(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 6 月 4 日 (04.06.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/108382 A1

(51) 国际专利分类号:
H04L 29/08 (2006.01) *H04L 12/24* (2006.01)

(21) 国际申请号: PCT/CN2019/119996

(22) 国际申请日: 2019 年 11 月 21 日 (21.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811415014.4 2018年11月26日 (26.11.2018) CN

(71) 申请人: 新 华 三 技 术 有 限 公 司 (**NEW H3C TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国浙江省杭州市滨江区长河路 466 号, Zhejiang 310052 (CN)。

(72) 发明人: 赵丽丽 (**ZHAO, Lili**); 中国北京市朝阳区广顺南大街 8 号院 1 号楼利星行中心 A 座640室, Beijing 100102 (CN)。

(74) 代理人: 北 京 博 思 佳 知 识 产 权 代 理 有 限 公 司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

(54) **Title:** MERGING SECURITY POLICIES OF PORTS

(54) **发明名称:** 端口的安全策略合并

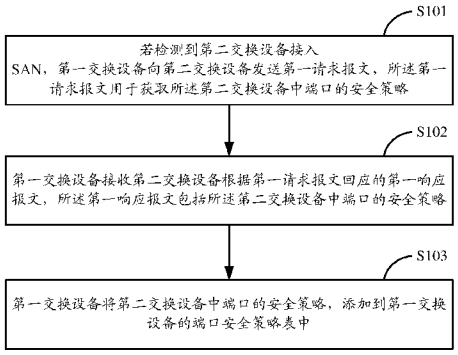

图 1

S101 If it is detected that a second switching device accesses an SAN, a first switching device sends a first request message to the second switching device, wherein the first request message is used for acquiring a security policy of a port in the second switching device

S102 The first switching device receives a first response message with which the second switching device responds according to the first request message, wherein the first response message comprises a security policy of a port in the second switching device

S103 The first switching device adds the security policy of the port in the second switching device to a port security policy table of the first switching device

(57) **Abstract:** Provided is a method for merging security policies of ports, wherein same is applied to a first switching device in a storage area network (SAN). The method comprises: if it is detected that a second switching device accesses an SAN, sending a first request message to the second switching device, wherein the first request message is used for acquiring a security policy of a port in the second switching device; receiving a first response message with which the second switching device responds according to the first request message, wherein the first response message comprises a security policy of a port in the second switching device; and adding

WO 2020/108382 A1

[见续页]

MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

the security policy of the port in the second switching device to a port security policy table of the first switching device.

(57) 摘要：本公开提供一种端口的安全策略合并方法，应用于存储区域网络SAN中的第一交换设备。若检测到第二交换设备接入SAN，向第二交换设备发送第一请求报文，第一请求报文用于获取所述第二交换设备中端口的安全策略。接收第二交换设备根据第一请求报文回应的第一响应报文，第一响应报文包括第二交换设备中端口的安全策略。将第二交换设备中端口的安全策略，添加到第一交换设备的端口安全策略表中。

端口的安全策略合并

背景技术

[01]存储区域网络（Storage Area Network，SAN）是用于提供服务器与存储设备之间进行数据传输的专用网络。SAN 中的服务器和存储设备通过交换机连接。

[02]为了保障 SAN 的网络安全，通常引入端口安全技术，以提供基于端口级别的安全控制。端口安全技术主要是指：建立交换机上的端口与通过该端口直接接入交换机的设备的绑定关系，作为端口的安全策略的一部分，以允许符合端口的安全策略的设备通过交换机登陆 SAN。

[03]在实际应用中，会有网络合并的情况。比如，将 SAN1 与 SAN2 合并。此时，需要对 SAN1 和 SAN2 中各个交换机的端口的安全策略进行合并，以达到合并后各交换机中端口的安全策略一致的效果。例如，设备 A 原本在 SAN1 中不允许通过交换机登录网络，网络合并后该设备 A 依然无法通过 SAN2 中的交换机登录网络。

[04]目前，合并端口的安全策略的操作需要人工手动完成，合并效率不高，且容易出错。

附图说明

[05]为了更清楚地说明本公开实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本公开的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[06]图 1 是本公开实施例示出的一种端口的安全策略合并方法流程图。

[07]图 2 是本公开实施例示出的第一交换设备检测第二交换设备的实现流程。

[08]图 3 是本公开实施例示出的第一交换设备向第二交换设备提供端口的安全策略的实现流程。

[09]图 4 是本公开实施例示出的 FC 协议报文示例。

[10]图 5A 是本公开实施例示出的一个 SAN 的示意图。

[11]图 5B 是本公开实施例示出的另一个 SAN 的示意图。

[12]图 5C 是本公开实施例示出的图 5A 和图 5B 合并后的 SAN 网络的示意图。

[13]图 6 是本公开实施例示出的一种端口的安全策略合并装置的结构示意图。

[14]图 7 是本公开实施例示出的一种交换设备的硬件结构示意图。

具体实施方式

[15]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公开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、本公开的一些方面相一致的装置和方法的例子。

[16]在本公开实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本公开实施例。在本公开实施例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。

[17]应当理解，尽管在本公开实施例可能采用术语第一、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，在不脱离本公开实施例范围的情况下，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”。

[18]本公开实施例提供一种端口的安全策略合并方法。该方法中，第一交换设备在感知到第二交换设备接入 SAN 时，利用与第二交换设备之间的报文交互，获取第二交换设备中端口的安全策略，以实现端口的安全策略自动合并，提升端口的安全策略的合并效率。

[19]为了使本公开实施例的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本公开实施例执行详细描述：

[20]参见图 1，为本公开实施例提供的端口的安全策略合并方法流程图。该流程应用于 SAN 中的第一交换设备。

[21]如图 1 所示，该流程可包括以下步骤：

[22] 步骤 S101，若检测到第二交换设备接入 SAN，第一交换设备向第二交换设备发送第一请求报文。

[23] 当第一交换设备检测到第二交换设备接入 SAN 时，第一交换设备需获取第二交换设备中端口的安全策略，此时，第一交换设备生成第一请求报文。该第一请求报文用于获取第二交换设备中端口的安全策略。

[24] 第一交换设备向第二交换设备发送第一请求报文。

[25] 这里，第一交换设备、第二交换设备、第一请求报文只是为便于描述而进行的命名，并非用于限定。

[26] 第一交换设备检测第二交换设备的过程在下文描述，这里暂不赘述。

[27] 步骤 S102，第一交换设备接收第二交换设备根据第一请求报文回应的第一响应报文。

[28] 在本公开实施例中，第二交换设备接收到步骤 S101 中的第一请求报文后，对第一请求报文进行解析，确定第一交换设备需获取第二交换设备自身端口的安全策略。第二交换设备获取端口的安全策略，并生成第一响应报文。可以理解的是，第一响应报文包括第二交换设备中端口的安全策略。

[29] 第二交换设备向第一交换设备发送第一响应报文。这里，第一响应报文只是为便于描述而进行的命名，并非用于限定。

[30] 作为示例而非限定，端口的安全策略可存储在第二交换设备中的端口安全策略表里。第二交换设备可直接从端口安全策略表中，获取第二交换设备的端口的安全策略。

[31] 参见表 1，为交换设备中的端口安全策略表示例。

端口安全策略表		
交换设备的端口标识	节点设备的标识	策略行为
交换设备 1 的端口 1	服务器 1	允许
交换设备 1 的端口 2	存储设备 1	允许
任意端口	服务器 2	拒绝

表 1

[32] 其中，每一条表项代表一个端口安全策略。比如，第一条表项表示的端口安全策略为：允许服务器 1 通过交换设备 1 的端口 1 接入网络。

[33]步骤 S103，第一交换设备将第二交换设备中端口的安全策略，添加到第一交换设备的端口安全策略表中。

[34]第一交换设备接收到第一响应报文后，解析并从中获取第二交换设备中端口的安全策略。第一交换设备将获取的端口的安全策略，添加到本交换设备的端口安全策略表中，即完成对端口的安全策略的合并。

[35]第一交换设备根据合并后的端口的安全策略，确定网络设备是否可以通过第一交换设备登录网络。

[36]至此，完成图 1 所示流程。

[37]通过图 1 所示流程可以看出，在本公开实施例中，第一交换设备在感知到第二交换设备接入 SAN 时，利用与第二交换设备之间的报文交互，获取第二交换设备中端口的安全策略，以实现端口的安全策略的自动合并，提升端口的安全策略的合并效率。

[38]下面对第一交换设备检测第二交换设备的过程进行具体描述。参见图 2，为本公开实施例示出的第一交换设备检测第二交换设备的实现流程，通过检测交换设备接入 SAN 的过程，可使第一交换设备快速发现新接入的交换设备，并获取到该交换设备的端口的安全策略。

[39]如图 2 所示，该流程可包括以下步骤:

[40]步骤 S201，第一交换设备学习 SAN 中各个交换设备的路由。

[41]当存在新的交换设备接入 SAN 时，SAN 中的各个交换设备会重新收集网络拓扑，并基于收集到的网络拓扑重新计算路由。即新的交换设备的接入触发 SAN 中各交换设备重新学习路由。

[42]第一交换设备将本次学习到的路由与路由表中已存在的路由进行比较，若此次学习到的路由未记录在路由表中，说明该路由为新学习到的路由，即新增的路由，将该新增的路由添加到路由表中。

[43]路由包括的目的地址为交换设备的地址。

[44]步骤 S202，若存在新增的路由，第一交换设备获取该路由包括的目的地址。

[45]步骤 S203，第一交换设备将目的地址对应的交换设备确定为第二交换设备。

[46]如前所述，路由包括的目的地址为交换设备的地址，因此，第一交换设备可根据从新增路由中获取到的目的地址，确定该目的地址对应的交换设备为接入 SAN 的交换设

备，即第二交换设备。

[47]至此，完成图 2 所示流程。

[48]通过图 2 所示流程，实现对第二交换设备的检测。

[49]参见图 3，为本公开实施例示出的第一交换设备向第二交换设备提供端口的安全策略的实现流程。

[50]如图 3 所示，该流程可包括以下步骤:

[51]步骤 S301，第一交换设备接收第二交换设备发送的第二请求报文。

[52]该第二请求报文用于获取第一交换设备中端口的安全策略。

[53]需要说明的是，本公开实施例中，第二交换设备发送第二请求报文、第一交换设备接收第二请求报文的过程与前述实施例步骤 101 相同，在此不再复述。

[54]这里，第二请求报文只是为便于描述而进行的命名，并非用于限定。

[55]步骤 S302，根据第二请求报文，第一交换设备获取第一交换设备中端口的安全策略。

[56]需要说明的是，本公开实施例中，第一交换设备获取自身端口的安全策略的过程与前述实施例步骤 102 中第二交换设备获取自身端口的安全策略的过程相同，在此不再复述。

[57]步骤 S303，第一交换设备向第二交换设备发送第二响应报文。

[58]需要说明的是，本公开实施例中，第一交换设备向第二交换设备发送第二响应报文的过程与前述实施例步骤 S102 中第二交换设备向第一交换设备发送第一响应报文的过程相同，在此不再复述。

[59]第二响应报文包括第一交换设备中端口的安全策略。

[60]这里，第二响应报文只是为便于描述而进行的命名，并非用于限定。

[61]至此，完成图 3 所示流程。

[62]通过图 3 所示流程，实现第一交换设备向第二交换设备提供第一交换设备中端口的安全策略。即第二交换设备获取到第一交换设备中端口的安全策略。

[63]可选的，作为一个实施例，第一交换设备和第二交换设备之间交互的请求报文和响应报文均为光纤通道（FC，Fiber channel）协议报文。

[64]参见图 4，为 FC 协议报文示例。

[65]FC 协议报文包括 FC 报文头和负载。在本公开实施例中该 FC 协议报文可具体为获取端口安全策略（Get Port Security Policies，GPSP）报文。为了方便描述，下文以 FC 协议报文说明。GPSP 报文为 FC 协议报文中的一种类型。

[66]FC 报文头包括路由控制（R_CTL）字段、类型特殊控制（CS_CTL）字段、目的标识符（D_ID）字段、源标识符（S_ID）字段以及数据结构类型（TYPE）字段。其中：

R_CTL 字段：请求报文中该字段的值为 02H，响应报文中该字段的值为 03H;

CS_CTL 字段：值为 00H;

D_ID 字段和 S_ID 字段：分别为目的交换设备的地址和源交换设备的地址;

TYPE 字段：值为 22H。

[67]请求报文的负载，如表 2 所述，包括命令码（Command Code）字段。Command Code 字段携带标识，比如，标识为 70000004H，用于表示当前请求报文为获取端口的安全策略的报文。接收到请求报文的交换设备根据 Command Code 字段携带的标识，确定请求报文为用于获取端口的安全策略的报文，从而向发送该请求报文的交换设备提供端口的安全策略。

负载内容	字节数（Bytes）
70000004H	4

表 2

[68]响应报文的负载，如表 3 所示。表 3 仅为示例性说明。

负载内容	字节数（Bytes）
端口安全策略表项的数量	4
端口安全策略表项 1	20
……	20
端口安全策略表项 n	20

表 3

[69]其中，端口安全策略表项 1~端口安全策略表项 n 为交换设备中端口安全策略表的表

项。

[70]本公开实施例通过对 FC 协议报文进行上述扩展，使交换设备之间可基于 FC 协议交互端口的安全策略。

[71]下面通过具体实施例对本公开实施例提供的方法进行描述：

[72]参见图 5A，为本公开实施例示出的一个 SAN 的示意图。

[73]图 5A 中，交换设备 521 当前已有的端口的安全策略，如表 4 所示。

交换设备 521 的端口安全策略表		
交换设备的端口标识	节点设备的标识	策略行为
交换设备 521 的端口 1	服务器 511	允许
交换设备 521 的端口 2	存储设备 531	允许
任意端口	服务器 513	拒绝

表 4

[74]其中，节点设备为与交换设备直连的服务器、存储设备或者其它交换设备；策略行为为允许，表示对应节点设备可以通过交换设备登录网络；策略行为为拒绝，表示对应节点设备不可以通过交换设备登录网络。比如，最后一条表项所代表的端口安全策略为：禁止服务器 513 通过任意端口接入网络。

[75]需要说明的是，在 SAN 中，端口标识或节点设备的标识通常利用全球名字（World Wide Name，WWN）表示。本公开实施例中，为了更加直观的展现交换设备与节点设备的绑定关系（即端口的安全策略），利用图 5A~图 5C 中示出的设备名称或端口名称表示。

[76]参见图 5B，为本公开实施例示出的另一个 SAN 的示意图。该组网中的交换设备 522 和交换设备 523 已通过自动合并或手动配置，具有相同的端口的安全策略，如表 5 和表 6 所示。

交换设备 522 的端口安全策略表		
交换设备的端口标识	节点设备的标识	策略行为
交换设备 522 的端口 1	存储设备 532	允许
交换设备 523 的端口 1	服务器 512	允许

表 5

交换设备 523 的端口安全策略表		
交换设备的端口标识	节点设备的标识	策略行为
交换设备 523 的端口 1	服务器 512	允许
交换设备 522 的端口 1	存储设备 532	允许

表 6

[77]其中，表 5 为交换设备 522 中当前已有的端口的安全策略；表 6 为交换设备 523 中当前已有的端口的安全策略。

[78]若将图 5A 与图 5B 所示 SAN 网络合并（合并后如图 5C 所示），图 5C 中的各个交换设备重新收集网络拓扑，并基于网络拓扑重新计算到各个交换设备的路由，即完成路由学习。

[79]交换设备 521 学习到达目的地址为交换设备 522 的地址的路由，以及目的地址为交换设备 523 的地址的路由；同理，交换设备 522 学习到达目的地址为交换设备 521 的地址的路由，以及目的地址为交换设备 523 的地址的路由；交换设备 523 学习到达目的地址为交换设备 521 的地址的路由，以及目的地址为交换设备 522 的地址的路由。

[80]交换设备 521~交换设备 523 分别将本次学习到的路由与各自路由表中的已有路由进行比较。比如，交换设备 521 在网络合并之前，路由表中没有目的地址为交换设备 522 的地址的路由，也没有目的地址为交换设备 523 的地址的路由。因此，交换设备 521 可确定此次学习到的目的地址为交换设备 522 的地址的路由、目的地址为交换设备 523 的地址的路由均为新增路由。同理，交换设备 522 可确定此次学习到的目的地址为交换设备 521 的地址的路由为新增路由。交换设备 523 可确定此次学习到的目的地址为交换设备 521 的地址的路由为新增路由。

[81]如前所述，交换设备 521 中存在两条新增路由。

[82]交换设备 521 基于目的地址为交换设备 522 的地址的新增路由，向交换设备 522 发送获取交换设备 522 中端口的安全策略的请求报文（记为 Packet11）。该 Packet11 的 R_CTL 字段为 02H，CS_CTL 字段为 00H，D_ID 字段为交换设备 522 的地址，S_ID 字段为交换设备 521 的地址，TYPE 字段为 22H，Command Code 字段为 70000004H。

[83]交换设备 522 接收到 Packet11 后，基于 R_CTL 字段（02H），确定 Packet11 为请求报文。基于 Command Code 字段（70000004H），确定 Packet11 为用于获取端口安全策略的请求报文。即确定交换设备 521 是要获取本设备中的端口的安全策略。因此，交换设备 522 从自身维护的端口安全策略表（表 5）中获取端口的安全策略。交换设备 522

向交换设备 521 发送响应报文（记为 Packet12），该 Packet12 的 R_CTL 字段为 03H，CS_CTL 字段为 00H，D_ID 字段为交换设备 521 的地址，S_ID 字段为交换设备 522 的地址，TYPE 字段为 22H，负载为从表 5 中获取的端口的安全策略。

[84] 交换设备 521 接收到 Packet12 后，基于 R_CTL 字段（03H），确定 Packet12 为响应报文，从该响应报文中获取到交换设备 522 中端口的安全策略，并添加到本地的端口安全策略表中，如表 7 所示。

交换设备 521 的端口安全策略表		
交换设备的端口标识	节点设备的标识	策略行为
交换设备 521 的端口 1	服务器 511	允许
交换设备 521 的端口 2	存储设备 531	允许
任意端口	服务器 513	拒绝
交换设备 522 的端口 1	存储设备 532	允许
交换设备 523 的端口 1	服务器 512	允许

表 7

[85] 交换设备 521 基于目的地址为交换设备 523 的地址的新增路由，向交换设备 523 发送获取交换设备 523 中端口的安全策略的请求报文（记为 Packet21）。该 Packet21 的 R_CTL 字段为 02H，CS_CTL 字段为 00H，D_ID 字段为交换设备 523 的地址，S_ID 字段为交换设备 521 的地址，TYPE 字段为 22H，Command Code 字段为 70000004H。

[86] 交换设备 523 接收到 Packet21 后，基于 R_CTL 字段（02H），确定 Packet21 为请求报文。基于 Command Code 字段（70000004H），确定 Packet21 为用于获取端口安全策略的请求报文。即确定交换设备 521 是要获取本设备中的端口的安全策略。因此，交换设备 523 从自身维护的端口安全策略表（表 6）中获取端口的安全策略。交换设备 523 向交换设备 521 发送响应报文（记为 Packet22），该 Packet22 的 R_CTL 字段为 03H，CS_CTL 字段为 00H，D_ID 字段为交换设备 521 的地址，S_ID 字段为交换设备 523 的地址，TYPE 字段为 22H，负载为从表 6 中获取的端口的安全策略。

[87] 交换设备 521 接收到 Packet22 后，基于 R_CTL 字段（03H），确定 Packet22 为响应报文，从该响应报文中获取到交换设备 523 中端口的安全策略。由于交换设备 523 中端口的安全策略与交换设备 522 中端口的安全策略相同，因此，表 6 不需要更新。

[88] 交换设备 522 基于目的地址为交换设备 521 的地址的新增路由，向交换设备 521 发送获取交换设备 521 中端口的安全策略的请求报文（记为 Packet31）。该 Packet31 的 R_CTL 字段为 02H，CS_CTL 字段为 00H，D_ID 字段为交换设备 521 的地址，S_ID 字

段为交换设备 522 的地址，TYPE 字段为 22H，Command Code 字段为 70000004H。

[89] 交换设备 521 接收到 Packet31 后，基于 R_CTL 字段（02H），确定 Packet31 为请求报文。基于 Command Code 字段（70000004H），确定 Packet31 为用于获取端口安全策略的请求报文。即确定交换设备 522 是要获取本设备中的端口的安全策略。因此，交换设备 521 从自身维护的端口安全策略表（表 4）中获取端口的安全策略。交换设备 521 向交换设备 522 发送响应报文（记为 Packet32），该 Packet32 的 R_CTL 字段为 03H，CS_CTL 字段为 00H，D_ID 字段为交换设备 522 的地址，S_ID 字段为交换设备 521 的地址，TYPE 字段为 22H，负载为从表 4 中获取的端口的安全策略。

[90] 交换设备 522 接收到 Packet32 后，基于 R_CTL 字段（03H），确定 Packet32 为响应报文，从该响应报文中获取到交换设备 521 中端口的安全策略，并添加到本地的端口安全策略表中，如表 8 所示。

交换设备 522 的端口安全策略表		
交换设备的端口标识	节点设备的标识	策略行为
交换设备 522 的端口 1	存储设备 532	允许
交换设备 523 的端口 1	服务器 512	允许
交换设备 521 的端口 1	服务器 511	允许
交换设备 521 的端口 2	存储设备 531	允许
任意端口	服务器 513	拒绝

表 8

[91] 交换设备 523 基于目的地址为交换设备 521 的地址的新增路由，向交换设备 521 发送获取交换设备 521 中端口的安全策略的请求报文（记为 Packet41）。该 Packet41 的 R_CTL 字段为 02H，CS_CTL 字段为 00H，D_ID 字段为交换设备 521 的地址，S_ID 字段为交换设备 523 的地址，TYPE 字段为 22H，Command Code 字段为 70000004H。

[92] 交换设备 521 接收到 Packet41 后，基于 R_CTL 字段（02H），确定 Packet41 为请求报文。基于 Command Code 字段（70000004H），确定 Packet41 为用于获取端口安全策略的请求报文。即确定交换设备 523 是要获取本设备中的端口的安全策略。因此，交换设备 521 从自身维护的端口安全策略表（表 4）中获取端口的安全策略。交换设备 521 向交换设备 523 发送响应报文（记为 Packet42），该 Packet42 的 R_CTL 字段为 03H，CS_CTL 字段为 00H，D_ID 字段为交换设备 523 的地址，S_ID 字段为交换设备 521 的地址，TYPE 字段为 22H，负载为从表 4 中获取的端口的安全策略。

[93] 交换设备 523 接收到 Packet42 后，基于 R_CTL 字段（03H），确定 Packet42 为响

应报文，从该响应报文中获取到交换设备 521 中端口的安全策略，并添加到本地的端口安全策略表中，如表 9 所示。

交换设备 523 的端口安全策略表		
交换设备的端口标识	节点设备的标识	策略行为
交换设备 523 的端口 1	服务器 512	允许
交换设备 522 的端口 1	存储设备 532	允许
交换设备 521 的端口 1	服务器 511	允许
交换设备 521 的端口 2	存储设备 531	允许
任意端口	服务器 513	拒绝

表 9

[94]至此，完成图 5C 中所有交换设备中端口的安全策略的合并。

[95]合并后，服务器 513 通过交换设备 521、交换设备 522、交换设备 523 均无法登录网络。

[96]以上对本公开实施例提供的方法进行了描述，下面对本公开实施例提供的装置进行描述：

[97]参见图 6，为本公开实施例提供的装置的结构示意图。该装置包括：发送单元 601、接收单元 602 以及添加单元 603，其中：

发送单元 601，用于若检测到第二交换设备接入所述 SAN，向所述第二交换设备发送第一请求报文，所述第一请求报文用于获取所述第二交换设备中端口的安全策略；

接收单元 602，用于接收所述第二交换设备根据所述第一请求报文回应的第一响应报文，所述第一响应报文包括所述第二交换设备中端口的安全策略；

添加单元 603，用于将所述第二交换设备中端口的安全策略，添加到所述第一交换设备的端口安全策略表中。

[98]作为一个实施例，所述装置还包括：

学习单元，用于学习所述 SAN 中交换设备的路由；

获取单元，用于若存在新增的路由，获取所述路由包括的目的地址，所述路由包括的目的地址为交换设备的地址；

确定单元，用于将所述目的地址对应的交换设备确定为所述第二交换设备。

[99]作为一个实施例，所述接收单元 602，还用于接收所述第二交换设备发送的第二请

求报文，所述第二请求报文用于获取所述第一交换设备中端口的安全策略；

获取单元，用于根据所述第二请求报文，获取所述第一交换设备中端口的安全策略；

所述发送单元 601，还用于向所述第二交换设备发送第二响应报文，所述第二响应报文包括所述第一交换设备中端口的安全策略。

[100] 作为一个实施例，所述请求报文和所述响应报文均为 FC 协议报文；

其中，所述请求报文携带用于表示所述请求报文为用于获取端口的安全策略的报文的标识。

[101] 至此，完成图 6 所示装置的描述。在本公开实施例中，第一交换设备在感知到第二交换设备接入 SAN 时，利用与第二交换设备之间的报文交互，获取第二交换设备中端口的安全策略，以实现端口的安全策略自动合并，提升端口的安全策略的合并效率。

[102] 下面对本公开实施例提供的交换设备进行描述：

[103] 参见图 7，为本公开实施例提供的一种交换设备的硬件结构示意图。该交换设备 700 可包括处理器 701、存储有机器可执行指令的机器可读存储介质 702 以及一个或多个输入/输出端口（图中未示出）。处理器 701 与机器可读存储介质 702 以及输入/输出端口可经由系统总线 703 通信。并且，通过读取并执行机器可读存储介质 702 中与端口的安全策略合并逻辑对应的机器可执行指令，处理器 701 可执行上文描述的端口的安全策略合并方法。

[104] 在本示例中对交换设备 700 的操作进行描述。若交换设备 700 检测到有另一交换设备新接入 SAN，则交换设备 700 向新接入的交换设备发送第一请求报文，以获取该新的交换设备中端口的安全策略。新的交换设备接收到第一请求报文后，将端口安全策略携带在第一响应报文中进行回应。交换设备 700 通过分析接收的第一响应报文获取该新接入交换设备中端口的安全策略，并将获取的安全策略添加到本地的端口安全策略表中。

[105] 交换设备 700 可以通过学习 SAN 中交换设备的路由来确定是否有新的设备接入 SAN。若存在新增的路由，则获取所述路由包括的目的地址，所述路由包括的目的地址为新接入交换设备的地址。交换设备 700 将获取的目的地址对应的交换设备确定为新接入交换设备。

[106] 交换设备 700 接收新接入交换设备发送的第二请求报文，所述第二请求报文用

于获取交换设备 700 中端口的安全策略。交换设备 700 向新接入交换设备发送第二响应报文，所述第二响应报文包括交换设备 700 中端口的安全策略。

[107] 在一个示例中，上述请求报文和响应报文均为光纤通道 FC 协议报文；其中，所述请求报文携带了用于表示请求报文为用于获取端口的安全策略的报文的标识。

[108] 本文提到的机器可读存储介质 702 可以是任何电子、磁性、光学或其他物理存储装置，可以包含或存储信息，如可执行指令、数据，等等。例如，所述机器可读存储介质 702 可以包括如下至少一个种存储介质：易失存储器、非易失性存储器、其它类型存储介质。其中，易失性存储器可为 RAM（Random Access Memory，随机存取存储器），非易失性存储器可为闪存、存储驱动器（如硬盘驱动器）、固态硬盘、存储盘（如光盘、DVD 等）。

[109] 本公开实施例还提供一种包括机器可执行指令的机器可读存储介质，例如图 7 中的机器可读存储介质 702，所述机器可执行指令可由交换设备中的处理器 701 执行，以实现以上描述的端口的安全策略合并方法。

[110] 至此，完成图 7 所示设备的描述。

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

权利要求书

1、一种端口的安全策略合并方法，应用于存储区域网络 SAN 中的第一交换设备，其特征在于，所述方法包括:

若检测到第二交换设备接入所述 SAN，向所述第二交换设备发送第一请求报文，所述第一请求报文用于获取所述第二交换设备中端口的安全策略;

接收所述第二交换设备根据所述第一请求报文回应的第一响应报文，所述第一响应报文包括所述第二交换设备中端口的安全策略;

将所述第二交换设备中端口的安全策略，添加到所述第一交换设备的端口安全策略表中。

2、如权利要求 1 所述的方法，其特征在于，所述向所述第二交换设备发送第一请求报文之前，还包括:

学习所述 SAN 中交换设备的路由;

若存在新增的路由，获取所述路由包括的目的地址，所述路由包括的目的地址为交换设备的地址;

将所述目的地址对应的交换设备确定为所述第二交换设备。

3、如权利要求 1 所述的方法，其特征在于，所述方法还包括:

接收所述第二交换设备发送的第二请求报文，所述第二请求报文用于获取所述第一交换设备中端口的安全策略;

根据所述第二请求报文，获取所述第一交换设备中端口的安全策略;

向所述第二交换设备发送第二响应报文，所述第二响应报文包括所述第一交换设备中端口的安全策略。

4、如权利要求 1 所述的方法，其特征在于：所述请求报文和所述响应报文均为光纤通道 FC 协议报文;

其中，所述请求报文携带用于表示所述请求报文为用于获取端口的安全策略的报文的标识。

5、一种端口的安全策略合并装置，应用于存储区域网络 SAN 中的第一交换设备，其特征在于，所述装置包括:

发送单元，用于若检测到第二交换设备接入所述 SAN，向所述第二交换设备发送第一请求报文，所述第一请求报文用于获取所述第二交换设备中端口的安全策略;

接收单元，用于接收所述第二交换设备根据所述第一请求报文回应的第一响应报文，所述第一响应报文包括所述第二交换设备中端口的安全策略;

添加单元，用于将所述第二交换设备中端口的安全策略，添加到所述第一交换设备的端口安全策略表中。

6、如权利要求 5 所述的装置，其特征在于，所述装置还包括：

学习单元，用于学习所述 SAN 中交换设备的路由；

获取单元，用于若存在新增的路由，获取所述路由包括的目的地址，所述路由包括的目的地址为交换设备的地址；

确定单元，用于将所述目的地址对应的交换设备确定为所述第二交换设备。

7、如权利要求 5 所述的装置，其特征在于，所述装置还包括：获取单元，

所述接收单元，还用于接收所述第二交换设备发送的第二请求报文，所述第二请求报文用于获取所述第一交换设备中端口的安全策略；

所述获取单元，用于根据所述第二请求报文，获取所述第一交换设备中端口的安全策略；

所述发送单元，还用于向所述第二交换设备发送第二响应报文，所述第二响应报文包括所述第一交换设备中端口的安全策略。

8、如权利要求 5 所述的装置，其特征在于：

所述请求报文和所述响应报文均为光纤通道 FC 协议报文；

其中，所述请求报文携带用于表示所述请求报文为用于获取端口的安全策略的报文的标识。

9、一种交换设备，其特征在于，所述交换设备包括：

处理器；以及

机器可读存储介质，所述机器可读存储介质存储有能够被所述处理器执行的机器可执行指令，

其中，通过读取并执行所述机器可执行指令，所述处理器被促使：

若检测到另一交换设备接入所述交换设备所在的存储区域网络 SAN，向所述另一交换设备发送第一请求报文，所述第一请求报文用于获取所述另一交换设备中端口的安全策略；

接收所述另一交换设备根据所述第一请求报文回应的第一响应报文，所述第一响应报文包括所述另一交换设备中端口的安全策略；

将所述另一交换设备中端口的安全策略，添加到所述交换设备的端口安全策略表中。

10、如权利要求 9 所述的设备，其特征在于，在向所述另一交换设备发送第一请求报文之前，所述处理器还被所述机器可执行指令促使：

学习所述 SAN 中交换设备的路由;

若存在新增的路由，获取所述路由包括的目的地址，所述路由包括的目的地址为交换设备的地址;

将所述目的地址对应的交换设备确定为所述另一交换设备。

11、如权利要求 9 所述的设备，其特征在于，所述处理器还被所述机器可执行指令促使:

接收所述另一交换设备发送的第二请求报文，所述第二请求报文用于获取所述交换设备中端口的安全策略;

根据所述第二请求报文，获取所述交换设备中端口的安全策略;

向所述另一交换设备发送第二响应报文，所述第二响应报文包括所述交换设备中端口的安全策略。

12、如权利要求 9 所述的设备，其特征在于：所述请求报文和所述响应报文均为光纤通道 FC 协议报文;

其中，所述请求报文携带用于表示所述请求报文为用于获取端口的安全策略的报文的标识。

13、一种机器可读存储介质，其特征在于，所述机器可读存储介质内存储有机器可执行指令,所述机器可执行指令被处理器执行时实现权利要求 1-4 任一所述的方法步骤。

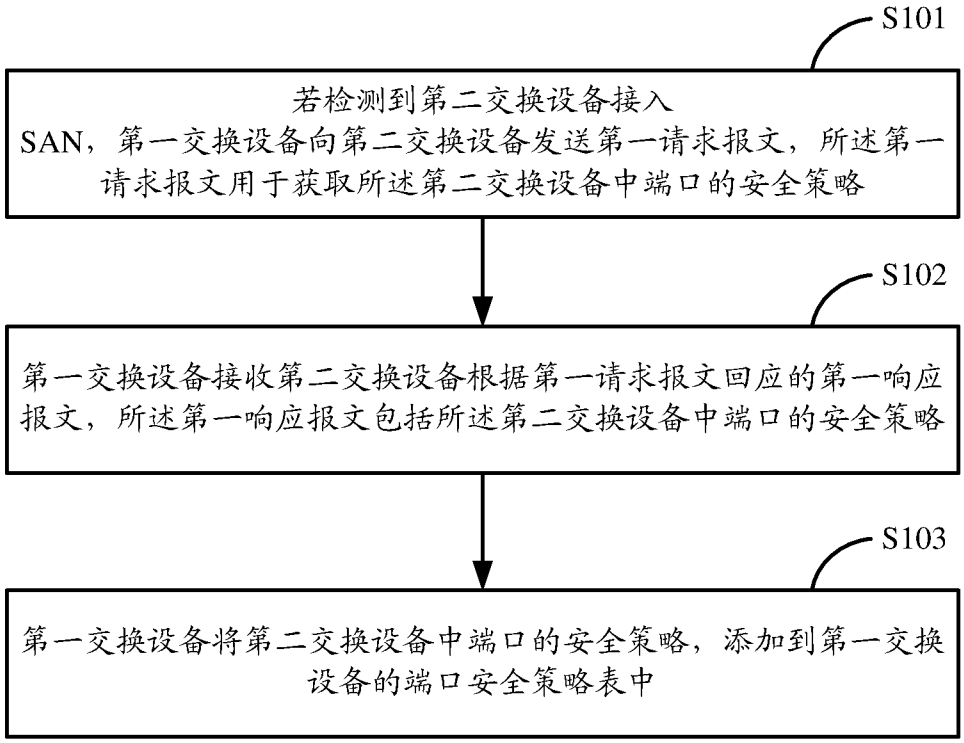
S101
若检测到第二交换设备接入SAN，第一交换设备向第二交换设备发送第一请求报文，所述第一请求报文用于获取所述第二交换设备中端口的安全策略
S102
第一交换设备接收第二交换设备根据第一请求报文回应的第一响应报文，所述第一响应报文包括所述第二交换设备中端口的安全策略
S103
第一交换设备将第二交换设备中端口的安全策略，添加到第一交换设备的端口安全策略表中

图 1

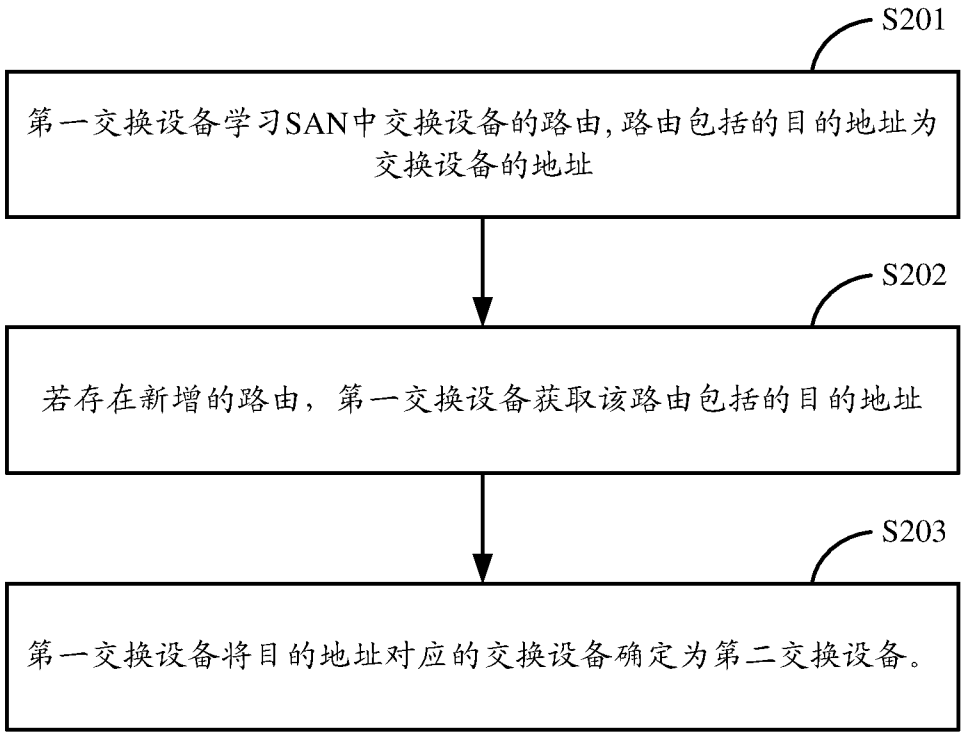
S201
第一交换设备学习SAN中交换设备的路由，路由包括的目的地址为交换设备的地址
S202
若存在新增的路由，第一交换设备获取该路由包括的目的地址
S203
第一交换设备将目的地址对应的交换设备确定为第二交换设备。

图 2

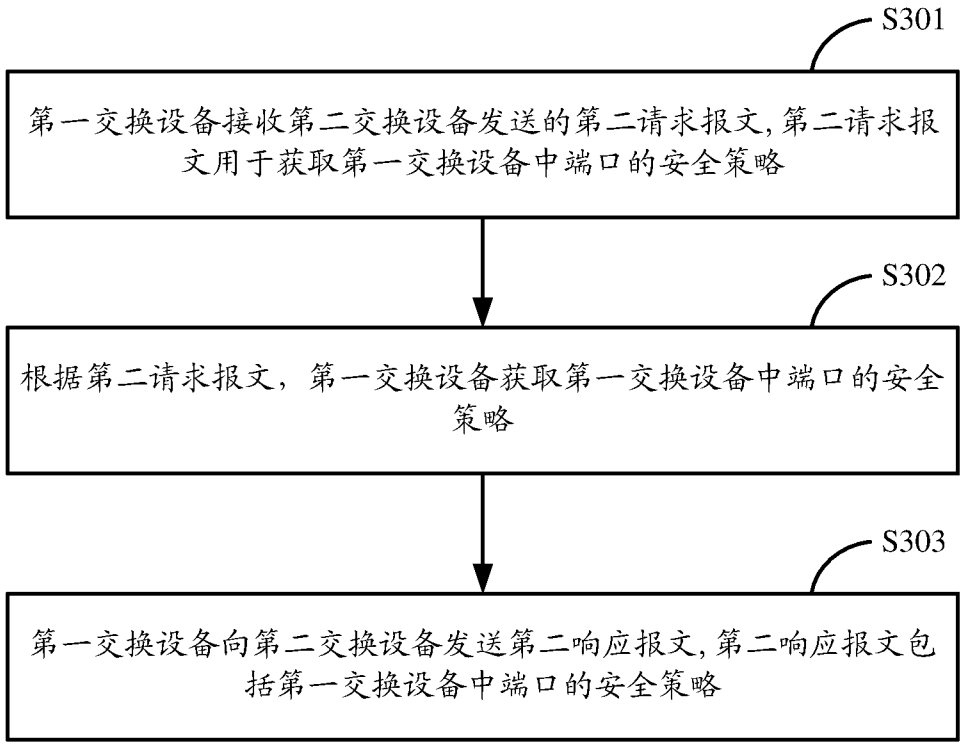
S301
第一交换设备接收第二交换设备发送的第二请求报文，第二请求报文用于获取第一交换设备中端口的安全策略
S302
根据第二请求报文，第一交换设备获取第一交换设备中端口的安全策略
S303
第一交换设备向第二交换设备发送第二响应报文，第二响应报文包括第一交换设备中端口的安全策略

图 3

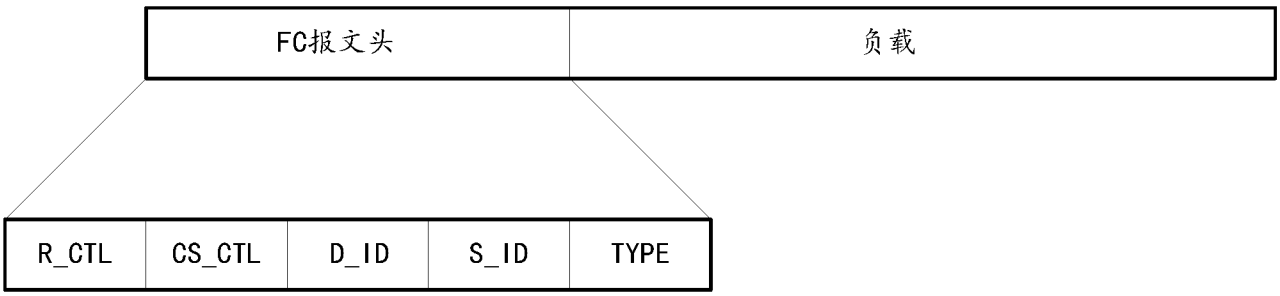
FC报文头
负载
R_CTL
CS_CTL
D_ID
S_ID
TYPE

图 4

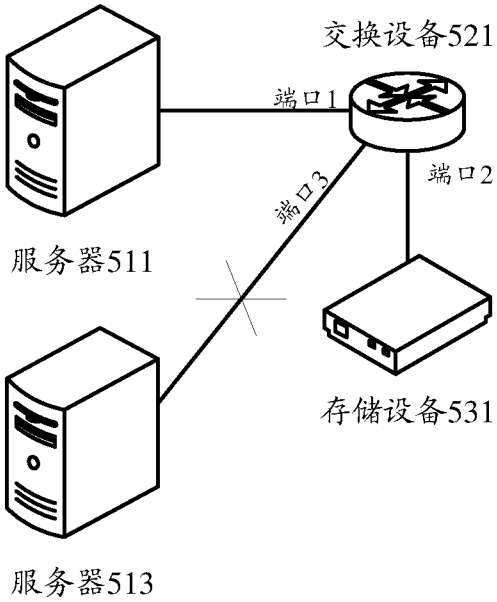
交换设备521
端口1
端口2
端口3
服务器511
存储设备531
服务器513

图 5A

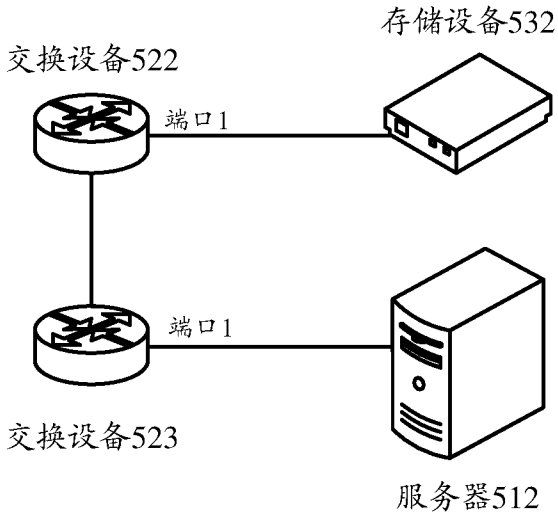
存储设备532
交换设备522
端口1
端口1
交换设备523
服务器512

图 5B

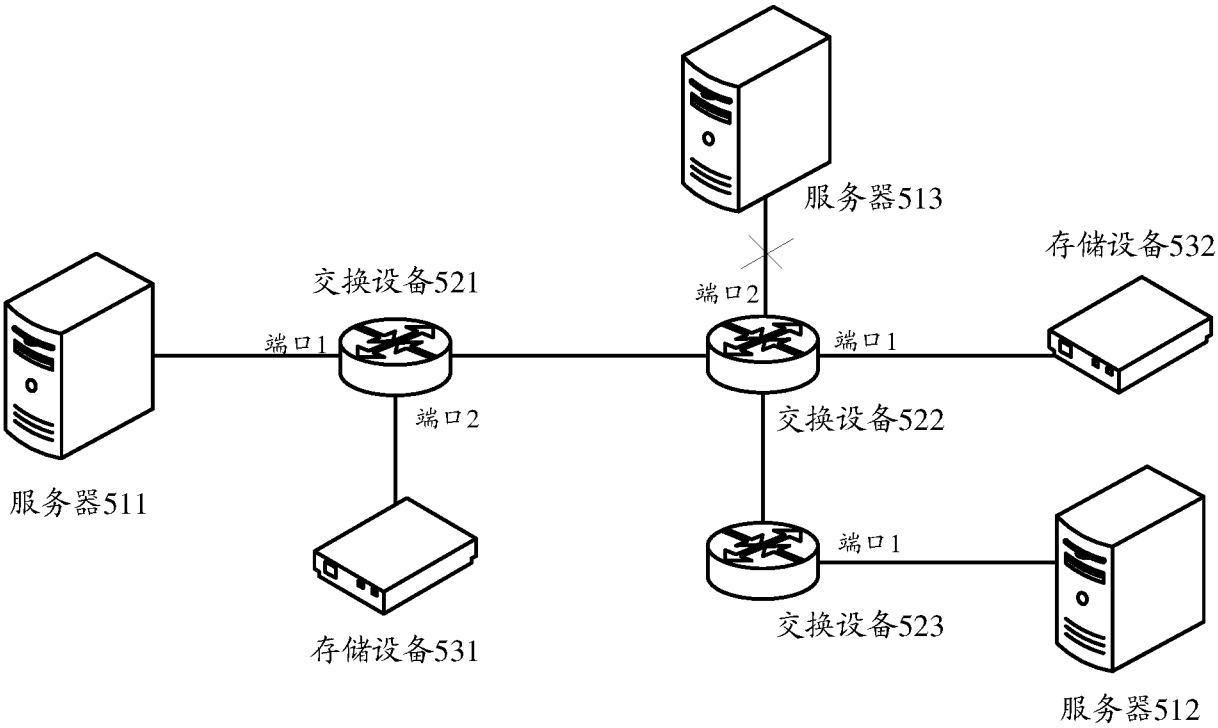
服务器513
存储设备532
交换设备521
端口2
端口1
端口1
端口2
交换设备522
服务器511
端口1
交换设备523
存储设备531
服务器512

图 5C

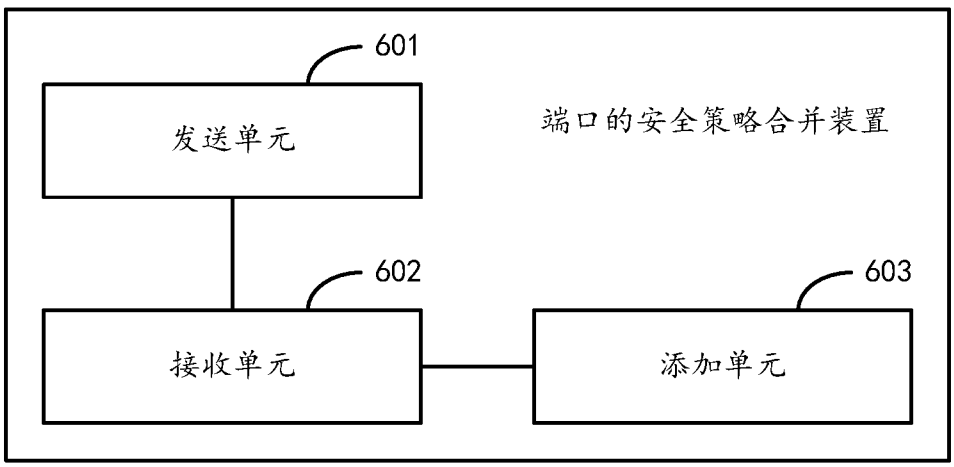
601
发送单元
端口的安全策略合并装置
602
603
接收单元
添加单元

图 6

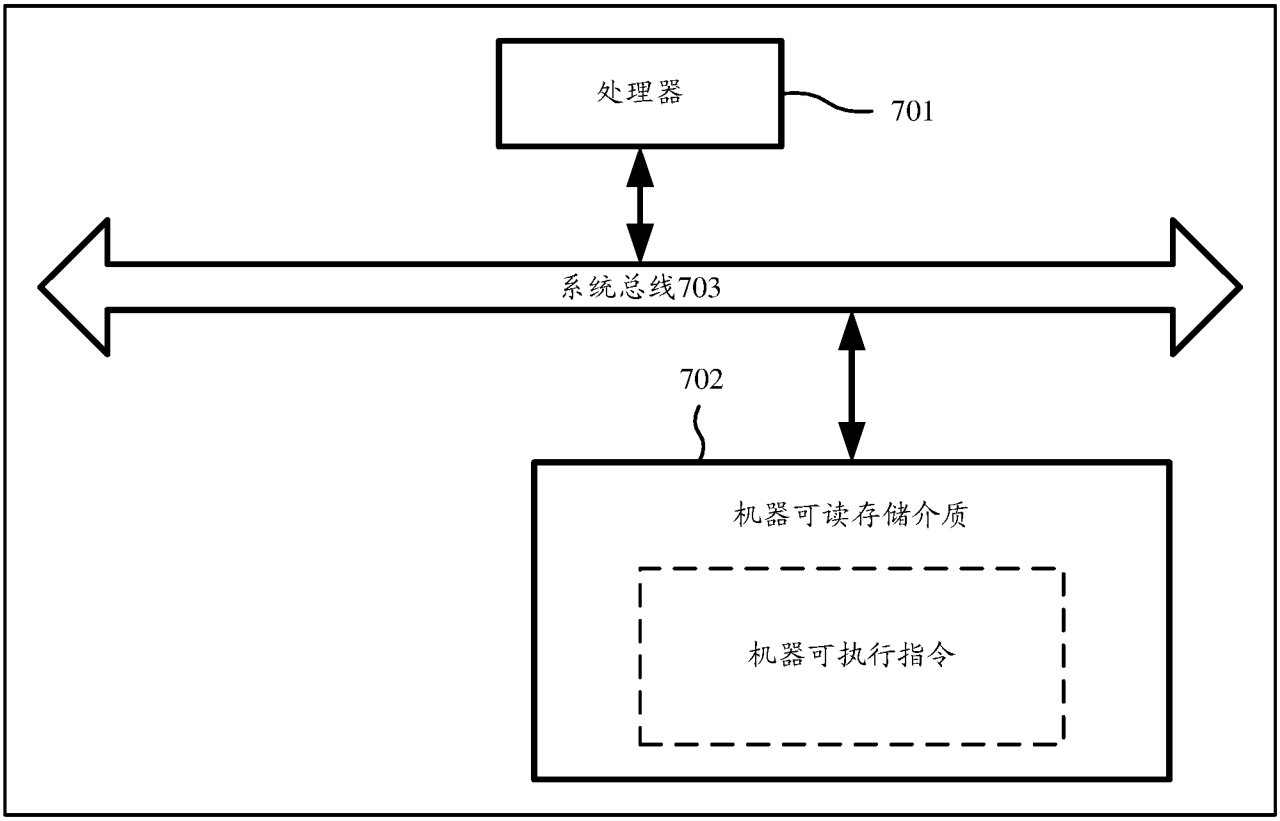

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/119996

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08(2006.01)i; H04L 12/24(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W; H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; VEN; CNKI; 3GPP: 交换, 设备, 交换机, 接入, 检测, 端口, 安全, 策略, 合并, 融合, 迁入, 迁移, 存储, 区域, 网络, 请求, 报文, 获取, 学习, SAN, FC, switch+, device+, access+, detect+, port+, security, policy, merg+, immigrat+, migrat+, storage, area, network, request, message+, packet+, gain+, get+, acquir+, learn+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 108259545 A (NEW H3C TECHNOLOGIES CO., LTD.) 06 July 2018 (2018-07-06) description, paragraphs 0002-0036	1-13
Y	CN 108092810 A (RUIJIE NETWORK CO., LTD.) 29 May 2018 (2018-05-29) description, paragraph 0061	1-13
A	US 2005091353 A1 (GOPISETTY, S.K. et al.) 28 April 2005 (2005-04-28) entire document	1-13
A	US 7817583 B2 (HEWLETT PACKARD DEVELOPMENT CO., L.P.) 19 October 2010 (2010-10-19) entire document	1-13

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 January 2020	**12 February 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/119996

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 108259545 A	06 July 2018	None	
CN 108092810 A	29 May 2018	None	
US 2005091353 A1	28 April 2005	None	
US 7817583 B2	19 October 2010	US 2004228290 A1	18 November 2004

国际检索报告

国际申请号
PCT/CN2019/119996

A. 主题的分类

H04L 29/08(2006.01)i; H04L 12/24(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; H04W; H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;VEN;CNKI;3GPP:交换，设备，交换机，接入，检测，端口，安全，策略，合并，融合，迁入，迁移，存储，区域，网络，请求，报文，获取，学习，SAN,FC,switch+, device+,access+,detect+,port+,security,policy,merg+,immigrat+,migrat+,storage,area,network,request,message+,packet+,gain+,get+,acquir+,learn+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 108259545 A (新华三技术有限公司) 2018年 7月 6日 (2018-07-06) 说明书第0002-0036段	1-13
Y	CN 108092810 A (锐捷网络股份有限公司) 2018年 5月 29日 (2018-05-29) 说明书第0061段	1-13
A	US 2005091353 A1 (GOPISETTY SANDEEP K等) 2005年 4月 28日 (2005-04-28) 全文	1-13
A	US 7817583 B2 (HEWLETT PACKARD DEVELOPMENT CO) 2010年 10月 19日 (2010-10-19) 全文	1-13

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 1月 17日	2020年 2月 12日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 李菲 电话号码 86-(010)-62412001

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/119996

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 108259545 A	2018年 7月 6日	无	
CN 108092810 A	2018年 5月 29日	无	
US 2005091353 A1	2005年 4月 28日	无	
US 7817583 B2	2010年 10月 19日	US 2004228290 A1	2004年 11月 18日