(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 107968825 B
(45)授权公告日 2021.06.29

(21)申请号 201711217639.5
(22)申请日 2017.11.28
(65)同一申请的已公布的文献号
申请公布号 CN 107968825 A
(43)申请公布日 2018.04.27
(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 黄珉
(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 29/08(2006.01)
H04L 12/801(2013.01)
H04L 29/06(2006.01)
(56)对比文件
US 2012303810 A1,2012.11.29
CN 101188558 A,2008.05.28
CN 103379118 A,2013.10.30
CN 101116052 A,2008.01.30
US 7055014 B1,2006.05.30
审查员 王一喆

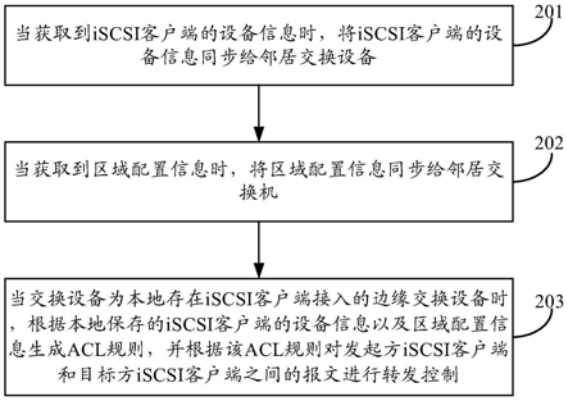
权利要求书3页 说明书9页 附图3页

(54)发明名称

一种报文转发控制方法及装置

(57)摘要

本发明提供一种报文转发控制方法及装置，所述方法包括：当获取到iSCSI客户端的设备信息时，将所述iSCSI客户端的设备信息同步给交换设备；当获取到区域配置信息时，将所述区域配置信息同步给邻居交换设备；当所述交换设备为本地存在iSCSI客户端接入的边缘交换设备时，根据本地保存的iSCSI客户端的设备信息以及区域配置信息生成访问控制列表ACL规则，并根据所述ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制。应用本发明可以实现iSCSI网络中硬件级的访问控制功能，提高存储设备的安全性，并节省网络和设备资源。



CN 107968825 B

1.一种报文转发控制方法,应用于互联网小型计算机系统接口iSCSI存储区域网络SAN网络中的交换设备,其特征在于,所述iSCSI SAN网络中各交换设备之间通过属于同一网段的接口建立有邻居关系,所述方法包括:

当获取到iSCSI客户端的设备信息时,将所述iSCSI客户端的设备信息同步给邻居交换设备;其中,所述iSCSI客户端的设备信息包括设备类型以及设备标识,所述设备类型包括发起方或目标方;

当获取到区域配置信息时,将所述区域配置信息同步给邻居交换设备;其中,所述区域配置信息包括属于同一区域的iSCSI客户端的设备标识;

当所述交换设备为本地存在iSCSI客户端接入的边缘交换设备时,根据本地保存的iSCSI客户端的设备信息以及区域配置信息生成访问控制列表ACL规则,并根据所述ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制;其中,本地保存的区域配置信息至少包括从邻居交换设备同步的区域配置信息。

2.根据权利要求1所述的方法,其特征在于,所述根据所述ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制,包括:

根据所述ACL规则,所述边缘交换设备允许同一区域内的发起方iSCSI客户端和目标方iSCSI客户端之间的报文交互,并禁止非同一区域内的发起方iSCSI客户端和目标方iSCSI客户端之间的报文交互。

3.根据权利要求2所述的方法,其特征在于,所述ACL规则包括:

禁止所有报文通过的第一类型ACL规则;和

允许同一区域内的发起方iSCSI客户端和目标方iSCSI客户端之间交互的报文通过的第二类型ACL规则,其中,同一区域内的发起方iSCSI客户端和目标方iSCSI客户端中,至少一方为本地接入且已注册的iSCSI客户端;

所述第二类型ACL规则的优先级高于第一类型ACL规则。

4.根据权利要求1所述的方法,其特征在于,

所述获取到的iSCSI客户端的设备信息包括:本地接入的iSCSI客户端发送的设备信息和/或邻居交换设备同步的iSCSI客户端的设备信息;

所述获取到的区域配置信息包括:本地接入的目标方iSCSI客户端发送的区域配置信息和/或邻居交换设备同步的区域配置信息和/或静态配置的区域配置信息。

5.根据权利要求4所述的方法,其特征在于,各交换设备之间通过链路状态协议数据单元LSP同步iSCSI客户端的设备信息以及区域配置信息。

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:

与邻居交换设备进行主备选举;

当本交换设备被选举为主交换设备时,周期性地向邻居交换设备发送通告报文;

当邻居交换设备被选举为主交换设备时,接收该邻居交换设备周期性发送的通告报文;

所述通告报文中携带有发送该报文的交换设备本地的所有LSP报文的标识信息;

接收到邻居交换设备发送的所述通告报文时,比较本地保存的LSP报文的标识信息与通告报文中携带的LSP报文的标识信息;

若两者不一致,则向该邻居交换设备请求通告报文中存在且本地不存在的LSP报文;或

者,向交换设备同步本地存在且通告报文中不存在的LSP报文。

7.一种报文转发控制装置,应用于互联网小型计算机系统接口iSCSI存储区域网络SAN网络中的交换设备,其特征在于,所述iSCSI SAN网络中各交换设备之间通过属于同一网段的接口建立有邻居关系,所述装置包括:

获取单元,用于获取iSCSI客户端的设备信息或区域配置信息;

同步单元,用于当所述获取单元获取到iSCSI客户端的设备信息时,将所述iSCSI客户端的设备信息同步给交换设备;其中,所述iSCSI客户端的设备信息包括设备类型以及设备标识,所述设备类型包括发起方或目标方;

所述同步单元,还用于当所述获取单元获取到区域配置信息时,将所述区域配置信息同步给邻居交换设备;其中,所述区域配置信息包括属于同一区域的iSCSI客户端的设备标识;

生成单元,用于当所述交换设备为本地存在iSCSI客户端接入的边缘交换设备时,根据本地保存的iSCSI客户端的设备信息以及区域配置信息生成访问控制列表ACL规则;其中,本地保存的区域配置信息至少包括从邻居交换设备同步的区域配置信息;

控制单元,用于根据所述ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制。

8.根据权利要求7所述的装置,其特征在于,

所述控制单元,具体用于根据所述ACL规则,所述边缘交换设备允许同一区域内的发起方iSCSI客户端和目标方iSCSI客户端之间的报文交互,并禁止非同一区域内的发起方iSCSI客户端和目标方iSCSI客户端之间的报文交互。

9.根据权利要求8所述的装置,其特征在于,所述ACL规则包括:

禁止所有报文通过的第一类型ACL规则;和

允许同一区域内的发起方iSCSI客户端和目标方iSCSI客户端之间交互的报文通过的第二类型ACL规则,其中,同一区域内的发起方iSCSI客户端和目标方iSCSI客户端中,至少一方为本地接入且已注册的iSCSI客户端;

所述第二类型ACL规则的优先级高于第一类型ACL规则。

10.根据权利要求7所述的装置,其特征在于,

所述获取到的iSCSI客户端的设备信息包括:本地接入的iSCSI客户端发送的设备信息和/或邻居交换设备同步的iSCSI客户端的设备信息;

所述获取到的区域配置信息包括:本地接入的目标方iSCSI客户端发送的区域配置信息和/或邻居交换设备同步的区域配置信息和/或静态配置的区域配置信息。

11.根据权利要求10所述的装置,其特征在于,各交换设备之间通过链路状态协议数据单元LSP同步iSCSI客户端的设备信息以及区域配置信息。

12.根据权利要求11所述的装置,其特征在于,所述装置还包括:

选举单元,用于与邻居交换设备进行主备选举;

所述同步单元,还用于当本交换设备被选举为主交换设备时,周期性地向邻居交换设备发送通告报文;

所述同步单元,还用于当邻居交换设备被选举为主交换设备时,接收该邻居交换设备周期性地发送的通告报文;其中,所述通告报文中携带有发送该报文的交换设备本地的所

有LSP报文的标识信息；

更新单元，用于当所述同步单元接收到邻居交换设备发送的所述通告报文时，比较本地保存的LSP报文的标识信息与通告报文中携带的LSP报文的标识信息；若两者不一致，则向该邻居交换设备请求通告报文中存在且本地不存在的LSP报文；或者，向交换设备同步本地存在且通告报文中不存在的LSP报文。

一种报文转发控制方法及装置

技术领域

[0001] 本发明涉及网络通信技术领域,尤其涉及一种报文转发控制方法及装置。

背景技术

[0002] iSCSI(Internet Small Computer System Interface,互联网小型计算机系统接口)是由IETF(The Internet Engineering Task Force,国际互联网工程任务组)开发的网络存储标准,目的是为了用IP(Internet Protocol,互联网协议)协议将存储设备连接在一起。由于IP网络的广泛应用,因此iSCSI能够在LAN(Local Area Network,局域网)、WAN(Wide Area Network,广域网)甚至Internet上进行数据传送,使得数据的存储不再受地域的限制。

[0003] iSCSI协议(RFC3720)定义了在TCP(Transmission Control Protocol传输控制协议)/IP网络发送、接收block(数据块)级的存储数据的规则和方法。发送端将SCSI(Small Computer System Interface,小型计算机系统接口)命令和数据封装到TCP/IP包中再通过网络转发,接收端收到TCP/IP包之后,将其还原为SCSI命令和数据并执行相应处理,处理完成之后将返回的SCSI命令和数据封装到TCP/IP包中传送回发送端。

[0004] iSCSI采用Client(客户端)/Server(服务器)工作模式。Client方作为Initiator(发起)设备发起iSCSI会话,对应于服务器。Server作为Target(目标)设备接收iSCSI会话请求,对应于存储设备。

[0005] iSCSI可以在不改变现有IP网络的情况下很方便地搭建SAN(Storage Area Network,存储区域网络),对设备和网络要求低,搭建成本较传统的FC(Fibre Channel,光纤通道)SAN有很大的优势,逐渐成为中小企业的首选以及IP存储区域网络的主流技术。

[0006] 然而实践发现,与FC SAN相比,iSCSI技术在管理上相对薄弱,网络本质上是iSCSI协议报文的传输介质,对iSCSI协议报文没有感知。Initiator和Target设备之间没有有效的访问控制手段,存储设备接入到网络后,只要路由可达,任何设备都可以向存储设备发起连接,这增加了存储设备的安全风险;另外,存储设备只能根据本地的策略来处理服务器的iSCSI请求,大量无效的iSCSI请求不仅会增加存储设备的负担,也占用了网络的带宽,对设备和网络都造成资源的浪费。

发明内容

[0007] 本发明提供一种报文转发控制方法及装置,以解决现有iSCSI网络中存储设备安全风险高,以及无效的iSCSI请求增加存储设备的负担,造成设备和网络资源浪费的问题。

[0008] 根据本发明实施例的第一方面,提供一种报文转发控制方法,应用于iSCSI SAN网络中的交换设备,所述iSCSI SAN网络中各交换设备之间通过属于同一网段的接口建立有邻居关系,所述方法包括:

[0009] 当获取到iSCSI客户端的设备信息时,将所述iSCSI客户端的设备信息同步给邻居交换设备;其中,所述iSCSI客户端的设备信息包括设备类型以及设备标识,所述设备类型

包括发起方或目标方；

[0010] 当获取到区域配置信息时，将所述区域配置信息同步给邻居交换设备；其中，所述区域配置信息包括属于同一区域的iSCSI客户端的设备标识；

[0011] 当所述交换设备为本地存在iSCSI客户端接入的边缘交换设备时，根据本地保存的iSCSI客户端的设备信息以及区域配置信息生成访问控制列表ACL规则，并根据所述ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制。

[0012] 根据本发明实施例的第二方面，提供一种报文转发控制装置，应用于iSCSI SAN网络中的交换设备，所述iSCSI SAN网络中各交换设备之间通过属于同一网段的接口建立有邻居关系，所述装置包括：

[0013] 获取单元，用于获取iSCSI客户端的设备信息或区域配置信息；

[0014] 同步单元，用于当所述获取单元获取到iSCSI客户端的设备信息时，将所述iSCSI客户端的设备信息同步给交换设备；其中，所述iSCSI客户端的设备信息包括设备类型以及设备标识，所述设备类型包括发起方或目标方；

[0015] 所述同步单元，还用于当所述获取单元获取到区域配置信息时，将所述区域配置信息同步给邻居交换设备；其中，所述区域配置信息包括属于同一区域的iSCSI客户端的设备标识；

[0016] 生成单元，用于当所述交换设备为本地存在iSCSI客户端接入的边缘交换设备时，根据本地保存的iSCSI客户端的设备信息以及区域配置信息生成访问控制列表ACL规则；

[0017] 控制单元，用于根据所述ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制。

[0018] 应用本发明实施例，当获取到iSCSI客户端的设备信息时，将iSCSI客户端的设备信息同步给邻居交换设备；当获取到区域配置信息时，将区域配置信息同步给邻居交换设备，进而，边缘交换设备根据本地保存的iSCSI客户端的设备信息以及区域配置信息生成访问控制列表ACL规则，并根据ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制，实现了iSCSI网络中硬件级的访问控制功能，提高了存储设备的安全性，并节省了网络和设备资源。

附图说明

[0019] 图1是本发明实施例提供的一种报文转发控制系统的架构示意图；

[0020] 图2是本发明实施例提供的一种报文转发控制方法的流程示意图；

[0021] 图3是本发明实施例提供的一种具体应用场景的架构示意图；

[0022] 图4是本发明实施例提供的一种报文转发控制装置的结构示意图；

[0023] 图5是本发明实施例提供的另一种报文转发控制装置的结构示意图。

具体实施方式

[0024] 为了使本技术领域的人员更好地理解本发明实施例中的技术方案，下面先对本发明实施例适用的系统架构进行简单说明。

[0025] 请参见图1，为本发明实施例提供的一种报文转发控制系统的架构示意图，如图1所示，在该报文转发控制系统中，各交换设备均使能iSCSI功能；其中：

[0026] 本地存在iSCSI客户端接入的交换设备称为边缘交换设备，本地不存在iSCSI客户端接入的交换设备称为中间交换设备。其中，iSCSI客户端的类型包括发起方和目标方，为了后续方便描述，将发起方iSCSI客户端记为Initiator设备，将目标方iSCSI客户端记为Target设备。

[0027] iSCSI客户端向接入的边缘交换设备注册，边缘交换设备上建立设备信息数据库。各交换设备通过属于同一网段的接口建立邻居关系，并在邻居之间相互交换设备信息数据库的信息，以保证各交换设备上设备信息数据库保持一致。

[0028] 为了使本发明实施例的上述目的、特征和优点能够更加明显易懂，下面结合附图对本发明实施例中技术方案作进一步详细的说明。

[0029] 请参见图2，为本发明实施例提供的一种报文转发控制方法的流程示意图，其中，该报文转发控制方法可以应用于图1中的交换设备，如图2所示，该报文转发控制方法可以包括：

[0030] 步骤201、当获取到iSCSI客户端的设备信息时，将iSCSI客户端的设备信息同步给邻居交换设备。

[0031] 本发明实施例中，当Initiator设备或Target设备初次上线时，需要向接入的边缘交换设备进行注册，在注册过程中，Initiator设备或Target设备可以向边缘交换设备上报自身的设备信息。

[0032] 其中，iSCSI客户端的设备信息可以包括设备类型、如发起方或目标方，以及设备标识(iSCSI ID)。

[0033] 边缘交换设备接收到Initiator设备或Target设备发送的iSCSI客户端的设备信息时，可以将接收到的iSCSI客户端的设备信息同步给邻居交换设备；邻居交换设备接收到该边缘交换设备同步的iSCSI客户端的设备信息时，可以判断自身是否存在其它邻居交换设备(即除了该边缘交换设备之外的其它邻居交换设备)，若存在，则该邻居交换设备需要进一步将该边缘交换设备同步过来的iSCSI客户端的设备信息同步给其它邻居交换设备。

[0034] 步骤202、当获取到区域配置信息时，将区域配置信息同步给邻居交换设备。

[0035] 本发明实施例中，Target设备向接入的边缘交换设备注册之后，还可以向该边缘交换设备上报区域配置信息，该区域配置信息包括属于同一区域的iSCSI客户端的设备标识(即iSCSI ID)。

[0036] 其中，该区域配置信息可以由Target设备根据本地访问策略生成，并上报给边缘交换设备。

[0037] 例如，假设Target A本地访问策略为允许Initiator A和Initiator B访问，则Target A生成的区域配置信息可以为Zone1(Target A,Initiator A,Initiator B)，即Target A,Initiator A,Initiator B均属于Zone(区域)1。

[0038] 本发明实施例中，边缘交换设备接收到本地接入的Target设备发送的区域配置信息时，边缘交换设备可以将该区域配置信息同步给邻居交换设备；邻居交换设备接收到该边缘交换设备同步的区域配置信息时，可以判断自身是否存在其它邻居交换设备(即除了该边缘交换设备之外的其它邻居交换设备)，若存在，则该邻居交换设备需要进一步将该边缘交换设备同步过来的区域配置信息同步给其它邻居交换设备。

[0039] 此外，在本发明实施例中，交换设备之间进行iSCSI客户端的设备信息以及区域配

置信息的同步时，不会将iSCSI客户端的设备信息以及区域配置信息同步给发送该iSCSI客户端的设备信息以及区域配置信息的交换设备。

[0040] 应该认识到，上述通过Target设备生成区域配置信息并上报给边缘交换设备仅仅是本发明实施例中交换设备获取区域配置信息的一种具体实现方式，而不是对本发明保护范围的限定，在本发明实施例中，区域配置信息也可以直接配置在交换设备上，例如，可以由用户(如管理员)直接将区域配置信息配置在边缘交换设备上，其具体实现在此不做赘述。

[0041] 步骤203、当交换设备为本地存在iSCSI客户端接入的边缘交换设备时，根据本地保存的iSCSI客户端的设备信息以及区域配置信息生成ACL规则，并根据该ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制。

[0042] 本发明实施例中，iSCSI SAN网络中各交换设备完成iSCSI客户端的设备信息以及区域配置信息的同步之后，边缘交换设备可以根据本地保存的iSCSI客户端的设备信息(包括Initiator设备或Target设备发送的iSCSI客户端的设备信息，或/和，邻居交换设备同步的iSCSI客户端的设备信息)和区域配置信息(包括Target设备发送的区域配置信息，或/和，邻居交换设备同步的区域配置信息，或/和，静态配置的区域配置信息)生成ACL(Access Control List，访问控制列表)规则，并根据该ACL规则进行报文转发控制。

[0043] 其中，该ACL规则用于指示该边缘交换设备允许同一区域内的Initiator设备和Target设备之间的报文交互，并禁止非同一区域内的Initiator设备和Target设备之间的报文交互。

[0044] 可见，在图2所示的方法流程中，边缘交换设备对iSCSI客户端提供接入服务和注册服务，以此获取iSCSI客户端的设备信息、区域配置信息，并且各交换设备之间同步iSCSI客户端的设备信息和区域配置信息，进而，边缘交换设备可以根据本地保存的iSCSI客户端的设备信息和区域配置信息生成对应的ACL规则，并根据该ACL规则控制报文转发，其中，ACL规则需要下发至转发芯片，由转发芯片根据ACL规则进行报文转发控制，因此，实现了iSCSI网络中硬件级的访问控制功能，提高了存储设备的安全性，并节省了网络和设备资源。

[0045] 在本发明其中一个实施例中，为了实现边缘交换设备允许同一区域内的Initiator设备和Target设备之间的报文交互，并禁止非同一区域内的Initiator设备和Target设备之间的报文交互，该边缘交换设备可以生成如下的ACL规则：

[0046] 第一类型ACL规则：指示交换设备禁止所有报文通过；

[0047] 第二类型ACL规则：指示交换设备允许同一区域内的Initiator设备和Target设备之间交互的报文通过，且同一区域内有交互需求的Initiator设备和Target设备中，至少一方为本地接入且已注册的iSCSI客户端；

[0048] 其中，第二类型ACL规则的优先级高于第一类型ACL规则。

[0049] 在该实施例中，边缘交换设备可以将该第一类型ACL规则和第二类型规则下发至Initiator设备或Target设备在该交换设备上的注册端口所在的VLAN(Virtual Local Area Network，虚拟局域网)。

[0050] 相应地，当边缘交换设备从Initiator设备或Target设备在该交换机上的注册端口接收到报文，或者，需要从Initiator设备或Target设备在该交换机上的注册端口发送报

文时,可以根据该报文查询该注册端口所在VLAN内的第二类型ACL规则,以确定是否存在匹配的第二类型ACL规则,若存在,则允许转发该报文;否则,根据该报文查询该VLAN内的第一类型ACL规则,并禁止转发该报文。

[0051] 进一步地,在本发明实施例中,为了保证各交换设备上保存的iSCSI客户端的设备信息以及区域配置信息能够保持一致,交换设备之间可以周期性交互自身保存的iSCSI客户端的设备信息以及区域配置信息。

[0052] 以交换设备之间通过LSP(Link State Protocol Data Unit,链路状态协议数据单元)报文实现iSCSI客户端的设备信息以及区域配置信息的同步为例。

[0053] 上述报文转发控制方法还可以包括:

[0054] 与邻居交换设备进行主备选举;

[0055] 当所述交换设备被选举为主交换设备时,周期性地向邻居交换设备发送通告报文;

[0056] 当邻居交换设备被选举为主交换设备时,接收该邻居交换设备周期性发送的通告报文;

[0057] 其中,通告报文携带有发送该报文的交换设备本地保存的所有LSP报文的标识信息。

[0058] 对于接收到通告报文的交换设备,比较本地的LSP报文的标识信息与通告报文中携带的LSP报文的标识信息;

[0059] 若两者不一致,则向该邻居交换设备请求通告报文中存在且本地不存在的LSP报文;或者,向交换设备同步本地存在且通告报文中不存在的LSP报文。

[0060] 在该实施例中,邻居交换设备之间可以进行主从交换设备竞选,其具体的竞选方式可以参见现有主从竞选方式,本发明实施例在此不做赘述。

[0061] 在该实施例中,主交换设备可以周期性地向从交换设备发送通告报文,该通告报文中携带有主交换设备本地所有的LSP报文的标识信息。

[0062] 从交换设备接收到主交换设备发送的通告报文时,可以比较本地的LSP报文的标识信息与通告报文中携带的LSP报文的标识信息;

[0063] 若该通告报文中的LSP报文的标识信息中包括本地不存在的LSP报文(本文中称为第一类型目标LSP报文)的标识信息,则从交换设备可以向主交换设备请求该第一类型目标LSP报文;

[0064] 若本地LSP报文的标识信息中包括通告报文中不存在的LSP报文(本文中称为第二类型目标LSP报文)的标识信息,则从交换设备可以向主交换设备发送该第二类型目标LSP报文。

[0065] 为了使本领域技术人员更好地理解本发明实施例提供的技术方案,下面结合具体应用场景对本发明实施例提供的技术方案进行说明。

[0066] 请参见图3,为本发明实施例提供的一种具体应用场景的架构示意图,如图3所示,在该应用场景中,Switch(交换机)A和Switch C为边缘交换设备,Switch B为中间交换设备,Switch A为服务器I1和服务器I2的网关,Switch C为存储设备T1和存储设备T2的网关。Switch A、Switch B与Switch C三层路由可达;Switch A的G1/0/1和Switch B的G1/0/1属于一个网段,加入VLAN10;Switch B的G1/0/2和Switch C的G1/0/2属于一个网段,加入

VLAN20。

[0067] 基于图3所示的应用场景，本发明实施例提供的报文转发控制方案实现流程如下：

[0068] 1、Switch A和Switch B通过周期性地发送Hello报文，在各自的接口上建立邻居关系，并进行主从交换设备竞选；其中，假设Switch A被选为主交换设备。

[0069] 2、Switch B和Switch C通过周期性地发送Hello报文，在各自的接口上建立邻居关系，并进行主从交换设备竞选。假设Switch C被选为主交换设备。

[0070] 3、服务器I1和服务器I2向Switch A注册，上报iSCSI客户端的设备信息；其中，该iSCSI客户端的设备信息中包括服务器I1和服务器I2的设备类型(发起方)以及设备标识(假设服务器I1的设备标识为I1，服务器I2的设备标识为I2)；

[0071] 存储设备T1和存储设备T2向Switch C注册，上报iSCSI客户端的设备信息；其中，该iSCSI客户端的设备信息中包括存储设备T1和存储设备T2的设备类型(目标方)以及设备标识(假设存储设备T1的设备标识为T1，存储设备T2的设备标识为T2)。

[0072] 在该实施例中，Initiator设备向边缘交换设备注册后，还可以向边缘交换设备获取Target设备列表；同理，Target设备向边缘交换设备注册后，还可以向边缘交换设备获取Initiator设备列表。

[0073] 4、存储设备T1和存储设备T2根据本地访问策略生成区域配置信息，并向Switch C上报区域配置信息。

[0074] 在该实施例中，假设存储设备T1上配置的访问策略为允许服务器I1访问，存储设备T2上配置的访问策略为允许服务器I2访问，则存储设备T1可以将自身和服务器I1配置在同一个区域中(假设为Zone1)，存储设备T2可以将自身和服务器I2配置在同一个区域中(假设为Zone2)，进而，存储设备T1向Switch C上报的区域配置信息为Zone1(I1,T1)，存储设备T2向Switch C上报的区域配置信息为Zone2(I2,T2)。

[0075] 在该实施例中，存储设备T2还可以向Switch C删除区域配置，还可以向Switch C获取其它存储设备上报的区域配置信息。

[0076] 此外，服务器I1、服务器I2以及存储设备T1和存储设备T2还可以分别向Switch A和Switch C注册关心状态变化事件，从而，Switch A(Switch C)可以在发生设备注册、设备去注册、区域配置信息更新等事件时通知服务器I1和服务器I2(存储设备T1和存储设备T2)。

[0077] 5、Switch A通过LSP报文向Switch B同步本地的iSCSI客户端的设备信息，Switch B接收到Switch A同步的LSP报文后，将其同步给Switch C；

[0078] Switch C通过LSP报文向Switch B同步本地的iSCSI客户端的设备信息以及区域配置信息，Switch B接收到Switch C同步的LSP报文后，将其同步给Switch A。

[0079] 6、Switch A每隔10S向Switch B发送CSNP(Complete Sequence Number PDU，全时序协议数据单元)报文，该CSNP报文中携带有Switch A本地所有LSP报文的标识信息，Switch B接收到Switch A发送的CSNP报文时，比较Switch B本地的LSP报文的标识信息和CSNP报文中包括的LSP报文的标识信息，若CSNP报文中包括本地不存在的LSP报文，则通过PSNP(Partial Sequence Number PDU，部分时序协议数据单元)报文向Switch A请求该部分LSP报文；若本地包括CSNP报文中不存在的LSP报文，则将该部分LSP报文同步给Switch A；

[0080] Switch C每隔10S向Switch B发送CSNP报文，该CSNP报文中携带有Switch C本地所有LSP报文的标识信息，Switch B接收到Switch C发送的CSNP报文时，比较Switch B本地的LSP报文的标识信息和CSNP报文中包括的LSP报文的标识信息，若CSNP报文中包括本地不存在的LSP报文，则通过PSNP报文向Switch C请求该部分LSP报文；若本地包括CSNP报文中不存在的LSP报文，则将该部分LSP报文同步给Switch C。

[0081] 7、Switch A根据本地的iSCSI客户端的设备信息以及区域配置信息生成如下ACL规则，并下发至服务器I1和服务器I2的在本交换设备的注册端口所在VLAN(即VLAN 10)：

[0082] a)、禁止所有报文通过(默认ACL规则)；

[0083] b)、允许源设备为服务器I1、目的设备为存储设备T1的报文通过；

[0084] c)、允许源设备为存储设备T1、目的设备为服务器I1的报文通过；

[0085] d)、允许源设备为服务器I2、目的设备为存储设备T2的报文通过；

[0086] e)、允许源设备为存储设备T2、目的设备为服务器I2的报文通过；

[0087] 其中，默认ACL规则的优先级低于其他ACL规则的优先级。

[0088] 在该实施例中，当Switch A从VLAN 10的入端口接收到报文，或者，接收到需要通过VLAN 10的出端口转发的报文时，先根据该报文查询ACL规则b～e，确定是否匹配的ACL规则，若匹配，则允许报文通过；否则，根据该报文查询ACL规则a，发现匹配，丢弃该报文。

[0089] 8、Switch C根据本地的iSCSI客户端的设备信息以及区域配置信息生成如下ACL规则，并下发至服务器T1和服务器T2的在本交换设备的注册端口所在VLAN(即VLAN 20)：

[0090] a)、禁止所有报文通过(默认ACL规则)；

[0091] b)、允许源设备为存储设备T1、目的设备为服务器I1的报文通过；

[0092] c)、允许源设备为服务器I1、目的设备为存储设备T1的报文通过；

[0093] d)、允许源设备为存储设备T2、目的设备为服务器I2的报文通过；

[0094] e)、允许源设备为服务器I2、目的设备为存储设备T2的报文通过；

[0095] 其中，默认ACL规则的优先级低于其他ACL规则的优先级。

[0096] 在该实施例中，当Switch C从VLAN 20的入端口接收到报文，或者，接收到需要通过VLAN 20的出端口转发的报文时，先根据该报文查询ACL规则b～e，确定是否匹配的ACL规则，若匹配，则允许报文通过；否则，根据该报文查询ACL规则a，发现匹配，丢弃该报文。

[0097] 其中，中间交换设备(如Switch B)不需要进行上述ACL规则下发处理。

[0098] 通过以上描述可以看出，在本发明实施例提供的技术方案中，当获取到iSCSI客户端的设备信息时，将iSCSI客户端的设备信息同步给邻居交换设备；当获取到区域配置信息时，将区域配置信息同步给邻居交换设备，进而，边缘交换设备根据本地保存的iSCSI客户端的设备信息以及区域配置信息生成访问控制列表ACL规则，并根据ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制，实现了iSCSI网络中硬件级的访问控制功能，提高了存储设备的安全性，并节省了网络和设备资源。

[0099] 请参见图4，为本发明实施例提供的一种报文转发控制装置的结构示意图，其中，所述装置可以应用于上述方法实施例中的交换设备，如图4所示，该报文转发控制装置可以包括：

[0100] 获取单元410，用于获取iSCSI客户端的设备信息或区域配置信息；

[0101] 同步单元420，用于当所述获取单元410获取到iSCSI客户端的设备信息时，将所述

iSCSI客户端的设备信息同步给交换设备;其中,所述iSCSI客户端的设备信息包括设备类型以及设备标识,所述设备类型包括发起方或目标方;

[0102] 所述同步单元420,还用于当所述获取单元410获取到区域配置信息时,将所述区域配置信息同步给邻居交换设备;其中,所述区域配置信息包括属于同一区域的iSCSI客户端的设备标识;

[0103] 生成单元430,用于当所述交换设备为本地存在iSCSI客户端接入的边缘交换设备时,根据本地保存的iSCSI客户端的设备信息以及区域配置信息生成访问控制列表ACL规则;

[0104] 控制单元440,用于根据所述ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制。

[0105] 在可选实施例中,所述控制单元440,具体用于根据所述ACL规则,所述边缘交换设备允许同一区域内的发起方iSCSI客户端和目标方iSCSI客户端之间的报文交互,并禁止非同一区域内的发起方iSCSI客户端和目标方iSCSI客户端之间的报文交互。

[0106] 在可选实施例中,所述ACL规则包括:

[0107] 禁止所有报文通过的第一类型ACL规则;和

[0108] 允许同一区域内的发起方iSCSI客户端和目标方iSCSI客户端之间交互的报文通过的第二类型ACL规则,其中,同一区域内的发起方iSCSI客户端和目标方iSCSI客户端中,至少一方为本地接入且已注册的iSCSI客户端;

[0109] 所述第二类型ACL规则的优先级高于第一类型ACL规则。

[0110] 在可选实施例中,所述获取到的iSCSI客户端的设备信息包括:本地接入的iSCSI客户端发送的设备信息和/或邻居交换设备同步的iSCSI客户端的设备信息;

[0111] 所述获取到的区域配置信息包括:本地接入的目标方iSCSI客户端发送的区域配置信息和/或邻居交换设备同步的区域配置信息和/或静态配置的区域配置信息。

[0112] 在可选实施例中,各交换设备之间通过链路状态协议数据单元LSP同步iSCSI客户端的设备信息以及区域配置信息。

[0113] 请一并参见图5,为本发明实施例提供的另一种报文转发控制装置的结构示意图,如图5所示,在图4所示报文转发控制装置的基础上,图5所示的报文转发控制装置还包括:

[0114] 选举单元450,用于与邻居交换设备进行主备选举;

[0115] 所述同步单元420,还用于当本交换设备被选举为主交换设备时,周期性地向邻居交换设备发送通告报文;

[0116] 所述同步单元420,还用于当邻居交换设备被选举为主交换设备时,接收该邻居交换设备周期性地发送的通告报文;其中,所述通告报文中携带有发送该报文的交换设备本地的所有LSP报文的标识信息;

[0117] 更新单元460,用于当所述同步单元420接收到邻居交换设备发送的所述通告报文时,比较本地保存的LSP报文的标识信息与通告报文中携带的LSP报文的标识信息;若两者不一致,则向该邻居交换设备请求通告报文中存在且本地不存在的LSP报文;或者,向交换设备同步本地存在且通告报文中不存在的LSP报文。

[0118] 上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程,在此不再赘述。

[0119] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本发明方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0120] 由上述实施例可见，当获取到iSCSI客户端的设备信息时，将iSCSI客户端的设备信息同步给邻居交换设备；当获取到区域配置信息时，将区域配置信息同步给邻居交换设备，进而，边缘交换设备根据本地保存的iSCSI客户端的设备信息以及区域配置信息生成访问控制列表ACL规则，并根据ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制，实现了iSCSI网络中硬件级的访问控制功能，提高了存储设备的安全性，并节省了网络和设备资源。

[0121] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本发明的其它实施方案。本申请旨在涵盖本发明的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本发明的一般性原理并包括本发明未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本发明的真正范围和精神由下面的权利要求指出。

[0122] 应当理解的是，本发明并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本发明的范围仅由所附的权利要求来限制。

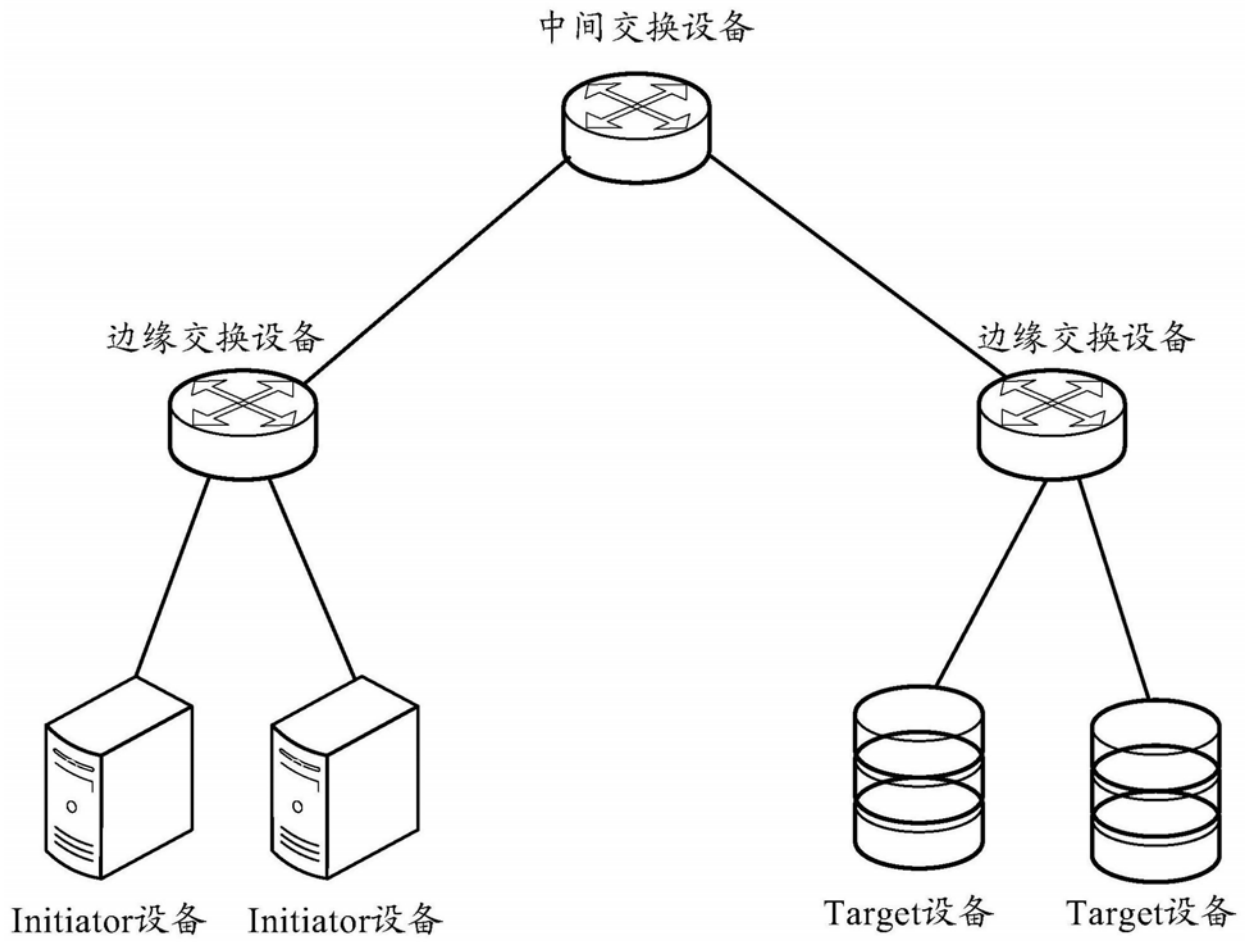

中间交换设备
边缘交换设备
边缘交换设备
Initiator设备
Initiator设备
Target设备
Target设备

图1

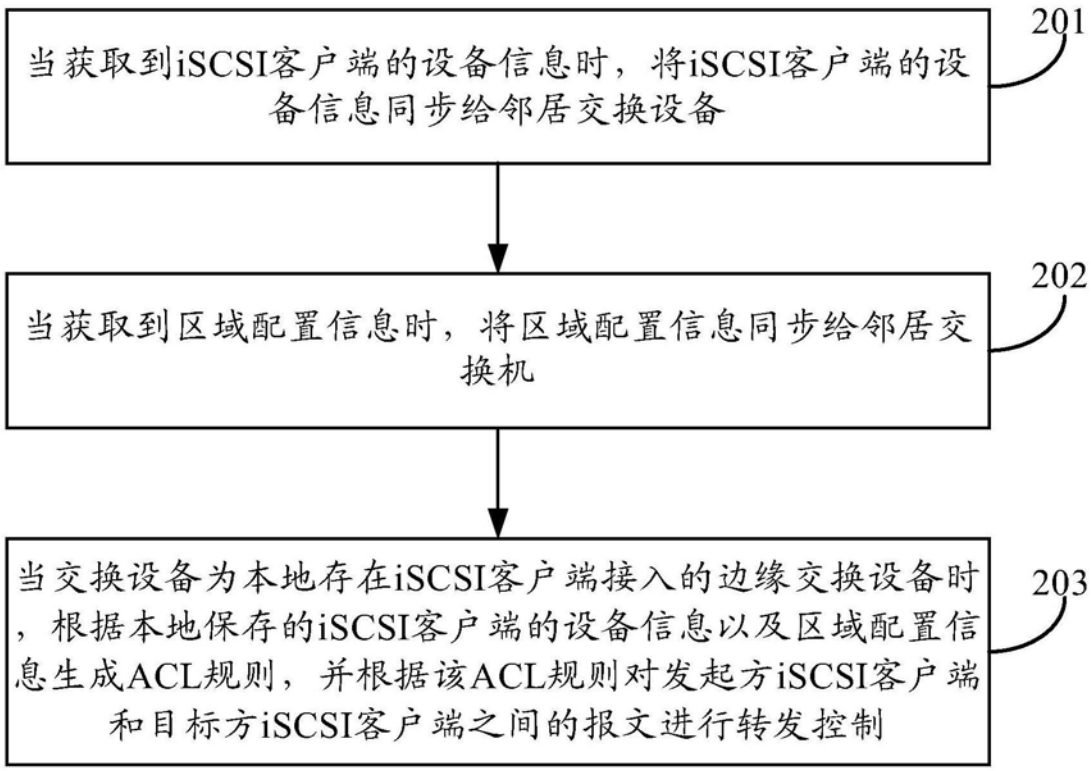

当获取到iSCSI客户端的设备信息时，将iSCSI客户端的设备信息同步给邻居交换设备
201
当获取到区域配置信息时，将区域配置信息同步给邻居交换机
202
当交换设备为本地存在iSCSI客户端接入的边缘交换设备时，根据本地保存的iSCSI客户端的设备信息以及区域配置信息生成ACL规则，并根据该ACL规则对发起方iSCSI客户端和目标方iSCSI客户端之间的报文进行转发控制
203

图2

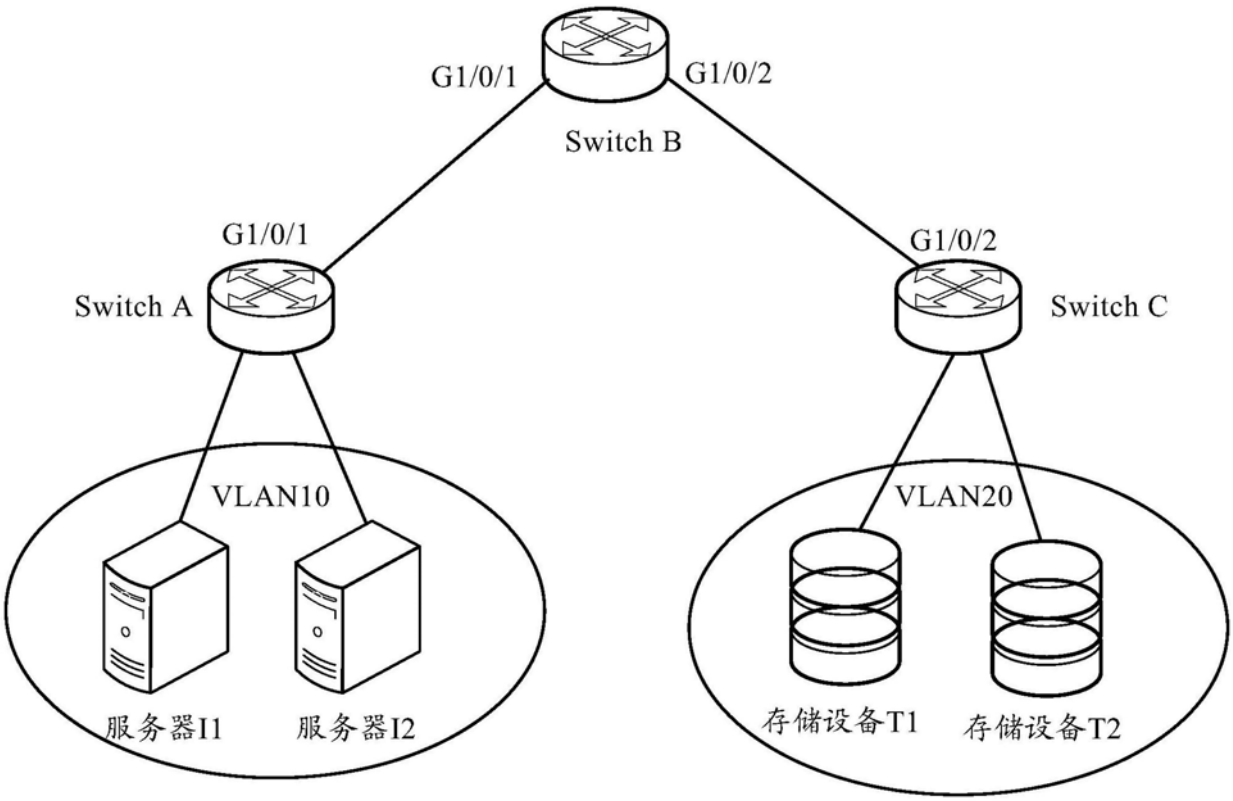

G1/0/1
G1/0/2
Switch B
G1/0/1
Switch A
G1/0/2
Switch C
VLAN10
VLAN20
服务器I1
服务器I2
存储设备T1
存储设备T2

图3

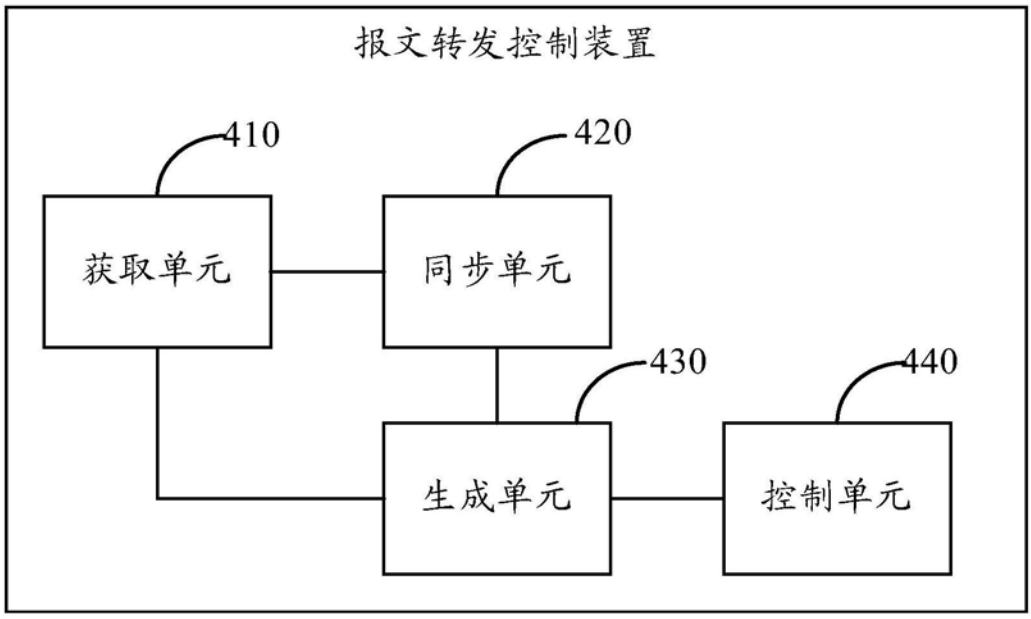

报文转发控制装置
410
420
获取单元
同步单元
430
440
生成单元
控制单元

图4

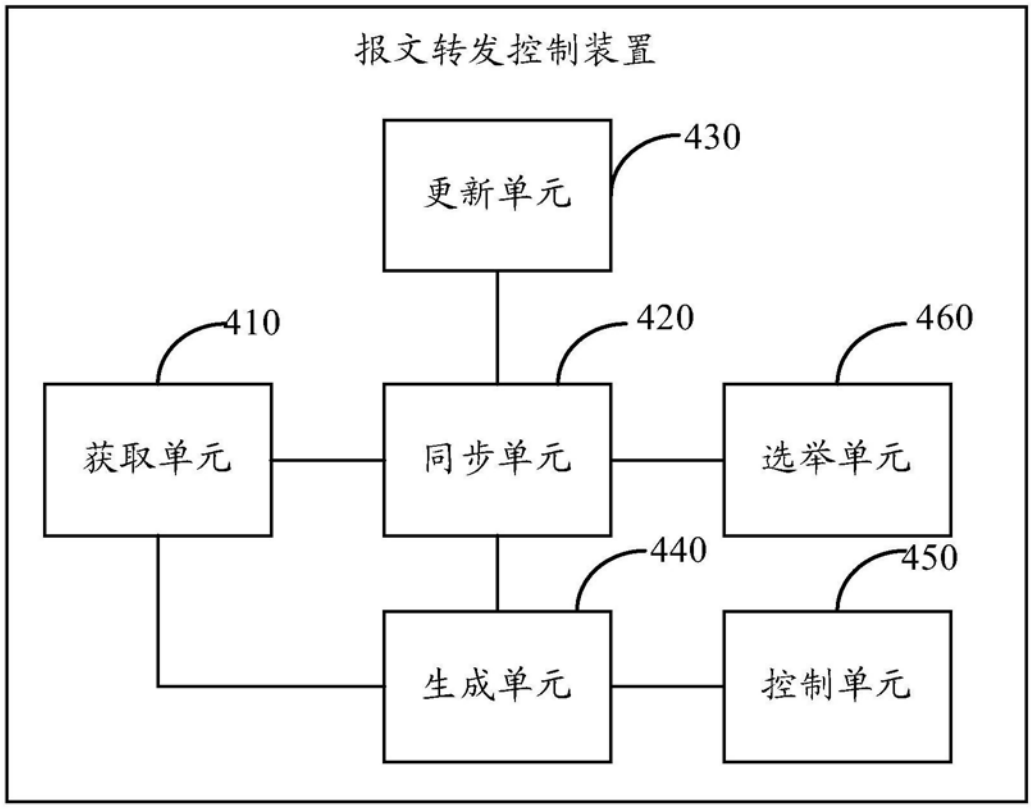

报文转发控制装置
更新单元
430
410
420
460
获取单元
同步单元
选举单元
440
450
生成单元
控制单元

图5