(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101888370 B
(45)授权公告日 2013.01.09

(21)申请号 200910107259.5

(22)申请日 2009.05.11

(73)专利权人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法律部

(72)发明人 秦超 袁立权

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 101426002 A,2009.05.06, 全文.
CN 101282338 A,2008.10.08, 全文.
CN 1794661 A,2006.06.28, 全文.
CN 101374159 A,2009.02.25, 全文.

审查员 李昌林

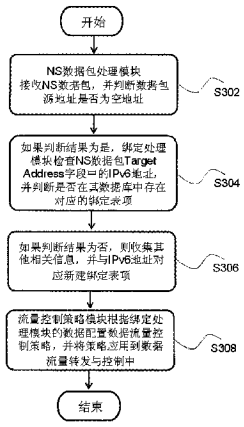
权利要求书 1 页 说明书 4 页 附图 4 页

(54)发明名称

防止 IPv6 地址被欺骗性攻击的装置与方法

(57)摘要

本发明公开了一种防止 IPv6 地址被欺骗性攻击的装置与方法，该方法包括：探测 NS 数据包；判断数据包源地址是否为空地址；如果判断结果为是，则检查 Target Address 字段中的 IPv6 地址，判断是否存在相应的绑定表项；如果判断结果为否，则收集相关信息与 IPv6 地址对应建立绑定表项；依据绑定表项数据制定数据流量的转发与控制策略，并将策略应用于数据流量的转发与控制中。本发明解决了基于各种地址分配机制进行地址分配的 IPv6 网络中所面临的地址被欺骗性攻击问题。



CN 101888370 B

1. 一种防止 IPv6 地址被欺骗性攻击的装置，其特征在于，所述装置包括：

邻居请求 NS 数据包处理模块，用于检查 NS 数据包源地址；

绑定处理模块，用于检查所述NS数据包目标地址Target Address字段中的IPv6地址，并判断是否在其数据库中存在对应的绑定表项；

流量控制策略模块，用于根据所述绑定处理模块的数据配置数据流量控制策略，并将所述策略应用到数据流量转发与控制中；

其中，所述 NS 数据包处理模块接收所述 NS 数据包并对所述 NS 数据包的源地址进行判断，如果源地址为空地址则把数据包发送给绑定处理模块处理；否则忽略所述 NS 数据包。

2. 根据权利要求 1 所述的装置，其特征在于，所述装置还包括地址有效性检查模块，用于在所述 NS 数据包处理模块判断数据包源地址为空地址之后，检查 Target Address 字段中 IPv6 地址的有效性。

3. 根据权利要求 2 所述的装置，其特征在于，所述地址有效性检查模块若判断所述 IPv6 地址有效，则将所述 NS 数据包发送给所述绑定处理模块；否则忽略所述 NS 数据包。

4. 根据权利要求 1 所述的装置，其特征在于，所述绑定处理模块若判断其数据库中不存在对应的绑定表项，则新建绑定表项；否则忽略所述 NS 数据包。

5. 一种防止 IPv6 地址被欺骗性攻击的方法，其特征在于，所述方法包括：

NS 数据包处理模块接收由节点 Node 发送的 NS 数据包，检查所述 NS 数据包的源地址字段，并判断所述源地址是否为空地址，如果判断结果为是，则把所述 NS 数据包发送给绑定处理模块处理；

所述绑定处理模块检查所述 NS 数据包 Target Address 字段中的 IPv6 地址，并判断是否在其数据库中存在对应的绑定表项，如果判断结果为否，则收集其它相关信息，并与 IPv6 地址对应新建绑定表项；

流量控制策略模块根据所述绑定处理模块的数据配置数据流量控制策略，并将所述策略应用到数据流量转发与控制中。

6. 根据权利要求 5 所述的方法，其特征在于，所述方法还包括，所述 NS 数据包处理模块判断所述源地址为空地址之后，进行地址有效性检查。

7. 根据权利要求 6 所述的方法，其特征在于，所述 NS 数据包处理模块判断 Target Address 字段中 IPv6 地址有效，则把所述 NS 数据包发送给所述绑定处理模块；否则忽略所述 NS 数据包。

8. 根据权利要求 5 所述的方法，其特征在于，所述方法还包括，若所述 NS 数据包处理模块判断所述 NS 数据包的源地址字段不为空，则忽略所述 NS 数据包。

9. 根据权利要求 5 所述的方法，其特征在于，所述方法还包括，若所述绑定处理模块判断在其数据库中存在对应的绑定表项，则忽略所述 NS 数据包。

防止 IPv6 地址被欺骗性攻击的装置与方法

技术领域

[0001] 本发明涉及网络通信安全领域，具体而言，是一种用来实现IPv6(InternetProtocol version 6) 网络中防止地址被欺骗性攻击的装置与方法。

背景技术

[0002] Internet 的高速发展与规模的急剧扩大，使现有的 IPv4(Internet Protocolversion 4) 在扩展性上面临很多问题，例如地址空间严重不足、正逐渐面临枯竭等，亟待解决。于是，一些延缓地址消耗的短期方案正在被实施，同时一些长期的解决方案如 IPv6 技术也在逐步被开发。

[0003] 随着 IPv6 网络的逐步部署和商用，在一些领域和应用场景中，例如宽带接入网络、数据骨干网络以及电信业务承载网等，IPv6 也暴露出许多与 IPv4 类似的安全问题。地址易被欺骗性攻击就是常见安全问题之一。

[0004] 目前，用于实现 IPv6 网络中防止地址被欺骗性攻击的方法主要是基于 DHCP Snooping（动态主机配置协议探听）的 IP Source Guard(IP 源地址防护）。接入设备，如交换机、Access Point、DSLAM（数字用户线路接入复用器）等，通过侦听 DHCP 报文，从而建立 DHCP Snooping绑定表，其中包含用户的MAC地址、IP地址、租用期、VLAN-ID（虚拟局域网标识）、端口等信息，以此进行源地址防护。上述现有的源地址防护方法，只能用在基于 DHCP 方式进行地址分配的 IPv6 网络中。而针对其它基于 StatelessAuto-configuration（无状态的自动配置）或者基于静态配置等方式进行地址分配的 IPv6 网络，尚无有效的解决方案。

发明内容

[0005] 针对基于 DHCP、Stateless Auto-configuration 或静态配置等方式进行地址分配的 IPv6 网络中所面临的地址被欺骗性攻击的问题，本发明提供了一种普遍适用的防止 IPv6 地址被欺骗性攻击的装置以及方法。

[0006] 根据本发明的防止 IPv6 地址被欺骗性攻击的装置包括：

[0007] 邻居请求 (NS) 数据包处理模块、绑定处理模块和流量控制策略模块。

[0008] 其中，NS 数据包处理模块用于处理 NS 数据包的接收并对 NS 数据包的源地址进行判断，如果源地址为空地址 (unspecified address) 则把数据包发送给绑定处理模块处理；否则忽略此 NS 数据包。

[0009] 绑定处理模块用于检查 NS 数据包 Target Address（目标地址）字段中的 IPv6 地址，并判断是否在其数据库中存在对应的绑定表项，如果判断结果为否，则收集其它相关信息与 IPv6 地址对应新建绑定表项；否则忽略此 NS 数据包。

[0010] 流量控制策略模块用于根据绑定处理模块的数据配置数据流量控制策略，并将策略应用到数据流量转发与控制中。

[0011] 进一步，上述装置还包括：地址有效性检查模块，用于在 NS 数据包处理模块判断

数据包源地址为空地址之后，检查 Target Address 字段中的 IPv6 地址，并判断此 IPv6 地址是否有效，若判断所述 IPv6 地址有效，则将 NS 数据包发送给绑定处理模块；否则忽略此 NS 数据包。其功能可根据具体的实施打开或关闭。

[0012] 为了实现上述目的，根据本发明的另一个方面，提供了一种防止 IPv6 地址被欺骗性攻击的方法。

[0013] 根据本发明的防止 IPv6 地址被欺骗性攻击的方法包括：

[0014] NS 数据包处理模块接收由 Node（节点）发送的 NS 数据包，检查 NS 数据包的源地址字段，并判断源地址是否为空地址，如果判断结果为是，则把 NS 数据包发送给绑定处理模块处理；否则忽略此 NS 数据包。

[0015] 绑定处理模块读取 NS 数据包 Target Address 字段中的 IPv6 地址，并判断是否在其数据库中存在对应的绑定表项，如果判断结果为否，则收集其它相关信息，并与 IPv6 地址对应新建绑定表项；如果判断结果为是，忽略此 NS 数据包。

[0016] 流量控制策略模块根据绑定处理模块的数据配置数据流量控制策略，并将策略应用到数据流量转发与控制；

[0017] 进一步地，在 NS 数据包处理模块判断数据包源地址为空地址之后，如果地址有效性检查功能被打开，上述方法还包括：地址有效性检查模块检查 NS 数据包 Target Address 字段中的 IPv6 地址，并判断此 IPv6 地址是否有效。如果判断结果为是，则把 NS 数据包发送给绑定处理模块处理；如果判断结果为否，则忽略此 NS 数据包；

[0018] 通过本发明，采用探测 NS 数据包来建立相应的绑定表项，并以此制定数据流量的转发与控制策略，解决了基于 DHCP、Stateless Auto-configuration 或静态配置等方式进行地址分配的 IPv6 网络中所面临的地址被欺骗性攻击问题，进而保障了 IPv6 网络通信的安全。

附图说明

[0019] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0020] 图 1：防止 IPv6 地址被欺骗性攻击装置的结构框图；

[0021] 图 2：地址有效性检查功能打开后的防止 IPv6 地址被欺骗性攻击装置的结构框图

[0022] 图 3：防止 IPv6 地址被欺骗性攻击方法的流程图；

[0023] 图 4：防止 IPv6 地址被欺骗性攻击方法的详细流程图；

具体实施方式

[0024] 功能概述

[0025] 考虑到现有的基于 DHCP Snooping IP Source Guard 源地址防护方法，只能用在基于 DHCP 方式进行地址分配的 IPv6 网络中，本发明实施例提供了一种普遍适用的防止 IPv6 地址被欺骗性攻击的方案。本方法通过采用探测 NS 数据包来建立相应的绑定表项，并以此制定数据流量的转发与控制策略，完善了 IPv6 网络的安全防护功能。

[0026] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本发明。

[0027] 装置实施例

[0028] 根据本发明的实施例，提供了一种防止 IPv6 地址被欺骗性攻击的装置，可以用于实现上述防止 IPv6 地址被欺骗性攻击的方法。图 1 是根据本发明实施例的防止 IPv6 地址被欺骗性攻击装置的结构框图，如图 1 所示，该装置包括：NS 数据包处理模块 2、绑定处理模块 4、流量控制策略模块 6，下面对上述结构进行详细描述。

[0029] NS 数据包处理模块 2，用于接收 NS 数据包并判断 NS 数据包的源地址是否为空地址，若不为空则忽略此 NS 数据包；绑定处理模块 4，连接至 NS 数据包处理模块 2，用于在所述 NS 数据包处理模块判断数据包源地址为空地址的情况下，检查 Target Address 字段中的 IPv6 地址，并判断是否在其数据库中存在对应的绑定表项，如果判断结果为否，则收集其它相关信息，并与 IPv6 地址对应新建绑定表项，若为是则忽略此 NS 数据包；流量控制策略模块 6，连接至绑定处理模块 4，用于根据绑定处理模块的数据配置数据流量控制策略，并将策略应用到数据流量转发与控制中。

[0030] 进一步，图 2 是根据本发明实施例的，地址有效性检查功能打开后的防止 IPv6 地址被欺骗性攻击装置的结构框图，如图 2 所示，该装置包括：NS 数据包处理模块 2、地址有效性检查模块 22、绑定处理模块 4、流量控制策略模块 6，下面对上述结构进行描述。

[0031] NS 数据包处理模块 2，用于接收 NS 数据包并判断 NS 数据包的源地址是否为空地址，若不为空则忽略此 NS 数据包；地址有效性检查模块 22，连接至 NS 数据包处理模块 2，用于在所述 NS 数据包处理模块判断数据包源地址为空地址的情况下，判断 Target Address 字段中的 IPv6 地址是否有效，若无效则忽略此 NS 数据包；绑定处理模块 4，连接至地址有效性检查模块 22，用于在所述地址有效性检查模块 22 的判断结果为是的情况下，检查 Target Address 字段中的 IPv6 地址并判断是否在其数据库中存在对应的绑定表项，如果判断结果为否，则收集其他相关信息，并与 IPv6 地址对应新建绑定表项，若为是则忽略此 NS 数据包；流量控制策略模块 6，连接至绑定处理模块 4，用于根据绑定处理模块的数据配置数据流量控制策略，并将策略应用到数据流量转发与控制中。

[0032] 方法实施例

[0033] 根据本发明的实施例，还提供了一种防止 IPv6 地址被欺骗性攻击的方法，图 3 是根据本发明实施例的防止 IPv6 地址被欺骗性攻击方法的流程图，如图 3 所示，该方法包括如下的步骤 S302 至步骤 S308：

[0034] 步骤 S302，NS 数据包处理模块接收 NS 数据包，并判断数据包源地址是否为空地址；

[0035] 步骤 S304，如果判断结果为是，绑定处理模块检查 NS 数据包 TargetAddress 字段中的 IPv6 地址，并判断是否在其数据库中存在对应的绑定表项；

[0036] 步骤 S306，如果判断结果为否，则收集其它相关信息，并与 IPv6 地址对应新建绑定表项；

[0037] 步骤 S308，流量控制策略模块根据绑定处理模块的数据配置数据流量控制策略，并将策略应用到数据流量转发与控制。

[0038] 需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0039] 下面对本发明实施例的实现过程进行详细描述。

[0040] 图 4 是根据本发明实施例的防止 IPv6 地址被欺骗性攻击方法的详细流程图，如图 4 所示，该流程包括如下的步骤 402 至步骤 422 ：

[0041] 步骤 402 ：NS 数据包处理模块接收由 Node（节点）发送的 NS 数据包 ；

[0042] 步骤 404 ：NS 数据包处理模块检查并判断 NS 数据包的源地址字段是否为空地址，如果判断结果为是，则进入步骤 406，否则转至步骤 422 ；

[0043] 步骤 406 ：判断是否需要进行地址有效性检查，如果判断结果为是，则进入步骤 408 ；否则，转至步骤 412 ；

[0044] 步骤 408 ：NS 数据包处理模块将 NS 数据包发送给地址有效性检查模块 ；

[0045] 步骤 410 ：地址有效性检查模块检查 Target Address 字段中的 IPv6 地址，判断此地址是否有效，如果判断结果为是，则进入步骤 412 ；否则，转至步骤 422 ；

[0046] 步骤 412 ：将 NS 数据包发送给绑定处理模块 ；

[0047] 步骤 414 ：绑定处理模块检查 Target Address 字段中的 IPv6 地址，并判断其数据库中是否存在有相应的表项，如果判断结果为否，则进入步骤 416 ；否则转至步骤 422 ；

[0048] 步骤 416 ：绑定处理模块收集其他相关信息，包括但不限于 ：源 MAC 地址、VLAN-ID、端口号等，并与 IPv6 地址对应新建绑定表项 ；

[0049] 步骤 418 ：绑定处理模块通知流量策略控制模块做配置修改，配置修改可以是新建、更改或删除等操作 ；

[0050] 步骤 420 ：流量策略控制模块修改流量控制策略，并将修改后的策略应用到流量转发与控制中，流程结束 ；

[0051] 步骤 422 ：忽略此 NS 数据包，流程结束 ；

[0052] 综上所述，通过本发明的上述实施例，提供了一种功能独立、普适性高的防止 IPv6 地址被欺骗性攻击的装置与方法，用于解决基于各种地址分配机制进行地址分配的 IPv6 网络中所面临的地址被欺骗性攻击，从而增强了 IPv6 网络设计和部署的灵活性，保障了网络中数据通信的安全。

[0053] 显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0054] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

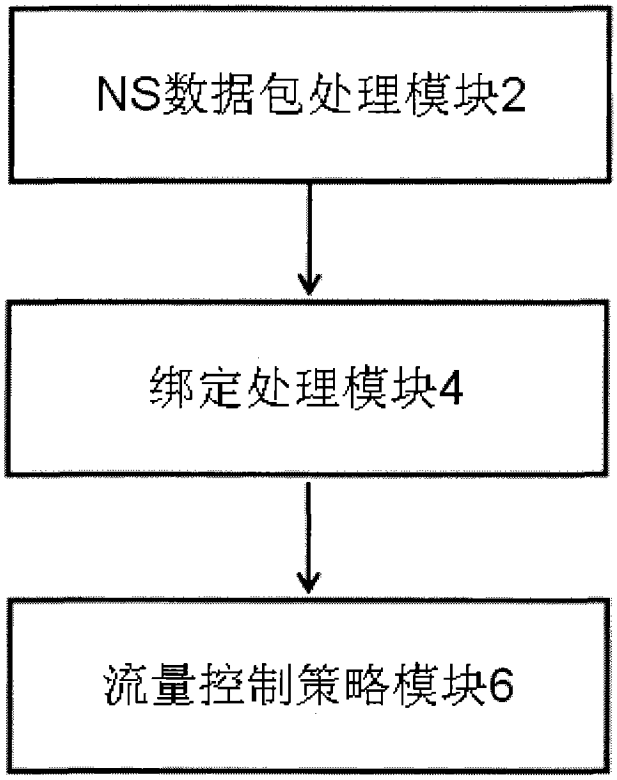


图 1

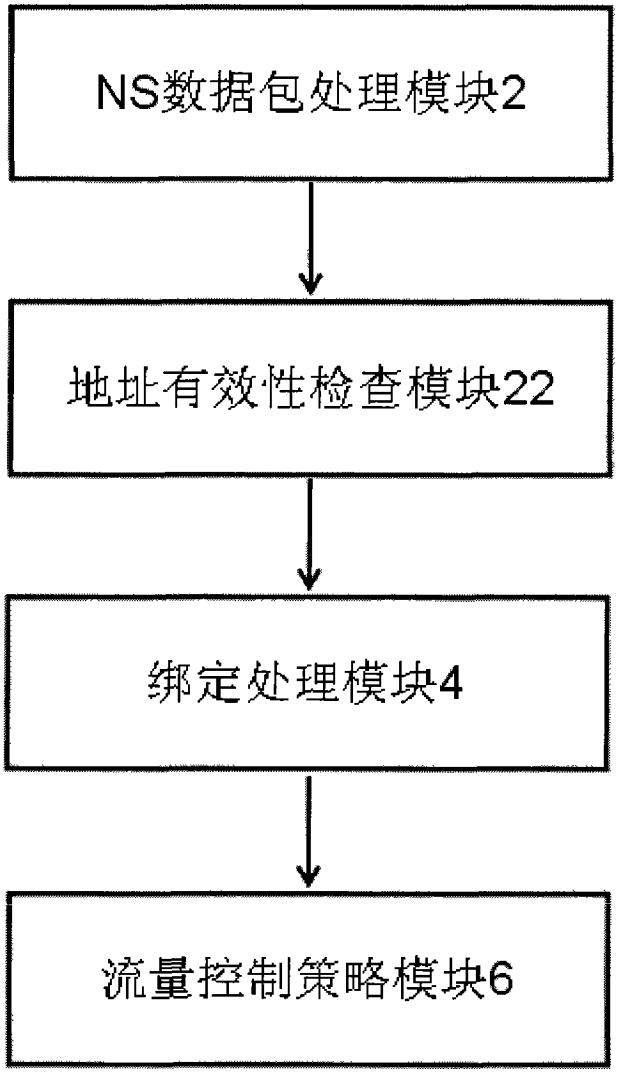


图 2

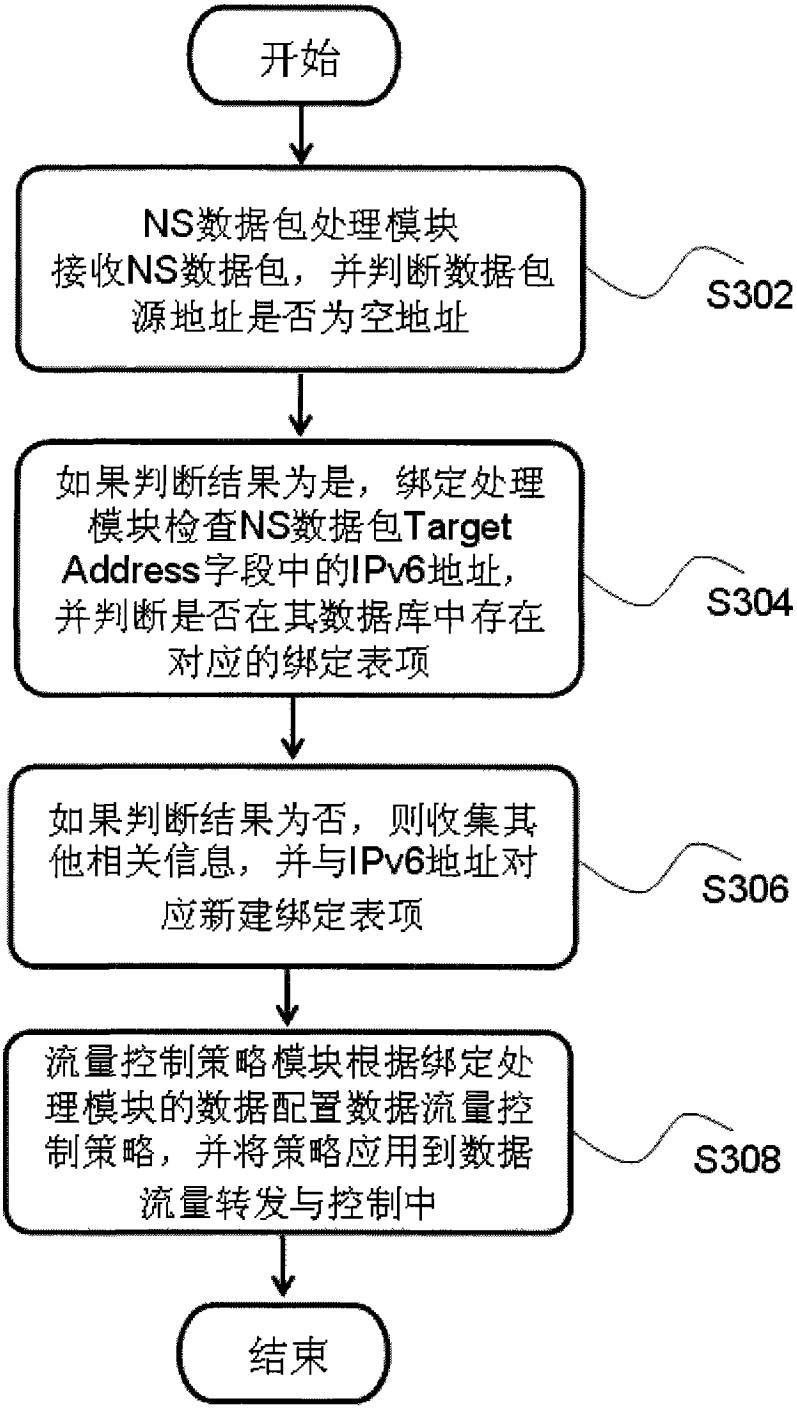

开始
NS数据包处理模块接收NS数据包，并判断数据包源地址是否为空地址
S302
如果判断结果为是，绑定处理模块检查NS数据包Target Address字段中的IPv6地址，并判断是否在其数据库中存在对应的绑定表项
S304
如果判断结果为否，则收集其他相关信息，并与IPv6地址对应新建绑定表项
S306
流量控制策略模块根据绑定处理模块的数据配置数据流量控制策略，并将策略应用到数据流量转发与控制中
S308
结束

图 3

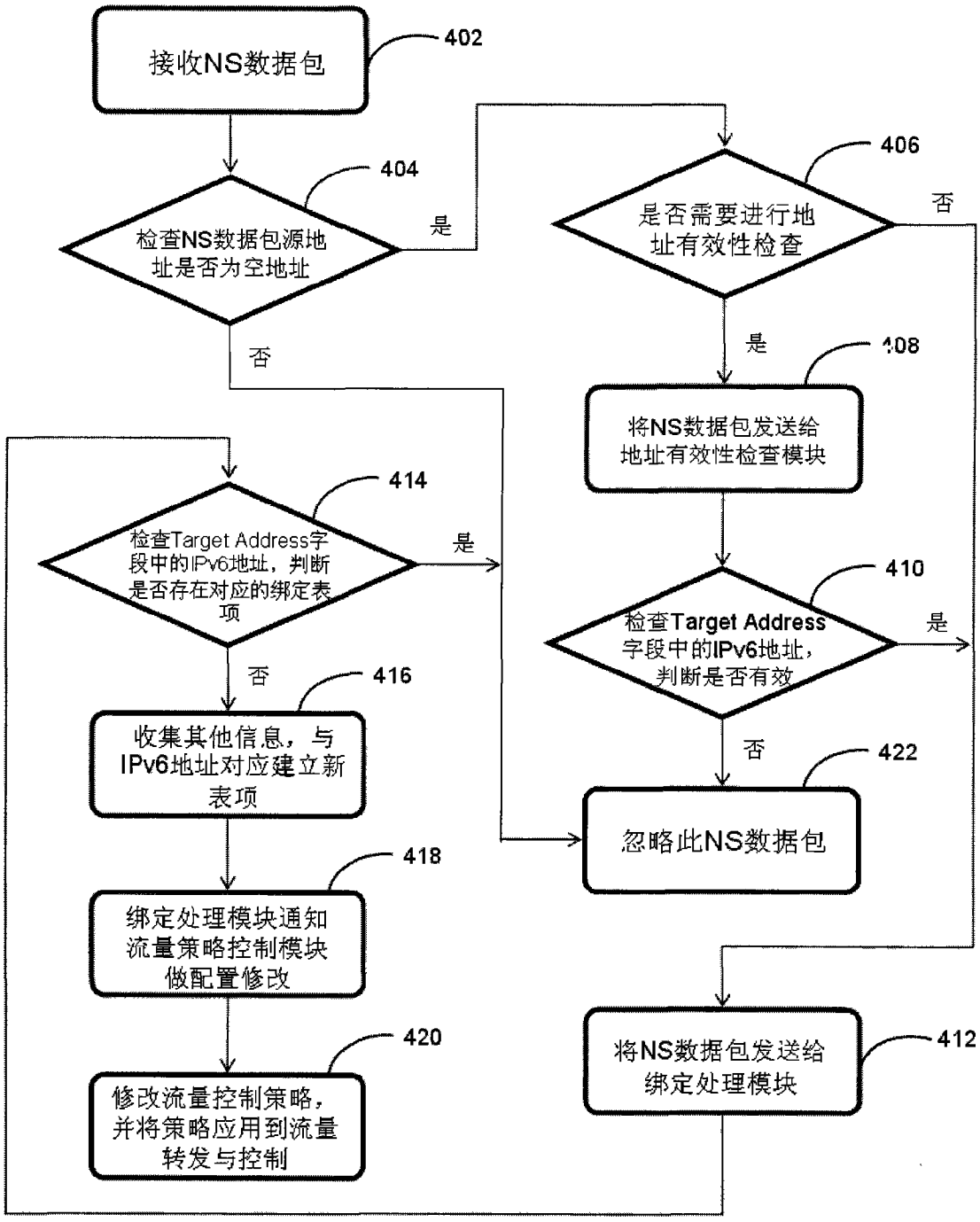

接收NS数据包
402
检查NS数据包源地址是否为空地址
404
是
否
是否需要进行地址有效性检查
406
否
是
将NS数据包发送给地址有效性检查模块
408
检查Target Address字段中的IPv6地址，判断是否存在对应的绑定表项
414
是
否
检查Target Address字段中的IPv6地址，判断是否有效
410
是
否
收集其他信息，与IPv6地址对应建立新表项
416
忽略此NS数据包
422
绑定处理模块通知流量策略控制模块做配置修改
418
修改流量控制策略，并将策略应用到流量转发与控制
420
将NS数据包发送给绑定处理模块
412

图 4