1或I2)来使用,因此在配置文件CONFIG-DNS中没有NETWORK-ID参数与服务器DNS#2相关联。

[0147] 作为变体,服务器DNS#2可以与设置NW1和NW2处的NETWORK-ID参数相关联。如果对每个活动连接接口使用不同的替代性DNS服务器,则每个替代性DNS服务器都有与之相关联的NETWORK-ID参数,该参数标识客户端装置T用来访问该替代性DNS服务器的连接接口。

[0148] 下面的表2展示了来自配置文件CONFIG-DNS的摘录。

[0149] [表2]

[0150]

| | | |
|---|---|---|
| DNS#11 | NOMINAL-RESOLVER＝1 | NETWORK-ID＝NW1 |
| DNS#21 | NOMINAL-RESOLVER＝1 | NETWORK-ID＝NW2 |
| DNS#2 | NOMINAL-RESOLVER＝0 | |

[0151] 注意,当客户端装置T是单接口时,也可以省略NETWORK-ID参数,也就是说该客户端装置具有单个活动连接接口并且仅连接到一个IP网络。在这种情况下,名义上的DNS服务器(即,与参数NOMINAL-RESOLVER＝1相关联的DNS服务器)缺少NETWORK-ID参数表明该服务器是由与该单个连接接口相关联的网络运营商提供或托管的名义上的DNS服务器。

[0152] 作为变体,可以使用不同的文件一方面存储由运营商提供的名义上的DNS服务器,另一方面存储替代性DNS服务器。

[0153] 此外,在此处描述的实施例中,客户端装置T仅使用配置文件CONFIG-DNS的与设置为0的NOMINAL-RESOLVER参数相关联的服务器来解析其DNS请求。与设置为1的NOMINAL-RESOLVER参数相关联的其他服务器在此用于发现实施NAT64功能的IP网络NW1和NW2,以及在适当的情况下该功能使用的一个或多个IPv6前缀。注意,如果没有替代性DNS服务器与连接接口相关联,则客户端装置T被配置成默认使用由与该连接接口相关联的网络的运营商提供的名义上的DNS服务器。

[0154] 在此处描述的实施例中,客户端装置T具有计算机的硬件架构,如图3中示意性展示的。该客户端装置特别地包括处理器2、随机存取存储器3、只读存储器4、非易失性闪速存储器5和通信装置6,在该非易失性闪速存储器中存储有例如本地配置文件CONFIG-DNS,该通信装置具体地包括连接接口I1和I2以及IPv6协议栈。

[0155] 只读存储器4是符合本发明的存储介质,该存储介质可以由客户端装置T的处理器

2读取,并且其上存储有根据本发明的计算机程序PROG1,该程序包括用于实施根据本发明的获得方法的指令。换句话说,计算机程序PROG1定义了客户端装置T的不同功能模块,这些功能模块允许该客户端装置实施根据本发明的获得方法。在此处描述的实施例中,这些模块包括(参见图2):插入模块M1,根据本发明,该插入模块被配置成将特定选项插入到客户端装置T向用来配置该客户端装置的DNS服务器寻址的DNS请求中,该选项在此被称为PREFIX64,并且在随后进行描述;发送模块M2,该发送模块被配置成将这些DNS请求发送到相关的DNS服务器;以及模块M3,该模块被配置成确定与其具有活动连接接口的IP网络是否实施用于将IPv4分组转换成IPv6分组的NAT64功能,并且反之亦然。在下文的描述中,为了简化起见,这种功能将由用于将IPv4分组转换成IPv6分组的功能来指定,即使该功能也能够将IPv6分组转换成IPv4分组。分组的转换需要用于将IPv4地址转换成IPv6地址的功能。

[0156] 模块M1、M2和M3的功能将在后面参考根据本发明的获得方法的步骤进行更详细的描述。

[0157] 在此处描述的实施例中,符合本发明的服务器DNS#11、DNS#21、DNS#2也具有计算机的硬件架构,如图4中示意性展示的。每个DNS服务器包括处理器7、随机存取存储器8、只读存储器9、非易失性闪速存储器10和通信装置11,在该通信装置中托管了根据IP网络的一个或多个连接接口。

[0158] 只读存储器9是符合本发明的存储介质,该存储介质可以由服务器的处理器7读取,并且其上存储有根据本发明的计算机程序PROG2,该程序包括用于实施根据本发明的处理方法的指令。换句话说,计算机程序PROG2定义了DNS服务器的不同功能模块,这些模块允许该计算机程序实施根据本发明的处理方法,并且更具体地,在此处描述的实施例中(参见图2)为:接收模块M4,该接收模块能够接收源自符合本发明的客户端装置的DNS请求;检测模块M5,该检测模块被配置成检测其接收的DNS请求是否包含特定选项PREFIX64;解析模块M6,该解析模块用于解析其接收的DNS请求;以及发送模块M7,该发送模块被配置成产生并且向调用该发送模块的客户端装置发送对其DNS请求的响应,这些响应在适当的情况下考虑由PREFIX64选项传送的指示。

[0159] 模块M4、M5、M6和M7的功能将在后面参考根据本发明的处理方法的步骤进行更详细的描述。

[0160] 现在参考图5到图10描述在特定实施例中分别由客户端装置T和替代性公共DNS服务器DNS#2实施的获得方法和处理方法的主要步骤。

[0161] 如先前提及的,本发明的特别优势在于其允许仅IPv6客户端装置(例如客户端装置T)寻求访问网络资源(例如服务器S),而无需事先知道该网络资源受益于的连接(仅IPv4、仅IPv6或IPv4/IPv6),并且不管该连接如何,都可以通过询问DNS服务器来获得该网络资源的IP地址,用该服务器借助于单个DNS请求来配置该网络资源,该请求针对网络资源请求AAAA类型的记录,换句话说,借助于用于获得IPv6地址以便在本发明的含义内访问该网络资源的请求。根据本发明,基于客户端装置的期望(这些期望可以来自例如偏好或客户端装置的配置),当网络资源具有IPv4连接时,该AAAA类型的单个请求允许其凭借其所包含的信息来获得伪IPv6地址或IPv4地址。因此避免了通信系统1的DNS服务器的过载,因为客户端装置T仅传输单一类型的DNS请求。此外,非常有利的是,本发明使得可以管理几个IP网络配置,并且适用于这些网络是否实施DNS64类型的功能。当地址转换功能在客户端装置T

上可用(例如CLAT功能)时,这也是合适的。

[0162] 参考图5,在此处描述的实施例中,客户端装置T最初经由其模块M3确定其连接到的并且可能用来访问网络资源的IP网络(在所考虑的示例中是NW1和NW2)是否实施了用于将IPv4地址转换成IPv6地址的NAT64功能(步骤E10)。该客户端装置继续对与其具有活动连接接口的每个IP网络进行该确定。在此,集中关注NAT64功能,该功能被配置成如先前讨论的通过使用NSP前缀或WKP前缀将IPv4地址转换成“IPv4嵌入的IPv6”地址(并且反之亦然)。应当注意,在此处考虑的示例中,没有特别关注“IPv4转换的IPv6”类型的地址,该地址是应用于表示IPv6世界中的IPv4网络资源的地址的“IPv4嵌入的IPv6”地址的特定变体。

[0163] 为此,客户端装置T可以以不同方式继续进行。

[0164] 因此,根据第一变体实施例,客户端装置T可以检测到其连接到的IP网络实施(或激活)NAT64功能,因为客户端装置T先前由IP网络的运营商配置有由这种NAT64功能使用的各种元素,如通常由NAT64功能使用的NAT64前缀(即NSP或WKP类型的IPv6前缀)。客户端装置T的这种配置可以由IP网络的运营商通过使用例如专用DHCPv6选项或如2007年9月名称为“Neighbor Discovery for IP version 6[IP版本6的邻居发现]”的IETF文档RFC 4861中描述的RA(路由器广告)选项,或者甚至是PCO协议的对象,经由一个或多个NAT64前缀的IP网络的显式广告来完成。在接收到这种广告时,客户端装置T将NAT64前缀存储在配置文件CONFIG-DNS中,该配置文件与对应的IP网络(即对应于该网络通过其接收广告的连接接口)相关联,例如,以包括NETWORK-ID参数和称为PREFIX64的参数的配对的形式。

[0165] 注意,多个NAT64前缀可以在同一个IP网络中使用。此外,几个不同的IP网络可以使用同一个NAT64前缀。其结果是,客户端装置T可以维护一个或多个{NETWORK-ID,PREFIX64}对,列出该客户端装置连接到的IP网络所使用的NAT64前缀(如果必要的话)。

[0166] 根据第二变体实施例,客户端装置T通过调用存储在配置文件CONFIG-DNS中的名义上的DNS服务器(即,在NOMINAL-RESOLVER参数设置为1的文件中相关联的DNS服务器),自动发现在与其具有活动连接接口的IP网络中存在NAT64功能。

[0167] 更具体地,在该第二变体中,客户端装置T发送请求DNS以获得与已知仅具有IPv4连接的给定网络资源(在下文中称为“测试”网络资源)的AAAA类型记录(在此也更简单地称为AAAA类型的DNS请求)相对应的IP地址。例如,该“测试”网络资源是已知仅IPv4的服务器。作为说明,与域名“myserver.example”相对应的“测试”服务器在此被视为网络资源,该域名的IP地址为IPv4地址“192.0.2.33”。

[0168] 该AAAA类型的DNS请求构成用于在本发明的含义内获得“测试”网络资源的IPv6地址的请求。这种DNS请求由客户端装置T通过使用IPv6发送到每个名义上的DNS服务器DNS#11和DNS#21。

[0169] 如果响应于该AAAA类型的DNS请求,客户端装置T从名义上的DNS服务器接收包括“测试”服务器的IPv6地址的肯定响应,这意味着在该名义上的DNS服务器上激活DNS64功能,并且因此托管该名义上的DNS服务器的IP网络实施NAT64功能。此外,包含在由客户端装置T接收的响应中的IPv6地址已经由名义上的DNS服务器针对仅IPv4测试服务器从其IPv4地址以及从根据其配置名义上的DNS服务器的NAT64前缀形成,该前缀如先前所强调的与由IP网络实施的NAT64功能使用的NAT64前缀一致。客户端装置T因此可以从该IPv6地址中提取相关的NAT64前缀;例如,为此,该客户端装置使用了文档RFC 6052的2.3节中规定的算

法。

[0170] 因此,作为说明,如果名义上的DNS服务器DNS#11返回包括针对“测试”服务器“myserver.example”的IPv6地址“2001:db8:122:3c0:0:221::/128”的肯定响应,已知与“测试”服务器相关联的IPv4地址和在文档RFC 6052中描述的算法,则客户端装置T提取对应的NAT64前缀:“2001:db8:122:300::/56”。客户端装置T然后为IP网络NW1保存该前缀,例如以配对{NETWORK-ID=NW1,PREFIX64=2001:db8:122:300::/56}的形式。

[0171] 客户端装置T也可以代替在该阶段继续提取NAT64前缀,直接将服务器DNS#11返回的IPv6地址保存在PREFIX64参数中并且存储配对{NETWORK-ID=NW1,PREFIX64=2001:db8:122:3c0:0:221::/128}。

[0172] 根据第三变体实施例,客户端装置T使用PCP协议,并且尤其是在文档RFC 7225中描述的机制来发现在该客户端装置与其具有活动连接接口的IP网络中存在NAT64功能。该机制允许客户端装置T检索与该客户端装置在实施机制时使用的连接接口相关联的NAT64前缀的列表。如果在这种实施方式中,该客户端装置检索至少一个NAT64前缀,则这意味着与所使用的连接接口相对应的IP网络实施NAT64功能。

[0173] 在步骤E10中实施的用于发现在IP网络中存在NAT64功能的过程也可以递归地执行。这种递归执行在客户端装置T经由中间设备连接到IP网络(例如,CPE)时特别有益。在这种情况下,CPE通过实施先前提及的技术之一来执行发现过程,然后将在该过程中发现的NAT64前缀传送给客户端装置T。为此,如先前提及的,CPE可以特别使用RA类型的广告消息。

[0174] 如果在步骤E10中,客户端装置T检测到其连接的IP网络之一中的NAT64功能被激活,则该客户端装置在配置文件CONFIG-DNS中将设置为1的称为NAT64_ENABLED的参数与该IP网络相关联。因此,在配置文件CONFIG-DNS中,对于在步骤E10中已经发现至少一个NAT64前缀的仅IPv6网络,NAT64_ENABLED参数被设置为“1”。另一方面,对于IPv4/IPv6“双栈”网络的仅IPv4网络和不具有NAT64功能的仅IPv6网络,NAT64_ENABLED参数被设置为“0”。

[0175] 注意,在此处描述的实施例中,客户端装置T再次执行用于检测存在NAT64功能的过程,该过程已经在每次其检测到由网络运营商提供的网络配置的改变时被描述,并且该过程可能会对DNS服务产生影响。如先前提及的,当客户端装置T处于漫游状态时,网络配置的改变可以显著地发生。这可以导致网络实施的NAT64功能所使用的一个或多个NAT64前缀的更新(如果必要的话),或者通过根据相关网络是否实施NAT64功能来维持或另一方面改变NAT64_ENABLED参数的值,或者改变与网络相关联的名义上的DNS服务器,等等。

[0176] 现在假设客户端装置T希望访问网络资源S,例如服务器S(步骤E20)。

[0177] 为此,如本身已知的,该客户端装置经由其活动连接接口之一及其发送模块M2向与该连接接口相关联的DNS服务器发送用于解析RM服务器的域名的DNS请求(步骤E70)。在此处考虑的说明性示例中,客户端装置T被配置成调用替代性服务器DNS#2来解析其DNS请求,而不管客户端装置T使用的连接接口如何。

[0178] 根据本发明,客户端装置T被配置成仅向用来配置该客户端装置的DNS服务器(在此,服务器DNS#2)传输类型AAAA的DNS请求,不论该客户端装置希望访问的网络资源S受益于的连接(IPv4、IPv6或IPv4/IPv6)如何,换句话说,仅用于获得IPv6地址以便访问该网络资源的DNS请求。表示为R-AAAA的该DNS请求通常包含(根据IETF文档RFC1035中描述的)与该请求试图解析的网络资源S相关联的域名和期望的记录类型,即AAAA。

[0179] 为了特别地管理网络资源S不与类型AAAA的记录相关联的特定情况,因为该网络资源仅具有IPv4连接(并且因此仅具有一个IPv4地址),所以本发明有利地提供了在请求R-AAAA被发送到服务器DNS#2之前,由客户端装置T的插入模块M1将附加的信息插入到该请求中(步骤E60)。在此处描述的实施例中,该信息被插入到为此目的引入的DNS协议的扩展EDNS(0)的选项中,在本说明书中称为PREFIX64。如果请求R-AAAA针对的网络资源S具有IPv4连接,则该选项表示由客户端装置T响应于该请求而从服务器DNS#2预期的IP地址类型。由客户端装置T预期的该IP地址类型可以是例如由DNS服务器形成的伪IPv6地址,或者如下文详细描述的IPv4地址。

[0180] 在此处描述的实施例中,PREFIX64选项被定义(并且由接收包含该选项的DNS请求的DNS服务器这样识别)成使得在包含该选项的请求R-AAAA针对的网络资源S仅具有IPv4连接时,该选项表示在来自DNS服务器的对请求R-AAAA的响应中,由客户端装置从该客户端装置用该请求询问的DNS服务器预期的IP地址类型。换句话说,如果网络资源具有双IPv4和IPv6连接,则不需要检测寻址到DNS服务器的DNS请求中的PREFIX64选项的该服务器来应用该选项定义的IP地址类型。

[0181] 在另一个实施例中,可以注意定义PREFIX64选项(并且因此确保其由接收包含该选项的DNS请求的DNS服务器这样识别),使得当该客户端的请求R-AAAA针对的网络资源具有IPv4连接时,该选项表示由客户端装置从响应于该请求而询问的DNS服务器预期的IP地址类型。换句话说,如果网络资源具有IPv4连接,并且即使该网络资源具有双IPv4和IPv6连接,需要被询问的DNS服务器来应用由PREFIX64选项定义的IP地址类型。

[0182] 可能会出现各种特定情况并且影响由客户端装置T插入到DNS请求的PREFIX64选项中的该信息的值。

[0183] 更具体地,如果客户端装置T考虑用来访问网络资源S的连接接口与设置为1的NAT64-ENABLED参数以及与至少一个NAT64前缀(对测试步骤E30响应“是”)相关联,则客户端装置T利用与连接接口相关联并且在步骤E10中确定的NAT64前缀或IPv6地址的值(并且存储在由客户端装置T维护并且与相关连接接口相关联的(NETWORK-ID,PREFIX64)配对之一中)来完成PREFIX64选项(步骤E40)。通过以这种方式完成请求R-AAAA的PREFIX64选项,客户端装置T向服务器DNS#2指示如果网络资源S具有IPv4连接,并且因此与该网络资源相关联的域名的解析导致获得IPv4地址,则客户端装置T希望从服务器DNS#2接收由该服务器从网络资源S的IPv4地址和在PREFIX64选项中完成的NAT64前缀形成的IPv6地址,或者,如果该选项包含IPv6地址,则该客户端装置希望例如通过使用先前提及的文档RFC 6052中描述的算法从该IPv6地址提取的NAT64前缀。

[0184] 相反(对测试步骤E30响应“否”),如果客户端装置T考虑用来访问网络资源S的连接接口与设置为0的NAT64-ENABLED参数相关联,则客户端装置T在请求R-AAAA的PREFIX64选项中设置预定义值,即,在此为零值“::ffff:0:0”(步骤E50)。该零值向服务器DNS#2指示响应于请求R-AAAA而预期的IP地址是IPv4地址,在这种情况下是资源S的IPv4地址。给出的零值的示例纯粹是为了说明的目的而提供的:作为变体,可以设想另一个预定义值,以向服务器DNS#2指示当该预定义值被服务器DNS#2识别为具有该含义时,响应于请求R-AAAA而预期资源S的IPv4地址。

[0185] 注意,有利的是,如果尽管客户端装置T已经确定其考虑使用的连接接口允许访问

实施NAT64功能的网络,但是该客户端装置希望自己从资源S的IPv4地址形成IPv6地址(例如为此目的配备了先前描述的CLAT功能),并且不想调用服务器DNS#2来形成该地址,或者如果该客户端装置被通知服务器DNS#2没有实施DNS64功能,则该客户端装置也可以将零值(或者更一般地,预定义值)插入到PREFIX64选项中。

[0186] 图6展示了可以设想用于由客户端装置插入到请求R-AAAA中的PREFIX64选项的第一格式。

[0187] 该格式包括三个字段:

[0188] -“选项代码”字段,该字段包括标识PREFIX64选项的代码;

[0189] -“选项长度”字段,该字段以八位字节为单位指示包含在PREFIX64选项中的数据大小。在此处描述的实施例中,等于16的数据大小具有特定的含义:这意味着PREFIX64字段包含IPv6地址并且不包含NAT64前缀;以及

[0190] -PREFIX64字段,该字段包含表示由客户端装置预期的IP地址类型的信息。在此处描述的实施例中,PREFIX64字段可以包含NAT64前缀、IPv6地址或零值(即值“::ffff:0:0”)。

[0191] 图7表示了可以设想用于PREFIX64选项并且使得可以包括一个或多个NAT64前缀(或从中提取NAT64前缀的IP地址)的第二格式。每个前缀的大小由“前缀长度”字段控制;如果该字段被设置为16,则意味着相关联的PREFIX64字段包含IPv6地址并且不包含前缀。“选项长度”字段与PREFIX64选项中供应的不同前缀的长度之和相对应。

[0192] 显然,格式的这些示例纯粹是为了说明而给出的,并且其他信息可以包括在PREFIX64选项中。

[0193] 注意,当PREFIX64字段的值包括使得可以提取这种NAT64前缀的NAT64前缀或IPv6地址时,该值应该是与客户端装置T考虑用来访问网络资源S(即,向其发送和/或从该网络资源接收数据)的连接接口相关联的IP网络在适当的情况下使用的NAT64前缀。如果客户端装置T考虑使用其所有活动连接接口,并且在步骤E10中已经为这些不同的连接接口发现了不同的NAT64前缀,则客户端装置T在请求R-AAAA中包括几个PREFIX64选项,其中每个选项包含NAT64前缀,例如通过使用图7中提出的选项格式。在变体实施例中,客户端装置T可以向服务器DNS#2发送几个DNS请求,每个请求包含标识不同NAT64前缀的PREFIX64选项。

[0194] 还要注意,具有几个活动连接接口的客户端装置T,换句话说,多接口客户端装置,可以选择其活动连接接口中的任一个来发送传达PREFIX64选项的AAAA请求。例如,终端可以经由支持与请求AAAA中包括的一个或多个NAT64前缀相关联的NAT64服务的相同网络或经由不同网络来发送请求AAAA。

[0195] 在已经将PREFIX64选项插入到DNS请求R-AAAA中之后,客户端装置T经由其活动连接接口之一将请求R-AAAA发送到服务器DNS#2(步骤E70)。

[0196] 在另一个实施例中,当网络资源具有至少一个IPv4连接时,PREFIX64选项被定义为通常表示由客户端装置响应于其请求R-AAAA而从DNS服务器预期的IP地址类型,并且除了PREFIX64选项之外并且在将其发送到服务器DNS#2之前,客户端装置T在其DNS请求R-AAAA中插入旨在向服务器DNS#2指示的附加指令,当PREFIX64选项包含IPv6前缀或包括这种前缀的IPv6地址时,仅当网络资源仅具有IPv4连接时,或者如果网络资源具有IPv4连接而与它具有或不具有IPv6连接的事实无关时,该网络资源是否必须根据IPv6格式从该前缀

和从资源的IPv4地址生成地址。该指令可以包含在DNS请求R-AAAA的可选参数中(例如,在图6和图7中以说明的方式表示的PREFIX64选项的字段中,其可以称为“方案ID”),旨在向DNS服务器传达与该方法相关的指示,该方法是DNS服务器必须应用以从其被询问的网络资源的IPv4地址形成“伪”IPv6地址。如果“方案ID”用于指定该可选参数,例如,可以为该参数定义以下值:

[0197] -值0指示仅当网络资源仅具有IPv4连接时,DNS服务器才必须生成伪IPv6地址;以及

[0198] -值1指示在网络资源具有IPv4连接时,DNS服务器才必须生成伪IPv6地址,即使该网络资源也具有IPv6连接。

[0199] 注意,可以为方案ID参数定义其他值,以向DNS服务器传输与用于形成伪IPv6地址的方法有关的其他类型的指令。作为说明:

[0200] -值2可以指示DNS服务器必须使用以根据文档RFC 6052的2.3节中定义的算法从IPv4地址形成伪IPv6地址;

[0201] -值3可以指示DNS服务器必须使用WKP前缀从IPv4地址形成伪IPv6地址;

[0202] -值4可以指示DNS服务器必须使用保证传输层的伪报头的“校验和”(完整性检查机制)的中立性的后缀;并且

[0203] -值5可以指示DNS服务器必须在附加部分中返回与目标资源相关联的IPv4地址。

[0204] 这些示例是以说明的方式给出的,并且可以设想客户端装置经由“方案ID”参数的其他值向DNS服务器传输其他指令。作为变体,其他指令可以由客户端装置经由其他介质传输到DNS服务器,例如请求R-AAAA的其他参数。

[0205] 现在参考图8描述由客户端装置T传输的类型AAAA的DNS请求、并且特别是请求R-AAAA如何由服务器DNS#2或更一般地由符合本发明的DNS服务器处理。

[0206] 在经由服务器DNS#22的接收模块M4接收到类型AAAA的DNS请求时(步骤F10),该服务器通过其检测模块M5检查该请求是否包含PREFIX64选项(测试步骤F20)。

[0207] 如果检测模块M5没有检测到PREFIX64选项(对测试步骤F20响应“否”),则该服务器以常规方式处理和解析类型AAAA的DNS请求,如现有技术中那样(步骤F30)。例如,在1987年11月名称分别为“Domain names-concept and facilities[域名-概念和设施]”和“Domain names-implementation and specification[域名-实施和规范]”的IETF文档RFC 1034和RFC 1035中描述了被实施用于该解析的机制。

[0208] 更具体地,服务器DNS#22通过其模块M6确定网络资源S的IPv6地址。以下将该IP地址表示为@IP(S)。

[0209] 如果服务器DNS#2是资源S的权威DNS服务器,并且如果资源S具有IPv6连接,则服务器DNS#2在本地具有资源S的IPv6地址,并且通过向客户端装置T传输该IPv6地址来对该客户端装置做出肯定响应。如果该服务器不是资源S的权威DNS服务器而是递归DNS服务器,则服务器DNS#2向权威DNS服务器(或另一个递归DNS服务器)传输旨在获得资源S的IPv6地址的类型AAAA的DNS请求。如果资源S具有IPv6连接,则向服务器DNS#2返回包含资源S的IPv6地址的肯定响应。然后,服务器DNS#2通过在其对请求R-AAAA的响应中向客户端装置T传输该IPv6地址来对该客户端装置做出肯定响应。否则,向服务器DNS#2返回否定响应,该服务器进而又对从客户端装置T接收到的DNS请求AAAA做出否定响应。

[0210] 在此处考虑的示例中,在步骤F10中,服务器DNS#2接收关于网络资源S的请求R-AAAA,并且如果网络资源S具有IPv4连接(并且在此处描述的实施例中仅具有这种连接),则客户端装置T已经将表示其响应于其DNS请求而预期的IP地址类型的PREFIX64选项插入到该请求中。在步骤F20中,检测模块M5检测到存在由客户端装置T插入到请求R-AAAA中的PREFIX64选项(对测试步骤F20响应“是”)。

[0211] 该检测模块提取由客户端装置T在检测到的选项的PREFIX64字段中输入的值(步骤F40)。

[0212] 然后该客户端装置通过其获得模块M6确定网络资源S的IP地址@IP(S)(步骤F50)。如先前针对步骤F30所描述的,如果服务器DNS#2是资源S的权威服务器,则其在本地具有其一个或多个IP地址,无论这些地址是IPv4地址还是IPv6地址或这两种类型的地址。否则,该服务器通过查询资源S的权威服务器DNS递归地获得资源S的IP地址。

[0213] 更具体地,该服务器向权威DNS服务器(直接或通过中间递归DNS服务器)传输旨在获得资源S的IPv6地址的类型AAAA的DNS请求。如果资源S具有IPv6连接,则权威DNS服务器向服务器DNS#2返回肯定响应,该肯定响应包含表示为@IPv6(S)的资源S的IPv6地址。

[0214] 否则,向服务器DNS#2返回否定响应。在这种情况下,在此处描述的实施例中,服务器DNS#2向权威DNS服务器(或另一个中间递归DNS服务器)传输旨在获得资源S的IPv4地址的类型A的DNS请求。然后该服务器从权威DNS服务器接收肯定响应,该肯定响应包含表示为@IPv4(S)的资源S的IPv4地址。

[0215] 注意,作为变体,服务器DNS#2可以同时向权威DNS服务器传输类型A和类型AAAA两者的DNS请求,以特别地预测网络资源S不支持IPv6连接。仅当对类型AAAA的请求的响应是否定的时,服务器DNS#2才会使用对类型A的请求的响应。

[0216] 在又一个变体中,如果PREFIX64选项被定义成使得其被考虑,包括当网络资源S具有双连接时,或者当DNS请求R-AAAA包括这方面的指令时(例如,如先前提及的方案ID参数,设置为1),服务器DNS#2可以同时或顺序地向权威DNS服务器传输类型A和AAAA两者的DNS请求,以确定资源S是否具有双IPv4和IPv6连接。

[0217] 如果由服务器DNS#2如此确定的地址@IP(S)是符合IPv6协议的地址@IPv6(S)(对测试步骤F60响应“是”),则服务器DNS#2通过向客户端装置T发送地址@IPv6(S)来对来自该客户端装置的请求R-AAAA做出肯定的响应(步骤F70)。换句话说,地址@IPv6(S)在对请求R-AAAA的响应中被发送到客户端装置T,该响应根据先前引用的文档RFC 3596的2.3节中描述的过程携带有类型AAAA。

[0218] 否则,这意味着网络资源S仅具有IPv4连接,而不具有IPv6连接。

[0219] 然后,服务器DNS#2检查由客户端装置T从插入到请求R-AAAA中的PREFIX64选项中提取的值(步骤F80)。

[0220] 如果提取的值等于“::ffff:0:0”(换句话说,等于定义零值的前缀)(步骤F80的输出处的分支(1)),这意味着客户端装置T希望根据IPv4协议接收网络资源S的地址@IPv4(S)(即根据IPv4格式并且例如没有嵌入到IPv6地址中),以例如通过使用如先前所描述的CLAT功能从该IPv4地址开始自行形成IPv6地址。

[0221] 然后,服务器DNS#2通过经由其发送模块M7向客户端装置T发送网络资源S的地址@IPv4(S)来响应来自该客户端装置的请求R-AAAA(步骤F90)。换句话说,地址@IPv4(S)在对

请求R-AAAA的DNS响应中被发送到客户端装置T,该响应携带有如先前引用的文档RFC3596中描述的类型AAAA。地址@IPv4(S)可以包括在DNS响应中,在DNS响应的附加部分(“附加部分”,尤其是在文档RFC 1034的3.7节中描述的)中(该地址随后按照其原始IPv4格式进行编码)或包括在响应的正文中。注意,如果响应的正文被选择为将地址@IPv4(S)传输到客户端装置T,则地址@IPv4(S)以IPv6地址的形式被编码,该IPv6地址例如通过使用已知前缀“::ffff:0:0/96”(也称为“IPv4映射的”IPv6地址并且在文档RFC 4291中进行了描述)来构造。作为变体,可以设想其他格式来对地址@IPv4(S)进行编码。

[0222] 应当注意,如果客户端装置T希望在网络资源S受益于IPv4连接时获得该网络资源的IPv4地址,则该客户端装置在其DNS请求中传输设置有已知前缀“::ffff:0:0/96”的PREFIX64选项和设置有零值的PREFIX64选项是等同的。

[0223] 因此,作为说明,如果地址@IPv4(S)=“198.51.100.1”和插入到DNS请求R-AAAA中的PREFIX64选项具有零值“::ffff:0:0”,则服务器DNS#2可以向客户端装置T发送对其DNS请求的响应,该DNS响应在响应的正文中包含地址@IP(S)=“::ffff:0:0:198.51.100.1”,该地址包含地址@IPv4(S)。

[0224] 如果从PREFIX 64选项中提取的值包含非零IPv6地址(步骤F80的输出处的分支(2)),则服务器DNS#2执行文档RFC 6052中描述的算法,以提取形成该IPv6地址的NAT64前缀(步骤F100)。然后,该服务器使用适当提取的NAT64前缀来从其地址@IPv4(S)形成网络资源S的IPv6地址(步骤F110)。然后该服务器通过经由其发送模块M7向客户端装置T发送为网络资源S如此形成的地址@IPv6(S)来响应来自该客户端装置的请求R-AAAA(步骤F120)。注意,对DNS请求AAAA的常规DNS响应可用于该目的。

[0225] 如果从PREFIX 64选项中提取的值包含NAT64前缀(步骤F80输出处的分支(3)),则服务器DNS#2直接执行步骤F110和F120,而不实施步骤F100。

[0226] 服务器DNS#2通过考虑在适当的情况下由客户端装置T传输的指令,从该服务器的地址@IPv4(S)形成网络资源S的地址@IPv6,该指令涉及用于形成必须应用的IPv6地址的方法。如先前所解释的,这种指令可以经由为该目的定义的参数(如先前描述的方案ID参数)在DNS请求R-AAAA中传输。如果客户端装置T在DNS请求中没有定义指令,则服务器DNS#2可以应用用于形成默认配置的IPv6地址的方法(例如执行文档RFC 6052中定义的算法,并且仅在AAAA记录不存在的情况这样做)。

[0227] 如果考虑当资源S至少具有IPv4连接时服务器DNS#2被配置成应用包含在PREFIX64选项中的IP地址类型的实施例,则在网络资源S具有双IPv4和IPv6连接时,从服务器DNS#2到客户端装置T的响应还可以包含几个IP地址。应当记得,服务器DNS#2的配置可以从PREFIX64选项的定义产生,或者从来自客户端装置T的如先前提及的插入到DNS请求R-AAAA中(例如在方案ID参数中)的指令产生。然后由服务器DNS#2获得的多个IP地址(该服务器然后包括资源的至少一个IPv4地址和一个IPv6地址)可以全部插入到响应的正文中(根据IPv6格式,包括从IPv4地址构造的伪IPv6地址),或者全部插入到DNS响应的附加部分中(这种IPv4地址然后可以根据IPv4格式进行编码),或者插入到响应的正文中根据IPv6格式编码的地址中,并且对于其他地址,插入到DNS响应的附加部分中。

[0228] 注意,根据客户端装置T用来访问网络资源S的连接接口,由服务器DNS#2响应于其请求AAAA而返回给客户端装置T的IP地址(或多个IP地址)可能不同。因此,向服务器DNS#2

传输类型AAAA的DNS请求的两个客户端装置T1和T2将从服务器DNS#2接收以下各项,这些请求针对仅具有IPv4连接的网络资源“myT3.name.example”(@IPv4(S)＝“198.51.100.1”)并且各自包括分别设置为针对T1的“2001:db8:1234::/96”和针对T2的“64:ff9b::/96”的PREFIX64选项:

[0229] -对于客户端装置T1:包括IPv6地址“2001:db8:1234::198.51.100.1”的DNS响应;并且

[0230] -对于客户端装置T2:包括IPv6地址“64:ff9b::198.51.100.1”的DNS响应。

[0231] 因此,由服务器DNS#2返回给客户端装置T1和T2的用于同一个网络资源的IPv6地址不一定相同。从这些IPv6地址,客户端装置T1和T2可以建立与网络资源S的通信,这些通信中的每一个都通过每个客户端装置连接到的IP网络的NAT64功能进行传输,即通过针对T1配置有前缀“2001:db8:1234::/96”的NAT64功能,以及通过针对T2配置有前缀“64:ff9b::/96”的NAT64功能。

[0232] 再次参考图5,在接收到来自服务器DNS#2的对客户端装置T的请求R-AAAA的DNS响应时(步骤E70),该客户端装置提取针对网络资源S的在响应中供应的IP地址@IP(S),以便使用该地址来访问资源S(步骤E80)。

[0233] 如果客户端装置T已经在其请求R-AAAA中包括PREFIX64选项中的零或预定义值,则该客户端装置使用由服务器DNS#2返回的地址@IP(S)来基于该网络资源先前配置的本地NAT64前缀,在本地构造网络资源S的“IPv4转换的IPv6”类型的伪IPv6地址。该NAT64前缀是客户端装置T在步骤E10中为其考虑用来访问资源S的IP网络发现的。然后,客户端装置T使用其在本地构造的伪IPv6地址作为发送到网络资源S的分组的目的地地址。

[0234] 否则,客户端装置T使用由服务器DNS#2返回的地址@IPv6(S)作为如发送到网络资源S的分组的目的地地址。

[0235] 注意,多接口客户端装置T必须基于由服务器DNS#2返回的IP地址来选择用于向网络资源S发送数据分组的连接接口。事实上,如果客户端装置T具有几个{NETWORK-ID,PREFIX64}配对,则客户端装置T选择NAT64前缀与服务器DNS#2返回的IPv6地址的第一位相对应的NETWORK-ID连接接口。例如,如果客户端装置T具有两个连接接口{NETWORK-ID＝WLAN,PREFIX64＝2001:db8:1234/96}和{NETWORK-ID＝RMNET,PREFIX64＝64:ff9b::/96},则要用于将数据发送到服务器DNS#2返回的地址“64:ff9b::1.2.3.4”的连接接口是连接接口RMNET。

[0236] 此外,如果客户端装置T在请求R-AAAA中向与客户端装置T的不同连接接口相对应的服务器DNS#2供应了几个NAT64前缀(例如,针对网络NW1的前缀“2001:db8:1234/96”和针对网络NW2的前缀“64:ff9b::/96”),则服务器DNS#2响应于客户端装置T(在所考虑的示例中,地址“2001:db8:1234::198.51.100.1”和地址“64:ff9b::198.51.100.1”)而传输与前缀一样多的IPv6地址。然后,客户端装置T必须使用与同被选择用于向网络资源发送分组的连接接口相关联的前缀相对应的IPv6地址,换句话说,经由网络NW1发送的分组的目的地地址“2001:db8:1234::198.51.100.1”以及经由网络NW2发送的分组的地址“64:ff9b::198.51.100.1”。

[0237] 选择错误的连接接口可能会影响体验质量。事实上,选择要传送到DNS服务器的一个或多个前缀允许客户端装置控制将如何建立与远程网络资源的通信。

[0238] 作为说明,参考图9的示例,如果PREFIX64选项包含前缀“2001:db8:1234/96”,则数据必须经由网络NW1进行交换。注意,具有目的地址“2001:db8:1234::198.51.100.1”但经由网络NW2传输的任何数据分组被重新路由到网络NW1(因为该网络公布前缀“2001:db::/32”)并且有被该网络拒绝的风险,因为从互联网网络可见的接口上不提供NAT64服务。

[0239] 参考图10的示例,如果DNS响应包含前缀“64:ff9b::/96”,则数据必须经由网络NW2进行交换。具有目的地地址“64:ff9b::198.51.100.1”并且经由网络NW1传输的任何数据分组都会被网络NW1拒绝,因为该网络没有任何路由(例如任何BGP(边界网关协议)路由)来路由分组。

[0240] 在先前描述的实施例中,PREFIX64选项由客户端装置T插入到其请求R-AAAA中。在客户端装置T经由CPE与IP网络通信的另一个实施例中,可以由CPE插入PREFIX64选项。根据本发明的获得方法然后由CPE(其然后在本发明的含义内被认为是客户端装置)实施。更具体地,如果CPE检测到IP网络中存在NAT64功能,则在从CPE连接到的局域网的设备接收到DNS请求AAAA时,CPE根据刚刚描述的模式修改该请求以包括PREFIX64选项。

[0241] 此外,在所描述的实施例中,实施根据本发明的处理方法的是替代性DNS服务器DNS#2。应当注意,当客户端装置T被配置成将其DNS请求寻址到这些名义上的DNS服务器时,本发明也适用于名义上的DNS服务器。

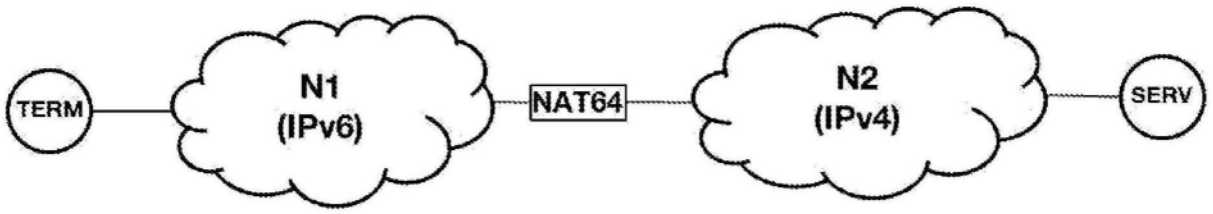

TERM
N1
(IPv6)
NAT64
N2
(IPv4)
SERV

图1

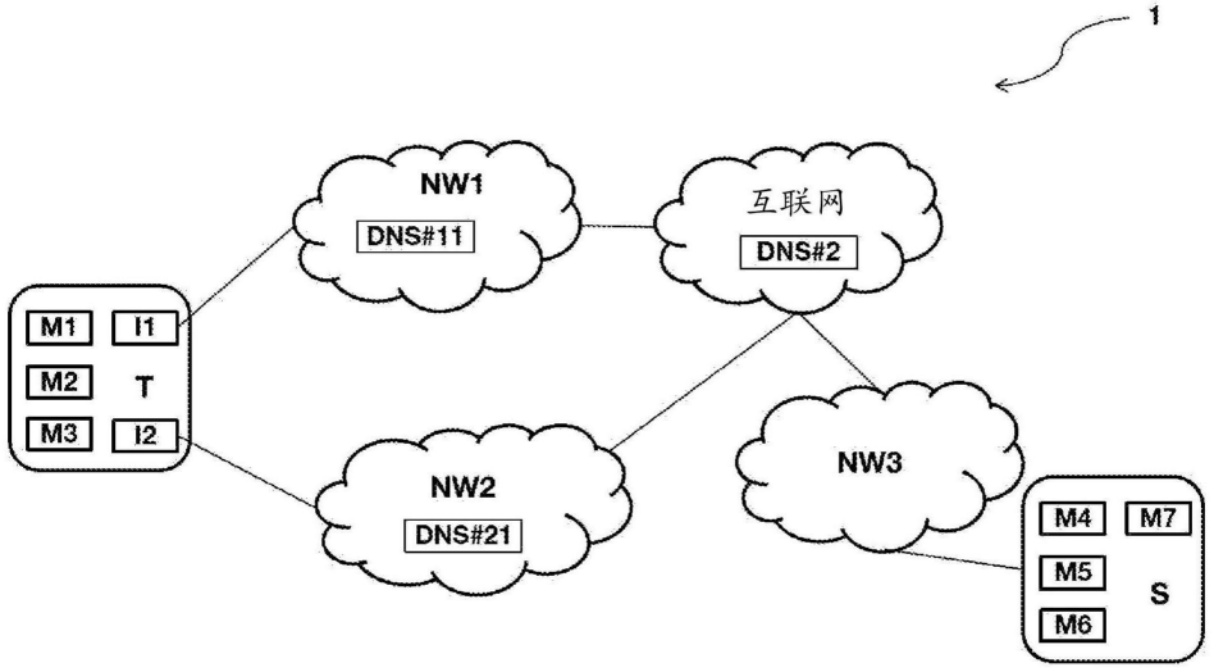

1
NW1
DNS#11
互联网
DNS#2
M1
I1
M2
T
M3
I2
NW2
DNS#21
NW3
M4
M7
M5
S
M6

图2

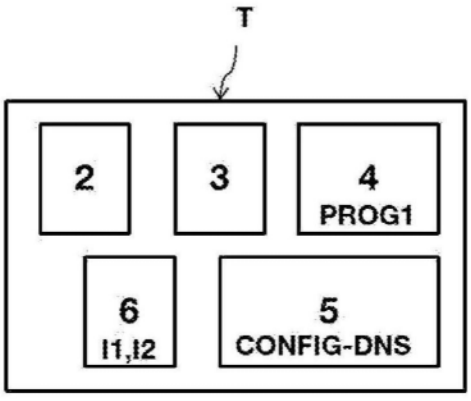

T
2
3
4
PROG1
6
I1,I2
5
CONFIG-DNS

图3

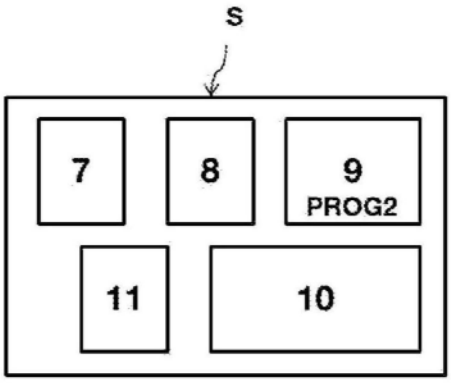

S
7
8
9
PROG2
11
10

图4

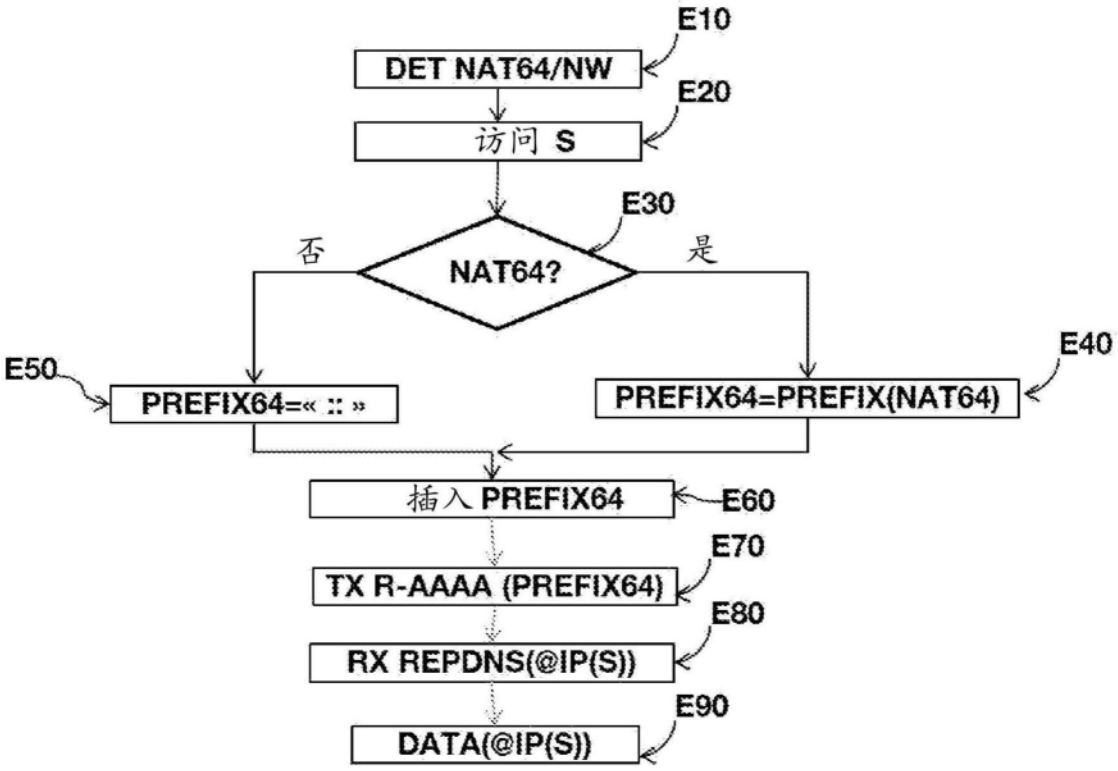

E10
DET NAT64/NW
E20
访问 S
E30
NAT64?
否
是
E50
PREFIX64=« :: »
E40
PREFIX64=PREFIX(NAT64)
插入 PREFIX64
E60
E70
TX R-AAAA (PREFIX64)
E80
RX REPDNS(@IP(S))
E90
DATA(@IP(S))

图5

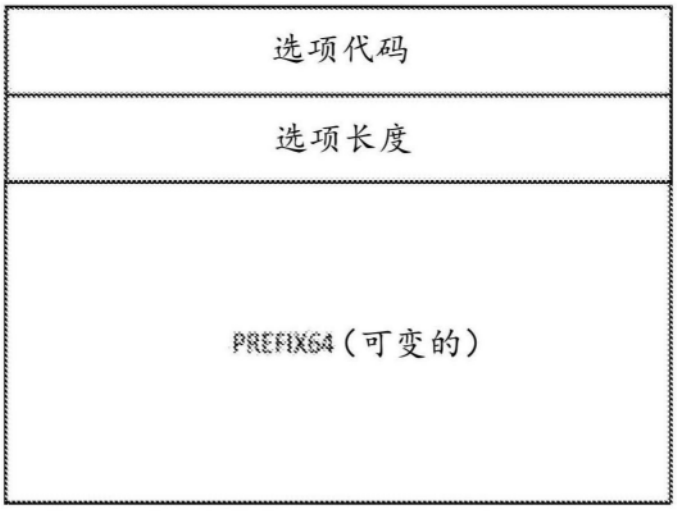

选项代码
选项长度
PREFIX64（可变的）

图6

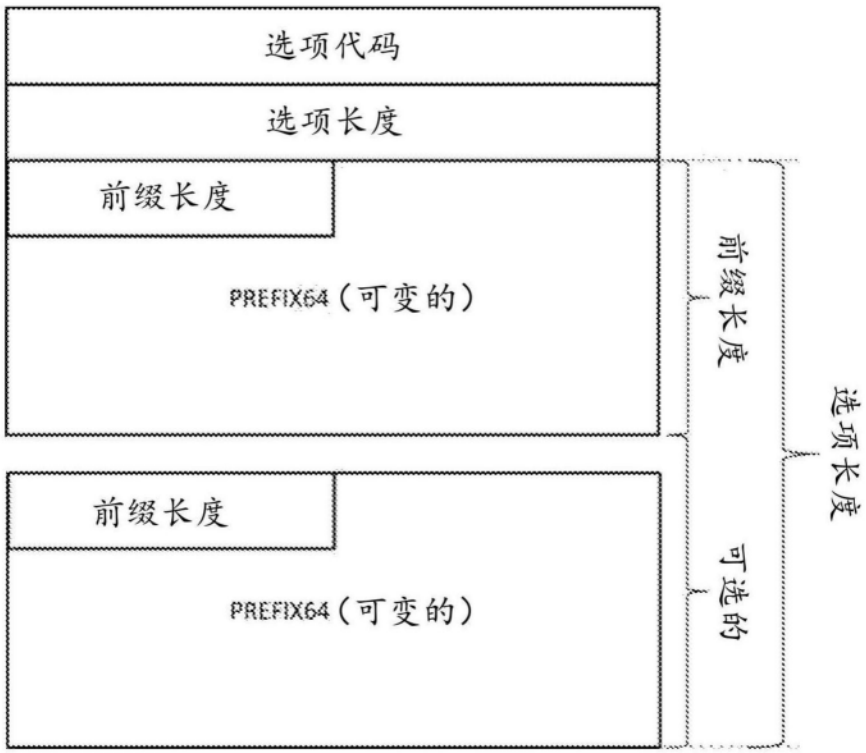

选项代码
选项长度
前缀长度
PREFIX64（可变的）
前缀长度
PREFIX64（可变的）
前缀长度
可选的
选项长度

图7

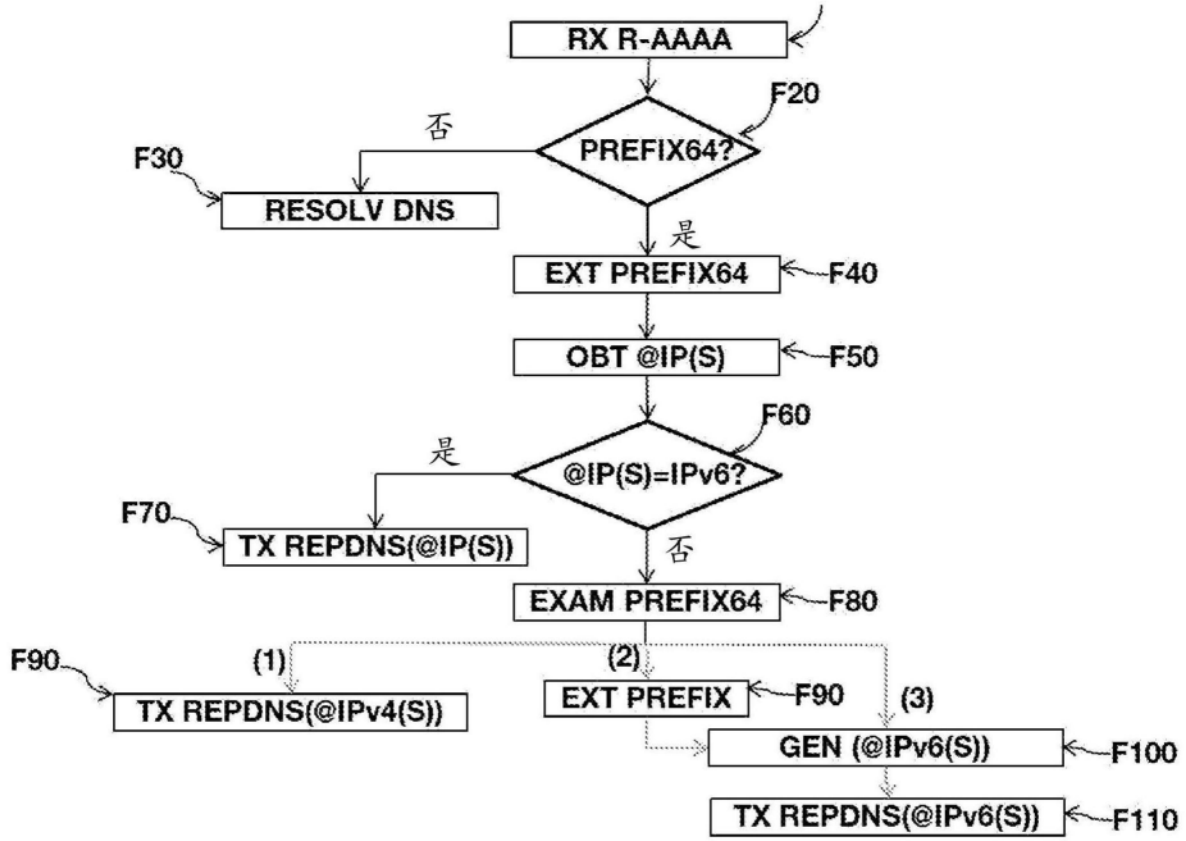

RX R-AAAA
F20
PREFIX64?
否
F30
RESOLV DNS
是
EXT PREFIX64
F40
OBT @IP(S)
F50
F60
@IP(S)=IPv6?
是
F70
TX REPDNS(@IP(S))
否
EXAM PREFIX64
F80
F90
(1)
(2)
(3)
TX REPDNS(@IPv4(S))
EXT PREFIX
F90
GEN (@IPv6(S))
F100
TX REPDNS(@IPv6(S))
F110

图8

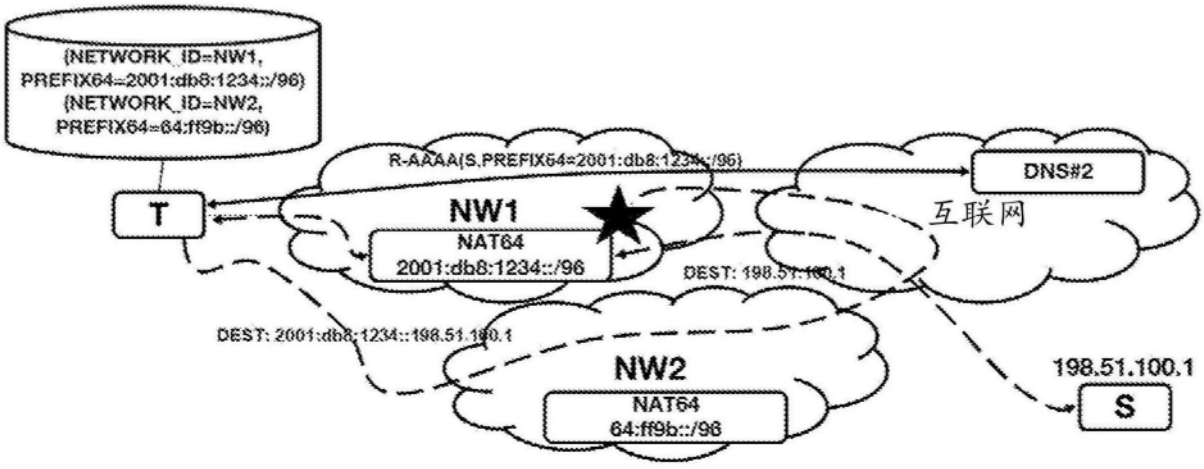

(NETWORK_ID=NW1,
PREFIX64=2001:db8:1234::/96)
(NETWORK_ID=NW2,
PREFIX64=64:ff9b::/96)
R-AAAA(S,PREFIX64=2001:db8:1234::/96)
DNS#2
T
NW1
NAT64
2001:db8:1234::/96
互联网
DEST: 198.51.100.1
DEST: 2001:db8:1234::198.51.100.1
NW2
NAT64
64:ff9b::/96
198.51.100.1
S

图9

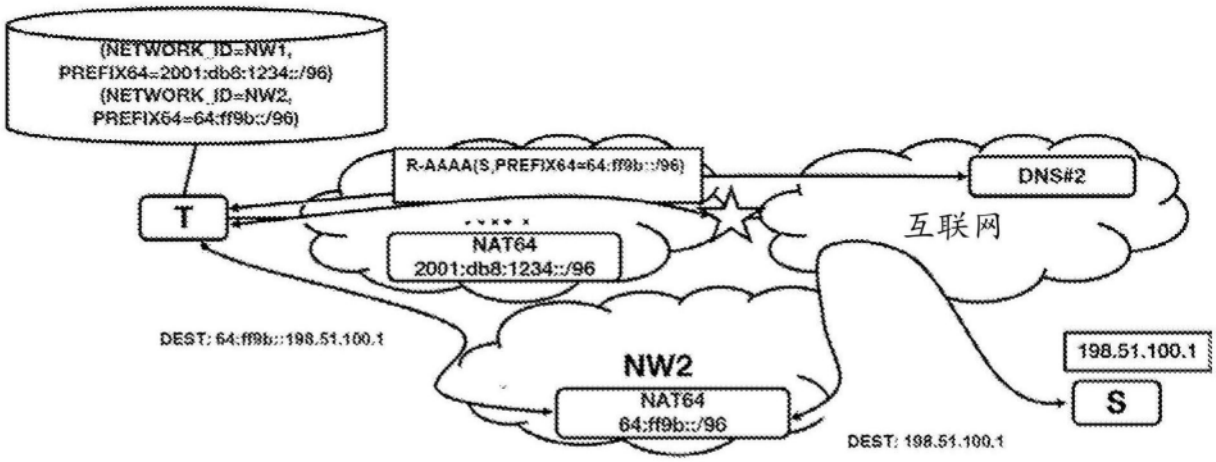

(NETWORK_ID=NW1,
PREFIX64=2001:db8:1234::/96)
(NETWORK_ID=NW2,
PREFIX64=64:ff9b::/96)
R-AAAA(S,PREFIX64=64:ff9b::/96)
DNS#2
T
NAT64
2001:db8:1234::/96
互联网
DEST: 64:ff9b::198.51.100.1
NW2
NAT64
64:ff9b::/96
198.51.100.1
S
DEST: 198.51.100.1

图10