(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102790808 A
(43)申请公布日 2012.11.21

(21)申请号 201110126408.X

(22)申请日 2011.05.16

(71)申请人 奇智软件(北京)有限公司
地址 100016 北京市朝阳区酒仙桥路 14 号兆维大厦 4 层东侧单元

(72)发明人 董斌雁

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 苏培华

(51)Int.Cl.
*H04L 29/12*(2006.01)
*H04L 29/08*(2006.01)

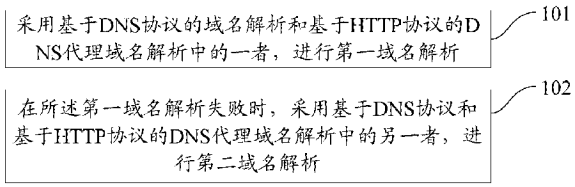
权利要求书 4 页 说明书 15 页 附图 6 页

(54)发明名称

一种域名解析方法和系统、一种客户端

(57)摘要

本发明提供了一种域名解析方法和系统、一种客户端，其中的域名解析方法具体包括：采用基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理域名解析中的一者，进行第一域名解析；在所述第一域名解析失败时，采用基于 DNS 协议和基于 HTTP 协议的 DNS 代理域名解析中的另一者，进行第二域名解析。本发明能够提高域名解析的成功率。




CN 102790808 A

1. 一种域名解析方法，其特征在于，包括：

采用基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理域名解析中的一者，进行第一域名解析；

在所述第一域名解析失败时，采用基于 DNS 协议和基于 HTTP 协议的 DNS 代理域名解析中的另一者，进行第二域名解析。

2. 如权利要求 1 所述的方法，其特征在于，所述基于 DNS 协议的域名解析包括：通过 UDP 传输方式，采用 DNS 协议进行域名解析。

3. 如权利要求 1 所述的方法，其特征在于，所述基于 DNS 协议的域名解析包括：通过 TCP 传输方式，采用 DNS 协议进行域名解析。

4. 根据权利要求 1、2 或 3 所述的方法，其特征在于，还包括：

设置网络服务参数，并依据所述网络服务参数进行当前域名解析，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者，所述网络服务参数包括重试次数和超时参数中的一者或多者。

5. 根据权利要求 1、2 或 3 所述的方法，其特征在于，还包括：

在当前域名解析成功后，记录所述当前域名解析所使用 DNS 服务器的游标位置，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者；

记录所述当前域名解析所使用的协议类型；

以所述游标位置和协议类型作为下次域名解析的定向依据。

6. 根据权利要求 1、2 或 3 所述的方法，其特征在于，还包括：

在当前域名解析成功后，得到相应的解析结果，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者；

依据所述解析结果，判断得到与所在客户端最合适的 DNS 服务器；

以所述 DNS 服务器作为下次域名解析的定向依据。

7. 根据权利要求 1、2 或 3 所述的方法，其特征在于，还包括：

设置 DNS 服务器的访问优先级顺序；

依据所述访问优先级顺序，选择 DNS 服务器进行当前域名解析，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者。

8. 根据权利要求 1、2 或 3 所述的方法，其特征在于，所述设置 DNS 服务器的访问优先级顺序的步骤，包括：

指定 DNS 服务器集合；

将所述 DNS 服务器集合中的 DNS 服务器随机散列到 DNS 服务器掩码中。

9. 根据权利要求 1、2 或 3 所述的方法，其特征在于，所述基于 HTTP 协议进行 DNS 代理域名解析的步骤，包括：

接收客户端发起的基于 HTTP 协议的域名解析请求，所述域名解析请求中包括域名参数；

从所述域名解析请求中解析域名参数；

依据解析得到的域名参数，向 DNS 服务器发起 DNS 查询请求；

解析 DNS 服务器返回的 DNS 应答，并返回给客户端。

10. 根据权利要求 9 所述的方法，其特征在于，所述客户端通过如下步骤发起域名解析

请求：

将需要解析的域名参数进行 base64 编码，并封装到 HTTP GET 命令请求的包头中；

向域名解析代理服务器发送所述 HTTP GET 命令请求；

所述从所述域名解析请求中解析域名参数的步骤，包括：

所述域名解析代理服务器的 CGI 程序接收所述 HTTP GET 命令请求；

所述 CGI 程序通过对所述 HTTP GET 命令请求进行 base64 解码，解析出所述域名参数。

11. 一种域名解析系统，其特征在于，包括客户端、域名解析代理服务器和 DNS 服务器，所述域名解析代理服务器与 DNS 服务器相连；

其中，所述客户端分别与所述域名解析代理服务器和 DNS 服务器相连，包括：

DNS 解析装置，用于与所述 DNS 服务器交互，采用 DNS 协议进行域名解析；

代理解析装置，用于与所述域名解析代理服务器交互，基于 HTTP 协议进行 DNS 代理域名解析；

第一调用模块，用于调用所述 DNS 解析装置和所述代理解析装置中的一者进行第一域名解析；及

第二调用模块，用于在所述第一域名解析失败时，调用所述 DNS 解析装置和所述代理解析装置中的另一者进行第二域名解析。

12. 如权利要求 11 所述的系统，其特征在于，所述 DNS 解析装置，具体用于，通过 UDP 传输方式，采用 DNS 协议进行域名解析。

13. 根据权利要求 11 所述的系统，其特征在于，所述 DNS 解析装置，具体用于，通过 TCP 传输方式，采用 DNS 协议进行域名解析。

14. 根据权利要求 11、12 或 13 所述的系统，其特征在于，所述客户端还包括：

第一设置模块，用于设置网络服务参数，由当前解析模块依据所述网络服务参数进行域名解析，其中，所述当前解析模块为第一解析模块和第二解析模块中的一者，所述网络服务参数包括重试次数和超时参数中的一者或多者。

15. 根据权利要求 11、12 或 13 所述的系统，其特征在于，所述客户端还包括：

第一记录模块，用于在当前域名解析成功后，记录所述当前域名解析所使用 DNS 服务器的游标位置，其中，所述当前域名解析为第一域名解析、和第二域名解析中的一者；

第二记录模块，用于记录所述当前域名解析所使用的协议类型；

第一定向模块，用于以所述游标位置和协议类型作为下次域名解析的定向依据。

16. 根据权利要求 11、12 或 13 所述的系统，其特征在于，所述客户端还包括：

结果获取模块，用于在当前域名解析成功后，得到相应的解析结果，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者；

判断模块，用于依据所述解析结果，判断得到与所在客户端最合适的 DNS 服务器；

第二定向模块，用于以所述 DNS 服务器作为下次域名解析的定向依据。

17. 根据权利要求 11、12 或 13 所述的系统，其特征在于，所述客户端还包括：

第二设置模块，用于设置 DNS 服务器的访问优先级顺序；

选择模块，用于依据所述访问优先级顺序，选择当前 DNS 服务器进行当前域名解析，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者。

18. 根据权利要求 11、12 或 13 所述的系统，其特征在于，所述第二设置模块包括：

指定单元，用于指定 DNS 服务器集合；及

随机散列单元，用于将所述 DNS 服务器集合中的 DNS 服务器随机散列到 DNS 服务器掩码中。

19. 根据权利要求 12 或 13 所述的系统，其特征在于，所述域名解析代理服务器，包括：

接收模块，用于接收客户端发起的基于 HTTP 协议的域名解析请求，所述域名解析请求中包括域名参数；

请求解析模块，用于从所述域名解析请求中解析域名参数；查询模块，用于依据解析得到的域名参数，向 DNS 服务器发起 DNS 查询请求；

应答解析模块，用于解析 DNS 服务器返回的 DNS 应答；及

返回模块，用于将所述 DNS 应答返回给客户端。

20. 根据权利要求 19 所述的系统，其特征在于，所述接收模块和所述请求解析模块为 CGI 程序；

所述 CGI 程序，具体用于接收来自所述客户端的 HTTP GET 命令请求，并通过对所述 HTTP GET 命令请求进行 base64 解码，解析出所述域名参数。

21. 一种客户端，其特征在于，其分别与所述域名解析代理服务器和 DNS 服务器相连，所述域名解析代理服务器与 DNS 服务器相连，包括：

DNS 解析装置，用于与所述 DNS 服务器交互，采用 DNS 协议进行域名解析；

代理解析装置，用于与所述域名解析代理服务器交互，基于 HTTP 协议进行 DNS 代理域名解析；

第一调用模块，用于调用所述 DNS 解析装置和所述代理解析装置中的一者进行第一域名解析；及

第二调用模块，用于在所述第一域名解析失败时，调用所述 DNS 解析装置和所述代理解析装置中的另一者进行第二域名解析。

22. 如权利要求 21 所述的客户端，其特征在于，所述 DNS 解析装置，具体用于，通过 UDP 传输方式，采用 DNS 协议进行域名解析。

23. 根据权利要求 21 所述的客户端，其特征在于，所述 DNS 解析装置，具体用于，通过 TCP 传输方式，采用 DNS 协议进行域名解析。

24. 如权利要求 21、22 或 23 所述的客户端，其特征在于，所述客户端还包括：

第一设置模块，用于设置网络服务参数，由当前解析模块依据所述网络服务参数进行域名解析，其中，所述当前解析模块为第一解析模块和第二解析模块中的一者，所述网络服务参数包括重试次数和超时参数中的一者或多者。

25. 根据权利要求 21、22 或 23 所述的客户端，其特征在于，所述客户端还包括：

第一记录模块，用于在当前域名解析成功后，记录所述当前域名解析所使用 DNS 服务器的游标位置，其中，所述当前域名解析为第一域名解析、和第二域名解析中的一者；

第二记录模块，用于记录所述当前域名解析所使用的协议类型；

第一定向模块，用于以所述游标位置和协议类型作为下次域名解析的定向依据。

26. 根据权利要求 21、22 或 23 所述的客户端，其特征在于，所述客户端还包括：

结果获取模块，用于在当前域名解析成功后，得到相应的解析结果，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者；

判断模块，用于依据所述解析结果，判断得到与所在客户端最合适的 DNS 服务器；

第二定向模块，用于以所述 DNS 服务器作为下次域名解析的定向依据。

27. 根据权利要求 21、22 或 23 所述的客户端，其特征在于，所述客户端还包括：

第二设置模块，用于设置 DNS 服务器的访问优先级顺序；

选择模块，用于依据所述访问优先级顺序，选择当前 DNS 服务器进行当前域名解析，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者。

28. 根据权利要求 21、22 或 23 所述的客户端，其特征在于，所述第二设置模块包括：

指定单元，用于指定 DNS 服务器集合；及

随机散列单元，用于将所述 DNS 服务器集合中的 DNS 服务器随机散列到 DNS 服务器掩码中。

# 一种域名解析方法和系统、一种客户端

## 技术领域

[0001] 本发明涉及数字网络通信技术领域，特别是涉及一种域名解析方法和系统、一种客户端。

## 背景技术

[0002] DNS(域名系统，Domain Name System)是一种用于TCP/IP(传输控制协议/因特网互联协议，Transmission Control Protocol/Internet Protocol)的应用程序的分布式数据库，它提供主机名字和IP地址之间的转换信息。

[0003] 目前通常采用的域名解析方法如下：1)客户端向DNS服务器发送域名解析请求；2)DNS服务器对域名进行解析；3)DNS服务器将解析结果返回给客户端；以及4)客户端从该结果中选择一个IP地址进行访问。

[0004] 目前，DNS协议在域名解析中采用UDP(用户数据包协议，User Datagram Protocol)来传输客户端发出的域名解析请求和DNS对该域名解析请求的响应。

[0005] UDP传输协议不属于连接型协议，因而具有资源消耗小，处理速度快的优点，通常能够在音频、视频和普通数据中得到广泛应用。但是，由于UDP传输协议并不提供数据传送的保证机制，如果在从发送方到接收方的传递过程中出现数据报的丢失，协议本身并不能做出任何检测或提示；因此，在网络质量令人不十分满意的环境下，UDP协议数据包丢失会比较严重，此时就不能提供正常的域名解析，从而导致不能正常连接网络服务，降低域名解析的成功率。

[0006] 总之，需要本领域技术人员迫切解决的一个技术问题就是：如何能够提高域名解析的成功率。

## 发明内容

[0007] 本发明所要解决的技术问题是提供一种域名解析方法和系统，能够提高域名解析的成功率。

[0008] 相应的，本发明还提供了一种客户端，用以保证上述方法和系统在实际中的应用。

[0009] 为了解决上述问题，本发明公开了一种域名解析方法，包括：

[0010] 采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的一者，进行第一域名解析；

[0011] 在所述第一域名解析失败时，采用基于DNS协议和基于HTTP协议的DNS代理域名解析中的另一者，进行第二域名解析。

[0012] 优选的，所述基于DNS协议的域名解析包括：通过UDP传输方式，采用DNS协议进行域名解析。

[0013] 优选的，所述基于DNS协议的域名解析包括：通过TCP传输方式，采用DNS协议进行域名解析。

[0014] 优选的，所述方法还包括：

[0015] 设置网络服务参数，并依据所述网络服务参数进行当前域名解析，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者，所述网络服务参数包括重试次数和超时参数中的一者或多者。

[0016] 优选的，所述方法还包括：

[0017] 在当前域名解析成功后，记录所述当前域名解析所使用 DNS 服务器的游标位置，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者；

[0018] 记录所述当前域名解析所使用的协议类型；

[0019] 以所述游标位置和协议类型作为下次域名解析的定向依据。

[0020] 优选的，所述方法还包括：

[0021] 在当前域名解析成功后，得到相应的解析结果，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者；

[0022] 依据所述解析结果，判断得到与所在客户端最合适的 DNS 服务器；

[0023] 以所述 DNS 服务器作为下次域名解析的定向依据。

[0024] 优选的，所述方法还包括：

[0025] 设置 DNS 服务器的访问优先级顺序；

[0026] 依据所述访问优先级顺序，选择 DNS 服务器进行当前域名解析，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者。

[0027] 优选的，所述设置 DNS 服务器的访问优先级顺序的步骤，包括：

[0028] 指定 DNS 服务器集合；

[0029] 将所述 DNS 服务器集合中的 DNS 服务器随机散列到 DNS 服务器掩码中。

[0030] 优选的，所述基于 HTTP 协议进行 DNS 代理域名解析的步骤，包括：

[0031] 接收客户端发起的基于 HTTP 协议的域名解析请求，所述域名解析请求中包括域名参数；

[0032] 从所述域名解析请求中解析域名参数；

[0033] 依据解析得到的域名参数，向 DNS 服务器发起 DNS 查询请求；

[0034] 解析 DNS 服务器返回的 DNS 应答，并返回给客户端

[0035] 优选的，所述客户端通过如下步骤发起域名解析请求：

[0036] 将需要解析的域名参数进行 base64 编码，并封装到 HTTP GET 命令请求的包头中；

[0037] 向域名解析代理服务器发送所述 HTTP GET 命令请求；

[0038] 所述从所述域名解析请求中解析域名参数的步骤，包括：

[0039] 所述域名解析代理服务器的 CGI 程序接收所述 HTTP GET 命令请求；

[0040] 所述 CGI 程序通过对所述 HTTP GET 命令请求进行 base64 解码，解析出所述域名参数。

[0041] 另一方面，本发明还公开了一种域名解析系统，包括客户端、域名解析代理服务器和 DNS 服务器，所述域名解析代理服务器与 DNS 服务器相连；

[0042] 其中，所述客户端分别与所述域名解析代理服务器和 DNS 服务器相连，包括：

[0043] DNS 解析装置，用于与所述 DNS 服务器交互，采用 DNS 协议进行域名解析；

[0044] 代理解析装置，用于与所述域名解析代理服务器交互，基于 HTTP 协议进行 DNS 代理域名解析；

[0045] 第一调用模块，用于调用所述 DNS 解析装置和所述代理解析装置中的一者进行第一域名解析；及

[0046] 第二调用模块，用于在所述第一域名解析失败时，调用所述 DNS 解析装置和所述代理解析装置中的另一者进行第二域名解析。

[0047] 优选的，所述 DNS 解析装置，具体用于，通过 UDP 传输方式，采用 DNS 协议进行域名解析。

[0048] 优选的，所述 DNS 解析装置，具体用于，通过 TCP 传输方式，采用 DNS 协议进行域名解析。

[0049] 优选的，所述客户端还包括：

[0050] 第一设置模块，用于设置网络服务参数，由当前解析模块依据所述网络服务参数进行域名解析，其中，所述当前解析模块为第一解析模块和第二解析模块中的一者，所述网络服务参数包括重试次数和超时参数中的一者或多者。

[0051] 优选的，所述客户端还包括：

[0052] 第一记录模块，用于在当前域名解析成功后，记录所述当前域名解析所使用 DNS 服务器的游标位置，其中，所述当前域名解析为第一域名解析、和第二域名解析中的一者；

[0053] 第二记录模块，用于记录所述当前域名解析所使用的协议类型；

[0054] 第一定向模块，用于以所述游标位置和协议类型作为下次域名解析的定向依据。

[0055] 优选的，所述客户端还包括：

[0056] 结果获取模块，用于在当前域名解析成功后，得到相应的解析结果，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者；

[0057] 判断模块，用于依据所述解析结果，判断得到与所在客户端最合适的 DNS 服务器；

[0058] 第二定向模块，用于以所述 DNS 服务器作为下次域名解析的定向依据。

[0059] 优选的，所述客户端还包括：

[0060] 第二设置模块，用于设置 DNS 服务器的访问优先级顺序；

[0061] 选择模块，用于依据所述访问优先级顺序，选择当前 DNS 服务器进行当前域名解析，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者。

[0062] 优选的，所述第二设置模块包括：

[0063] 指定单元，用于指定 DNS 服务器集合；及

[0064] 随机散列单元，用于将所述 DNS 服务器集合中的 DNS 服务器随机散列到 DNS 服务器掩码中。

[0065] 优选的，所述域名解析代理服务器，包括：

[0066] 接收模块，用于接收客户端发起的基于 HTTP 协议的域名解析请求，所述域名解析请求中包括域名参数；

[0067] 请求解析模块，用于从所述域名解析请求中解析域名参数；查询模块，用于依据解析得到的域名参数，向 DNS 服务器发起 DNS 查询请求；

[0068] 应答解析模块，用于解析 DNS 服务器返回的 DNS 应答；及

[0069] 返回模块，用于将所述 DNS 应答返回给客户端。

[0070] 优选的，所述接收模块和所述请求解析模块为 CGI 程序；

[0071] 所述 CGI 程序，具体用于接收来自所述客户端的 HTTP GET 命令请求，并通过对所

述 HTTP GET 命令请求进行 base64 解码，解析出所述域名参数。

[0072] 另一方面，本发明还公开了一种客户端，其分别与所述域名解析代理服务器和 DNS 服务器相连，所述域名解析代理服务器与 DNS 服务器相连，包括：

[0073] DNS 解析装置，用于与所述 DNS 服务器交互，采用 DNS 协议进行域名解析；

[0074] 代理解析装置，用于与所述域名解析代理服务器交互，基于 HTTP 协议进行 DNS 代理域名解析；

[0075] 第一调用模块，用于调用所述 DNS 解析装置和所述代理解析装置中的一者进行第一域名解析；

[0076] 第二调用模块，用于在所述第一域名解析失败时，调用所述 DNS 解析装置和所述代理解析装置中的另一者进行第二域名解析。

[0077] 优选的，所述 DNS 解析装置，具体用于，通过 UDP 传输方式，采用 DNS 协议进行域名解析。

[0078] 优选的，所述 DNS 解析装置，具体用于，通过 TCP 传输方式，采用 DNS 协议进行域名解析。

[0079] 优选的，所述客户端还包括：

[0080] 第一设置模块，用于设置网络服务参数，由当前解析模块依据所述网络服务参数进行域名解析，其中，所述当前解析模块为第一解析模块和第二解析模块中的一者，所述网络服务参数包括重试次数和超时参数中的一者或多者。

[0081] 优选的，所述客户端还包括：

[0082] 第一记录模块，用于在当前域名解析成功后，记录所述当前域名解析所使用 DNS 服务器的游标位置，其中，所述当前域名解析为第一域名解析、和第二域名解析中的一者；

[0083] 第二记录模块，用于记录所述当前域名解析所使用的协议类型；

[0084] 第一定向模块，用于以所述游标位置和协议类型作为下次域名解析的定向依据。

[0085] 优选的，所述客户端还包括：

[0086] 结果获取模块，用于在当前域名解析成功后，得到相应的解析结果，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者；

[0087] 判断模块，用于依据所述解析结果，判断得到与所在客户端最合适的 DNS 服务器；

[0088] 第二定向模块，用于以所述 DNS 服务器作为下次域名解析的定向依据。

[0089] 优选的，所述客户端还包括：

[0090] 第二设置模块，用于设置 DNS 服务器的访问优先级顺序；

[0091] 选择模块，用于依据所述访问优先级顺序，选择当前 DNS 服务器进行当前域名解析，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者。

[0092] 优选的，所述第二设置模块包括：

[0093] 指定单元，用于指定 DNS 服务器集合；及

[0094] 随机散列单元，用于将所述 DNS 服务器集合中的 DNS 服务器随机散列到 DNS 服务器掩码中。

[0095] 与现有技术相比，本发明具有以下优点：

[0096] 本发明在进行域名解析时，可在基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理域名解析之间动态转换；由于在基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理

域名解析中的一者解析失败时，本发明均可自动转换到另一者进行域名解析，因此，相对于现有技术，能够提高 DNS 解析的成功率。

[0097] 其次，所述基于 DNS 协议的域名解析既可以包括通过 UDP 传输方式，采用 DNS 协议进行域名解析，又可以包括通过 TCP 传输方式，采用 DNS 协议进行域名解析；在实际应用中，可在 UDP 传输协议和 TCP 传输协议之间动态转换；由于在 UDP 传输协议和 TCP 传输协议中的一者解析失败时，可以自动转换到另一者进行域名解析，因此，相对于现有技术只使用 UDP 传输协议，而由于 UDP 本身丢包严重的缺陷，可能不能正常解析的情形，本发明能够提高 DNS 解析的成功率。

[0098] 再者，由于基于 HTTP 协议的 DNS 代理域名解析，无需调用任意 Windows 应用层网络 API，而是通过 DNS 报文代理服务，所以不容易受 LSP 恶意代码对 DNS 协议的篡改、拦截、过滤、重定向等影响，不受 hosts 文件篡改等攻击影响；因此，还能够有效防止域名解析过程中恶意代码的攻击，从而提高域名解析的安全性。

[0099] 另外，客户端应用程序还可以根据自身网络服务需求，自行设定其它网络服务参数，如在网络情况特别差的情况下，通过设定的重试次数提高解析成功率，又如，通过设定的超时参数，避免网络通讯情况较差的情况下，DNS 应答不能及时返回，而客户端应用程序必须等待的问题

[0100] 进一步，本发明还可通过记录当前成功解析域名解析代理服务器游标位置及所使用的协议类型（UDP、TCP 传输协议和基于 HTTP 协议的 DNS 代理域名解析中的一者），下次解析时，可以使用该协议类型，直接定向到前一个成功域名解析代理服务器。

[0101] 更进一步，本发明还可以支持随机设定 DNS 解析服务器访问优先顺序，从而实现客户端 DNS 解析服务均衡负载。

## 附图说明

[0102] 图 1 是本发明一种域名解析方法实施例 1 的流程图；

[0103] 图 2 是本发明一种域名解析方法实施例 2 的流程图；

[0104] 图 3 本发明一种域名解析代理服务器与客户端和 DNS 服务器之间的关系示意图；

[0105] 图 4 是本发明一种域名解析方法实施例 3 的流程图；

[0106] 图 5 是本发明一种域名解析方法实施例 4 的流程图；

[0107] 图 6 是本发明一种域名解析方法实施例 5 的流程图；

[0108] 图 7 是本发明一种域名解析方法实施例 6 的流程图；

[0109] 图 8 是本发明一种域名解析系统实施例的结构图；

[0110] 图 9 是本发明一种客户端实施例的结构图。

## 具体实施方式

[0111] 为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本发明作进一步详细的说明。

[0112] 本发明实施例的核心构思之一在于，增加了域名解析的选择项，也即，除了传统的基于 DNS 协议的域名解析外，还可以包括基于 HTTP 协议的 DNS 代理域名解析。这样，在进行域名解析时，可在基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理域名解析之间动

态转换。由于在基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理域名解析中的一者解析失败时，本发明均可自动转换到另一者进行域名解析，因此，相对于现有技术，能够提高 DNS 解析的成功率。

[0113] 参照图 1，示出了本发明一种域名解析方法实施例的流程图，具体可以包括：

[0114] 步骤 101、采用基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理域名解析中的一者，进行第一域名解析；

[0115] 步骤 102、在所述第一域名解析失败时，采用基于 DNS 协议和基于 HTTP 协议的 DNS 代理域名解析中的另一者，进行第二域名解析。

[0116] 在本发明的一种优选实施例中，所述基于 DNS 协议的域名解析可以包括：通过 UDP 传输方式，采用 DNS 协议进行域名解析。

[0117] 在本发明的另一种优选实施例中，所述基于 DNS 协议的域名解析可以包括：通过 TCP 传输方式，采用 DNS 协议进行域名解析。

[0118] 以上对基于 DNS 协议的域名解析的两种传输方式进行了详细介绍，可以理解，本领域技术人员可以根据需要联合使用所述两种传输方式，或者，使用其中任一种传输方式，本发明对此不加以限制。

[0119] 例如，在本发明的一种优选实施例中，联合使用所述两种传输方式的域名解析方法具体可以包括：

[0120] 步骤 S1、通过 UDP 和 TCP 传输方式中的一者，采用 DNS 协议进行第三域名解析；

[0121] 步骤 S2、在所述第三域名解析失败时，通过所述 UDP 和 TCP 传输方式中的另一者，采用 DNS 协议进行第四域名解析。

[0122] 本优选实施例相当于增加了 DNS 基础所依赖传输层协议的选择项，也即，除了传统的 UDP 传输协议外，还可以包括 TCP（传输控制协议，Transmission Control Protocol）传输协议；这样，在使用 DNS 协议进行域名解析时，可在 UDP 传输协议和 TCP 传输协议之间动态转换。由于在 UDP 传输协议和 TCP 传输协议中的一者解析失败时，可以自动转换到另一者进行 DNS 解析，因此，相对于现有技术，能够进一步提高 DNS 解析的成功率。

[0123] UDP 传输协议和 TCP 传输协议的主要区别是两者在如何实现信息的可靠传递方面不同，具体表现在，

[0124] 1、UDP 传输协议不提供数据传送的保证机制，如果在从发送方到接收方的传递过程中出现数据报的丢失，协议本身并不能做出任何检测或提示；因此，在网络质量令人不十分满意的环境下，UDP 协议数据包丢失会比较严重；但是，其不属于连接型协议，具有资源消耗小，处理速度快的优点；

[0125] 2、TCP 传输协议中包含了专门的传递保证机制，当数据接收方收到发送方传来的信息时，会自动向发送方发出确认消息；发送方只有在接收到该确认消息之后才继续传送其它信息，否则将一直等待直到收到确认信息为止；因此，TCP 传输协议能够保障传输的可靠性；但是，由于其属于连接型协议，故相对于 UDP 传输协议，具有资源消耗大，处理速度慢的优点。

[0126] 由于本发明的宗旨是为了提高 DNS 解析的成功率，故在实际中，可由客户端选择优选采用哪种传输协议；对于客户端而言，在实际中，UDP 和 TCP 等传输协议主要用于发送 DNS 查询请求，以及接收 DNS 应答；这里，所述客户端可以为 Windows 客户端，也可以为

Linux 客户端，这里仅以 Windows 客户端为例进行说明，其它系统的客户端相互参照即可。

[0127] 例如，Windows 客户端对 DNS 解析的处理速度有要求，故可优选采用 UDP 传输协议，相应地，所述方法具体可以包括：

[0128] 步骤 A1、采用 UDP 传输协议进行 UDP 域名解析；

[0129] 步骤 A2、在 UDP 域名解析失败时，采用 TCP 传输协议进行 TCP 域名解析。

[0130] 又如，Windows 客户端对 DNS 解析的处理速度没有要求，只是一味追求 DNS 解析的成功率，故可优选采用 TCP 传输协议，相应地，所述方法具体可以包括：

[0131] 步骤 B1、采用 TCP 传输协议进行 TCP 域名解析；

[0132] 步骤 B2、在 TCP 域名解析失败时，采用 UDP 传输协议进行 UDP 域名解析。

[0133] 在优选采用 UDP 传输协议时，虽然可以发挥处理速度快的优势，但在 DNS 解析成功率方面具有风险，而本发明刚好可以通过 TCP 传输协议弥补这一风险；在优选采用 TCP 传输协议时，可以充分发挥可靠性高的优势，并且，以 UDP 传输协议作为候补以预防 TCP 传输失败的情形。总之，本领域技术人员可以根据实际需要，确定优先采用哪种传输协议，本发明的宗旨是为了提高 DNS 解析的成功率，而不会对具体的优先顺序加以限制。

[0134] 参照图 2，示出了本发明一种域名解析方法实施例 2 的流程图，具体可以包括：

[0135] 步骤 201、采用基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理域名解析中的一者进行第一域名解析；

[0136] 步骤 202、在所述第一域名解析失败时，采用基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理域名解析中的另一者进行第二域名解析；

[0137] 其中，所述基于 DNS 协议的域名解析，具体可以包括：

[0138] 步骤 203、通过 UDP 和 TCP 传输方式中的一者，采用 DNS 协议进行第三域名解析；

[0139] 步骤 204、在所述第三域名解析失败时，通过所述 UDP 和 TCP 传输方式中的另一者，采用 DNS 协议进行第四域名解析。

[0140] 相对于实施例 1，本实施例提供 UDP 传输协议、TCP 传输协议和基于 HTTP 协议的 DNS 代理域名解析三个选择项进行域名解析；这样，相对于实施例 1，本实施例具体可以包括如下两种情形：

[0141] 情形 1、在所述第三域名解析和 / 或第四域名解析失败时，基于 HTTP 协议进行 DNS 代理域名解析；

[0142] 情形 2、在进行所述第三域名解析和 / 或第四域名解析之前，基于 HTTP 协议进行 DNS 代理域名解析，若所述 DNS 代理域名解析失败，则执行第三域名解析步骤。

[0143] 这样，在采用 UDP 传输协议和 TCP 传输协议解析失败时，能够进一步提高 DNS 解析的成功率。

[0144] 现有域名解析方法通常需要调用 Windows 应用层 API，而 Windows 应用层 API 不仅允许正常程序过滤和修改 Windows 网络协议，而且更令恶意程序有机可乘。

[0145] 由于基于 HTTP 协议的 DNS 代理解析无需调用任意 Windows 应用层网络 API，而是通过 DNS 报文代理服务，所以不受 LSP 恶意代码对 DNS 协议的篡改、拦截、过滤、重定向等影响，不受 hosts 文件篡改等攻击影响；因此，相对于实施例 1，本实施例不仅能够进一步提供 DNS 解析的成功率，而且有效防止域名解析过程中恶意代码的攻击，从而提高域名解析的安全性。

[0146] 在具体实现中，所述采用HTTP DNS代理协议进行第三域名解析或者第四域名解析的步骤，具体可以包括：

[0147] 步骤C1、接收客户端发起的基于HTTP协议的域名解析请求，所述域名解析请求中可以包括域名参数；

[0148] HTTP协议定义了与服务器交互的不同方法，最基本的方法是GET和POST。事实上GET适用于多数请求，而保留POST仅用于更新站点。根据HTTP规范，GET用于信息获取，而且应该是安全的和幂等的。

[0149] 在本发明的一种优选实施例中，为了提高域名解析的安全性，所述客户端可以通过GET方法发起域名解析请求：

[0150] 子步骤D1、将需要解析的域名参数进行base64编码，并封装到HTTPGET命令请求的包头中；

[0151] 子步骤D2、向域名解析代理服务器发送所述HTTP GET命令请求。

[0152] 当然，除了GET外，本领域技术人员还可以根据实际需要，采用其他请求，如POST等，本发明对此不加以限制。

[0153] 为了更有效避免基于域名过滤的网络攻击，在本发明的一种优选实施例中，在将需要解析的域名参数进行base64编码前，所述客户端发起域名解析请求的步骤，还可以包括：

[0154] 子步骤D3、将需要解析的域名参数进行加密，以加密后的域名参数进行base64编码。

[0155] 将域名参数通过加密方式发送给域名解析代理服务器，即使恶意代码劫持HTTP通讯，也无法解密。因此，能够避免基于域名过滤的网络攻击。

[0156] 步骤C2、从所述域名解析请求中解析域名参数；

[0157] 参照图3，示出了域名解析代理服务器与客户端和DNS服务器之间的关系示意图，其中，客户端应用程序可直接通过IP连接该域名解析代理服务器，相对于现有技术客户端与DNS服务器进行之间通信交互，本实施例采用域名解析代理服务器作为代理媒介，用于分别实现与客户端和DNS服务器之间的通信：一方面，其可以基于HTTP协议安全解析来自客户端的域名解析请求，并基于DNS协议传输给DNS服务器；另一方面，其可以基于DNS协议安全解析来自DNS服务器的DNS应答，并基于HTTP协议返回给客户端。

[0158] 在本发明的一种优选实施例中，域名解析代理服务器可以指定CGI程序处理来自客户端的HTTP GET命令请求，相应地，域名解析代理服务器可以通过如下步骤从所述域名解析请求中解析域名参数：

[0159] 子步骤E1、所述域名解析代理服务器的CGI程序接收所述HTTP GET命令请求；

[0160] 子步骤E2、所述CGI程序通过对所述HTTP GET命令请求进行base64解码，解析出所述域名参数。

[0161] CGI(通用网关接口，Common Gate Interface)程序，通常运行在服务器上，提供与客户端应用程序（如浏览器）之间的接口。CGI程序通常被用来解释处理来自表单的输入信息，并在服务器产生相应的处理，或将相应的信息反馈给浏览器。

[0162] CGI程序处理请求的原理通常为：通过Internet把用户请求送到服务器；服务器接收用户请求并交给CGI程序处理；CGI程序把处理结果传送给服务器；服务器把结果送回

到用户。依据上述原理，步骤 102- 步骤 104 均由 CGI 程序来完成。

[0163] 对应于客户端加密主机域名的情形，在本发明的一种优选实施例中，在所述 CGI 程序对所述 HTTP GET 命令请求进行 base64 解码前，所述从域名解析请求中解析域名参数的步骤，还可以包括：

[0164] 对所述 HTTP GET 命令请求进行解密，以解密后的 HTTP GET 命令请求进行 base64 解码。

[0165] 步骤 C3、依据解析得到的域名参数，向 DNS 服务器发起 DNS 查询请求；

[0166] 步骤 C4、解析 DNS 服务器返回的 DNS 应答，并返回给客户端 .

[0167] 在本发明的一种优选实施例中，所述步骤 104 具体可以包括：

[0168] 将 DNS 服务器返回的 DNS 应答作为 GET 应答的内容，进行加密和 base64 编码后，返回给客户端。

[0169] 总之，由于采用 HTTP DNS 代理协议进行域名解析的过程无需调用 Windows 应用层网络 API，而是通过 DNS 报文代理服务，所以不受 LSP 恶意代码对 DNS 协议的篡改、拦截、过滤、重定向等影响，不受 hosts 文件篡改等攻击影响。概括而言，本发明能够实现基于 HTTP DNS 代理的安全 DNS 域名解析，从而能够提高域名解析的成功率，防止恶意代码针对 Windows 网络应用层及 DNS 协议本身的攻击。

[0170] 参照图 4，示出了本发明一种域名解析方法实施例 3 的流程图，具体可以包括：

[0171] 步骤 401、优先采用普通 DNS 传输层协议进行域名解析；

[0172] 步骤 402、优先采用 UDP 传输协议；

[0173] 步骤 403、采用 UDP 传输协议进行 UDP 解析；

[0174] 步骤 404、判断 UDP 解析是否成功，若是，则执行步骤 405，否则，执行步骤 406；

[0175] 步骤 405、返回解析成功的响应，并结束本次解析；

[0176] 步骤 406、采用 TCP 传输协议进行 TCP 解析；

[0177] 步骤 407、判断 TCP 解析是否成功，若是，则执行步骤 405，否则，执行步骤 408；

[0178] 步骤 408、基于 HTTP 协议进行 DNS 代理域名解析；

[0179] 步骤 409、判断所述 DNS 代理域名解析是否成功，若是，则执行步骤 405，否则，执行步骤 410；

[0180] 步骤 410、返回解析失败的响应。

[0181] 另外，上述优先采用基于 DNS 协议的域名解析只是作为示例，本领域技术人员可以根据实际需要，优先采用基于 HTTP 协议的 DNS 代理域名解析；上述优先采用 UDP 传输层协议也只是作为示例，本发明还可以优先采用 TCP 传输协议。

[0182] 总之，本发明实现了在 UDP 传输层协议模式解析、TCP 传输层协议模式解析、基于 HTTP 协议的 DNS 代理域名解析三种模式的自动转换，而不会对具体的转换顺序加以限制。

[0183] 参照图 5，示出了本发明一种域名解析方法实施例 4 的流程图，具体可以包括：

[0184] 步骤 501、设置网络服务参数，并依据所述网络服务参数进行当前域名解析，其中，所述网络服务参数可以包括重试次数和超时参数中的一者或多者；

[0185] 所述当前域名解析具体可以包括：

[0186] 步骤 502、采用基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理域名解析中的一者进行第一域名解析；

[0187] 步骤503、在所述第一域名解析失败时，采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的另一者进行第二域名解析；

[0188] 其中，所述基于DNS协议的域名解析，具体可以包括：

[0189] 步骤504、通过UDP和TCP传输方式中的一者，采用DNS协议进行第三域名解析；

[0190] 步骤505、在所述第三域名解析失败时，通过所述UDP和TCP传输方式中的另一者，采用DNS协议进行第四域名解析。

[0191] 相对于实施例2，本实施例可以依据设置的网络服务参数进行当前域名解析，其中，所述网络服务参数具体可以包括：

[0192] 1、重试次数；

[0193] 现有技术中，Windows客户端未能提供设置DNS Server的编程接口，只能设置面向全Windows客户端的DNS Server，不能设置重试次数选项；而如果只使用UDP协议作为DNS协议的传输层协议，则由于UDP本身的缺陷，可能不能正常解析。

[0194] 针对上述情况，本发明能够在网络情况特别差的情况下，通过重试可以提高解析成功率。

[0195] 2、超时参数。

[0196] 在实际中，所述超时参数一般表示客户端得到DNS应答的最大时间；所述超时参数能够避免网络通讯情况较差的情况下，DNS应答不能及时返回，而客户端应用程序必须等待的问题。

[0197] 当然，除了重试次数和超时参数外，客户端应用程序还可以根据自身网络服务需求，自行设定其它网络服务参数，如单次接收等，从而能够提高DNS解析成功率，增强用户体验。

[0198] 另外，DNS应答不能及时返回时，本实施例还可以提供接口在任意时刻取消当前DNS查询请求。

[0199] 参照图6，示出了本发明一种域名解析方法实施例5的流程图，具体可以包括：

[0200] 步骤601、采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的一者进行第一域名解析；

[0201] 步骤602、在所述第一域名解析失败时，采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的另一者进行第二域名解析；

[0202] 其中，所述基于DNS协议的域名解析，具体可以包括：

[0203] 步骤603、通过UDP和TCP传输方式中的一者，采用DNS协议进行第三域名解析；

[0204] 步骤604、在所述第三域名解析失败时，通过所述UDP和TCP传输方式中的另一者，采用DNS协议进行第四域名解析；

[0205] 步骤605、在当前域名解析成功后，记录所述当前域名解析所使用DNS服务器的游标位置，其中所述当前域名解析为第一域名解析和第二域名解析中的一者；

[0206] 步骤606、记录所述当前域名解析所使用的协议类型；

[0207] 步骤607、以所述游标位置和协议类型作为下次域名解析的定向依据。

[0208] 相对于实施例2，本实施例通过记录当前成功解析域名解析代理服务器游标位置及所使用的协议类型(UDP、TCP传输协议和基于HTTP协议的DNS代理域名解析技术中的一者)，下次解析时，可以使用该协议类型，直接定向到前一个成功域名解析代理服务器。

[0209] 在本发明的一种优选实施例中，所述方法还可以包括：

[0210] 在每次域名解析成功后，得到相应的解析结果；

[0211] 依据所述解析结果，判断得到与所在客户端最合适的 DNS 服务器；

[0212] 以所述 DNS 服务器作为下次域名解析的定向依据。

[0213] 在具体实现中，可以提供自定义 DNS 服务器设置程序接口、根据解析结果动态，智能判断与哪个 DNS 服务器通讯最合适，从而实现了客户端负载均衡机制。

[0214] 参照图 7，示出了本发明一种域名解析方法实施例 6 的流程图，具体可以包括：

[0215] 步骤 701、设置 DNS 服务器的访问优先级顺序；

[0216] 步骤 702、依据所述访问优先级顺序，选择当前 DNS 服务器进行当前域名解析；

[0217] 所述当前域名解析具体可以包括：

[0218] 步骤 703、采用基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理域名解析中的一者进行第一域名解析；

[0219] 步骤 704、在所述第一域名解析失败时，采用基于 DNS 协议的域名解析和基于 HTTP 协议的 DNS 代理域名解析中的另一者进行第二域名解析；

[0220] 其中，所述基于 DNS 协议的域名解析，具体可以包括：

[0221] 步骤 705、通过 UDP 和 TCP 传输方式中的一者，采用 DNS 协议进行第三域名解析；

[0222] 步骤 706、在所述第三域名解析失败时，通过所述 UDP 和 TCP 传输方式中的另一者，采用 DNS 协议进行第四域名解析。

[0223] 相对于实施例 2，本实施例支持编程接口级设置自定义的 DNS 服务器并且设置访问优先顺序。

[0224] 在具体实现中，本发明可以提供如下 DNS 协议封装接口层：

[0225] CDns 类提供了 DNS 协议的封装。

[0226] CDns::CDns 构造函数中，实例化 m_DnsUdp，m_DnsTcp，m_DnsHttp 三个类分别对应基于 UDP、TCP、HTTP 的 DNS 解析传输层实例化对象。

[0227] 创建 DNS Cache

[0228] 实例化 CDnsCache 类在其构造函数 CDnsCache::CDnsCache() 中初始化临界区变量，清空当前 map 内容，设置 Cache（缓存）容量。

[0229] CDns::SetOption 提供了应用程序根据自身需要对 DNS 解析各个环节的选项设置，如单次接收、发送 UDP 数据报的超时时间。是否逐个遍历 DNS 服务器，设置自定义服务器等。

[0230] CDns::gethostbyname 提供了类 Winsock DNS 编程接口服务。

[0231] 在上述 DNS 协议封装接口层的基础上，本发明可以提供类 Winsock setsockopt 接口，可以设置特定的 DNS 解析服务器集合：例如缺省优先访问 Open DNS 或 Google DNS，又如，禁用本地 DNS 服务器，直接优先访问广域网 DNS Server，在这种情况下，还可以有效防范基于内网 ARP（地址解析协议，Address Resolution Protocol）代理欺骗机制的 DNS ID 欺骗。

[0232] A) 若设置 OpenDNS 服务器 (208.67.222.222/208.67.220.220) 作为优先解析服务器，则可以享受 OpenDNS 服务器的优点，具体表现在：

[0233] OpenDNS 识别和阻止钓鱼网站；

[0234] OpenDNS 有一个高性能的按地理分布的网络和多个冗余备份连接，会根据访问选择最近的地理位置；可以不用通过电信或者网通提供的 DNS 解析，从而这样可以避免被域名劫持、广告等困扰；

[0235] 具有更稳定的特点。它可以自动纠正拼写错误：如果拼写错误（比如少了个字母），OpenDNS 也能引导到正确的网站，或者提供一个相似网站的搜索列表。

[0236] B) 若设置 Google DNS 服务器 (8.8.8.8/8.8.4.4) 作为优先解析服务器，则可以享受 Google DNS 服务器的优点，具体表现在：

[0237] 减少 DNS 访问延迟时间；

[0238] 共享 Cache 的均衡负载；

[0239] 预取域名解析；

[0240] 广泛地理覆盖的分布式服务器集群服务。

[0241] 在本发明的一种优选实施例中，还可以支持随机设定 DNS 解析服务器访问优先顺序，从而实现客户端 DNS 解析服务均衡负载；相应地，所述所述设置 DNS 服务器的访问优先级顺序的步骤，具体可以包括：

[0242] 指定 DNS 服务器集合；

[0243] 将所述 DNS 服务器集合中的 DNS 服务器随机散列到 DNS 服务器掩码中。

[0244] 调用者可指定一个 DNS 服务器集合，并且可以设定 DNS 服务器随机散列到 DNS 服务器连接掩码中，不同的客户端就对应不同的 DNS 服务器优先策略，实现了基于客户端的动态 DNS 解析均衡负载。

[0245] 总之，本发明能够通过对 UDP 和 TCP 传输协议以及支持 HTTP DNS 代理协议进行自动转换，来实现提供 DNS 解析成功率的目的。

[0246] 本发明能够支持 IPV4(Internet Protocol Version 4) 和 IPV6(Internet Protocol Version 6)，支持 DNS SEC(DNS 安全扩展，Domain Name System Security Extensions)，并且可以服务方式提供 DNS 解析，提供具有应用程序调用的安全认证接口，实现跨进程的安全 DNS 解析服务，支持递归方式 DNS 查询。

[0247] 在实际中，本发明可以应用于众多安全产品（例如，“360 卫士”的系统急救箱、木马云查杀引擎、主机防御系统等产品）中，从而可以面向客户端应用程序提供更加安全、更加稳定的 DNS 解析服务。

[0248] 参照图 8，示出了本发明一种域名解析系统实施例的结构图，其具体可以包括客户端 801、域名解析代理服务器 802 和 DNS 服务器 803，所述域名解析代理服务器 802 和 DNS 服务器 803 相连；

[0249] 其中，所述客户端 801 分别与所述域名解析代理服务器 802 和 DNS 服务器相连 803，包括：

[0250] DNS 解析装置 811，用于与所述 DNS 服务器 803 交互，采用 DNS 协议进行域名解析；

[0251] 代理解析装置 812，用于与所述域名解析代理服务器 802 交互，基于 HTTP 协议进行 DNS 代理域名解析；

[0252] 第一调用模块 813，用于调用所述 DNS 解析装置和所述代理解析装置中的一者进行第一域名解析；

[0253] 第二调用模块 814，用于在所述第一域名解析失败时，调用所述 DNS 解析装置和所

述代理解析装置中的另一者进行第二域名解析。

[0254] 在本发明的一种优选实施例中，所述 DNS 解析装置，可具体用于通过 UDP 传输方式，采用 DNS 协议进行域名解析。

[0255] 在本发明的另一种优选实施例中，所述 DNS 解析装置，可具体用于通过 TCP 传输方式，采用 DNS 协议进行域名解析。

[0256] 在本发明的另一种优选实施例中，所述客户端 801 还可以包括：

[0257] 第一设置模块，用于设置网络服务参数，由当前解析模块依据所述网络服务参数进行域名解析，其中，所述当前解析模块为第一解析模块和第二解析模块中的一者，所述网络服务参数包括重试次数和超时参数中的一者或多者。

[0258] 在本发明的再一种优选实施例中，所述客户端 801 还可以包括：

[0259] 第一记录模块，用于在当前域名解析成功后，记录所述当前域名解析所使用 DNS 服务器的游标位置，其中，所述当前域名解析为第一域名解析、和第二域名解析中的一者；

[0260] 第二记录模块，用于记录所述当前域名解析所使用的协议类型；

[0261] 第一定向模块，用于以所述游标位置和协议类型作为下次域名解析的定向依据。

[0262] 在本发明实施例中，优选的是，所述客户端 801 还可以包括：

[0263] 结果获取模块，用于在当前域名解析成功后，得到相应的解析结果，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者；

[0264] 判断模块，用于依据所述解析结果，判断得到与所在客户端最合适的 DNS 服务器；

[0265] 第二定向模块，用于以所述 DNS 服务器作为下次域名解析的定向依据。

[0266] 在本发明实施例中，优选的是，所述客户端 801 还可以包括：

[0267] 第二设置模块，用于设置 DNS 服务器的访问优先级顺序；

[0268] 选择模块，用于依据所述访问优先级顺序，选择当前 DNS 服务器进行当前域名解析，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者。

[0269] 在本发明实施例中，优选的是，所述第二设置模块可以进一步包括：

[0270] 指定单元，用于指定 DNS 服务器集合；及

[0271] 随机散列单元，用于将所述 DNS 服务器集合中的 DNS 服务器随机散列到 DNS 服务器掩码中。

[0272] 在本发明的一种优选实施例汇总，所述域名解析代理服务器可以具体包括：

[0273] 接收模块，用于接收客户端发起的基于 HTTP 协议的域名解析请求，所述域名解析请求中包括域名参数；

[0274] 请求解析模块，用于从所述域名解析请求中解析域名参数；

[0275] 查询模块，用于依据解析得到的域名参数，向 DNS 服务器发起 DNS 查询请求；

[0276] 应答解析模块，用于解析 DNS 服务器返回的 DNS 应答；及

[0277] 返回模块，用于将所述 DNS 应答返回给客户端。

[0278] 在本发明实施例中，优选的是，所述接收模块和所述请求解析模块均可为 CGI 程序；

[0279] 所述 CGI 程序，可具体用于接收来自所述客户端的 HTTP GET 命令请求，并通过对所述 HTTP GET 命令请求进行 base64 解码，解析出所述域名参数。

[0280] 对于系统实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关

之处参见方法实施例的部分说明即可。

[0281] 参照图 9，示出了本发明一种客户端实施例的结构图，其分别与所述域名解析代理服务器和 DNS 服务器相连，所述域名解析代理服务器与 DNS 服务器相连，所述客户端具体可以包括：

[0282] DNS 解析装置 901，用于与所述 DNS 服务器交互，采用 DNS 协议进行域名解析；

[0283] 代理解析装置 902，用于与所述域名解析代理服务器交互，基于 HTTP 协议进行 DNS 代理域名解析；

[0284] 第一调用模块 903，用于调用所述 DNS 解析装置和所述代理解析装置中的一者进行第一域名解析；及

[0285] 第二调用模块 904，用于在所述第一域名解析失败时，调用所述 DNS 解析装置和所述代理解析装置中的另一者进行第二域名解析。

[0286] 在本发明的一种优选实施例中，所述 DNS 解析装置，可具体用于通过 UDP 传输方式，采用 DNS 协议进行域名解析。

[0287] 在本发明的另一种优选实施例中，所述 DNS 解析装置，可具体用于通过 TCP 传输方式，采用 DNS 协议进行域名解析。

[0288] 在本发明的另一种优选实施例中，所述客户端 801 还可以包括：

[0289] 第一设置模块，用于设置网络服务参数，由当前解析模块依据所述网络服务参数进行域名解析，其中，所述当前解析模块为第一解析模块和第二解析模块中的一者，所述网络服务参数包括重试次数和超时参数中的一者或多者。

[0290] 在本发明的再一种优选实施例中，所述客户端 801 还可以包括：

[0291] 第一记录模块，用于在当前域名解析成功后，记录所述当前域名解析所使用 DNS 服务器的游标位置，其中，所述当前域名解析为第一域名解析、和第二域名解析中的一者；

[0292] 第二记录模块，用于记录所述当前域名解析所使用的协议类型；

[0293] 第一定向模块，用于以所述游标位置和协议类型作为下次域名解析的定向依据。

[0294] 在本发明实施例中，优选的是，所述客户端 801 还可以包括：

[0295] 结果获取模块，用于在当前域名解析成功后，得到相应的解析结果，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者；

[0296] 判断模块，用于依据所述解析结果，判断得到与所在客户端最合适的 DNS 服务器；

[0297] 第二定向模块，用于以所述 DNS 服务器作为下次域名解析的定向依据。

[0298] 在本发明实施例中，优选的是，所述客户端 801 还可以包括：

[0299] 第二设置模块，用于设置 DNS 服务器的访问优先级顺序；

[0300] 选择模块，用于依据所述访问优先级顺序，选择当前 DNS 服务器进行当前域名解析，其中，所述当前域名解析为第一域名解析和第二域名解析中的一者。

[0301] 在本发明实施例中，优选的是，所述第二设置模块可以进一步包括：

[0302] 指定单元，用于指定 DNS 服务器集合；及

[0303] 随机散列单元，用于将所述 DNS 服务器集合中的 DNS 服务器随机散列到 DNS 服务器掩码中。

[0304] 对于客户端实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0305] 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

[0306] 以上对本发明所提供的一种域名解析方法和系统、一种客户端，进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

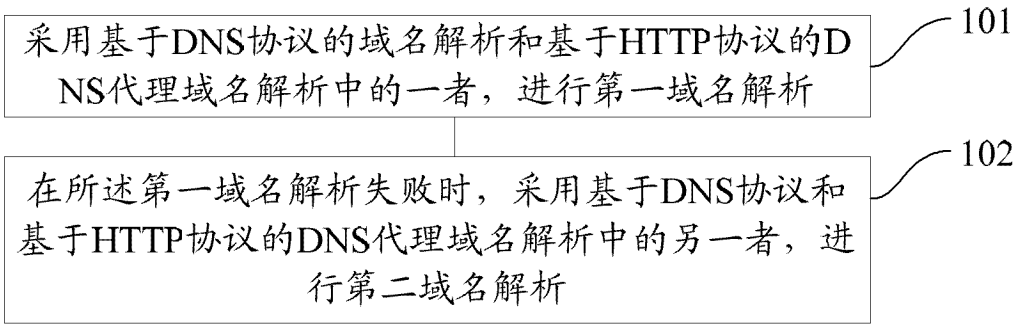

采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的一者，进行第一域名解析
101
在所述第一域名解析失败时，采用基于DNS协议和基于HTTP协议的DNS代理域名解析中的另一者，进行第二域名解析
102

图 1

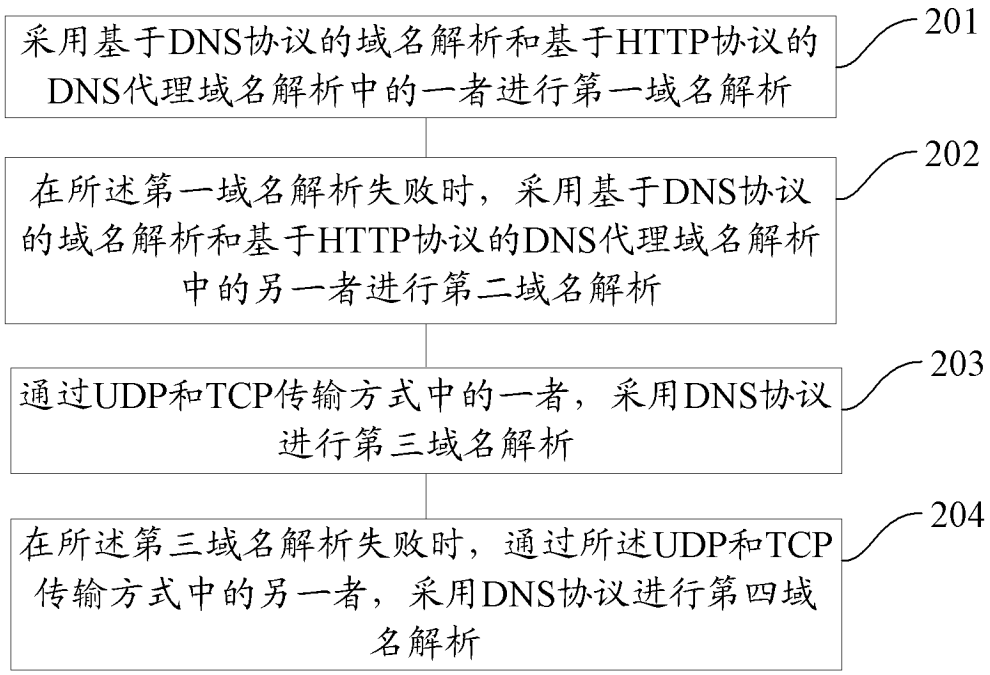

采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的一者进行第一域名解析
201
在所述第一域名解析失败时，采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的另一者进行第二域名解析
202
通过UDP和TCP传输方式中的一者，采用DNS协议进行第三域名解析
203
在所述第三域名解析失败时，通过所述UDP和TCP传输方式中的另一者，采用DNS协议进行第四域名解析
204

图 2

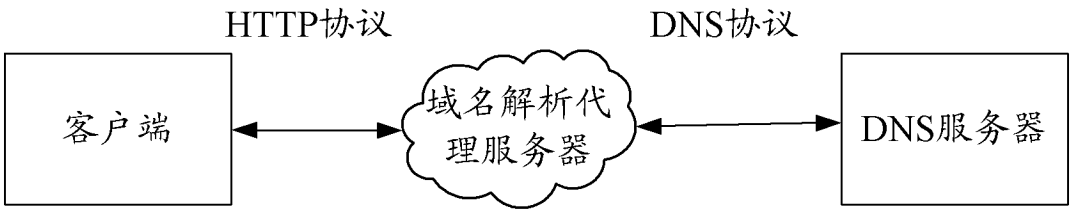

HTTP协议
DNS协议
客户端
域名解析代理服务器
DNS服务器

图 3

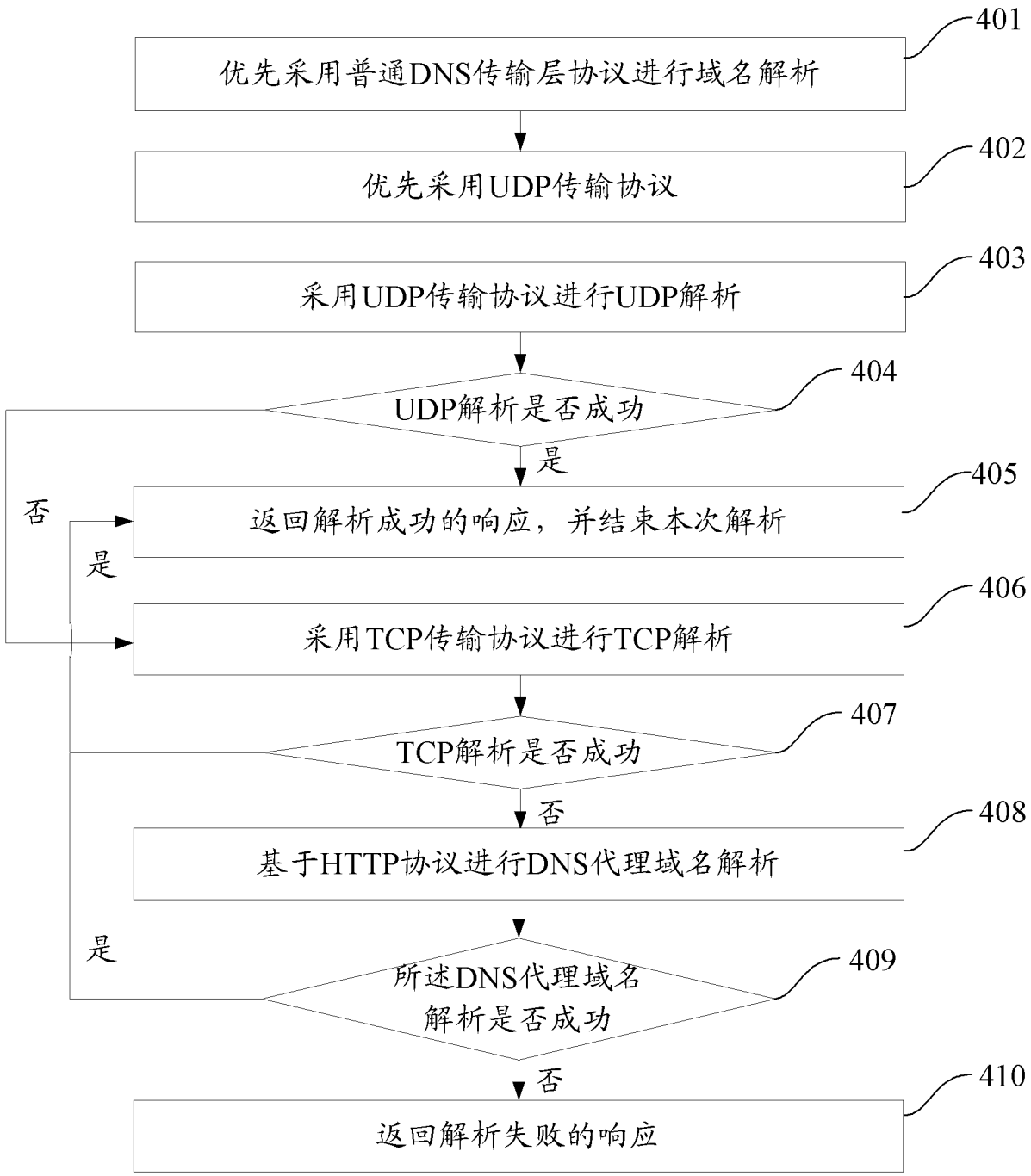

401
优先采用普通DNS传输层协议进行域名解析
402
优先采用UDP传输协议
403
采用UDP传输协议进行UDP解析
404
UDP解析是否成功
是
否
405
返回解析成功的响应，并结束本次解析
是
406
采用TCP传输协议进行TCP解析
407
TCP解析是否成功
否
408
基于HTTP协议进行DNS代理域名解析
是
409
所述DNS代理域名
解析是否成功
否
410
返回解析失败的响应

图 4

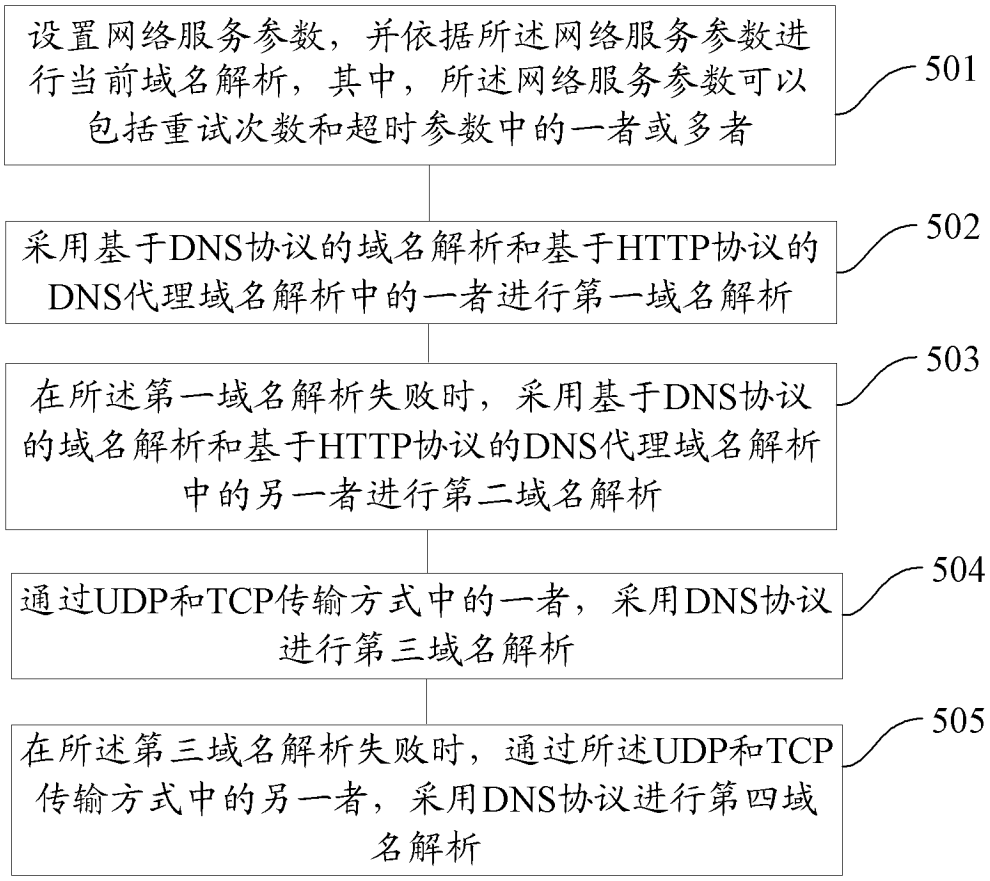

设置网络服务参数，并依据所述网络服务参数进行当前域名解析，其中，所述网络服务参数可以包括重试次数和超时参数中的一者或多者
501
采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的一者进行第一域名解析
502
在所述第一域名解析失败时，采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的另一者进行第二域名解析
503
通过UDP和TCP传输方式中的一者，采用DNS协议进行第三域名解析
504
在所述第三域名解析失败时，通过所述UDP和TCP传输方式中的另一者，采用DNS协议进行第四域名解析
505

图 5

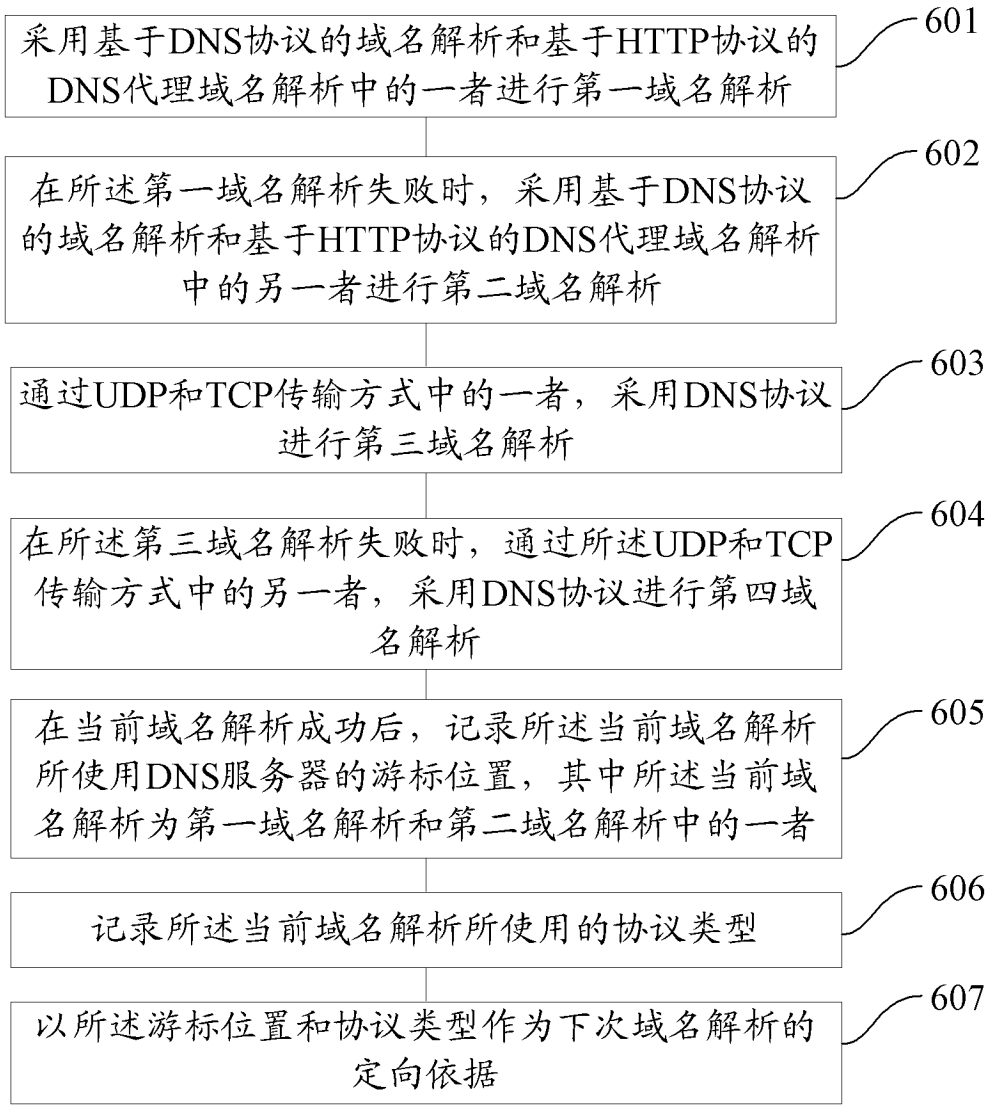

采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的一者进行第一域名解析
601
在所述第一域名解析失败时，采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的另一者进行第二域名解析
602
通过UDP和TCP传输方式中的一者，采用DNS协议进行第三域名解析
603
在所述第三域名解析失败时，通过所述UDP和TCP传输方式中的另一者，采用DNS协议进行第四域名解析
604
在当前域名解析成功后，记录所述当前域名解析所使用DNS服务器的游标位置，其中所述当前域名解析为第一域名解析和第二域名解析中的一者
605
记录所述当前域名解析所使用的协议类型
606
以所述游标位置和协议类型作为下次域名解析的定向依据
607

图 6

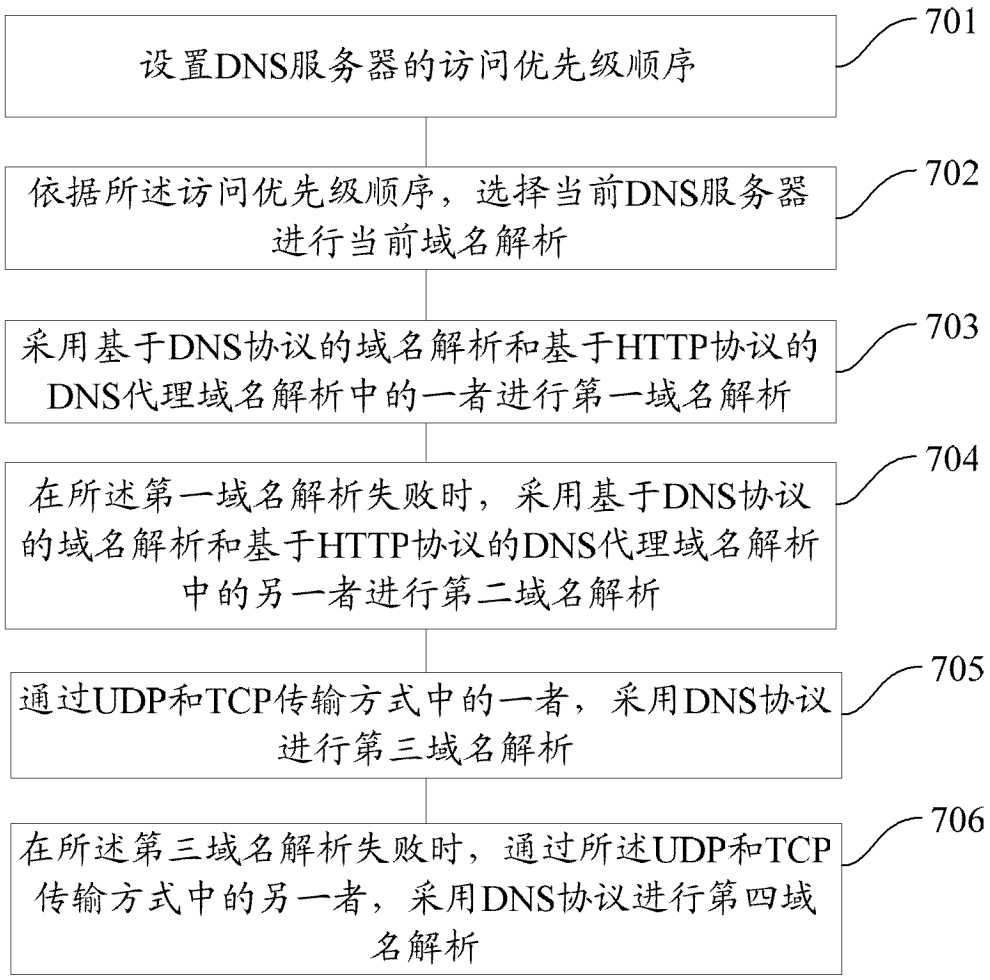

设置DNS服务器的访问优先级顺序
701
依据所述访问优先级顺序，选择当前DNS服务器进行当前域名解析
702
采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的一者进行第一域名解析
703
在所述第一域名解析失败时，采用基于DNS协议的域名解析和基于HTTP协议的DNS代理域名解析中的另一者进行第二域名解析
704
通过UDP和TCP传输方式中的一者，采用DNS协议进行第三域名解析
705
在所述第三域名解析失败时，通过所述UDP和TCP传输方式中的另一者，采用DNS协议进行第四域名解析
706

图 7

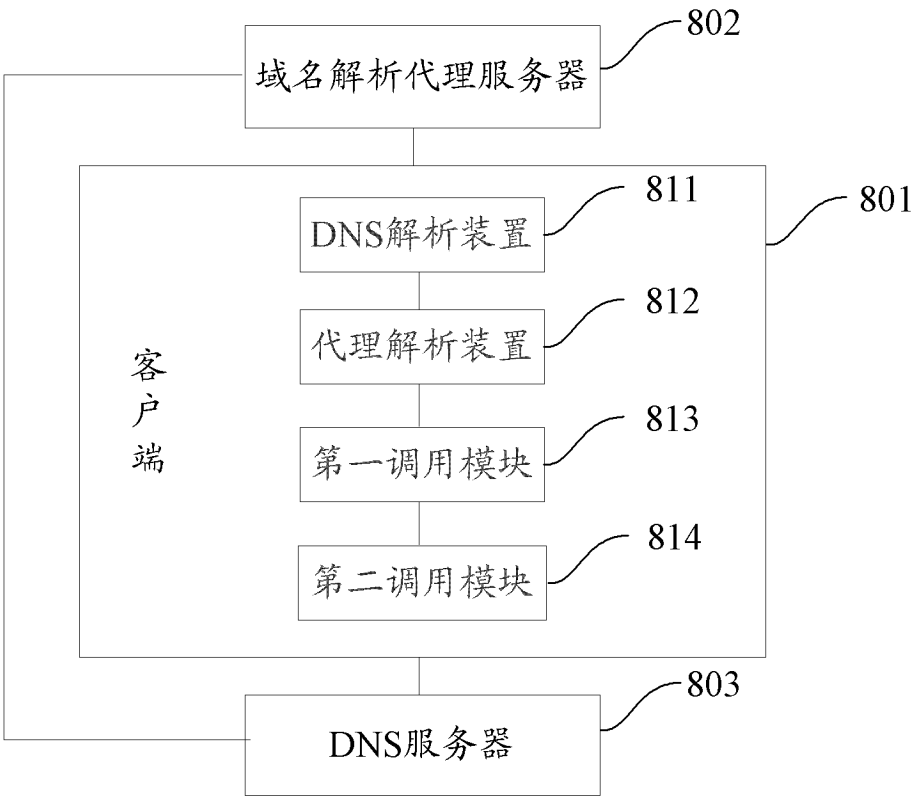

802
域名解析代理服务器
801
811
DNS解析装置
812
代理解析装置
客户端
813
第一调用模块
814
第二调用模块
803
DNS服务器

图 8

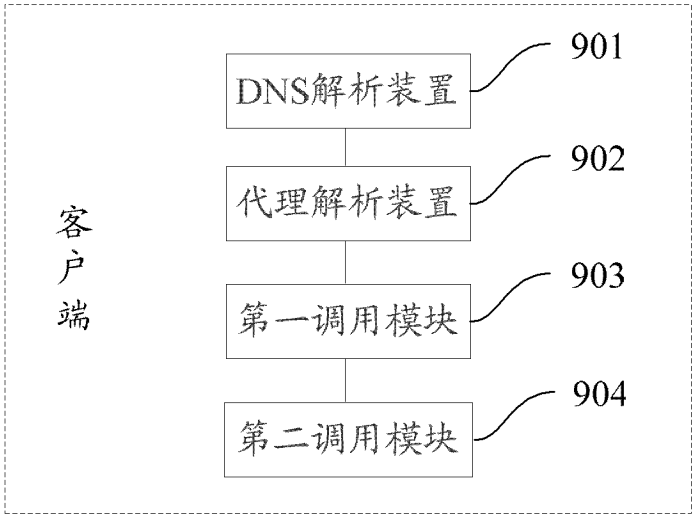

901
DNS解析装置
902
代理解析装置
客户端
903
第一调用模块
904
第二调用模块

图 9