(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 107547510 B
(45)授权公告日 2020.03.06

(21)申请号 201710536608.X

(22)申请日 2017.07.04

(65)同一申请的已公布的文献号
申请公布号 CN 107547510 A

(43)申请公布日 2018.01.05

(73)专利权人 新华三技术有限公司
地址 310052 浙江省杭州市滨江区长河路466号

(72)发明人 罗琳

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/741(2013.01)
H04L 12/721(2013.01)

(56)对比文件
CN 101222513 A,2008.07.16,
CN 104394243 A,2015.03.04,
CN 102186261 A,2011.09.14,
US 2008031189 A1,2008.02.07,
CN 101552783 A,2009.10.07,
IETF.“RFC 6620-FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses”.《https://tools.ietf.org/pdf/rfc6620.pdf》.2012,

审查员 张洁

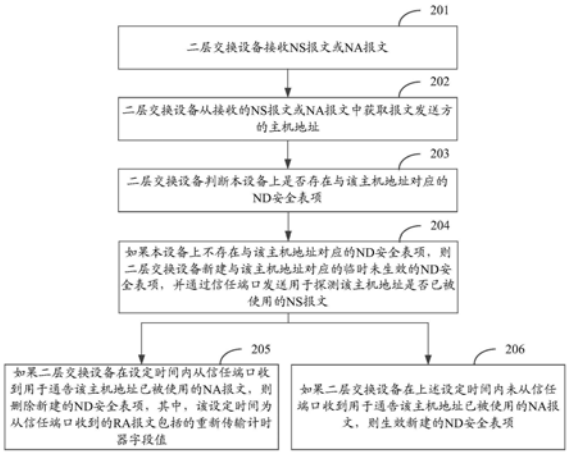
权利要求书3页 说明书9页 附图3页

(54)发明名称

一种邻居发现协议安全表项处理方法和装置

(57)摘要

本申请提供一种邻居发现协议ND安全表项处理方法，应用于二层交换设备，其通过信任端口连接路由器网关、通过验证端口连接主机，方法为：接收NS报文或NA报文；从报文中获取报文发送方的主机地址；如果本设备上不存在与该主机地址对应的ND安全表项，则新建与该主机地址对应的临时未生效的ND安全表项，通过信任端口发送探测该主机地址是否已被使用的NS报文；若在设定时间内从信任端口收到通告该主机地址已被使用的NA报文则删除新建的ND安全表项；若在设定时间内未从信任端口收到NA报文则生效该ND安全表项；设定时间为从信任端口收到的RA报文包括的重新传输计时器字段值。该方法使得ND安全内表项的表项探测时长可动态调整。



CN 107547510 B

1.一种邻居发现协议安全表项处理方法,其特征在于,所述方法应用于二层交换设备,所述二层交换设备通过信任端口连接路由器网关、通过验证端口连接主机,所述方法包括:

接收邻居请求NS报文或邻居通告NA报文;

从所述NS报文或NA报文中获取报文发送方的主机地址;

如果本设备上不存在与所述主机地址对应的邻居发现协议ND安全表项,则

新建与所述主机地址对应的临时未生效的ND安全表项,并通过信任端口发送用于探测所述主机地址是否已被使用的NS报文;如果在设定时间内从信任端口收到用于通告所述主机地址已被使用的NA报文,则删除新建的ND安全表项;如果在设定时间内未从信任端口收到用于通告所述主机地址已被使用的NA报文,则生效新建的ND安全表项;

其中,所述设定时间为从信任端口收到的路由通告RA报文包括的重新传输计时器字段值,用于通告NS报文的重传时间。

2.如权利要求1所述的方法,其特征在于,本设备上存在与所述主机地址对应的ND安全表项且该ND安全表项的状态为无效;所述方法还包括:

如果所述NS报文或NA报文从本设备的验证端口收到,则根据所述NS报文或NA报文的媒体接入控制MAC地址和入端口更新该ND安全表项的内容;

如果所述NS报文或NA报文从本设备的信任端口收到,则删除该ND安全表项。

3.如权利要求1所述的方法,其特征在于,本设备上存在与所述主机地址对应的ND安全表项且该ND安全表项的状态为有效;所述方法还包括:

如果该ND安全表项记录的MAC地址和入端口与所述NS报文或NA报文的MAC地址和入端口一致,则更新该ND安全表项的老化时间;

如果该ND安全表项记录的MAC地址和入端口与所述NS报文或NA报文的MAC地址和入端口不一致,则通过该ND安全表项记录的入端口发送用于探测所述主机地址是否仍被使用的NS报文;当在所述设定时间内从该ND安全表项记录的入端口收到用于通告所述主机地址仍被使用的NA报文时,保持该ND安全表项的内容不变,并更新该ND安全表项的老化时间;当在所述设定时间内未从该ND安全表项记录的入端口收到用于通告所述主机地址仍被使用的NA报文时,根据所述NS报文或NA报文的MAC地址和入端口更新该ND安全表项的内容,并更新该ND安全表项的老化时间。

4.如权利要求1所述的方法,其特征在于,在生效新建的ND安全表项后,所述方法还包括:

为生效的ND安全表项设置老化时间,所述老化时间为从信任端口收到的RA报文包括的可达时间字段值与一随机时间的和值;

当生效的ND安全表项到达所述老化时间时,通过该ND安全表项记录的入端口发送用于探测所述主机地址是否仍被使用的NS报文;如果在所述设定时间内从该ND安全表项记录的入端口收到用于通告所述主机地址仍被使用的NA报文,则更新该ND安全表项的老化时间,如果在所述设定时间内未从该ND安全表项记录的入端口收到用于通告所述主机地址仍被使用的NA报文,则删除该ND安全表项。

5.如权利要求1所述的方法,其特征在于,所述从所述NS报文或NA报文中获取报文发送方对应的主机地址,包括:

对于重复地址检测DAD NS报文,从该报文的内容中获取报文发送方的主机地址;

对于非DAD NS报文或NA报文，从该报文的源地址字段中获取报文发送方的主机地址。

6.一种邻居发现协议安全表项处理装置，其特征在于，所述装置应用于二层交换设备，所述二层交换设备通过信任端口连接路由器网关、通过验证端口连接主机，所述装置包括：

接收单元，用于接收邻居请求NS报文或邻居通告NA报文；

主机地址获取单元，用于从所述NS报文或NA报文中获取报文发送方的主机地址；

邻居发现协议ND安全表项处理单元，用于在本设备上不存在与所述主机地址对应的ND安全表项时，新建与所述主机地址对应的临时未生效的ND安全表项，并通过信任端口发送用于探测所述主机地址是否已被使用的NS报文；如果在设定时间内所述接收单元从信任端口收到用于通告所述主机地址已被使用的NA报文，则删除新建的ND安全表项；如果在设定时间内所述接收单元未从信任端口收到用于通告所述主机地址已被使用的NA报文，则生效新建的ND安全表项；其中，所述设定时间为从信任端口收到的路由通告RA报文包括的重新传输计时器字段值，用于通告NS报文的重传时间。

7.如权利要求6所述的装置，其特征在于，本设备上存在与所述主机地址对应的ND安全表项且该ND安全表项的状态为无效；

所述ND安全表项处理单元，还用于如果所述NS报文或NA报文从本设备的验证端口收到，则根据所述NS报文或NA报文的媒体接入控制MAC地址和入端口更新该ND安全表项的内容；如果所述NS报文或NA报文从本设备的信任端口收到，则删除该ND安全表项。

8.如权利要求6所述的装置，其特征在于，本设备上存在与所述主机地址对应的ND安全表项且该ND安全表项的状态为有效；

所述ND安全表项处理，还用于如果该ND安全表项记录的MAC地址和入端口与所述NS报文或NA报文的MAC地址和入端口一致，则更新该ND安全表项的老化时间；如果该ND安全表项记录的MAC地址和入端口与所述NS报文或NA报文的MAC地址和入端口不一致，则通过该ND安全表项记录的入端口发送用于探测所述主机地址是否仍被使用的NS报文；当在所述设定时间内从该ND安全表项记录的入端口所述接收单元收到用于通告所述主机地址仍被使用的NA报文时，保持该ND安全表项的内容不变，并更新该ND安全表项的老化时间；当在所述设定时间内所述接收单元未从该ND安全表项记录的入端口收到用于通告所述主机地址仍被使用的NA报文时，根据所述NS报文或NA报文的MAC地址和入端口更新该ND安全表项的内容，并更新该ND安全表项的老化时间。

9.如权利要求6所述的装置，其特征在于，在生效新建的ND安全表项后，所述ND安全表项处理单元，还用于：

为生效的ND安全表项设置老化时间，所述老化时间为从信任端口收到的RA报文包括的可达时间字段值与一随机时间的和值；

当生效的ND安全表项到达所述老化时间时，通过该ND安全表项记录的入端口发送用于探测所述主机地址是否仍被使用的NS报文；如果在所述设定时间内所述接收单元从该ND安全表项记录的入端口收到用于通告所述主机地址仍被使用的NA报文，则更新该ND安全表项的老化时间，如果在所述设定时间内所述接收单元未从该ND安全表项记录的入端口收到用于通告所述主机地址仍被使用的NA报文，则删除该ND安全表项。

10.如权利要求6所述的装置，其特征在于，所述主机地址获取单元具体用于：

对于重复地址检测DAD NS报文，从该报文的内容中获取报文发送方的主机地址；

对于非DAD NS报文或NA报文，从该报文的源地址字段中获取报文发送方的主机地址。

一种邻居发现协议安全表项处理方法和装置

技术领域

[0001] 本申请涉及通信技术领域，尤其涉及一种ND(Neighbor Discovery，邻居发现协议)安全表项处理方法和装置。

背景技术

[0002] RFC(request for comments，请求注解协议)6620定义描述了IPv6(Internet Protocol Version 6，互联网协议第6版)的源地址验证机制：在连接路由器网关和主机的二层交换设备上生成ND安全表项，用于验证到达二层交换设备的数据报文的合法性；如果数据报文的源地址未记录在ND安全表项中则该数据报文不合法会被丢弃，如果数据报文的源地址已记录在ND安全表项中则该数据报文合法会被正常转发。ND安全表项为数据报文的转发和丢弃提供了凭证，保证了源地址的有效性，可以防止非法报文的攻击。

发明内容

[0003] 有鉴于此，本申请提供一种ND安全表项处理方法和装置，用于动态调整 ND安全表项的表项探测时长，保证了在各类网络下的适应性。

[0004] 具体地，本申请是通过如下技术方案实现的：

[0005] 本申请第一方面，提供了一种ND安全表项处理方法，所述方法应用于二层交换设备，所述二层交换设备通过信任端口连接路由器网关、通过验证端口连接主机，所述方法包括：

[0006] 接收NS报文或NA报文；

[0007] 从所述NS报文或NA报文中获取报文发送方的主机地址；

[0008] 如果本设备上不存在与所述主机地址对应的ND安全表项，则

[0009] 新建与所述主机地址对应的临时未生效的ND安全表项，并通过信任端口发送用于探测所述主机地址是否已被使用的NS报文；如果在设定时间内从信任端口收到用于通告所述主机地址已被使用的NA报文，则删除新建的ND安全表项；如果在设定时间内未从信任端口收到用于通告所述主机地址已被使用的NA 报文，则生效新建的ND安全表项；其中，所述设定时间为从信任端口收到的 RA报文包括的重新传输计时器字段值。

[0010] 本申请第二方面，提供了一种ND安全表项处理装置，所述装置可以应用于二层交换设备，所述二层交换设备通过信任端口连接路由器网关、通过验证端口连接主机，所述二层交换设备具有实现上述方法的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块或单元。

[0011] 一种可能的实现方式中，所述装置包括：

[0012] 接收单元，用于接收NS报文或NA报文；

[0013] 主机地址获取单元，用于从所述NS报文或NA报文中获取报文发送方的主机地址；

[0014] ND安全表项处理单元，用于在本设备上不存在与所述主机地址对应的ND 安全表项时，新建与所述主机地址对应的临时未生效的ND安全表项，并通过信任端口发送用于探

测所述主机地址是否已被使用的NS报文;如果在设定时间内所述接收单元从信任端口收到用于通告所述主机地址已被使用的NA报文,则删除新建的ND安全表项;如果在设定时间内所述接收单元未从信任端口收到用于通告所述主机地址已被使用的NA报文,则生效新建的ND安全表项;其中,所述设定时间为从信任端口收到的RA报文包括的重新传输计时器字段值。

[0015] 另一种可能的实现方式中,所述装置包括通信接口、处理器、存储器和总线,所述通信接口、所述处理器和所述存储器之间通过总线相互连接;所述处理器通过读取所述存储器中存储的逻辑指令,执行本申请第一方面所述的ND 安全表项处理方法。

[0016] 本申请将RA报文中包括的重新传输计时器字段值,也即NS报文的重传时间,作为判断ND安全表项何时生效的表项探测时长;由于在不同网络中,NS报文的重传时间是不同的,这也使得在无状态配置网络中,二层交换设备生效ND安全内表项的时长可动态调整,解决了在不同网络环境中固定时间或人工配置时间无法匹配所有网络的时延的问题。

附图说明

[0017] 图1是RA报文的格式示意图;

[0018] 图2是本申请提供的方法流程图;

[0019] 图3是本申请提供的一个具体实施例的组网图;

[0020] 图4是本申请提供的装置功能模块框图;

[0021] 图5是本申请提供的图4所示装置的硬件架构图。

具体实施方式

[0022] 这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0023] 在本申请使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0024] 应当理解,尽管在本申请可能采用术语第一、第二、第三等来描述各种信息,但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如,在不脱离本申请范围的情况下,第一信息也可以被称为第二信息,类似地,第二信息也可以被称为第一信息。取决于语境,如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0025] 以下,首先对ND协议进行简单介绍。

[0026] ND协议使用的报文类型包括:

[0027] 1)RS(Router Solicitation,路由请求)报文,类型号为133,主机发送RS 报文用于向路由器网关发出请求,请求前缀和其它配置信息,用于主机的自动配置。

[0028] 2)RA(Router Advertisement,路由通告)报文,类型号为134,路由器网关周期地

发出RA报文,或因响应RS报文而发送RA报文。RA报文的格式如图1所示,这里仅介绍其中与本申请有关的部分字段:

[0029] 重新传输计时器(Retrans Timer):单位为毫秒,通告重传NS报文的间隔,一般用于地址解析和邻居不可达检测机制。

[0030] 可达时间(Reachable time):单位为毫秒,通告邻居可达时间,一般用于邻居不可达检测机制。

[0031] 3)NS(Neighbor Solicitation,邻居请求)报文,类型号为135,可用于地址解析,即请求目标节点的链路层地址,以节点(主机或路由器网关)A要获取节点B的链路层地址为例,此时NS报文的源地址为节点A的IPv6地址,目的地址为节点B的被请求节点组播地址;也可用于可达性检测,以节点A要验证节点B是否可达为例,此时NS报文的源地址为节点A的IPv6地址,目的地址为节点B的IPv6地址;也可用于DAD(Duplicate Address Detection,重复地址检测),确认该地址是否已被其它节点使用,此时NS报文的源地址为未指定地址“::”,目的地址为待检测的IPv6地址对应的被请求节点组播地址,报文内容中包含了待检测的IPv6地址。

[0032] 本申请中,有时会使用DAD NS报文来指代用于进行重复地址检测的NS 报文,使用非DAD NS报文来指代用于地址解析或可达性检测的NS报文。

[0033] 4)NA(Neighbor Advertisement,邻居通告)报文,类型号为136,用于对 NS报文进行响应,或者节点在链路层变化时也可以主动发送NA报文,向邻居节点通告本节点的变化信息。

[0034] 5)Redirect(重定向)报文,类型号为137,当满足一定的条件时,缺省网关通过向源主机发送重定向报文,使该源主机重新选择正确的下一跳地址进行后续报文的发送。

[0035] ND协议功能强大,但是协议本身没有安全机制,容易被攻击者利用。攻击者可以仿冒主机或路由器网关发送伪造的ND报文,对网络进行攻击,这可能会改写路由器网关或者主机上的邻居表项,导致被仿冒用户的报文错误的发送到攻击者的终端上。

[0036] 目前可以通过源地址验证机制来解决这一问题,即通过在连接路由器网关和主机的二层交换设备上生成ND安全表项,来验证数据报文的合法性。

[0037] 在无状态地址自动生成网络中,ND安全表项的建立流程如下:

[0038] 当二层交换设备从验证端口(即二层交换设备上连接主机的二层端口,也称非信任端口)收到未知源地址的ND报文或者数据报文时,可以新建一个临时未生效的ND安全表项,此时该ND安全表项处于无效状态;随后二层交换设备通过接收上述报文的接口所属VLAN内的信任端口(即二层交换设备上连接路由器网关的二层端口)发送两次间隔250ms的DAD NS报文进行探测,以确认上述报文的源地址是否与信任端口侧的设备地址冲突。如果二层交换设备在指定时间内(比如500ms)未收到NA报文,则说明地址不冲突,ND安全表项正式生效;反之,如果二层交换设备在指定时间内收到NA报文,则说明局域网中已存在冲突地址,ND安全表项不生效。

[0039] 在现有技术中,上述用来生效ND安全表项的指定时间(以下简称表项探测时长)一般为一固定时间或人工配置的一段时间,由于在不同网络中的时延不同,故DAD NS报文在网络中的传输时间也不同,固定或人工配置的表项探测时长无法匹配所有网络的时延。

[0040] 本申请提供一种ND安全表项的处理方案来解决目前所面临的困境。请参考图2,为

本申请提供的方法流程图，该方法可应用于二层交换设备，该二层交换设备通过信任端口连接路由器网关，通过验证端口连接主机。如图2所示，该流程可包括以下步骤：

[0041] 步骤201：二层交换设备接收NS报文或NA报文。

[0042] 步骤202：二层交换设备从接收的NS报文或NA报文中获取报文发送方的主机地址。

[0043] 其中，对于DAD NS报文，其源地址为未指定地址(一般用“::”表示)，目的地址为该DAD NS报文发送方的主机地址所对应的被请求节点组播地址，该DAD NS报文发送方的主机地址包含在报文内容中，因此二层交换设备在根据报文类型和报文源地址确定接收的报文为DAD NS报文时，可以从该报文的内容中获取到报文发送方的主机地址。

[0044] 对于非DAD NS报文或NA报文，其源地址为报文发送方的主机地址，目的地址为该报文发送方的邻居主机的主机地址，因此二层交换设备在根据报文类型和报文源地址确定接收的报文为非DAD NS报文或NA报文时，可以直接从该报文的源地址字段中获取到报文发送方的主机地址。

[0045] 步骤203：二层交换设备判断本设备上是否存在与该主机地址对应的ND安全表项。

[0046] ND安全表项记录了合法主机的信息，包括该合法主机的IP地址和MAC (Medium Access Control，媒体接入控制)地址，该合法主机所属的VLAN(Virtual Local Area Network，虚拟局域网)，以及该合法主机发送的报文在二层交换设备上的入端口。后续，只有IP地址、MAC地址、VLAN和入端口与ND安全表项完全匹配的数据报文，才可以被二层交换设备正常转发，否则将被丢弃。

[0047] 在步骤203中，二层交换设备可以根据报文发送方的IP地址和VLAN来查找对应的ND安全表项。

[0048] 步骤204：如果本设备上不存在与该主机地址对应的ND安全表项，则二层交换设备新建与该主机地址对应的临时未生效的ND安全表项，并通过信任端口发送用于探测该主机地址是否已被使用的NS报文。

[0049] 这里，用于探测该主机地址是否已被使用的NS报文，即是DAD NS报文。

[0050] 步骤205：如果二层交换设备在设定时间内从信任端口收到用于通告该主机地址已被使用的NA报文，则删除新建的ND安全表项，其中，该设定时间为从信任端口收到的RA报文包括的重新传输计时器字段值。

[0051] 在现有技术中，对于从信任端口收到的RA报文，二层交换设备会直接对该 RA报文进行广播；对于从验证端口收到的RA报文，二层交换设备会直接丢弃。

[0052] 而在本申请中，对于从验证端口收到的RA报文，二层交换设备也会直接丢弃；但对于从信任端口收到的RA报文，二层交换设备会解析该RA报文，从中获取通告给无状态主机的参数，包括报文的重新传输计时器字段值和可达时间字段值，其中可达时间字段值将在下文ND安全表项的老化方案中使用到，这里暂不详述。

[0053] 重新传输计时器字段值用于通告NS报文的重传时间，即主机在发出NS报文后隔多久重发一次NS报文。不同的网络有不同的NS报文重传时间，本申请将NS报文的重传时间作为ND安全表项的表项探测时长，可以使ND安全表项的表项探测时长能够适应各类网络的时延。

[0054] 步骤206：如果二层交换设备在上述设定时间内未从信任端口收到用于通告该主机地址已被使用的NA报文，则生效新建的ND安全表项。

[0055] 作为一个实施例,步骤203中二层交换设备在判断本设备上是否存在与该主机地址对应的ND安全表项时,其判断结果还可能是本设备上存在与该主机地址对应的ND安全表项,但该ND安全表项的状态为无效。这表示二层交换设备之前已经收到了相同IP地址和相同VLAN的主机发送的NS报文并新建了对应的ND安全表项,因还未从信任端口收到应答的NA报文或是还未到达NS报文的重传时间,故该ND安全表项还存在且处于无效状态。

[0056] 基于此,在一种情况下,如果该NS报文或NA报文是从本设备的验证端口收到,则当报文为NS报文时表示该主机地址对应的主机可能发生主机迁移,当该报文为NA报文时表示可能有其它主机在使用该主机地址,二层交换设备可以根据该NS报文或NA报文的MAC地址和入端口更新该ND安全表项的内容,即将该ND安全表项中记录的MAC地址字段和入端口字段更新为该NS报文或 NA报文的MAC地址值和入端口值。在另一种情况下,如果该NS报文或NA 报文是从本设备的信任端口收到,则表示已经有路由器网关或其它服务器占用了该主机地址,在信任端口侧的路由器网关或服务器占用了某主机地址的情况下,该主机地址将不再分配给验证端口侧的主机使用,故二层交换设备可以删除该ND安全表项。

[0057] 作为一个实施例,步骤203中二层交换设备在判断本设备上是否存在与该主机地址对应的ND安全表项时,其判断结果还可能是本设备上存在与所述主机地址对应的ND安全表项,且该ND安全表项的状态为有效。这表示二层交换设备之前已经收到了相同IP地址和相同VLAN的主机发送的NS报文并新建了对应的ND安全表项,并且因为在NS报文的重传时间内未收到应答的NA报文,该ND安全表项已经从临时未生效状态变为有效状态。

[0058] 基于此,在一种情况下,如果该ND安全表项记录的MAC地址和入端口与该NS报文或NA报文的MAC地址和入端口一致,则二层交换设备可以更新该 ND安全表项的老化时间,即刷新该ND安全表项的存活时间。在另一种情况下,如果该ND安全表项记录的MAC地址和入端口与该NS报文或NA报文的MAC 地址和入端口不一致,则二层交换设备可以通过该ND安全表项记录的入端口发送用于探测该主机地址是否仍被使用的NS报文。当在上述设定时间(即NS 报文的重传时间)内从该ND安全表项记录的入端口收到用于通告该主机地址仍被使用的NA报文时,二层交换设备可以保持该ND安全表项的内容(即ND 全表项中的IP地址字段、VLAN字段、MAC地址字段、入端口字段等)不变,并更新该ND安全表项的老化时间;当在上述设定时间内未从该ND安全表项记录的入端口收到用于通告该主机地址仍被使用的NA报文时,二层交换设备可以根据该NS报文或NA报文的MAC地址和入端口更新该ND安全表项的内容,并更新该ND安全表项的老化时间。

[0059] 通过图2所示的流程可以看出,本申请将RA报文中包括的重新传输计时器字段值,也即NS报文的重传时间,作为判断ND安全表项何时生效的表项探测时长;由于在不同网络中,NS报文的重传时间是不同的,这也使得在无状态配置网络中,二层交换设备生效ND安全内表项的时长可动态调整,解决了在不同网络环境中固定时间或人工配置时间无法匹配所有网络的时延的问题。

[0060] 现有技术中,为了防止已经关闭(或下线)的主机继续占用ND安全表项的规格,还要考虑ND安全表项的老化流程。

[0061] 目前,在无状态地址自动生成网络中,ND安全表项的老化流程如下:

[0062] 如果ND安全表项在有效状态超时时间内未收到ND更新报文(如NS报文、NA报文等),则进入无效状态;随后二层交换设备可以向ND安全表项对应的入端口发送两次DAD NS

报文进行探测。如果二层交换设备在ND安全表项的无效状态超时时间内未收到对应主机应答的NA报文，则说明原主机已经跟该入端口断开连接，二层交换设备可以删除对应的ND安全表项；如果二层交换设备在ND安全表项的无效状态超时时间内收到对应主机应答的NA报文，则说明原主机未跟该入端口断开，二层交换设备可以保留对应的ND安全表项，使该ND安全表项重新进入有效状态。

[0063] 本申请提出了一种新的ND安全表项老化方法，具体过程如下：

[0064] 1)在新建的ND安全表项生效后，为该生效的ND安全表项设置老化时间，该老化时间为从信任端口收到的RA报文所包括的可达时间字段值与一随机时间的和值。

[0065] 2)当该生效的ND安全表项到达上述老化时间时，通过该ND安全表项记录的入端口发送用于探测该主机地址是否仍被使用的NS报文。如果在设定时间内从该ND安全表项记录的入端口收到用于通告该主机地址仍被使用的NA报文，则更新该ND安全表项的老化时间，如果在设定时间内未从该ND安全表项记录的入端口收到用于通告该主机地址仍被使用的NA报文，则删除该ND安全表项。这里的设定时间，即步骤205中所说的从信任端口收到的RA报文包括的重新传输计时器字段值，也即NS报文的重传时间。

[0066] 这里的可达时间用于通告邻居可达时间，例如，当主机A向主机B发送NS 报文，探测主机B是否可达，如果主机A收到主机B应答的NA报文，则认为主机B在该可达时间内是可达的。当超过该可达时间后，主机A可以再次向主机B发送NS报文，确认主机B是否仍可达。

[0067] 由于各主机之间本身就可以通过NS报文和NA报文来探测对端主机是否可达，因此，本申请可以利用这一机制，将ND安全表项的老化时间设置成可达时间字段值与一随机时间的和值，通过主机之间来往的NS报文和NA报文，及时更新ND安全表项的老化时间，减少不必要的DAD NS报文探测操作。

[0068] 例如，假设在二层交换设备上保存了主机A和主机B对应的ND安全表项，主机A上保存了主机B的邻居表项(类似于到主机B的路由表)；当主机A上保存的主机B的邻居表项到达可达时间时，主机A将发送目的地址是主机B的 IPv6地址的NUD(Neighbor Unreachability Detection，邻居可达性探测)报文， NUD报文是NS报文的一种。二层交换设备收到该NUD报文后将刷新主机A 对应的ND安全表项的老化时间。之后，如果二层交换设备收到主机B应答的 NA报文，将刷新主机B对应的ND安全表项的老化时间；如果二层交换设备没有收到主机B应答的NA报文，当主机B对应的ND安全表项的老化时间超时后，届时二层交换设备可以通过主机B对应的ND安全表项记录的入端口向主机B发送DAD NS报文。

[0069] 另外，本申请中，之所以将可达时间字段值加上一随机时间作为最终的老化时间，是考虑到实际应用中可能存在大量主机同时上线的情况，这意味着二层交换设备上同时会生成大量的ND安全表项，如果这些ND安全表项同时老化，将对二层交换设备的CPU(Central Processing Unit，中央处理器)造成较大的冲击。为了将老化探测离散化，因此本申请在老化时间中引入了随机时间。

[0070] 为了使本领域技术人员更加清楚和明白，以下结合图3所示的组网场景来描述本申请的实现过程。

[0071] 在图3所示的无状态地址自动配置组网图中，Device A为网关设备，定期发送RA报文通告网关和前缀。HostA和HostB为无状态主机，根据RA报文内的IPv6前缀网段生成IPv6地址，并将DeviceA对应的本地链路地址作为网关。 Device B为二层交换设备，其中与

DeviceA相连的端口为信任端口，与HostA、HostB相连的端口为非信任端口。

[0072] 对于上述组网，报文及处理的步骤如下：

[0073] 1.无状态主机Host A、Host B上线时发送RS报文请求网关。

[0074] 2.网关Device A定期发送RA报文通告网关和前缀。二层交换设备DeviceB 侦听VLAN内信任端口的RA报文，获取RA报文中通告给无状态主机的各项参数，包含RA报文的重新传输计时器字段记录的NS报文的重传时间，以及 RA报文的可达时间字段记录的可达时间等。

[0075] 3.Host A、Host B主机收到RA报文后，根据RA报文中携带的前缀选项生成IPv6地址，地址生效前会发送DAD报文进行冲突检测。

[0076] 4.Device B从非信任端口收到DAD报文，添加分别与HostA和HostB对应的临时未生效的ND安全表项，再从HostA和HostB的入端口所属VLAN内的其它信任端口发送DAD NS报文进行探测；其中，ND安全表项的表项探测时长为侦听Device A的RA报文获取到的NS报文的重传时间。

[0077] 5.到达ND安全表项的表项探测时长后，这里假设Device B在上述NS报文的重传时间内，未收到从HostA和HostB的入端口所属VLAN内的其它信任端口回应的NA报文，Device B将临时未生效的ND安全表项更新为有效的ND 安全表项，并设置ND安全表项的老化时间为从RA报文中获取的可达时间字段值加上一随机时间的和值。Device B上添加了HostA和HostB对应的ND安全表项后，来自HostA和来自HostB的数据报文能正常通过。

[0078] 6.Host A与Host B通信后互相学习到对端的邻居表项，Host A发送给Host B的NS报文可以匹配上Device B上保存的Host A对应的ND安全表项，Device B可以刷新Host A对应的ND安全表项的老化时间，即将其老化时间恢复成可达时间字段值与一随机时间的和值。同理，二层交换设备上保存的Host B对应的ND安全表项的老化时间也可以按照这一流程被刷新。

[0079] 7.Host A上的Host B表项到达可达时间，Host A发送NUD报文。该NUD 报文可以匹配上Device B上保存的Host A对应的ND安全表项，Device B可以刷新Host A对应的ND安全表项的老化时间。如果Host B无应答，则二层交换设备上保存的Host B对应的ND安全表项的老化时间不会刷新。

[0080] 8.Device B上保存的Host B对应的ND安全表项到达老化时间，Device B 从对应端口发送DAD NS报文，设置超时时间为从RA报文中获取到的NS报文的重传时间，如果在该超时时间内未从该对应端口收到应答，则删除本设备上保存的Host B对应的ND安全表项。

[0081] 以上对本申请提供的方法进行了描述。下面对本申请提供的装置进行描述。

[0082] 参见图4，为本申请提供的一种ND安全表项处理装置的功能模块框图，该装置可以应用于二层交换设备，所述二层交换设备通过信任端口连接路由器网关、通过验证端口连接主机。如图4所示，所述装置可以包括以下单元：

[0083] 接收单元401，用于接收NS报文或NA报文。

[0084] 主机地址获取单元402，用于从所述NS报文或NA报文中获取报文发送方的主机地址。

[0085] ND安全表项处理单元403，用于在本设备上不存在与所述主机地址对应的 ND安全表项时，新建与所述主机地址对应的临时未生效的ND安全表项，并通过信任端口发送用于

探测所述主机地址是否已被使用的NS报文;如果在设定时间内所述接收单元401从信任端口收到用于通告所述主机地址已被使用的NA 报文,则删除新建的ND安全表项;如果在设定时间内所述接收单元401 未从信任端口收到用于通告所述主机地址已被使用的NA报文,则生效新建的ND安全表项;其中,所述设定时间为从信任端口收到的RA报文包括的重新传输计时器字段值。

[0086] 在其中一种实施方式中,如果本设备上存在与所述主机地址对应的ND安全表项且该ND安全表项的状态为无效;则

[0087] 所述ND安全表项处理单元403,还可以用于如果所述NS报文或NA报文从本设备的验证端口收到,则根据所述NS报文或NA报文的媒体接入控制MAC 地址和入端口更新该ND安全表项的内容;如果所述NS报文或NA报文从本设备的信任端口收到,则删除该ND安全表项。

[0088] 在其中一种实施方式中,如果本设备上存在与所述主机地址对应的ND安全表项且该ND安全表项的状态为有效;则

[0089] 所述ND安全表项处理403,还可以用于如果该ND安全表项记录的MAC 地址和入端口与所述NS报文或NA报文的MAC地址和入端口一致,则更新该 ND安全表项的老化时间;如果该ND安全表项记录的MAC地址和入端口与所述NS报文或NA报文的MAC地址和入端口不一致,则通过该ND安全表项记录的入端口发送用于探测所述主机地址是否仍被使用的NS报文;当在所述设定时间内所述接收单元401从该ND安全表项记录的入端口收到用于通告所述主机地址仍被使用的NA报文时,保持该ND安全表项的内容不变,并更新该ND 安全表项的老化时间;当在所述设定时间内所述接收单元401未从该ND安全表项记录的入端口收到用于通告所述主机地址仍被使用的NA报文时,根据所述NS报文或NA报文的MAC地址和入端口更新该ND安全表项的内容,并更新该ND安全表项的老化时间。

[0090] 在其中一种实施方式中,在生效新建的ND安全表项后,所述ND安全表项处理单元403,还可以用于:为生效的ND安全表项设置老化时间,所述老化时间为从信任端口收到的RA报文包括的可达时间字段值与一随机时间的和值;当生效的ND安全表项到达所述老化时间时,通过该ND安全表项记录的入端口发送用于探测所述主机地址是否仍被使用的NS报文;如果在所述设定时间内所述接收单元401从该ND安全表项记录的入端口收到用于通告所述主机地址仍被使用的NA报文,则更新该ND安全表项的老化时间,如果在所述设定时间内所述接收单元401未从该ND安全表项记录的入端口收到用于通告所述主机地址仍被使用的NA报文,则删除该ND安全表项。

[0091] 在其中一种实施方式中,所述主机地址获取单元402具体用于:对于重复地址检测DAD NS报文,从该报文的内容中获取报文发送方的主机地址;对于非DAD NS报文或NA报文,从该报文的源地址字段中获取报文发送方的主机地址。

[0092] 需要说明的是,本发明实施例中对单元的划分是示意性的,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式。在本申请的实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0093] 至此,完成图4所示装置的描述。

[0094] 参见图5,本申请还提供一种二层交换设备的硬件架构图,该二层交换设备包括:

通信接口501、处理器502、存储器503和总线504;其中,通信接口501、处理器502和存储器503通过总线504完成相互间的通信。

[0095] 其中,通信接口501,用于与其它节点通信。处理器502可以是一个中央处理器(CPU),存储器503可以是非易失性存储器(non-volatile memory),并且存储器503中存储有ND安全表项处理逻辑指令,处理器502可以执行存储器 503中存储的ND安全表项处理逻辑指令,以实现上述图2所示流程中的二层交换设备的功能。

[0096] 至此,完成图5所示的硬件结构描述。

[0097] 以上所述仅为本申请的较佳实施例而已,并不用以限制本申请,凡在本申请的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本申请保护的范围之内。

类型 Type	编码 Code			校验和 Checksum
目前跳数限制 Cur Hop Limit	M	O	保留 Rsrvd	路由器生存期 Router Lifetime
可达时间 Reachable time				
重新传输计时器 Retrans Timer				
选项 Options……				

图1

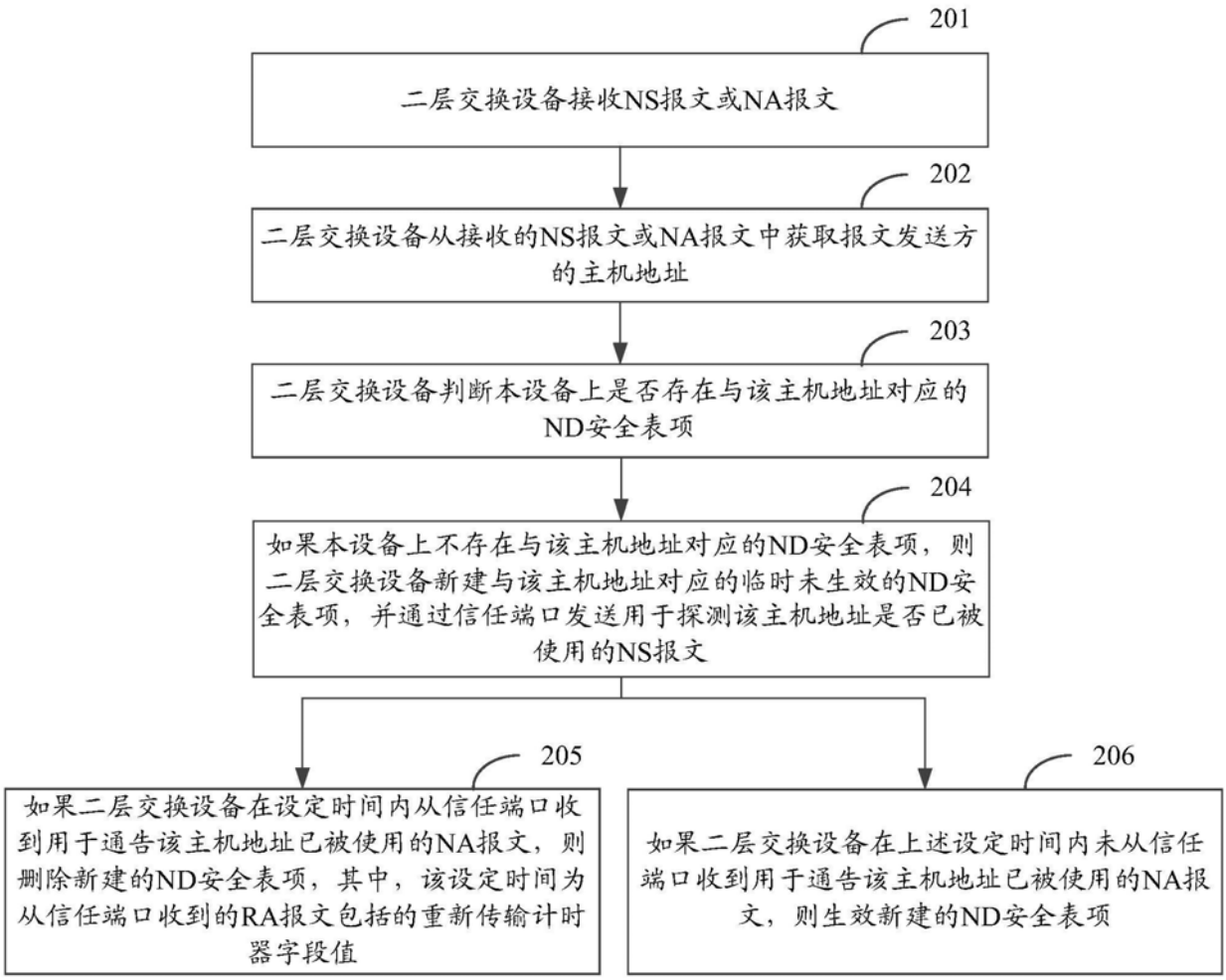


图2

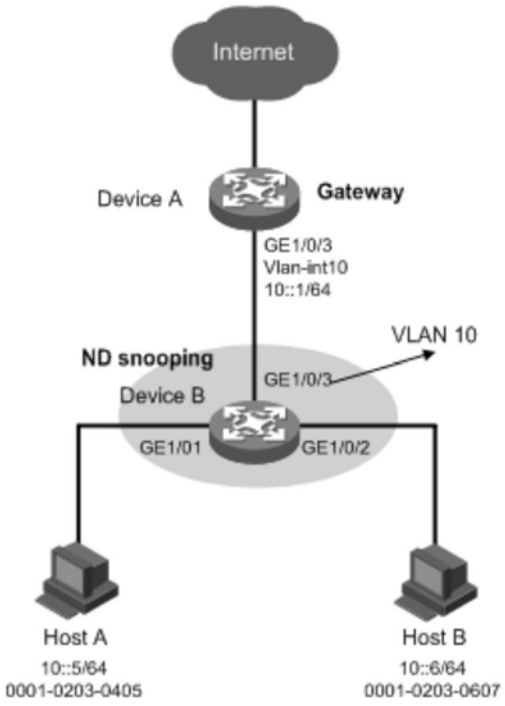

Internet
Device A
Gateway
GE1/0/3
Vlan-int10
10::1/64
VLAN 10
ND snooping
Device B
GE1/0/3
GE1/01
GE1/0/2
Host A
10::5/64
0001-0203-0405
Host B
10::6/64
0001-0203-0607

图3

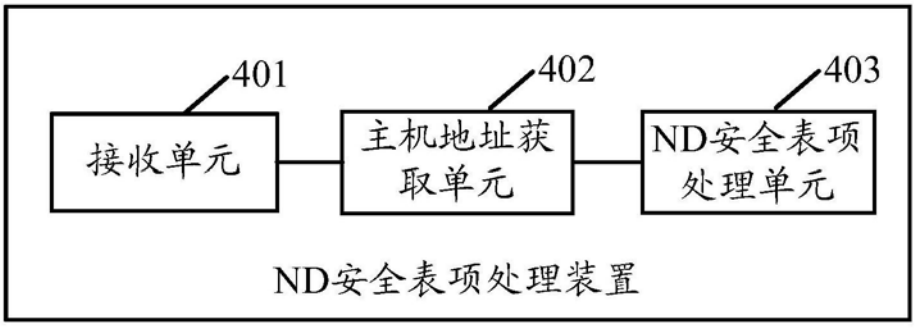

401
402
403
接收单元
主机地址获取单元
ND安全表项处理单元
ND安全表项处理装置

图4

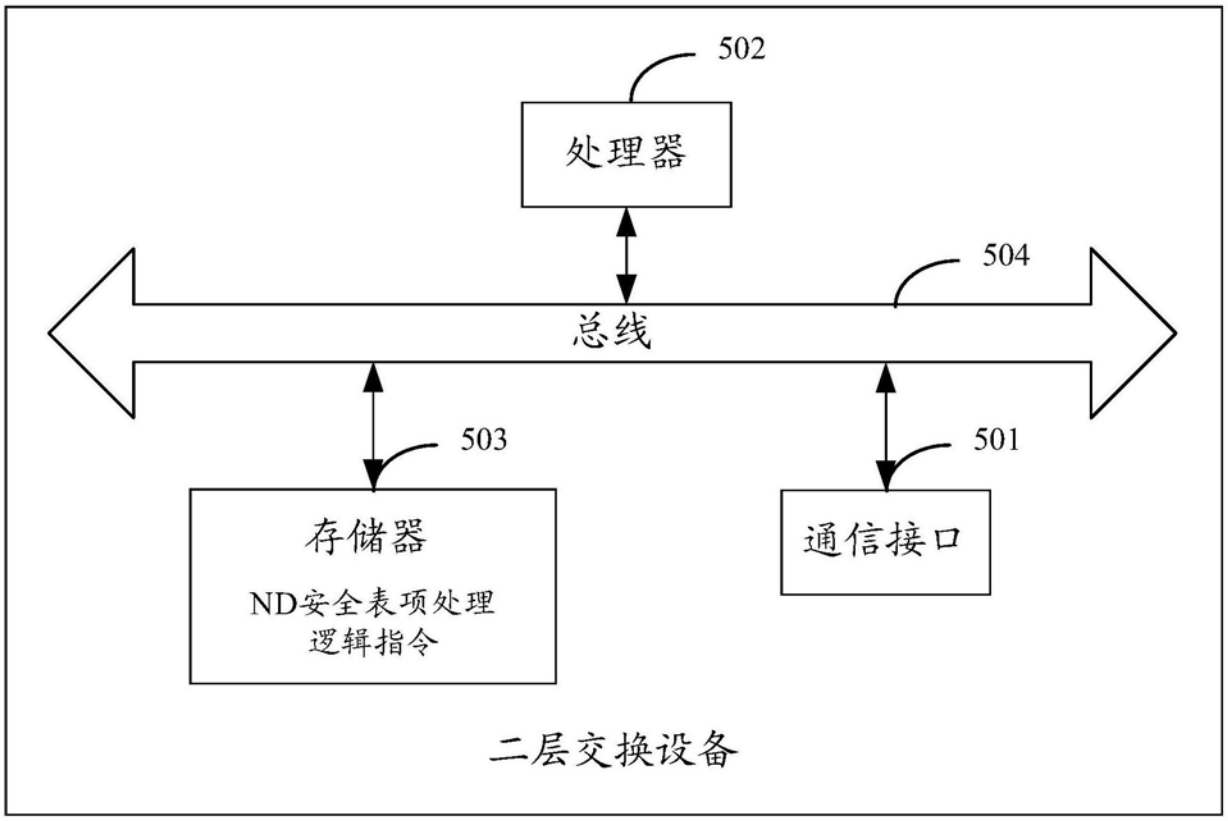


图5