(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 108881328 B
(45)授权公告日 2021.02.23

(21)申请号 201811150122.3

(22)申请日 2018.09.29

(65)同一申请的已公布的文献号
申请公布号 CN 108881328 A

(43)申请公布日 2018.11.23

(73)专利权人 北京东土军悦科技有限公司
地址 100041 北京市石景山区实兴东街18号院1号楼2层01

(72)发明人 孙大娟

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 孟金喆

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/12(2006.01)
H04L 12/741(2013.01)
H04L 12/801(2013.01)

(56)对比文件
CN 106657161 A,2017.05.10
CN 103067197 A,2013.04.24
CN 101547147 A,2009.09.30
CN 101931573 A,2010.12.29
CN 101432721 A,2009.05.13
CN 107517225 A,2017.12.26
CN 1536497 A,2004.10.13
CN 102790773 A,2012.11.21
CN 107864094 A,2018.03.30
CN 102223278 A,2011.10.19
CN 102333011 A,2012.01.25
CN 103095603 A,2013.05.08
US 2016315964 A1,2016.10.27
US 2017373949 A1,2017.12.28
EP 2013759 A4,2011.03.23
US 2018191357 A1,2018.07.05
US 7430164 B2,2008.09.30
US 7283476 B2,2007.10.16
CN 101267433 A,2008.09.17
CN 105072613 A,2015.11.18

审查员 徐思毅

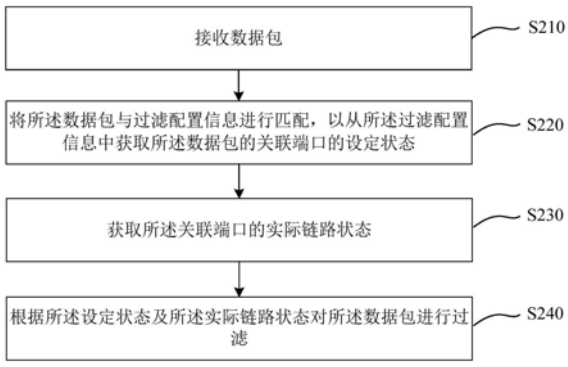
权利要求书2页 说明书10页 附图2页

(54)发明名称

数据包过滤方法、装置、网关设备及存储介质

(57)摘要

本发明实施例公开了一种数据包过滤方法、装置、网关设备及存储介质，该方法包括：接收数据包；将所述数据包与过滤配置信息进行匹配，以从所述过滤配置信息中获取所述数据包的关联端口的设定状态；获取所述关联端口的实际链路状态；根据所述设定状态及所述实际链路状态对所述数据包进行过滤。本发明实施例在基于网络地址转换的包过滤的现有过滤规则的基础上，增加了数据链路动态检测来对数据包进行过滤，使得网关设备能够对通过不同路径接收到的相同数据包进行过滤，在传输可靠性的基础上减少了网络流量，减少了网络带宽的占用，从而在一定程度上提高网络带宽的传输效率和网络的防御能力。



CN 108881328 B

1.一种数据包过滤方法,应用于网络地址转换NAT网关,其特征在于,包括:

接收数据包;

将所述数据包与过滤配置信息进行匹配,以从所述过滤配置信息中获取所述数据包的关联端口的设定状态;

获取所述关联端口的实际链路状态;

根据所述设定状态及所述实际链路状态对所述数据包进行过滤;

所述过滤配置信息包括:转发表和链路状态表,所述转发表包括:入口虚拟局域网标识、源主机IP地址、网关入口IP地址、匹配组标识、网关出口IP地址、目的主机IP地址、协议类型、动作表标识和链路状态表标识,其中,所述链路状态表标识用于指示转发表项关联的链路状态表项;

所述将所述数据包与过滤配置信息进行匹配,以从所述过滤配置信息中获取所述数据包的关联端口的设定状态,包括:

确定所述数据包中携带的目的IP地址属于NAT网关的入口IP地址;

将所述数据包与所述转发表中的各表项进行匹配,确定所述数据包对应的链路状态表标识;

根据所述数据包对应的链路状态表标识,读取所述链路状态表中与该链路状态表标识对应的关联端口的设定状态;

所述根据所述设定状态及所述实际链路状态对所述数据包进行过滤,包括:

根据所述匹配组标识和所述动作表标识确定所述数据包的第一处理动作;

根据所述链路状态表标识确定所述数据包的第二处理动作;

若所述第一处理动作与所述第二处理动作不同,则按照优先级确定所述数据包的最终处理动作;

所述根据所述设定状态及所述实际链路状态对所述数据包进行过滤,包括:

若所述设定状态与所述实际链路状态不一致,则不允许所述数据包通过。

2.根据权利要求1所述的方法,其特征在于,根据所述设定状态及所述实际链路状态对所述数据包进行过滤,包括:

若所述设定状态与所述实际链路状态一致,则允许所述数据包通过,修改所述数据包中携带的地址信息,并转发修改后的数据包。

3.根据权利要求2所述的方法,其特征在于,修改所述数据包中携带的地址信息,并转发修改后的数据包,包括:

分别将所述数据包中携带的源IP地址和目的IP地址,修改为所述过滤配置信息中与所述数据包匹配的网关出口IP地址和目的主机IP地址,并将所述数据包中携带的MAC地址修改为与所述目的主机IP地址对应的MAC地址;

从所述网关出口IP地址对应的端口转发所述修改后的数据包。

4.一种数据包过滤装置,应用于网络地址转换NAT网关,其特征在于,包括:

数据包接收模块,用于接收数据包;

数据包匹配模块,用于将所述数据包与过滤配置信息进行匹配,以从所述过滤配置信息中获取所述数据包的关联端口的设定状态;

链路状态获取模块,用于获取所述关联端口的实际链路状态;

数据包过滤模块，用于根据所述设定状态及所述实际链路状态对所述数据包进行过滤

所述过滤配置信息包括：转发表和链路状态表，所述转发表包括：入口虚拟局域网标识、源主机IP地址、网关入口IP地址、匹配组标识、网关出口IP地址、目的主机IP地址、协议类型、动作表标识和链路状态表标识，其中，所述链路状态表标识用于指示转发表项关联的链路状态表项；

所述数据包匹配模块包括：地址确定单元，用于确定所述数据包中携带的目的IP地址属于NAT网关的入口IP地址；

标识确定单元，用于将所述数据包与所述转发表中的各表项进行匹配，确定所述数据包对应的链路状态表标识；

状态确定单元，用于根据所述数据包对应的链路状态表标识，读取所述链路状态表中与该链路状态表标识对应的关联端口的设定状态；

所述数据包过滤模块包括：第一确定单元，用于根据所述匹配组标识和所述动作表标识确定所述数据包的第一处理动作；

第二确定单元，用于根据所述链路状态表标识确定所述数据包的第二处理动作；

第三确定单元，用于若所述第一处理动作与所述第二处理动作不同，则按照优先级确定所述数据包的最终处理动作；

所述数据包过滤模块用于：若所述设定状态与所述实际链路状态不一致，则不允许所述数据包通过。

5.根据权利要求4所述的装置，其特征在于，所述数据包过滤模块具体用于：若所述设定状态与所述实际链路状态一致，则允许所述数据包通过，修改所述数据包中携带的地址信息，并转发修改后的数据包。

6.一种网关设备，其特征在于，包括：

一个或多个处理器；

存储器，用于存储一个或多个程序，

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-3中任一所述的数据包过滤方法。

7.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求1-3中任一所述的数据包过滤方法。

数据包过滤方法、装置、网关设备及存储介质

技术领域

[0001] 本发明实施例涉及通信技术，尤其涉及一种数据包过滤方法、装置、网关设备及存储介质。

背景技术

[0002] 在计算机科学中，安全就是防止未授权的使用者访问信息，试图破坏或更改信息，是一个系统保护信息的机密性和完整性的能力。就目前而言，对局域网的保护，防火墙仍然不失为一种有效的手段。防火墙技术主要分为包过滤和应用代理两类，其中包过滤作为最早发展起来的一种技术，其应用非常广泛。包过滤是对流经网络防火墙的所有数据包逐个检查，并依据所制定的安全策略来决定数据包是否通过。

[0003] 传统包过滤技术，大多是在网络层实现，只是简单的对当前正在通过的数据包进行检测，查看源/目的IP地址、端口号以及协议类型(UDP(User Datagram Protocol，用户数据报协议)/TCP(Transmission Control Protocol，传输控制协议))等，结合访问控制规则对数据包实施有选择的通过。这种技术实现简单，处理速度快，对应用透明，但是它存在的问题也很多，主要表现在：1)所有可能会用到的端口都必须静态开放；2)不能对数据传输状态进行判断；3)无法过滤审核数据包上层的内容。

[0004] 此外，还有一种流过滤防火墙方案，在状态包过滤防火墙中，数据包被截获后，状态包过滤防火墙从数据包中提取连接状态信息(TCP的连接状态信息，如：TCP_SYN(Synchronize Sequence Numbers，同步序列编号)、TCP_ACK(Acknowledgement，确认字符)，以及UDP和ICMP(Internet Control Message Protocol，因特网控制报文协议)的模拟连接状态信息)，并把这些信息放到动态连接表中动态维护，当后续数据包来时，将后续数据包及其状态信息和其前一时刻的数据包及其状态信息进行比较，防火墙就能做出决策：后续的数据包是否允许通过，从而达到保护网络安全的目的。但是，此方案中连接状态信息是数据包协议里携带的信息，是逻辑上的状态，仍然不能基于链路层进行判断。

[0005] NAT(Network Address Translation，网络地址转换)本质上是一种允许在互联网的不同地方重复使用相同的IP地址集的机制，其工作原理是重写通过路由器的数据包的识别信息。基于NAT的包过滤技术中，NAT网关可以同时执行地址转换和包过滤，包过滤的标准取决于NAT的动态状态(如数据流量、业务内容等)。包过滤的策略的选择可能有不同的粒度，例如，NAT如何处理非请求的数据包取决于源/目标IP地址、源/目的端口号，处理的行为在不同的NAT上会有所不同。

[0006] 但是，通过NAT网关位于不同网络内的终端可以相互通信，不同网络的两个终端有可能存在多条链路，两个终端在通信时虽然NAT同时执行地址转换和包过滤，但还很有可能会出现：接收侧终端会从多条冗余的链路上获得多份相同的数据，这样不仅浪费了网络带宽，增加了网络流量，还会影响网络的传输效率。

发明内容

[0007] 本发明提供一种数据包过滤方法、装置、网关设备及存储介质，以减少网络流量，减少网络带宽的占用，提高网络带宽的传输效率和网络的防御能力。

[0008] 第一方面，本发明实施例提供了一种数据包过滤方法，应用于NAT网关，包括：

[0009] 接收数据包；

[0010] 将所述数据包与过滤配置信息进行匹配，以从所述过滤配置信息中获取所述数据包的关联端口的设定状态；

[0011] 获取所述关联端口的实际链路状态；

[0012] 根据所述设定状态及所述实际链路状态对所述数据包进行过滤。

[0013] 可选的，根据所述设定状态及所述实际链路状态对所述数据包进行过滤，包括：

[0014] 若所述设定状态与所述实际链路状态一致，则允许所述数据包通过，修改所述数据包中携带的地址信息，并转发修改后的数据包。

[0015] 可选的，修改所述数据包中携带的地址信息，并转发修改后的数据包，包括：

[0016] 分别将所述数据包中携带的源IP地址和目的IP地址，修改为所述过滤配置信息中与所述数据包匹配的网关出口IP地址和目的主机IP地址，并将所述数据包中携带的MAC地址修改为与所述目的主机IP地址对应的MAC地址；

[0017] 从所述网关出口IP地址对应的端口转发所述修改后的数据包。

[0018] 可选的，根据所述设定状态及所述实际链路状态对所述数据包进行过滤，包括：

[0019] 若所述设定状态与所述实际链路状态不一致，则不允许所述数据包通过。

[0020] 可选的，所述过滤配置信息包括：转发表和链路状态表，其中，所述转发表中包括链路状态表标识，所述链路状态表标识用于指示转发表项关联的链路状态表项；

[0021] 将所述数据包与过滤配置信息进行匹配，以从所述过滤配置信息中获取所述数据包的关联端口的设定状态，包括：

[0022] 确定所述数据包中携带的目的IP地址属于NAT网关的入口IP地址；

[0023] 将所述数据包与所述转发表中的各表项进行匹配，确定所述数据包对应的链路状态表标识；

[0024] 根据所述数据包对应的链路状态表标识，读取所述链路状态表中与该链路状态表标识对应的关联端口的设定状态。

[0025] 可选的，所述转发表包括：入口虚拟局域网标识、源主机IP地址、网关入口IP地址、匹配组标识、网关出口IP地址、目的主机IP地址、协议类型、动作表标识和链路状态表标识；

[0026] 根据所述设定状态及所述实际链路状态对所述数据包进行过滤，包括：

[0027] 根据所述匹配组标识和所述动作表标识确定所述数据包的第一处理动作；

[0028] 根据所述链路状态表标识确定所述数据包的第二处理动作；

[0029] 若所述第一处理动作与所述第二处理动作不同，则按照优先级确定所述数据包的最终处理动作。

[0030] 第二方面，本发明实施例还提供了一种数据包过滤装置，应用于NAT网关，包括：

[0031] 数据包接收模块，用于接收数据包；

[0032] 数据包匹配模块，用于将所述数据包与过滤配置信息进行匹配，以从所述过滤配置信息中获取所述数据包的关联端口的设定状态；

[0033] 链路状态获取模块，用于获取所述关联端口的实际链路状态；

[0034] 数据包过滤模块，用于根据所述设定状态及所述实际链路状态对所述数据包进行过滤。

[0035] 可选的，所述数据包过滤模块具体用于：若所述设定状态与所述实际链路状态一致，则允许所述数据包通过，修改所述数据包中携带的地址信息，并转发修改后的数据包。

[0036] 第三方面，本发明实施例还提供了一种网关设备，包括：

[0037] 一个或多个处理器；

[0038] 存储器，用于存储一个或多个程序，

[0039] 当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如本发明任意实施例所述的数据包过滤方法。

[0040] 第四方面，本发明实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现如本发明任意实施例所述的数据包过滤方法。

[0041] 本发明实施例在基于NAT的包过滤的现有过滤规则的基础上，增加了数据链路动态检测来对数据包进行过滤，即根据网关设备所接收数据包的关联端口的设定状态与实际链路状态对数据包进行过滤，使得网关设备能够对通过不同路径接收到的相同数据包进行过滤，在传输可靠性的基础上减少了网络流量，减少了网络带宽的占用，从而在一定程度上提高网络带宽的传输效率和网络的防御能力。

附图说明

[0042] 图1是现有技术的网络拓扑示意图；

[0043] 图2是本发明实施例一提供的数据包过滤方法的流程图；

[0044] 图3是本发明实施例二提供的数据包过滤装置的结构示意图；

[0045] 图4是本发明实施例三提供的网关设备的结构示意图。

具体实施方式

[0046] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部结构。

[0047] 图1是现有技术的网络拓扑示意图，如图1所示，设备2发出的数据包可以通过两种路径到达NAT网关，分别为：设备2→NAT网关，以及，设备2→设备3→NAT网关。也就是说，NAT网关可能收到两份相同的来自设备2的数据包，通常情况下，设备2→NAT网关的路径比较短，数据可靠性比较高；而设备2→设备3→NAT网关的路径比较长，可靠性较差。按照现有的NAT网关的过滤规则，不考虑物理链路状态，这两个相同的数据包均会允许通过，浪费网络带宽，增加网络流量，影响网络的传输效率。图1中，eth表示网关端口。

[0048] 实施例一

[0049] 图2是本发明实施例一提供的数据包过滤方法的流程图，本实施例可适用于基于网络地址转换进行数据包过滤的情况，尤其是针对通过不同路径传输到网关设备的相同数据包的过滤。该方法可以由数据包过滤方法装置来执行，该装置可以通过软件和/或硬件实现，该装置可集成在网关设备中，例如NAT网关。如图2所示，该方法具体包括如下步骤：

[0050] S210,接收数据包。

[0051] 其中,在如图1所示的包括网关设备的网络拓扑中,网关设备一般可以通过多条路径接收到相同的数据包。

[0052] S220,将所述数据包与过滤配置信息进行匹配,以从所述过滤配置信息中获取所述数据包的关联端口的设定状态。

[0053] 其中,过滤配置信息是预先设置的存储于网关设备中的过滤规则,本发明实施例在现有过滤规则的基础上,增加了物理链路状态的相关规则,现有过滤规则如源/目的IP地址、数据包中具体字段等。将数据包与过滤配置信息进行匹配,是指按照过滤配置信息中的各项,逐一将数据包的对应信息与过滤匹配信息的各项进行匹配比较,若命中过滤配置信息中的内容,表示当前项匹配,若未命中,表示当前项不匹配。若数据包无法与过滤配置信息匹配,则丢弃该数据包,不进行转发操作。

[0054] 关联端口指的是网关设备上与数据包关联的端口,关联端口的设定状态包括:连接(Link Up)和断开(Link Down)。示例性的,网关设备通过不同路径接收到相同的数据包,那么关联端口指网关设备上连接最优路径的端口。

[0055] S230,获取所述关联端口的实际链路状态。

[0056] 其中,可以通过检测网关设备上的关联端口,来获取关联端口的实际链路状态。关联端口的实际链路状态包括:连接(Link Up)和断开(Link Down)。需要说明的是,设定状态是从过滤配置信息中获取到的端口的状态信息,实际链路状态是指在实际网络拓扑中检测到的端口的当前物理状态。

[0057] S240,根据所述设定状态及所述实际链路状态对所述数据包进行过滤。

[0058] 其中,若所述设定状态与所述实际链路状态一致,则允许所述数据包通过,修改所述数据包中携带的地址信息,并转发修改后的数据包。其中地址信息是指源IP地址、目的IP地址和MAC(Media Access Control,媒体介入控制)地址。当然,若根据过滤配置信息中的现有过滤规则,需要对数据包进行修改后转发,则除了修改地址信息之外,还要修改数据包中的相关字段内容。若所述设定状态与所述实际链路状态不一致,则不允许所述数据包通过。

[0059] 本实施例的技术方案,在基于NAT的包过滤的现有过滤规则的基础上,增加了数据链路动态检测来对数据包进行过滤,即根据网关设备所接收数据包的关联端口的设定状态与实际链路状态对数据包进行过滤,使得网关设备能够对通过不同路径接收到的相同数据包进行过滤,在传输可靠性的基础上减少了网络流量,减少了网络带宽的占用,从而在一定程度上提高网络带宽的传输效率和网络的防御能力。

[0060] 进一步的,修改所述数据包中携带的地址信息,并转发修改后的数据包,包括:分别将所述数据包中携带的源IP地址和目的IP地址,修改为所述过滤配置信息中与所述数据包匹配的网关出口IP地址和目的主机IP地址,并将所述数据包中携带的MAC地址修改为与所述目的主机IP地址对应的MAC地址;从所述网关出口IP地址对应的端口转发所述修改后的数据包。上述修改地址信息的过程就是完成网络地址转换的过程。修改完地址信息后,便可以顺利将修改后的数据包转发到相应的目标设备。

[0061] 本发明实施例中的过滤配置信息至少包括:转发表和链路状态表。转发表主要存储现有过滤规则,转发表包括如下表项:入口虚拟局域网标识、源主机IP地址、网关入口IP

地址、匹配组标识(匹配组ID)、网关出口IP地址、目的主机IP地址、协议类型和动作表标识(动作表ID),除此之外,本发明实施例在转发表中增加了一条表项,即链路状态表标识(链路状态表ID),用于指示转发表项关联的链路状态表项。也就是说,链路状态表和转发表通过链路状态表标识来进行关联。链路状态表包括如下表项:链路状态表标识、端口号和端口链路状态。

[0062] 此外,过滤配置信息还可以包括匹配组和动作表。其中,匹配组用于存储过滤数据包的相关信息,这些信息可以根据数据流量和业务内容进行设置,例如,字段具体内容,将某字段的内容修改为目标内容等。示例性的,若数据包中匹配到字段具体内容,则该数据包对应的处理动作为过滤,即过滤包含某些字段的数据包;若数据包中包含某字段,将该字段的内容修改为目标内容,该数据包对应的处理动作是修改后转发,即修改数据包中某字段后转发修改后的数据包。匹配组与转发表通过匹配组ID来进行关联。动作表用于存储数据包的处理动作,例如,转发、丢弃或修改。动作表与转发表通过动作表ID来进行关联。匹配组与动作表是现有的过滤规则,本发明实施例对此不进行详细描述。

[0063] 表1 NAT转发表项

[0064]

转发表ID	入口VLAN ID	源主机IP地址	网关入口IP地址	匹配组ID	网关出口IP地址	目的主机IP地址	协议类型	动作表ID	链路状态表ID

[0065] 表2链路状态表项

[0066]

链路状态表ID	端口号	端口链路状态

[0067] 表1中,转发表ID表示转发表所设置的各条过滤规则的编号,例如,按序从1开始排列。

[0068] 入口VLAN(Virtual Local Area Network,虚拟局域网)ID,即入口虚拟局域网标识,是指NAT网关上接收当前数据包的入口所在的VLAN的标识。

[0069] 源主机IP地址是指NAT网关接收到的当前数据包中携带的源IP地址。

[0070] 网关入口IP地址是指NAT网关上接收当前数据包的入口的IP地址。

[0071] 网关出口IP地址是指当NAT网关转发当前数据包时,通过该网关出口IP地址对应的端口转发当前数据包。

[0072] 目的主机IP地址是指当NAT网关转发当前数据包时,将该当前数据包转发至该目的主机IP地址对应的设备。

[0073] 匹配组是与转发表关联的另外一个表,匹配组ID可以理解为匹配组中的行号。若转发表中匹配组ID为0,则表示不检查此项,若转发表中匹配组ID为非0,则到匹配组中的相应行去进行信息匹配,以根据匹配组确定数据包的处理动作。

[0074] 动作表是与转发表关联的另外一个表,动作表ID可以理解为动作表中的行号。若转发表中动作表ID为0,则表示不检查此项,若转发表中动作表ID为非0,则到动作表中相应行去进行信息匹配,以根据动作表确定数据包的处理动作。

[0075] 协议类型是指当前数据包所支持的协议类型,例如,UDP、TCP和ICMP等。

[0076] 链路状态表ID可以理解为链路状态表中的行号。端口号是指NAT网关的端口的编号。端口链路状态可以是连接或断开,链路状态表中的端口链路状态即通过数据包与过滤

配置信息的匹配可以获取到的端口的设定状态。

[0077] 需要说明的是，表1所示的转发表主要体现源主机IP地址、网关入口IP地址、网关出口IP地址、目的主机IP地址之间的映射关系，其中的入口虚拟局域网标识、源主机IP地址、网关入口IP地址、匹配组ID和协议类型，这些表项是需要与数据包中的信息进行匹配的。动作表ID为了决策出数据包的具体处理动作。网关出口IP地址和目的主机IP地址，这两个表项是根据网关设备所在的网络拓扑预先设置的转发信息，在决策出需要转发数据包时，根据网关出口IP地址和目的主机IP地址，改写数据包中携带的地址信息，完成数据包的转发。转发表和链路状态表均为静态配置。

[0078] 可选的，S220中将所述数据包与过滤配置信息进行匹配，以从所述过滤配置信息中获取所述数据包的关联端口的设定状态，包括：确定所述数据包中携带的目的IP地址属于NAT网关的入口IP地址；将所述数据包与所述转发表中的各表项进行匹配，确定所述数据包对应的链路状态表标识；根据所述数据包对应的链路状态表标识，读取所述链路状态表中与该链路状态表标识对应的关联端口的设定状态。

[0079] 其中，网关设备接收到数据包后，先检查数据包中携带的目的IP地址是否属于该网关设备的入口IP地址，以确定该数据包是发往NAT网关的，而不是发往其他设备的。具体的，如果数据包中携带的目的IP地址命中转发表中的网关入口IP地址，可以将数据包收取并进行后续匹配步骤，否则网关设备丢弃该数据包。收取该数据包后，按照转发表中与上述命中的网关入口IP地址属于同一行的各表项，对数据包与转发表进行匹配，若匹配成功(即与数据包相关的信息均命中)且处理动作为转发，将该数据包中携带的源IP地址修改为所命中表项对应的网关出口IP地址，将数据包中携带的目的IP地址修改为所命中表项对应的目的主机IP地址(即将目的主机IP地址作为真实的目的地址)，将数据包中携带的MAC地址修改为与目的主机IP地址对应的MAC地址，并将修改后的数据包从上述网关出口IP地址对应的端口转出。具体的，与目的主机IP地址对应的MAC地址可以通过DRP(Distributed Redundancy Protocol，分布式冗余协议)获取。若匹配不成功(即至少一个与数据包相关的信息未命中)或者所有信息均命中但处理动作为丢弃，则丢弃该数据包。

[0080] 可选的，S240中根据所述设定状态及所述实际链路状态对所述数据包进行过滤，包括：根据所述匹配组标识和所述动作表标识确定所述数据包的第一处理动作；根据所述链路状态表标识确定所述数据包的第二处理动作；若所述第一处理动作与所述第二处理动作不同，则按照优先级确定所述数据包的最终处理动作。

[0081] 本可选实施方式中，考虑到根据现有过滤规则确定的处理动作与根据物理链路状态确定的处理动作存在冲突的情况，利用规则优先级来确定最终的处理动作，能够保证及时对数据包给出合理的处理动作。例如，物理链路的优先级高于现有过滤规则的优先级，则以物理链路确定的处理动作为准。

[0082] 下面以图1所示的网络拓扑为例进行说明，NAT转发表中部分信息设置如表3所示，链路状态表中部分信息设置如表4所示。

[0083] 表3 NAT转发表

[0084]

转发表ID	入口VLAN ID	源主机IP地址	网关入口IP地址	匹配组ID	网关出口IP地址	目的主机IP地址	协议类型	动作表ID	链路状态表ID
1	100	192.168.2.2	192.168.1.2	0	192.168.2.7	230.1.1.70	UDP	0	1
2	100	192.168.3.2	192.168.1.3	0	192.168.2.7	230.1.1.70	UDP	0	2

[0085] 表4链路状态表

[0086]

链路状态表ID	端口号	端口链路状态
1	eth1	LINK UP
2	eth1	LINK DOWN

[0087] 基于图1所示的网络拓扑，上述表3和表4所示的过滤配置信息，在现有过滤规则的基础上，添加设备2→NAT网关和设备2→设备3→NAT网关的两条物理链路状态的检测，当设备2→NAT网关的链路可靠时，允许设备2→NAT设备的数据包通过，不允许设备2→设备3→NAT网关的数据包通过；当设备2→NAT网关的链路不可靠时，允许设备2→设备3→NAT网关的数据包通过。这样优先选择设备2→NAT网关的链路，只有当设备2→NAT网关的链路出现故障时，才允许设备2→设备3→NAT网关的数据包路通过。

[0088] 具体的，根据图1所示的网络拓扑中各设备和NAT网关的IP地址分配，以及端口配置，通过上述表3和表4中的过滤配置信息，可知，通过设备2→NAT这条路径发来的数据包A，命中了转发表ID为1的这行信息中的源IP地址和网关入口IP地址；通过设备3→NAT网关这条路径发来的数据包B，命中了转发表ID为2的这行信息中的源IP地址和网关入口IP地址。其中，具体可以结合数据包内容判断数据包B是否与数据包A相同，即需要判断数据包B是设备3原始发出的数据包，还是设备2发出的数据包A通过设备2→设备3→NAT网关这条路径到达NAT网关。本实施例中，数据包B与数据包A是相同的数据包且通过不同路径到达NAT网关。

[0089] 根据关联的链路状态表，若数据包A的关联端口eth1的实际链路状态与链路状态表中eth1设定的端口链路状态一致，为连接(即设备2→NAT网关之间的链路连接)，允许数据包A通过，阻止数据包B通过；若数据包B的关联端口eth1的实际链路状态与链路状态表中eth1设定的端口链路状态一致，为断开(即设备2→NAT网关链路断开)，允许数据包B通过。例如，获取的eth1的实际链路状态为连接，则数据包A被允许通过，可以转发，数据包B被丢弃。由此，NAT网关根据端口链路状态对来自设备2的通过不同路径传输的两个相同的数据包进行过滤，只允许一个数据包通过，避免目的主机接收到两份相同的数据包，节省网络带宽。

[0090] 实施例二

[0091] 图3是本发明实施例二提供的数据包过滤装置的结构示意图，该装置可以集成在网关设备中，例如NAT网关。如图3所示，该装置包括：

[0092] 数据包接收模块310，用于接收数据包；

[0093] 数据包匹配模块320，用于将所述数据包与过滤配置信息进行匹配，以从所述过滤配置信息中获取所述数据包的关联端口的设定状态；

[0094] 链路状态获取模块330，用于获取所述关联端口的实际链路状态；

[0095] 数据包过滤模块340，用于根据所述设定状态及所述实际链路状态对所述数据包进行过滤。

[0096] 可选的，所述数据包过滤模块340具体用于：若所述设定状态与所述实际链路状态一致，则允许所述数据包通过，修改所述数据包中携带的地址信息，并转发修改后的数据包。

[0097] 进一步的，所述数据包过滤模块340具体用于：分别将所述数据包中携带的源IP地址和目的IP地址，修改为所述过滤配置信息中与所述数据包匹配的网关出口IP地址和目的主机IP地址，并将所述数据包中携带的MAC地址修改为与所述目的主机IP地址对应的MAC地址；从所述网关出口IP地址对应的端口转发所述修改后的数据包。

[0098] 可选的，所述数据包过滤模块340具体用于：若所述设定状态与所述实际链路状态不一致，则不允许所述数据包通过。

[0099] 上述过滤配置信息可以包括：转发表和链路状态表，其中，所述转发表中包括链路状态表标识，所述链路状态表标识用于指示转发表项关联的链路状态表项。

[0100] 数据包匹配模块320包括：

[0101] 地址确定单元，用于确定所述数据包中携带的目的IP地址属于NAT网关的入口IP地址；

[0102] 标识确定单元，用于将所述数据包与所述转发表中的各表项进行匹配，确定所述数据包对应的链路状态表标识；

[0103] 状态确定单元，用于根据所述数据包对应的链路状态表标识，读取所述链路状态表中与该链路状态表标识对应的关联端口的设定状态。

[0104] 进一步的，上述转发表可以包括：入口虚拟局域网标识、源主机IP地址、网关入口IP地址、匹配组标识、网关出口IP地址、目的主机IP地址、协议类型、动作表标识和链路状态表标识。

[0105] 数据包过滤模块340包括：

[0106] 第一确定单元，用于根据所述匹配组标识和所述动作表标识确定所述数据包的第一处理动作；

[0107] 第二确定单元，用于根据所述链路状态表标识确定所述数据包的第二处理动作；

[0108] 第三确定单元，用于若所述第一处理动作与所述第二处理动作不同，则按照优先级确定所述数据包的最终处理动作。

[0109] 本发明实施例所提供的数据包过滤装置可执行本发明任意实施例所提供的数据包过滤方法，具备执行方法相应的功能模块和有益效果。未在本实施例中详尽描述的技术细节，可参见本发明任意实施例提供的数据包过滤方法。

[0110] 实施例三

[0111] 本发明实施例三提供了一种网关设备，包括：

[0112] 一个或多个处理器；

[0113] 存储器，用于存储一个或多个程序，

[0114] 当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如本发明任意实施例所述的基于网络地址转换的数据包过滤方法。

[0115] 图4是本发明实施例三提供的网关设备的结构示意图，如图4所示，该网关设备包括：处理器410、存储器420和至少两个端口430。网关设备中处理器410的数量可以是一个或多个，图4中以一个处理器410为例；网关设备中的处理器410、存储器420和至少两个端口

430可以通过总线或其他方式连接，图4中以通过总线连接为例。

[0116] 存储器420作为一种计算机可读存储介质，可用于存储软件程序、计算机可执行程序以及模块，如本发明实施例中的数据包过滤方法对应的程序指令/模块(例如，数据包过滤装置中的数据包接收模块310、数据包匹配模块320、链路状态获取模块330和数据包过滤模块340)。处理器410通过运行存储在存储器420中的软件程序、指令以及模块，从而执行网关设备的各种功能应用以及数据处理，即实现上述的数据包过滤方法。

[0117] 存储器420可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序；存储数据区可存储根据终端的使用所创建的数据等。此外，存储器420可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他非易失性固态存储器件。在一些实例中，存储器420可进一步包括相对于处理器410远程设置的存储器，这些远程存储器可以通过网络连接至网关设备。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0118] 至少两个端口430可用于接收或发送数据包。

[0119] 实施例四

[0120] 本发明实施例四还提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现如本发明任意实施例所述的数据包过滤方法。

[0121] 本发明实施例的计算机存储介质，可以采用一个或多个计算机可读的介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0122] 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0123] 计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0124] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明操作的计算机程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如Java、Smalltalk、C++，还包括常规的过程式程序设计语言—诸如”C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)域连接到用户计算机，或者，可以连接到外部计算机(例如利用因特网服务提

供商来通过因特网连接)。

[0125] 注意,上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员会理解,本发明不限于这里所述的特定实施例,对本领域技术人员来说能够进行各种明显的变化、重新调整和替代而不会脱离本发明的保护范围。因此,虽然通过以上实施例对本发明进行了较为详细的说明,但是本发明不仅仅限于以上实施例,在不脱离本发明构思的情况下,还可以包括更多其他等效实施例,而本发明的范围由所附的权利要求范围决定。

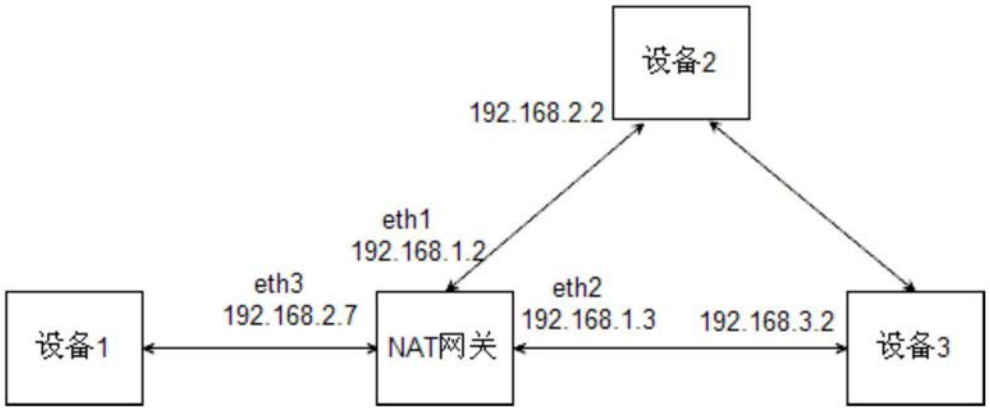

设备2
192.168.2.2
eth1
192.168.1.2
eth3
192.168.2.7
eth2
192.168.1.3
192.168.3.2
设备1
NAT网关
设备3

图1

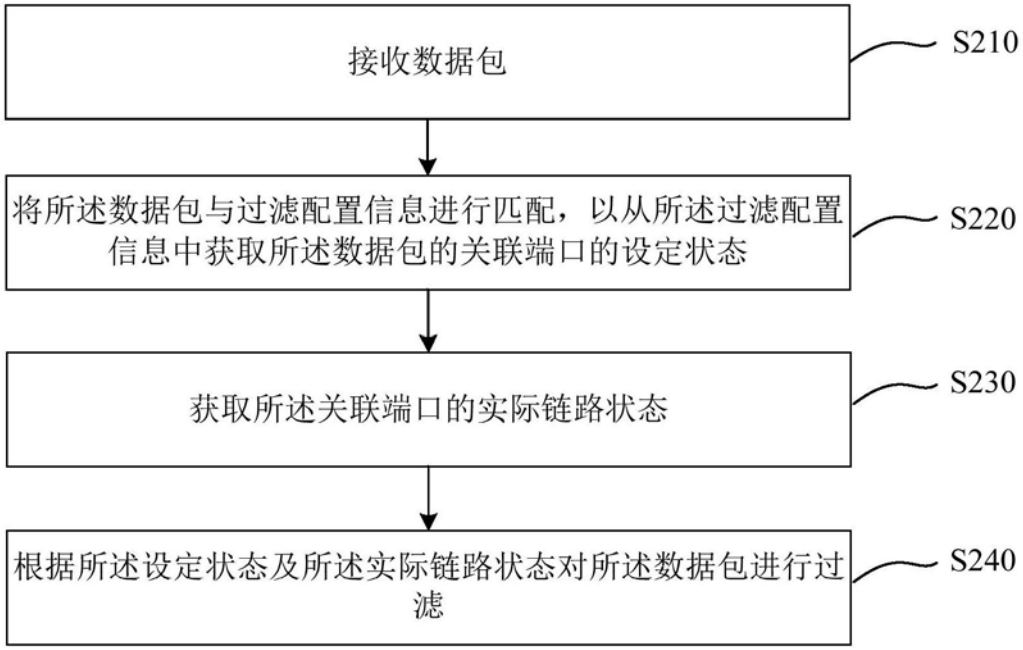

接收数据包
S210
将所述数据包与过滤配置信息进行匹配，以从所述过滤配置信息中获取所述数据包的关联端口的设定状态
S220
获取所述关联端口的实际链路状态
S230
根据所述设定状态及所述实际链路状态对所述数据包进行过滤
S240

图2

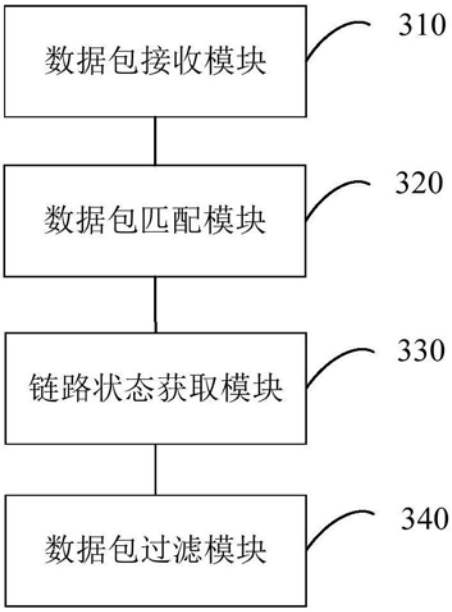

数据包接收模块
310
数据包匹配模块
320
链路状态获取模块
330
数据包过滤模块
340

图3

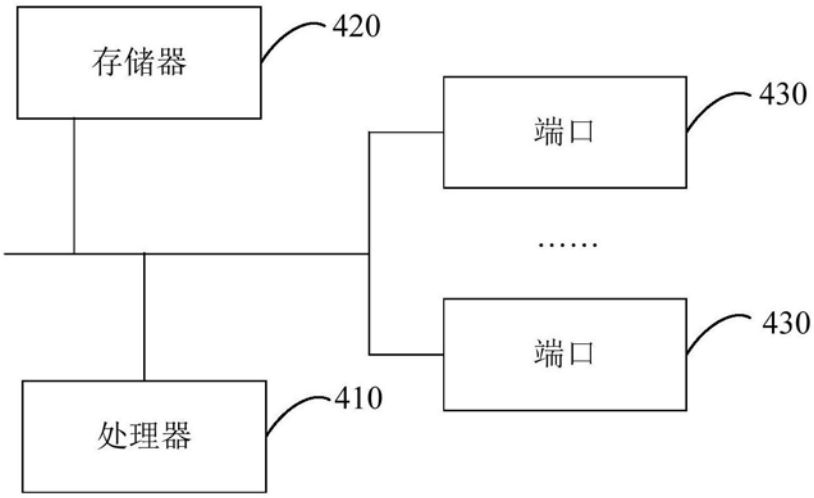

存储器
420
端口
430
……
端口
430
处理器
410

图4