



(12) 发明专利

(10) 授权公告号 CN 103621028 B

(45) 授权公告日 2016. 05. 11

(21) 申请号 201280018455. 5

H04L 12/931(2013. 01)

(22) 申请日 2012. 04. 06

H04L 12/44(2006. 01)

(30) 优先权数据

2011-091105 2011. 04. 15 JP

(56) 对比文件

(85) PCT国际申请进入国家阶段日

2013. 10. 14

US 2008/0189769 A1, 2008. 08. 07,

(86) PCT国际申请的申请数据

PCT/JP2012/059471 2012. 04. 06

WO 2011/030490 A1, 2011. 03. 17,

(87) PCT国际申请的公布数据

W02012/141086 JA 2012. 10. 18

CN 101390342 A, 2009. 03. 18,

匿名 . OPENFLOW SWITCH SPECIFICATION

(73) 专利权人 日本电气株式会社

VERSION 1. 1. 0 IMPLEMENTED. 《http://
www. openflow. org/documents/
openflow-spec-v1. 1. 0. pdf1》. 2011, 第 1-56 页.

地址 日本东京都

审查员 孟娜

(72) 发明人 川本雅也

(74) 专利代理机构 北京市金杜律师事务所

11256

代理人 王茂华 庞淑敏

(51) Int. Cl.

H04L 12/773(2013. 01)

权利要求书2页 说明书8页 附图7页

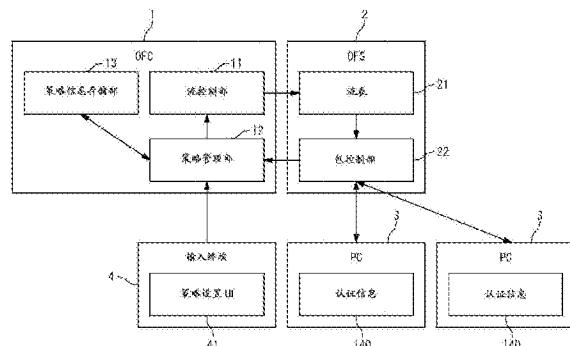
(54) 发明名称

控制网络访问策略的计算机系统、控制器和方法

(57) 摘要

根据本发明的计算机系统包括：控制器以及交换机，所述交换机针对符合由所述控制器设置的流条目的接收包，实施中继操作，所述中继操作使用所述流条目来调节。所述交换机向所述控制器传输不符合由所述交换机设置的流条目的接收包。所述控制器查询包括在所述接收包中的认证信息且对所述接收包进行认证。在被确定为有效的所述接收包的报头信息之中，所述控制器将所述交换机设置为调节如下包的中继操作的流条目，所述包包括识别所述接收包的传输源的信息。因而，使得开放流协议环境的计算机系统中的网络访问策略控制变得容易。

CN 103621028 B



1. 一种计算机系统,包括:

控制器;以及

交换机,所述交换机被配置为针对符合由所述控制器设置的流条目的接收包执行中继操作,所述中继操作由所述流条目限定,

其中所述交换机被配置为向所述控制器传输不符合在所述交换机中设置的所述流条目的所述接收包,

其中所述控制器被配置为参考包括在所述接收包中的认证信息以对所述接收包进行认证,且在所述交换机中设置用于限定包的所述中继操作的所述流条目,所述流条目包括位于被确定为有效的所述接收包的报头信息中且用于识别所述接收包的源的信息,

其中所述控制器包括其中记录有用于限定中继操作策略的策略信息的存储设备,且被配置为在所述交换机中设置符合与包括在被确定为有效的所述接收包中的认证信息对应的所述策略信息的所述流条目,

其中所述认证信息包括用于识别所述策略信息的策略 ID 和在认证中使用的第一认证 ID,

其中将用于识别所述策略信息的所述策略 ID 与第二认证 ID 相关的所述策略信息被记录在所述存储设备中;以及

其中所述控制器被配置为将如下所述接收包确定为有效接收包,在所述接收包中与被包括在所述认证信息中的所述策略 ID 相关的所述第二认证 ID 与所述第一认证 ID 对应。

2. 根据权利要求 1 所述的计算机系统,其中所述控制器被配置为参考所述认证信息以对所述接收包进行认证,且在所述交换机中设置用于限定包的丢弃的所述流条目,所述流条目包括位于被确定为不正确的所述接收包的报头信息中且用于识别所述接收包的源的信息。

3. 根据权利要求 1 所述的计算机系统,其中所述策略信息包括与用于识别所述策略信息的所述策略 ID 相关的多个策略,以及

其中所述控制器被配置为从所述存储设备提取在与包括在所述认证信息中的所述策略 ID 相关的所述多个策略之中的符合被确定为有效的所述接收包的报头信息的策略,且在所述交换机中设置符合被提取的所述策略的所述流条目。

4. 一种在计算机系统中使用的控制器,其中所述计算机系统包括:

所述控制器;以及

交换机,所述交换机被配置为针对符合由所述控制器设置的流条目的接收包执行中继操作,所述中继操作由所述流条目限定,

其中所述交换机被配置为向所述控制器传输不符合在所述交换机中设置的所述流条目的所述接收包,以及

其中所述控制器被配置为参考包括在所述接收包中的认证信息以对所述接收包进行认证,且在所述交换机中设置用于限定包的所述中继操作的所述流条目,所述流条目包括位于被确定为有效的所述接收包的报头信息中且用于识别所述接收包的源的信息,

其中所述控制器包括其中记录有用于限定中继操作策略的策略信息的存储设备,且被配置为在所述交换机中设置符合与包括在被确定为有效的所述接收包中的认证信息对应的所述策略信息的所述流条目,

其中所述认证信息包括用于识别所述策略信息的策略 ID 和在认证中使用的第一认证 ID,

其中将用于识别所述策略信息的所述策略 ID 与第二认证 ID 相关的所述策略信息被记录在所述存储设备中;以及

其中所述控制器被配置为将如下所述接收包确定为有效接收包,在所述接收包中与被包括在所述认证信息中的所述策略 ID 相关的所述第二认证 ID 与所述第一认证 ID 对应。

5. 一种控制策略的方法,包括:

通过控制器从交换机接收不符合所述交换机中设置的流条目的接收包;

通过所述控制器参考包括在所述接收包中的认证信息,来对所述接收包进行认证;

通过所述控制器在所述交换机中设置限定包的中继操作的所述流条目,所述流条目包括位于被确定为有效的所述接收包的报头信息中且用于识别所述接收包的源的信息,

通过所述控制器来保持用于限定中继操作策略的策略信息,以及

其中所述设置限定所述中继操作的所述流条目包括:

通过所述控制器在所述交换机中设置符合与包括在被确定为有效的所述接收包中的认证信息对应的策略信息的所述流条目,

其中所述认证信息包括用于识别所述策略信息的策略 ID 和在认证中使用的第一认证 ID,

其中将用于识别所述策略信息的所述策略 ID 与第二认证 ID 相关的所述策略信息通过所述控制器来保持;以及

其中在所述认证中,所述控制器将如下所述接收包确定为有效接收包,在所述接收包中与包括在所述认证信息中的所述策略 ID 相关的所述第二认证 ID 与所述第一认证 ID 对应。

6. 根据权利要求 5 所述的方法,还包括:

通过所述控制器在所述交换机中设置限定包的丢弃的所述流条目,所述流条目包括位于被确定为不正确的所述接收包的报头信息中且用于识别所述接收包的源的信息。

7. 根据权利要求 5 所述的方法,其中所述策略信息包括与用于识别所述策略信息的所述策略 ID 相关的多个策略,以及

其中所述设置限定所述中继操作的所述流条目包括:

通过所述控制器从存储设备提取在与包括在所述认证信息中的所述策略 ID 相关的所述多个策略之中的符合被确定为有效的所述接收包的报头信息的策略;以及

通过所述控制器在所述交换机中设置符合被提取的所述策略的所述流条目。

控制网络访问策略的计算机系统、控制器和方法

技术领域

[0001] 本发明涉及控制网络访问策略的计算机系统、控制器、方法以及程序，并且特别地涉及使用开放流(open flow)技术控制网络访问策略的计算机系统和方法。

背景技术

[0002] 随着使用网络的信息系统的普及，诸如 IP 网络的网络不断大规模化和复杂化，并且另外不断需要高度灵活性。由于网络设备的设置不断复杂化且需要设置的设备的数目不断增加，针对网络的设计管理中的负担不断增加。

[0003] 例如，作为用于个人计算机(此后称为 PC)的广泛使用的访问控制方法之一，已知的一种方法是在与 PC 相邻的终端 L2 交换机中形成基于 MAC 的 VLAN(虚拟局域网)，以仅仅允许来自具有指定 MAC 地址的 PC 的连接。然而，在该方法中，在连接成数十万台 PC 的环境中，需要针对添加或删除数十万个 MAC 地址或数千台 L2 交换机的日常维护，管理员的负担增加。

[0004] 作为用于解决这种问题的描述，存在由开放流联盟提议的开放技术(<http://www.openflowswitch.org/>) (称为非专利文献 1)。在根据该技术的开放流系统中，被称为开放流控制器(OFC :Open Flow Controller)的服务器能够集成、设置和管理被称为开放流交换机(OFS 开放流交换机)的网络交换机。因此，通过在 OFC 中设置用于整体开放流系统的网络策略(此后称为策略)，能够控制所有 OFS。

[0005] 将参考图 1 解释使用开放流协议的计算机系统的配置和操作。参考图 1，根据本发明的相关技术的计算机系统包括开放流控制器 100(此后称为 OFC 100)、包括多个开放流交换机 2-1 至 2-n (此后 称为 OFS 2-1 至 2-n)的交换机组 20 以及包括多个主机计算机 3-1 至 3-i (此后称为主机 3-1 至 3-i)的主机组 30。此处，n 和 i 分别是 2 或更大的自然数。在下面的解释中，当不区分时，OFS 2-1 至 2-n 中的每一个被称为 OFS 2，且当不区分时，主机 3-1 至 3-i 中的每一个称为主机 3。

[0006] OFC 100 执行主机 3 之间的通信路径的设置以及该路径上用于 OFS 2 的转发操作(中继操作)等的设置。在这种情况下，OFC 100 在包括在 OFS 2 的流表中设置流条目，流条目将用于识别流(包数据)的规则和用于限定用于该流的操作的动作关联。通信路径上的 OFS 2 根据 OFC 100 设置的流条目确定接收的包数据的转发目的地，并执行转发操作。因而，主机 3 能够使用 OFC 100 所设置的通信路径与另一主机 3 传送和接收包数据。即，在使用开放流的计算机系统中，因为用于设置通信路径的 OFC 100 和用于执行转发操作的 OFS 是分离的，所以整个系统中的通信能够统一地被控制和管理。

[0007] 参考图 1，当从主机 3-1 向主机 3-i 传输包时，OFS 2-1 参考从主机 3-1 接收的包中的传输目的地信息(报头信息：例如，目的地 MAC 地址或目的地 IP 地址)，且在包括在 OFS 2-1 的流表中搜索对应于该报头信息的条目。例如，在非专利文献 1 中定义了流表中设置的条目的内容。

[0008] 当在流表中并未描述关于接收包数据的条目时，OFS 2-1 向 OFC 100 传递包数据

(此后称为第一包)或第一包的报头信息(或第一包本身)。已经从 OFS 2-1 接收第一包的 OFC 100 基于诸如包括在包中的源主机和目的地主机的信息确定路径 40。

[0009] OFC 100 指示路径 40 上的所有 OFS 2 设置限定包的传输目的地的流条目(发布流表更新指令)。路径 40 上的 OFS 2 根据流表更新指令更新其本身管理的流表。此后, OFS 2 根据更新的流表开始包的传输,且经由通过由 OFC 100 确定的路径 40 将包传输到目的地主机 3-i。

[0010] 然而,在如上所述的开放流技术中,诸如 PC (个人电脑) 等与 开放流系统连接的主机终端通过 IP 地址或 MAC 地址被而被识别。因此,在其中连接数十万台 PC 的环境中,需要针对成数十万个 IP 地址或 MAC 地址中的每一个设置策略,因而负担增加。再者,因为 IP 地址和 MAC 地址能够被伪造,存在非授权访问的风险,且需要应对措施。

[0011] 例如,在 JP 2005-4549 (称为专利文献 1) 中描述了关于策略控制的系统。在专利文献 1 中,描述了一种策略服务器,其具有用于网络设备的访问控制功能或基于策略服务器本身维持的安全策略的应用服务器,然而,并未公开开放流环境的系统中的策略控制。

[0012] 引用列表

[0013] [专利文献 1]JP 2005-4549

[0014] [非专利文献 1] 开放流交换机规范版本 1.0.0 (无线协议 0x01) 2009 年 12 月 31 日

发明内容

[0015] 鉴于从上述情况,本发明的目的是提供一种根据开放流协议环境的计算机系统,其能够容易地控制网络访问策略。

[0016] 而且,本发明的另一目的是在根据开放流协议环境中的网络中增加防御非授权访问的安全性程度。

[0017] 在一个方面中,根据本发明的计算机系统包括控制器和交换机,所述交换机被配置为针对与由所述控制器设置的流条目对应的接收包,执行中继操作,其所述中继操作由所述流条目限定。所述交换机向控制器传输与交换机本身中设置的流条目不对应的接收包。所述控制器参考包括在所述接收包中的认证信息以对接收包进行认证。此处,所述控制器设置交换机中的流条目,所述流条目限定如下包的中继操作,所述包包括位于被确定为有效的所述接收包的报头信息中且用于识别所述接收包的传输源的信息。

[0018] 在另一方面中,根据本发明的策略控制方法包括:控制器从交 换机接收与所述交换机中设置的流条目不对应的接收包;所述控制器通过参考包括在所述接收包中的认证信息来对接收包进行认证;以及所述控制器在交换机中设置限定用于如下包的中继操作的流条目,所述包包括位于被确定为有效的接收包的报头信息中且用于识别所述接收包的传输源的信息。

[0019] 在另一方面中,如上所述的策略控制方法优选地通过计算机执行的程序实现。

[0020] 根据本发明,可以容易地在根据开放流协议环境的计算机系统中执行网络访问策略控制。

[0021] 而且,可以改善防御未授权访问或使用欺骗地址的干扰的安全性级别。

附图说明

[0022] 如上所述的本发明的目的、优点和特征将从结合附图的实施例的描述更加显现，在所述附图中：

- [0023] 图 1 是示出使用开放流协议的计算机系统的配置的示例的图示；
- [0024] 图 2 是示出根据本发明的计算机系统的配置的示例的图示；
- [0025] 图 3 是示出根据本发明的策略信息的示例的图示；
- [0026] 图 4 是示出根据本发明的策略信息的具体示例的图示；
- [0027] 图 5A 是示出根据本发明的流条目的具体示例的图示；
- [0028] 图 5B 是示出根据本发明的流条目的具体示例的图示；
- [0029] 图 6 是示出根据本发明的计算机系统中的通信操作和策略设置的示例的顺序图；以及
- [0030] 图 7 是示出由根据本发明的开放流控制器执行的策略控制操作的示例的流程图。

具体实施方式

[0031] 此后，将参考附图描述本发明的实施例。在附图中，相同或相似的参考数字指示相同、相似或等效组件。

[0032] (计算机系统的配置)

[0033] 同图 1 中示出的系统一样，根据本发明的计算机系统使用开放流技术执行通信路径的构建和传输包数据的控制。图 2 是示出根据本发明的计算机系统的配置的示例的图示。根据本发明的计算机系统与图 1 中示出的系统的不同于之处在于，开放流控制器 (OFC) 和主机终端(例如 PC) 的配置，而其他配置(例如 OFS) 与图 1 中示出的系统类似。

[0034] 将参考图 2 解释根据本发明的第一实施例的计算机系统的配置。参考图 2，根据本发明的计算机系统包括开放流控制器 1(OpenFlow Controller 此后称为 OFC 1)，多个开放流交换机 2(开放流交换机：此后称为 OFS 2)、多个主机终端 3(例如 PC) 和输入终端 4。

[0035] OFC1 经由安全信道网络连接到多个 OFS 2，且通过网络更新 OFS 2 的流表 21。因而，经由 OFS 2 彼此连接的多个主机终端 3 之间的通信得以控制。OFS 2 设置在多个主机终端 3 之间，且根据流表 21 中设置的流条目，中继从主机终端 3 或其他网络(未示出)向传输目的地传输的包。

[0036] OFC 1 根据开放流技术，控制用于在系统中传输包的通信路径的构建和包传输操作。此处，开放流技术指示这样的技术：其中 OFC 1 根据路由策略(流条目：流+动作)在通信路径上的 OFS 2 或 OFVS 33 中设置关于多层和单位流的路径信息，以便执行路径控制或节点控制(详情参见非专利文献 1)。因而，路径控制功能与路由器和交换机分离，且可以通过控制器的集中控制而实现最佳路由和流量管理。应用了开放流技术的 OFS 2 和 OFVS 33 将通信作为端对端的流来对待，而不是像常规路由器或交换机那样以包或帧为单位来处理。

[0037] 参考图 2，将解释根据本发明的 OFC 1 的详细配置。OFC 1 优选地通过具有存储设备和 CPU 的计算机来实施。在 OFC 1 中，流控制部 11 和策略管理部 12 的功能中的每一个通过执行存储在存储设备中的程序的计算机(未示出)来实现。

[0038] 流控制部 11 根据开放流协议执行对交换机中的流条目(规则+ 动作)的设置或删

除。因而，OFS 2 根据接收包的报头信息执行与规则相关的动作(例如，包的中继或撤消)。

[0039] 在流条目中设置的规则中，例如，限定了关于 OSI (开放系统互连)参考模型的层 1 至层 4 的地址和标识符的组合，其被包括在 TCP/IP 的包数据的报头信息中。例如，作为规则，设置了层 1 的物理端口、层 2 的 MAC 地址、VLAN 标签(VLAN id)、层 3 的 IP 地址和层 4 的端口号的组合。VLAN 标签中，可以添加优先级(VLAN 优先级)。

[0040] 此处，可以将通过流控制部 11 而在规则中设置的标识符或地址等设置为预定范围。而且，优选地，目的地和源的地址等被区分，以被设置为规则。例如，作为规则，设置了 MAC 目的地地址的范围、用于识别连接目的地应用的目的地端口号的范围和用于识别连接源应用的源端口号的范围。此外，作为规则，可以设置用于识别数据传输协议的标识符。

[0041] 作为流条目中的动作集，例如，限定了用于处理 TCP/IP 的包数据的方法。例如，设置了指示是否中继接收包数据的信息以及在中继情况的传输目的地。此外，作为动作，可以设置指示包数据的复制或撤消的信息。

[0042] 根据本发明的流控制部 11 根据来自策略管理部 12 的指令在指令指示的 OFS 2 中设置流条目。

[0043] 策略管理部 12 将从输入终端 4 提供的策略信息 130 变换成容易搜索的格式，且将它记录在策略信息存储部 13 中。图 3 是指示在策略信息存储部 13 中记录的策略信息 130 的配置的图示。参考图 3，在策略信息存储部 13 中，策略 ID 131、认证 ID 132 和策略 133 相关联，以便作为策略信息 130 被记录。

[0044] 策略 ID 131 是用于唯一识别策略信息 130 的标识符。认证 ID 132 是用于认证策略 133 是否应用于第一包(第一包的源主机或目的地主机)的信息(例如密码)。策略 133 是用于限定用于主机终端 3 的网络访问策略的信息。在策略 133 中，限定了用于限定源主机或目的地主机的条件、用于限定访问方法的协议和优先级等。

[0045] 图 4 是示出策略信息 130 的具体示例的图示。在策略信息 130 中，作为策略 ID 131，设置了策略标识符“用于会计部门普通员工的策略”，其识别作为多个策略 133 “策略 1 至策略 3,...”的应用目标，并且设置了用于认证是否应用了策略 133 的认证 ID 132 “XXXXX”。此处，策略 1 指示允许使用 HTTP (超文本传输协议) 向 10.11.12.1 的 IP 地址转发包，且其优先级是“10”。策略 2 指示允许使用 FTP (文件传输协议) 向 10.11.12.2 的 IP 地址转发包，且其优先级是“20”。策略 3 指示允许使用 RDP (原创桌面协议) 来自 10.11.12.0/24 的 IP 地址的连接，且其优先级是“30”。

[0046] 策略管理部 12 检查包括在从 OFS 2 告知的第一包中的认证信息 140，策略信息 130 被记录在策略信息存储部 13 中以对第一包进行认证。

[0047] 具体而言，主机终端 3 在包的数据区域中添加包括策略 ID 的认证信息 140 以将其传输到目的地主机。策略管理部 12 通过关键字来搜索策略信息存储部 13，该关键字是包括在从 OFS 2 告知的第一包中的认证信息 140 的策略 ID，并且提取具有与认证信息 140 的策略 ID 对应的策略 ID 131 的策略信息 130。然后，策略管理部 12 通过检查认证信息 140 的认证 ID 与策略信息 130 中的认证 ID 132 来对第一包进行认证。

[0048] 当第一包有效(认证 ID 匹配)时，策略管理部 12 指示流控制部 11 设置用于转发第一包的流条目。在这种情况下，流控制部 11 在基于报头信息而计算的通信路径上的 OFS 2 中，设置遵循与第一包的报头信息对应的策略 133 的流条目。

[0049] 另一方面,在与包括在第一包中的策略 ID 对应的策略 ID 131 未被记录在策略信息存储部 13 中的情况下或在认证信息 ID 不匹配的情况下,策略管理部 12 确定认证失败。在这种情况下,策略管理部 12 指示流控制部 11 设置用于丢弃第一包的流条目。响应于该指令,流控制部 11 在作为第一包的通知源的 OFS 2 中设置流条目,使得该流条目包括至少作为第一包的报头信息的一部分的规则和用于丢弃包的动作。根据非专利文献 1 中描述的开放流协议,执行选择作为流条目的设置目标的 OFS 2 的方法、计算通信路径的方法以及通过流控制部 11 设置和管理流条目的方法。

[0050] 图 5A 和图 5B 指示在终端 A 成功通过策略管理部 12 的认证且应用了图 4 中示出的策略 1 的情形中交换机中设置的流条目的一个示例。此处,将解释流条目,其在 OFS 2 中设置,其中端口 0/1 与终端 A 连接,而端口 0/2 与网络服务器连接。

[0051] 参考图 5A 和 5B,在流条目中,作为规则 211,限定了匹配字段和匹配字段的值(匹配值)。此外,作为动作信息 212,限定了动作和优先级。在策略 1 中,限定允许“到 10.11.12.1 的 HTTP 连接,且优先级是 10”。在 OFS 2 中,设置用于限定关于来自经过认证的终端 A 且目的地为 IP 地址“10.11.12.1”的包的中继操作流条目(图 5A),并且设置用于限定关于来自网络服务器(被分配了 IP 地址“10.11.12.1”)且目的地为经过认证的终端 A 的包的中继操作的流条目(图 5B)。

[0052] 参考图 5A,在规则 211 中,“0/1”被限定为输入端口,“终端 A 的 MAC 地址”被限定为源 MAC 地址,“终端 A 的 VLAN ID”被限定为输入 VLAN ID,“0x0800 (IPv4)”被限定为以太网类型,“6 (TCP)”被限定为 IP 协议(协议号)、“终端 A 的 IP 地址”被限定为源 IP 地址、“10.11.12.1”被限定为目的地 IP 地址、“80 (HTTP)”被限定为目的地端口号,且在其他匹配字段中限定“任意”。此外,在动作信息 212 中,限定了“向端口“0/2”输出接收包且其优先级为“10””。

[0053] 根据图 5A 中示出的流条目,OFS2 向连接到网络服务器的端口“0/2”输出包,该包是通过 HTTP 通信从经过认证的终端 A 传输来的,且目的地为 IP 地址“10.11.12.1”。

[0054] 此外,参考图 5B,在规则 211 中,“0/2”被限定为输入端口,“终端 A 的 MAC 地址”被限定为目的地 MAC 地址,“0x0800 (IPv4)”被限定为以太网类型,“6 (TCP)”被限定为 IP 协议(协议号)、“10.11.12.1”被限定为源 IP 地址、“终端 A 的 IP 地址”被限定为目的地 IP 地址、“80 (HTTP)”被限定为目的地端口号,且在其他匹配字段中限定“任意”。此外,在动作信息 212 中,限定“向端口“0/1”输出接收包且其优先级为“10””。

[0055] 根据图 5B 中示出的流条目,OFS 2 向连接到终端 A 的端口“0/1”输出包,该包是通过 HTTP 通信从 IP 地址“10.11.12.1”的网络服务器传输来的,且目的地为 IP 地址“终端 A 的 IP 地址”。

[0056] 如上所述,根据本发明,在 OFS 2 中设置根据与经过认证的第一包(主机终端 3)对应的策略的流条目。在如上所述的一个示例中,解释了用于策略 1 的流条目的设置,然而,当存在需要认证的多个策略时,相应地设置流条目。

[0057] OFS 2 包括流表 21,其中流条目通过 OFC 1 来设置,且包控制部 22 根据流表 21 中设置的流条目转发或丢弃接收包。像常规方式一样,基于来自 OFC 1 的流模式请求设置用于 OFS 2 的流条目。当在流表 21 中没有与接收包的报头信息对应的流条目(规则)时,包控制部 22 向 OFC 1 转发接收包,该接收包是第一包。因而,OFS 2 向 OFC 1 发送从主机终端

3 传输的认证信息 140。另一方面,当存在与接收包的报头信息对应的流条目时,包控制部 22 根据流条目的动作处理包。作为用于接收包的动作,示例了向另一 OFS 2 或终端 3 转发包或者丢弃包。尽管在图 2 中仅示出连接到两个主机终端 3 的端部交换机,但是无需多言的是,如图 1 所指示,主机终端 3 经由其他 OFS 2 与另一主机终端 3 连接。此外,OFS 2 优选地是物理交换机,但是可以通过虚拟交换机实现,只要根据开放流协议操作即可。

[0058] 主机终端 3 优选地通过具有 CPU (未示出) 和 RAM 的计算机设备(物理服务器) 实现,且包括其中记录有认证信息 140 的存储设备(未示出)。备选地,主机终端 3 可以通过虚拟机实现。主机终端 3 在需要传输的包的数据区域中添加认证信息 140。其他配置类似于能够执行包通信的常规计算机系统或虚拟机。尽管在图 2 中仅指 示了两个主机终端 3,但是无需多言的是,如图 1 所示,本系统包括经由多个 OFS 2 彼此连接的其他主机终端 3。

[0059] 尽管在图 2 中的系统中仅提供一个主机终端 3,但是一般提供多个主机终端 3。

[0060] 输入终端 4 是具有策略设置 UI (用户界面)41 的计算机设备。策略设置 UI 41 是用于在 OFC 1 中设置策略信息的用户界面,且将来自用户的指令输出到 OFC 1 的策略管理部 12。因而,OFC 1 中设置任意策略信息 130。策略信息 130 的设置方法并不限于此,且策略信息 130 可以通过使用移动存储介质来设置。

[0061] 此外,诸如监控器或打印机之类的输出设备可以连接到 OFC 1。策略管理部 12 能够基于在认证中失败的第一包中的报头信息(源端口号或源 MAC 地址),识别包的源 OFS 2 或目的地主机终端 3。通过经由输出设备可视地输出该认证结果,不仅对非授权访问的监控而且对非授权访问的源的识别都是可能的。

[0062] 根据上述配置,在根据本发明的计算机系统中,在控制器端使用符合开放流协议的第一包执行针对该包(访问)的认证,且基于认证结果控制针对该包的转发操作。根据本发明,因为通过主机终端 3 插入在包中的认证信息由控制流的 OFC 1 来认证,所以 OFC 1 能够深入控制从具有不同网络访问策略的主机终端 3 的通信。此外,在本发明中,应用策略 133 的主机终端 3 能够通过针对每个策略信息 130 而给出的认证 ID 132 而被识别。因此,策略容易改变和管理,而无需针对 IP 地址和 MAC 地址中的每一个设置策略。而且,因为根据本发明的 OFC 1 通过使用第一包的包认证来控制访问,非所以授权访问(例如 :具有伪造地址的包的侵入)能够在作为网络入口的主机端的端部 OFS 2 被阻断。

[0063] (操作)

[0064] 接下来,参考图 6 和 7,将详细解释根据本发明的计算机系统的通信操作和访问控制操作。

[0065] 图 6 是示出在根据本发明的计算机系统中的策略设置和通信操 作的一个示例的顺序图。图 7 是示出由根据本发明的 OFC 1 执行的策略控制操作的一个示例的流程图。

[0066] 参考图 6,首先当计算机系统启动时,策略信息 130 之前已从输入终端 4 记录到 OFC 1 的策略信息存储部 13 中(步骤 S11, S12)。具体而言,经由输入终端 4 输入的策略信息 130 被提供给策略管理部 12,以便作为数据库而被记录在策略信息存储部 13 中。因而,策略信息存储部 13 通过最新策略信息 130 来更新。此处,策略信息存储部 13 能够总是被策略管理部 12 搜索。此外,在步骤 S11 和 S12 处的策略信息存储部 13 的更新可以在系统的操作期间执行。

[0067] 随后,将解释在从主机终端 3 向系统传输包的情况下访问控制和通信操作。主

机终端 3 向网络传输包, 该包包括认证信息 140, 其中添加有加密策略 ID 和认证 ID (步骤 S21)。在这种情况下, 来自主机终端 3 的包被转移到 OFS 2。

[0068] OFS 2 确定从主机终端 3 接收的包的报头信息是否符合(对应于)流表 21 中设置的流条目的规则, 且当存在匹配规则(未示出)时根据与规则相关的动作处理接收包(例如, 向其他 OFS 2 转发或丢弃)。具体而言, OFS 提取从主机终端 3 接收的包的报头信息(发送和接收 IP 地址、MAC 地址、端口号、或协议等)。然后, OFS 2 比较报头信息和流表 21, 以确认是否存在匹配流条目。当存在匹配流条目时, OFS 2 执行在流条目中描述的动作(转发或丢弃), 且完成转发操作。

[0069] 另一方面, 当在流表 21 中并未设置符合(对应于)接收包的报头信息的流条目(其中的规则)时, OFS 2 告知 OFC1 中的策略管理部 12 所述接收包, 该接收包为第一包(步骤 S22, PackeIN)。

[0070] 在 PacketIN 之后, 策略管理部 12 对第一包进行认证, 且根据认证结果向流控制部 11 指示包处理方法(步骤 S23, S24)。流控制部 11 根据来自策略管理部 12 的指令, 在作为被控制目标的 OFS 2 的流表 21 中设置流条目(步骤 S25)。因而, OFS 2 根据在流表 21 中新设置的流条目处理在步骤 S21 接收的包。

[0071] 参考图 7, 将详细解释接收第一包的策略管理部 12 的操作(图 6 中的步骤 23 至 S25)。

[0072] OFC 1 分析从 OFS 2 接收的第一包的数据区域以获得认证信息 140 (策略 ID 和认证 ID) (步骤 S101)。随后, OFC 1 将获得的认证信息 140 (策略 ID 和认证 ID) 与记录在策略信息存储部 13 中的策略信息 130 进行比较, 以执行认证(步骤 S102)。具体而言, 策略管理部 12 在策略信息存储部 13 中搜索对应于认证信息 140 (策略 ID 和认证 ID) 的策略信息 130。此时, 如果对应于认证信息 140 的策略信息 130 被记录在策略信息存储部 13 中, 则策略管理部 12 确定认证成功, 且如果并未被记录, 则确定认证失败(步骤 S102)。

[0073] 在步骤 S102, 当认证成功时, 策略管理部 12 从策略信息存储部 13 获得与包括在认证信息 140 中的策略 ID 对应的策略信息 130 (步骤 S103)。OFC 1 设置与作为控制目标的 OFS 2 中所获得的策略信息 130 对应的流条目(步骤 S104)。

[0074] 具体而言, 策略管理部 12 参考与认证成功的认证信息 140 对应的策略信息 130, 且指示流控制部 11 基于与第一包的报头信息对应的策略 133 来设置流条目。在这种情况下, 和常规开放流系统的情况一样, 计算通信路径, 且确定作为流条目的设置目标的 OFS 2。通过经由安全信道的流模式请求, 流控制部 11 基于来自策略管理部 12 的指令在确定的 OFS 2 中设置流条目。在这种情况下, 优选地设置包括源 MAC 地址的规则和与策略 133 对应的动作。因而, 基于 OFC 1 中原先设置的策略控制其包通过 OFC 1 认证的主机(即经过认证的主机终端)的通信。此外, 作为流条目中设置的规则, 除了源 MAC 地址外, 可以限定目的地地址或目的地端口号。因而, 实现了基于认证主机终端的访问目的地的控制。

[0075] 作为指定示例, 将解释如下情况中的流条目的设置, 其中策略管理部 12 响应于认证信息 140 获得图 4 中示出的策略信息 130 且源 MAC 地址“0000.0000.0001”、目的地 IP 地址“10.11.12.1”和协议“HTTP”被包括在第一包的报头信息中。在这种情况下, 策略管理部 12 指示设置与图 4 中示出的策略 1 对应的流条目。因而, 流控制部 11 在通信路径上的 OFS 2 中设置流条目, 其中在流条目中, 规则包括“0000.0000.0001”的管理源

MAC 地址,“10.11.12.1”的目的地 IP 地址和“HTTP”的协议,且流条目的动作是向连接到“10.11.12.1”的端口转发包。而且,流控制部 11 将“10”设置为用于在 OFS 2 中应用该流条目的优先级。

[0076] 此后,其中流表 21 被更新的 OFS 2 根据该流表执行包控制。

[0077] 另一方面,在步骤 S102,如果认证失败,则 OFC 1 在作为第一包的告知源的 OFS 2 的流表 21 中设置流条目,该流条目至少将第一包的报头信息的至少一部分限定为规则,且将包的丢弃限定为动作(步骤 S105)。因此,优选地设置如下流条目,在该流条目中规则包括源 MAC 地址且动作是包的丢弃。这样,其包并未通过 OFC 1 认证的源主机(非认证主机终端)的通信在作为网络入口的 OFS 2 被阻断。此外,作为用于限定包的丢弃的流条目的规则,除了源 MAC 地址,可以限定目的地地址或目的地口号。这样,能够相对于非认证主机终端的访问目的地中的每一个,限制访问。

[0078] 如上所述,根据本发明的 OFC 1 经由第一包的通知从主机终端 3 接收认证信息 140 以对它进行认证,且设置流条目,在该流条目中规则指示源是该主机终端且基于策略限定动作。因此,在根据本发明的系统中,通过预先在应用策略的主机终端 3 中添加认证信息 140,能够针对终端中的每一个控制策略。即,在本发明中,不必准备用于针对主机终端中的每一个应用策略的配置(策略信息)。例如,尽管需要对于数十万个设备进行配置以在连接数十万台 PC 的网络中设计灵活的策略控制,但是在本发明中,因为不需针对 PC 中的每一个的配置,因此容易执行设计操作。

[0079] 此外,在本发明中,在从网络终端 3 到网络的最初连接中执行使用认证信息的认证。因此,可以在初始访问阶段阻断使用欺骗 ID 地址或 MAC 地址的未授权访问,且可以增加开放流系统的安全性级别。

[0080] 另外,在根据本发明的计算机系统中使用的 OFS 仅需要符合常规开放流协议(例如,开放流交换机说明书版本 1.0 所定义的协议),且如上述实施例所述,用于网络策略的控制或非授权访问的防止可以通过仅改变 OFC 或主机终端的功能实现。即,根据本发明,在现有开放流系统中,通过仅改变 OFC 和主机终端的功能,可以实现针对网络策略的上述控制或非授权访问的防止。因此,可以低成本地且容易地在现有系统中添加诸如用于网络策略的控制之类的功能。

[0081] 如上所述,已经详细解释了本发明的实施例,然而,指定配置不限于上述实施例,且本发明还可以包括在不偏离本发明精神的范围内修改的配置。在上面的解释中,解释了其中源 MAC 地址被包括在认证之后设置的流条目的规则中的一个示例,然而,本发明不限于此,只要源主机终端被识别即可。例如,作为规则,可以限定源 IP 地址或连接到源主机终端的端口号。

[0082] 本申请基于日本专利申请 No. 2011-91105,且其公开内容通过引用结合于此。

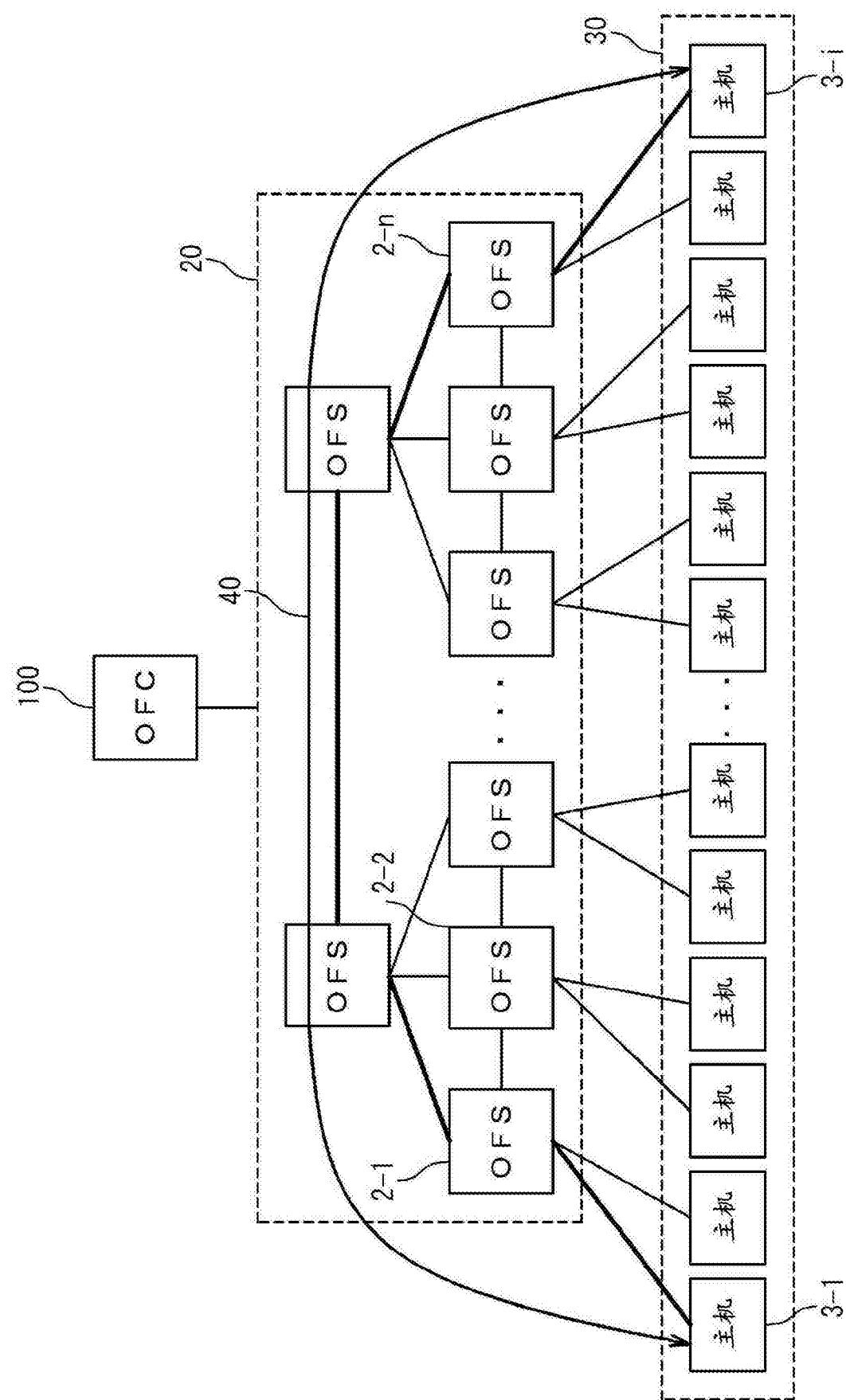


图 1

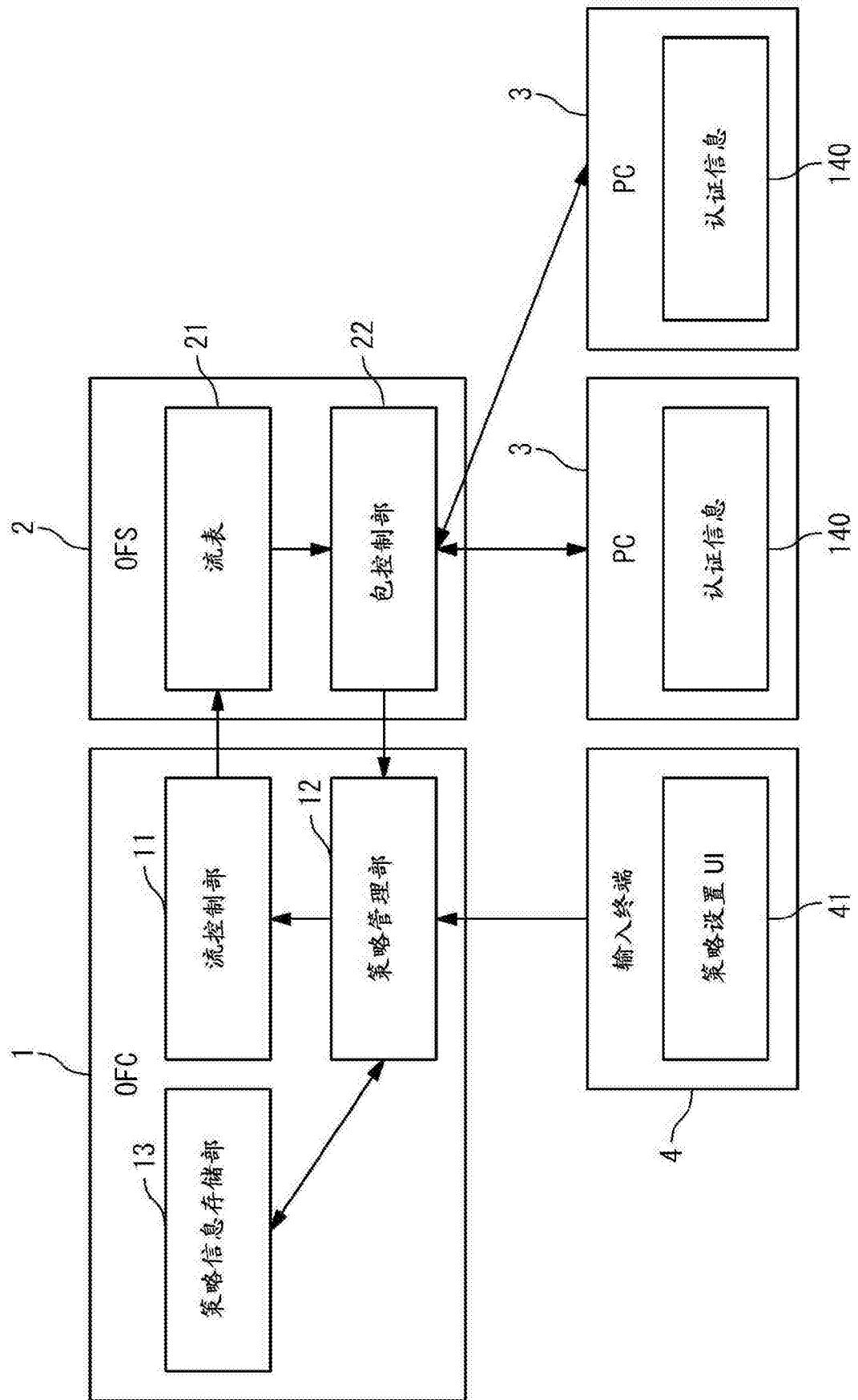


图 2

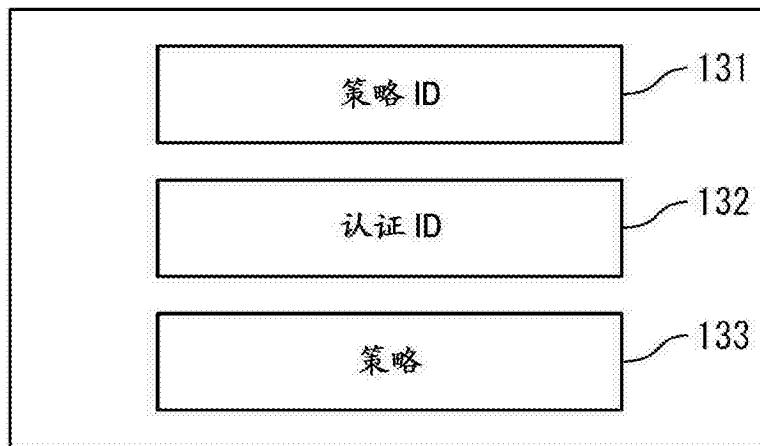
130

图 3

131	策略 ID	针对会计部门普通员工的策略
132	认证 ID	XXXXX
133	策略 1	允许到 10.11.12.1 的 HTTP 连接。优先级是 10。
133	策略 2	允许到 10.11.12.2 的 FTP 连接。优先级是 20。
133	策略 3	允许来自 10.11.12.0/24 的 RDP 连接。优先级是 30。

图 4



规则		动作信息 动作：输出 发往端口：0/2 优先级：10
匹配字段	匹配值	
输入端口	0/1	
源 mac 地址	终端 A 的 MAC 地址	
目的地 mac 地址	任意	
输入 VLAN ID	终端 A 的 VLAN ID	
输入 VLAN 优先级	任意	
以太网类型	0X0800	
tos/dscp	任意	
IP 协议	6	
源 IP 地址	终端 A 的地址	
目的地 IP 地址	10.11.12.1	
源端口	任意	
目的地端口	80	

图 5A



规则		动作信息
匹配字段	匹配值	
输入端口	0/2	动作：输出 发往端口：0/1 优先级：10
源 mac 地址	任意	
目的地 mac 地址	终端 A 的 MAC 地址	
输入 VLAN ID	任意	
输入 VLAN 优先级	任意	
以太网类型	0X0800	
tos/dscp	任意	
IP 协议	6	
源 IP 地址	10.11.12.1	
目的地 IP 地址	终端 A 的 IP 地址	
目的地端口	80	

图 5B

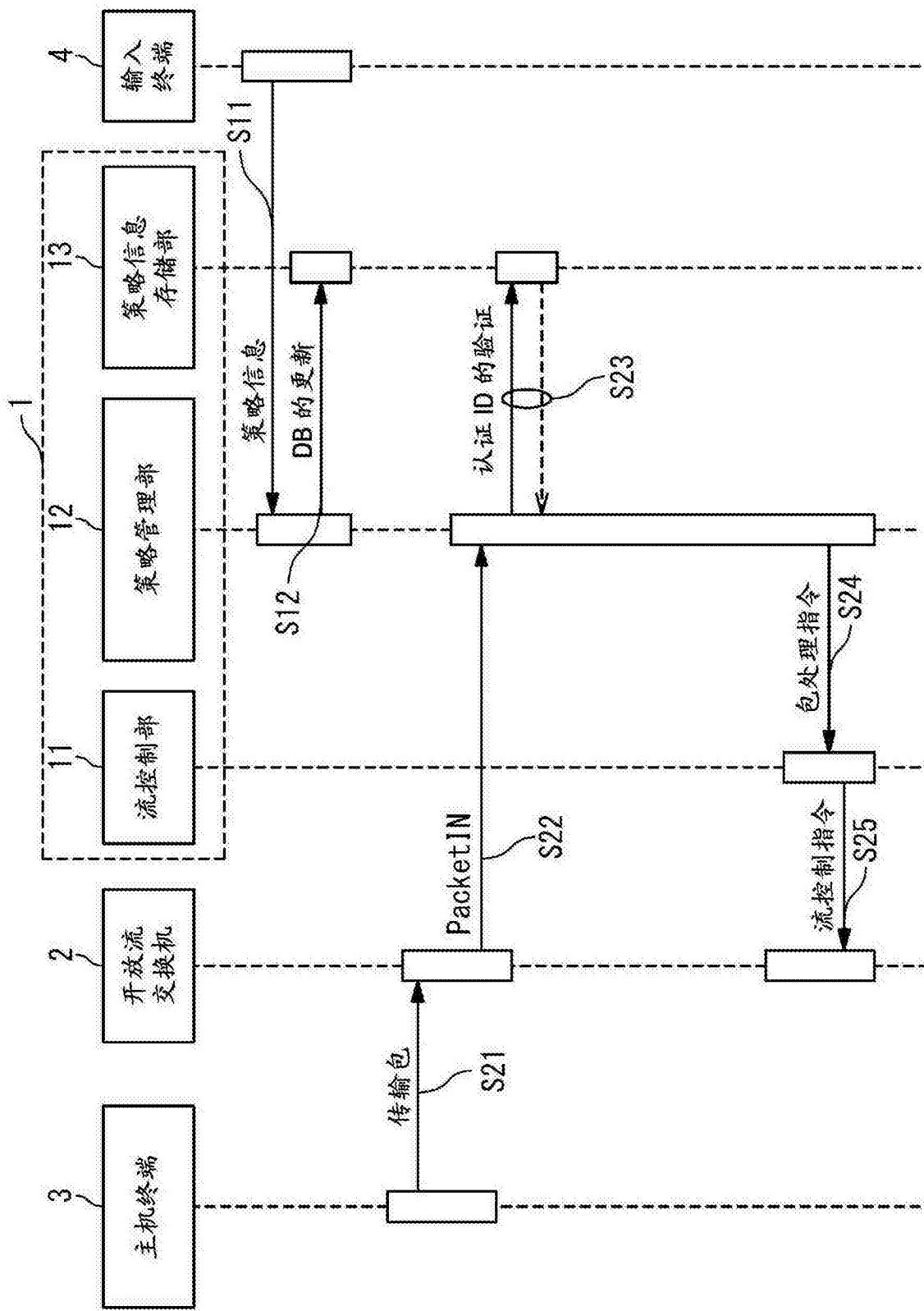


图 6

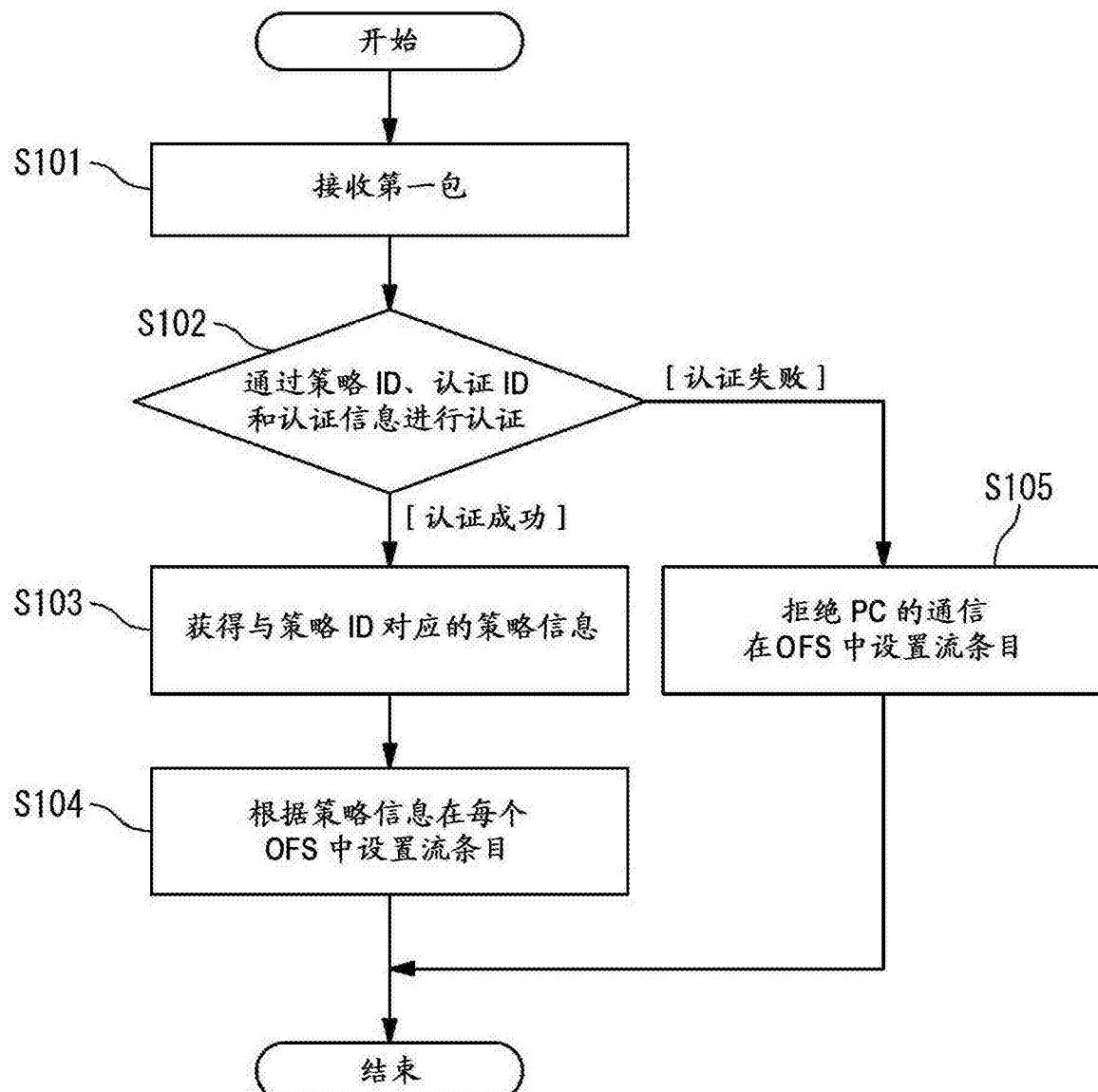


图 7