

(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
2015 年 10 月 22 日 (22.10.2015) WIPO | PCT



(10) 国际公布号
WO 2015/157935 A1

- (51) 国际专利分类号:
H04L 12/70 (2013.01)
- (21) 国际申请号: PCT/CN2014/075481
- (22) 国际申请日: 2014 年 4 月 16 日 (16.04.2014)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 梁剑耀 (LIANG, Jianyao); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 冯强 (FENG, Qiang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市西城区裕民路 18 号北环中心 A 座 2002, Beijing 100029 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, 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, 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))。

(54) Title: FLOW TABLE ENTRY MANAGEMENT METHOD AND DEVICE

(54) 发明名称: 一种流表项管理方法及设备

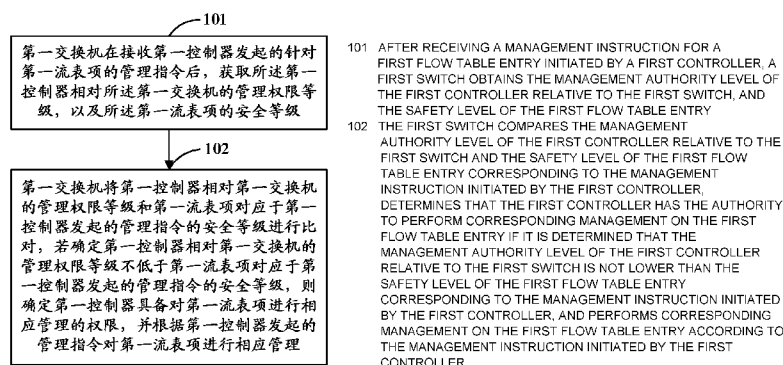


图 1 / Fig. 1

(57) Abstract: A flow table entry management method and device are disclosed. After receiving a management instruction for any flow table entry from any controller connected with any switch, said any switch can firstly judge, according to the obtained management authority level of said any controller relative to said any switch and the safety level of said any flow table entry, whether the management authority level of said any controller relative to said any switch is not lower than the safety level of said any flow table entry corresponding to the management instruction initiated by said any controller, determine that said any controller has the authority to perform corresponding management on said any flow table entry when it is determined that the judging result is yes, and perform corresponding management on said any flow table entry according to the management instruction initiated by said any controller, thereby achieving the purpose of protecting the flow table entry effectively and improving the system security furthermore on the basis of avoiding the operation phenomena of deleting or modifying the flow table entry arbitrarily and so forth.

(57) 摘要:

[见续页]

WO 2015/157935 A1



一种流表项管理方法及设备，任一交换机在接收到与其相连接的任一控制器发起的针对任一流表项的管理指令后，可首先根据获取到的所述任一控制器相对所述任一交换机的管理权限等级以及所述任一流表项的安全等级，判断所述任一控制器相对所述任一交换机的管理权限等级是否不低于所述任一流表项对应于所述任一控制器发起的管理指令的安全等级，并在确定判断结果为是时，确定所述任一控制器具备对所述任一流表项进行相应管理的权限，并根据所述任一控制器发起的管理指令对所述任一流表项进行相应管理，从而在避免了对流表项进行随意删除或修改等操作现象的基础上，达到了有效保护流表项、进而提高系统安全性的目的。

一种流表项管理方法及设备

技术领域

本发明涉及 SDN（Software-Defined Networking，软件定义网络）技术领域，尤其涉及一种基于 OpenFlow 协议的流表项管理方法及设备。

背景技术

OpenFlow协议是目前SDN领域最热门的协议，在OpenFlow协议中，将网络设备的控制功能与转发功能进行分离，进而将控制功能全部集中到远程控制器（Controller）上完成，而OpenFlow交换机（Switch）可仅负责在本地进行简单高速的数据转发等操作。具体地，在OpenFlow交换机的运行过程中，其数据转发的依据为流表，控制器可通过事先规定好的OpenFlow协议接口来控制OpenFlow交换机中的流表，从而达到控制数据转发的目的。

但是，由于目前在OpenFlow协议中还缺少对流表中的各流表项的权限控制，从而导致可能会存在流表项被随意修改的问题，降低系统的安全性。

例如，在某些场景中，OpenFlow交换机会保存一些默认的重要流表项，如，在即插即用自组网的场景中，OpenFlow交换机会保存与自组网相关的默认流表项，若该默认流表项被该OpenFlow交换机根据某一控制器下发的控制指令（也可称为管理指令）所删除，则OpenFlow交换机的自组网功能就会失效；再有，针对多个控制器操作同一OpenFlow交换机的场景，若与A控制器相关的流表项被该OpenFlow交换机根据B控制器下发的控制指令所修改或删除，则A控制器将无法继续根据该流表项进行相应的控制操作，从而会影响到A控制器的相应处理过程。

因此，目前亟需提供一种对OpenFlow协议中的流表项进行相应的权限控制的方法，以解决上述各问题。

发明内容

本发明实施例提供了一种流表项管理方法及设备，以解决目前存在的缺少对流表项的权限控制所导致的系统安全性较低的问题。

第一方面，提供了一种流表项管理方法，应用于流表项管理系统，所述流表项管理系统包括至少一个交换机以及至少一个控制器，其中，针对所述至少一个交换机中的任一交换机，所述至少一个控制器中存在一个或多个控制器与所述任一交换机相连接，并且，与所述任一交换机相连接的一个或多个控制器中的每个控制器相对于所述任一交换机设置有相应的管理权限等级，所述方法包括：

第一交换机在接收第一控制器发起的针对第一流表项的管理指令后，获取所述第一控制器相对所述第一交换机的管理权限等级，以及所述第一流表项的安全等级；其中，所述第一流表项对应不同的管理指令分别设置有相应的安全等级，所述安全等级用于表示对所述第一流表项进行管理的控制器所应具有的管理权限等级；所述第一交换机为所述至少一个交换机中的任一交换机，所述第一控制器为与所述第一交换机相连接的一个或多个控制器中的任一控制器，所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项或所述第一交换机中存储的任一已创建流表项；

所述第一交换机将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级，则确定所述第一控制器具备对所述第一流表项进行相应管理的权限，并根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理。

结合第一方面，在第一方面的第一种可能的实现方式中，所述方法还包括：所述第一交换机若确定所述第一控制器相对所述第一交换机的管理权限等级低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级，则确定所述第一控制器不具备对所述第一流表项进行相应管理的权限，

并拒绝执行根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理的操作。

结合第一方面或第一方面的第一种可能的实现方式，在第一方面的第二种可能的实现方式中，所述第一控制器发起的管理指令中携带有所述第一控制器的网络协议地址以及所述第一流表项的匹配域；

获取所述第一控制器相对所述第一交换机的管理权限等级，包括：

根据所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址以及预先设置的、与所述第一交换机相连接的各控制器相对所述第一交换机的管理权限等级和与所述第一交换机相连接的各控制器的网络协议地址之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址相对应的管理权限等级，并将查询到的管理权限等级作为获取到的所述第一控制器相对所述第一交换机的管理权限等级；其中，预先设置的、与所述第一交换机相连接的各控制器相对所述第一交换机的管理权限等级和与所述第一交换机相连接的各控制器的网络协议地址之间的关联关系存储在所述第一交换机中；

获取所述第一流表项的安全等级，包括：

根据所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域以及预先设置的各流表项的安全等级与各流表项的匹配域之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域对应的安全等级，并将查询到的安全等级作为获取到的所述第一流表项的安全等级；其中，当所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系携带在所述第一控制器发起的管理指令中，当所述第一流表项为所述第一交换机中存储的任一已创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系存储在所述第一交换机中。

结合第一方面或第一方面的第一种可能的实现方式，在第一方面的第三

种可能的实现方式中，获取到的所述第一流表项的安全等级至少包括所述第一流表项对应于内容修改管理指令的第一安全等级和/或所述第一流表项对应于内容查看管理指令的第二安全等级；

其中，所述内容修改管理指令至少包括创建指令、修改指令以及删除指令中的一种或多种；所述内容查看管理指令至少包括查看指令。

结合第一方面的第三种可能的实现方式，在第一方面的第四种可能的实现方式中，将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级，则确定所述第一控制器具备对所述第一流表项进行相应管理的权限，包括：

当所述第一控制器发起的管理指令为创建指令、修改指令或删除指令时，将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项的第一安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第一安全等级，则确定所述第一控制器具备对所述第一流表项进行相应的创建、修改或删除的权限；或者，

当所述第一控制器发起的管理指令为查看指令时，将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项的第二安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第二安全等级，则确定所述第一控制器具备对所述第一流表项进行查看的权限。

结合第一方面的第三种可能的实现方式，在第一方面的第五种可能的实现方式中，在确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理，包括：

若确定所述第一控制器发起的管理指令为创建指令，则根据所述第一控制器发起的管理指令，在所述第一交换机本地创建所述第一流表项，并将所

述第一控制器发起的管理指令中携带的所述第一流表项的安全等级填写入预先增加的所述第一流表项的流表项权限域中；或者，

若确定所述第一控制器发起的管理指令为修改指令或删除指令，则根据所述第一控制器发起的管理指令，查找所述第一交换机本地存储的所述第一流表项，并对查找到的所述第一流表项进行相应的修改处理或删除处理；

或者，若确定所述第一控制器发起的管理指令为查看指令，则根据所述第一控制器发起的管理指令，查找所述第一交换机本地存储的所述第一流表项，并将查找到的所述第一流表项返回给所述第一控制器。

结合第一方面的第四种可能的实现方式，在第一方面的第六种可能的实现方式中，当所述第一控制器发起的管理指令为创建指令时，在确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第一安全等级的同时或之后，且在根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理之前，所述方法还包括：

将所述第一流表项的第一安全等级与所述第一流表项的第二安全等级进行比对，并确定所述第一流表项的第一安全等级不低于所述第一流表项的第二安全等级。

第二方面，提供了一种交换机，应用于流表项管理系统，所述流表项管理系统包括至少一个所述交换机以及至少一个控制器，其中，所述至少一个控制器中存在一个或多个控制器与所述交换机相连接，并且，与所述交换机相连接的一个或多个控制器中的每个控制器相对于所述交换机设置有相应的管理权限等级，所述交换机包括：

指令接收模块，用于接收第一控制器发起的针对第一流表项的管理指令，所述第一控制器为与所述交换机相连接的一个或多个控制器中的任一控制器，所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项或所述交换机中存储的任一已创建流表项；

权限获取模块，用于在所述指令接收模块接收到所述第一控制器发起的管理指令后，获取所述第一控制器相对所述交换机的管理权限等级，以及所

述第一流表项的安全等级；其中，所述第一流表项对应不同的管理指令分别设置有相应的安全等级，所述安全等级用于表示对所述第一流表项进行管理的控制器所应具有的管理权限等级；

权限比对模块，用于根据所述权限获取模块获取到的所述第一控制器相对所述交换机的管理权限等级，以及所述第一流表项的安全等级，将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，以确定所述第一控制器相对所述交换机的管理权限等级是否不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级；

执行模块，用于在所述权限比对模块确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时，确定所述第一控制器具备对所述第一流表项进行相应管理的权限，并根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理。

结合第二方面，在第二方面的第一种可能的实现方式中，所述执行模块，还用于在所述权限比对模块确定所述第一控制器相对所述交换机的管理权限等级低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时，确定所述第一控制器不具备对所述第一流表项进行相应管理的权限，并拒绝执行根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理的操作。

结合第二方面或第二方面的第一种可能的实现方式，在第二方面的第二种可能的实现方式中，所述指令接收模块接收到的所述第一控制器发起的管理指令中携带有所述第一控制器的网络协议地址以及所述第一流表项的匹配域；

所述权限获取模块，具体用于根据所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址以及预先设置的、与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制

器的网络协议地址之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址相对应的管理权限等级，并将查询到的管理权限等级作为获取到的所述第一控制器相对所述交换机的管理权限等级；其中，预先设置的、与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制器的网络协议地址之间的关联关系存储在所述交换机中；以及，

具体用于根据所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域以及预先设置的各流表项的安全等级与各流表项的匹配域之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域相对应的安全等级，并将查询到的安全等级作为获取到的所述第一流表项的安全等级；其中，当所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系携带在所述第一控制器发起的管理指令中，当所述第一流表项为所述交换机中存储的任一已创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系存储在所述交换机中。

结合第二方面或第二方面的第一种可能的实现方式，在第二方面的第三种可能的实现方式中，所述权限获取模块获取到的所述第一流表项的安全等级至少包括所述第一流表项对应于内容修改管理指令的第一安全等级和/或所述第一流表项对应于内容查看管理指令的第二安全等级；

其中，所述内容修改管理指令至少包括创建指令、修改指令以及删除指令中的一种或多种；所述内容查看管理指令至少包括查看指令。

结合第二方面的第三种可能的实现方式，在第二方面的第四种可能的实现方式中，所述权限比对模块，具体用于当所述第一控制器发起的管理指令为创建指令、修改指令或删除指令时，将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项的第一安全等级进行比对，若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等

级，则确定所述第一控制器具备对所述第一流表项进行相应的创建、修改或删除的权限；或者，

具体用于当所述第一控制器发起的管理指令为查看指令时，将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项的第二安全等级进行比对，若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第二安全等级，则确定所述第一控制器具备对所述第一流表项进行查看的权限。

结合第二方面的第三种可能的实现方式，在第二方面的第五种可能的实现方式中，所述执行模块，具体用于在所述权限比对模块确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，若确定所述第一控制器发起的管理指令为创建指令，则根据所述第一控制器发起的管理指令，在所述交换机的本地创建所述第一流表项，并将所述第一控制器发起的管理指令中携带的所述第一流表项的安全等级填写入预先增加的所述第一流表项的流表项权限域中；或者，

若确定所述第一控制器发起的管理指令为修改指令或删除指令，则根据所述第一控制器发起的管理指令，查找所述交换机的本地存储的所述第一流表项，并对查找到的所述第一流表项进行相应的修改或删除处理；或者，

若确定所述第一控制器发起的管理指令为查看指令，则根据所述第一控制器发起的管理指令，查找所述交换机本地存储的所述第一流表项，并将查找到的所述第一流表项返回给所述第一控制器。

结合第二方面的第四种可能的实现方式，在第二方面的第六种可能的实现方式中，所述权限比对模块，还用于当所述第一控制器发起的管理指令为创建指令时，在确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等级的同时或之后，且在所述执行模块根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理之前，将所述第一流表项的第一安全等级与所述第一流表项的第二安全等级进行比对，并确定所述第一流表项的第一安全等级不低于所述第一流表项的第二安全等级。

第三方面，提供了一种交换机，应用于流表项管理系统，所述流表项管理系统包括至少一个所述交换机以及至少一个控制器，其中，所述至少一个控制器中存在一个或多个控制器与所述交换机相连接，并且，与所述交换机相连接的一个或多个控制器中的每个控制器相对于所述交换机设置有相应的管理权限等级，所述交换机包括：

接收器，用于接收第一控制器发起的针对第一流表项的管理指令，所述第一控制器为与所述交换机相连接的一个或多个控制器中的任一控制器，所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项或所述交换机中存储的任一已创建流表项；

处理器，用于在所述接收器接收到所述第一控制器发起的管理指令后，获取所述第一控制器相对所述交换机的管理权限等级，以及所述第一流表项的安全等级，并将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，以及，在确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时，确定所述第一控制器具备对所述第一流表项进行相应管理的权限，并根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理；

其中，所述第一流表项对应不同的管理指令分别设置有相应的安全等级，所述安全等级用于表示对所述第一流表项进行管理的控制器所应具有的管理权限等级。

结合第三方面，在第三方面的第一种可能的实现方式中，所述处理器，还用于在确定所述第一控制器相对所述交换机的管理权限等级低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时，确定所述第一控制器不具备对所述第一流表项进行相应管理的权限，并拒绝执行根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理的操作。

结合第三方面或第三方面的第一种可能的实现方式，在第三方面的第二种可能的实现方式中，所述接收器接收到的所述第一控制器发起的管理指令

中携带有所述第一控制器的网络协议地址以及所述第一流表项的匹配域；

所述处理器，具体用于根据所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址以及预先设置的、与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制器的网络协议地址之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址相对应的管理权限等级，并将查询到的管理权限等级作为获取到的所述第一控制器相对所述交换机的管理权限等级；其中，预先设置的、与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制器的网络协议地址之间的关联关系存储在所述交换机中；以及，

具体用于根据所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域以及预先设置的各流表项的安全等级与各流表项的匹配域之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域相对应的安全等级，并将查询到的安全等级作为获取到的所述第一流表项的安全等级；其中，当所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系携带在所述第一控制器发起的管理指令中，当所述第一流表项为所述交换机中存储的任一已创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系存储在所述交换机中。

结合第三方面或第三方面的第一种可能的实现方式，在第三方面的第三种可能的实现方式中，所述处理器获取到的所述第一流表项的安全等级至少包括所述第一流表项对应于内容修改管理指令的第一安全等级和/或所述第一流表项对应于内容查看管理指令的第二安全等级；

其中，所述内容修改管理指令至少包括创建指令、修改指令以及删除指令中的一种或多种；所述内容查看管理指令至少包括查看指令。

结合第三方面的第三种可能的实现方式，在第三方面的第四种可能的实

现方式中, 所述处理器, 具体用于当所述第一控制器发起的管理指令为创建指令、修改指令或删除指令时, 将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项的第一安全等级进行比对, 若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等级, 则确定所述第一控制器具备对所述第一流表项进行相应的创建、修改或删除的权限; 或者,

具体用于当所述第一控制器发起的管理指令为查看指令时, 将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项的第二安全等级进行比对, 若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第二安全等级, 则确定所述第一控制器具备对所述第一流表项进行查看的权限。

结合第三方面的第三种可能的实现方式, 在第三方面的第五种可能的实现方式中, 所述处理器, 具体用于在确定所述第一控制器具备对所述第一流表项进行相应管理的权限时, 若确定所述第一控制器发起的管理指令为创建指令, 则根据所述第一控制器发起的管理指令, 在所述交换机的本地创建所述第一流表项, 并将所述第一控制器发起的管理指令中携带的所述第一流表项的安全等级填写入预先增加的所述第一流表项的流表项权限域中; 或者,

若确定所述第一控制器发起的管理指令为修改指令或删除指令, 则根据所述第一控制器发起的管理指令, 查找所述交换机的本地存储的所述第一流表项, 并对查找到的所述第一流表项进行相应的修改或删除处理; 或者,

若确定所述第一控制器发起的管理指令为查看指令, 则根据所述第一控制器发起的管理指令, 查找所述交换机本地存储的所述第一流表项, 并将查找到的所述第一流表项返回给所述第一控制器。

结合第三方面的第四种可能的实现方式, 在第三方面的第六种可能的实现方式中, 所述处理器, 还用于当所述第一控制器发起的管理指令为创建指令时, 在确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等级的同时或之后, 且在根据所述第一控制器发起的管

理指令对所述第一流表项进行相应管理之前，将所述第一流表项的第一安全等级与所述第一流表项的第二安全等级进行比对，并确定所述第一流表项的第一安全等级不低于所述第一流表项的第二安全等级。

在本发明实施例所述技术方案中，由于任一交换机在接收到与其相连接的任一控制器发起的针对任一流表项的管理指令后，可首先根据获取到的所述任一控制器相对所述任一交换机的管理权限等级以及所述任一流表项的安全等级，判断所述任一控制器相对所述任一交换机的管理权限等级是否不低于所述任一流表项对应于所述任一控制器发起的管理指令的安全等级，并在确定判断结果为是时，确定所述任一控制器具备对所述任一流表项进行相应管理的权限，并根据所述任一控制器发起的管理指令对所述任一流表项进行相应管理，从而在避免了对流表项进行随意删除或修改等操作现象的基础上，达到了有效保护流表项、进而提高系统安全性的目的。

附图说明

为了更清楚地说明本发明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要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，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。

图 1 所示为本发明实施例一中所述流表项管理方法的流程示意图；

图 2 所示为本发明实施例二中所述交换机的结构示意图；

图 3 所示为本发明实施例三中所述交换机的结构示意图。

具体实施方式

本发明实施例提供了一种流表项管理方法及设备，所述方法可应用于流表项管理系统中，所述流表项管理系统可包括至少一个交换机以及至少一个控制器，其中，针对所述至少一个交换机中的任一交换机，所述至少一个控制器中存在一个或多个控制器与所述任一交换机相连接，并且，与所述任一

交换机相连接的一个或多个控制器中的每个控制器相对于所述任一交换机设置有相应的管理权限等级，具体地，所述方法包括：

第一交换机在接收第一控制器发起的针对第一流表项的管理指令后，获取所述第一控制器相对所述第一交换机的管理权限等级，以及所述第一流表项的安全等级；其中，所述第一流表项对应不同的管理指令分别设置有相应的安全等级，所述安全等级用于表示对所述第一流表项进行管理的控制器所应具有的管理权限等级；所述第一交换机为所述至少一个交换机中的任一交换机，所述第一控制器为与所述第一交换机相连接的一个或多个控制器中的任一控制器，所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项或所述第一交换机中存储的任一已创建流表项；

所述第一交换机将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级，则确定所述第一控制器具备对所述第一流表项进行相应管理的权限，并根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理。

在本发明实施例所述技术方案中，由于任一交换机在接收到与其相连接的任一控制器发起的针对任一表项的管理指令后，可首先根据获取到的所述任一控制器相对所述任一交换机的管理权限等级以及所述任一表项的安全等级，判断所述任一控制器相对所述任一交换机的管理权限等级是否不低于所述任一表项对应于所述任一控制器发起的管理指令的安全等级，并在确定判断结果为是时，确定所述任一控制器具备对所述任一表项进行相应管理的权限，并根据所述任一控制器发起的管理指令对所述任一表项进行相应管理，从而在避免了对流表项进行随意删除或修改等操作现象的基础上，达到了有效保护流表项、进而提高系统安全性的目的。

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施

例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

实施例一：

本发明实施例一提供了一种流表项管理方法，如图 1 所示，其为本发明实施例一中所述流表项管理方法的流程示意图，所述流表项管理方法可应用于本发明实施例所述的流表项管理系统中，所述流表项管理系统可包括至少一个交换机以及至少一个控制器，其中，针对所述至少一个交换机中的任一交换机，所述至少一个控制器中存在一个或多个控制器与所述任一交换机相连接，并且，与所述任一交换机相连接的一个或多个控制器中的每个控制器相对于所述任一交换机设置有相应的管理权限等级。具体地，所述流表项管理方法可包括以下步骤：

步骤 101：第一交换机在接收第一控制器发起的针对第一流表项的管理指令后，获取所述第一控制器相对所述第一交换机的管理权限等级，以及所述第一流表项的安全等级。

其中，在本发明所述实施例中，所述第一流表项对应不同的管理指令分别设置有相应的安全等级，所述安全等级可用于表示对所述第一流表项进行管理的控制器所应具有的管理权限等级；所述第一交换机为所述流表项管理系统中包括的所述至少一个交换机中的任一交换机，所述第一控制器为与所述第一交换机相连接的一个或多个控制器中的任一控制器，所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项或所述第一交换机中存储的任一已创建流表项。

进一步地，需要说明的是，在本发明所述实施例中，如无特殊说明，所述流表项管理系统中包括的各交换机通常指的是 OpenFlow 交换机，本发明实施例对此不再赘述。

进一步地，在本发明所述实施例中，所述第一交换机所接收到的所述第一控制器发起的管理指令可为创建指令、删除指令、修改指令或查看指令等，

本发明实施例对此不作任何限定。并且，所述第一控制器发起的管理指令中通常可携带有所述第一控制器的网络协议地址以及所述第一控制器发起的管理指令所针对的第一流表项的匹配域等信息。另外需要说明的是，所述第一控制器发起的管理指令中还可携带有相应的掩码字符等信息、以进行流表项的模糊匹配等，本发明实施例对此也不作任何限定。

进一步地，需要说明的是，所述第一控制器发起的管理指令中所携带的流表项的匹配域可为一个或多个流表项的匹配域。也就是说，在本发明所述实施例中，所述第一控制器发起的管理指令可为针对一个流表项或多个流表项的管理指令，本发明实施例对此不作任何限定。

进一步地，在本发明所述实施例中，针对所述流表项管理系统中包括的任一交换机，即所述第一交换机，与所述第一交换机相连接的一个或多个控制器中的每个控制器相对于所述第一交换机的管理权限等级通常可由配置点（如 OpenFlow Configuration Point）配置完成。其中，所述配置点可为一独立网元，也可集成在相应的控制器中的集成网元，本发明实施例对此不作任何限定。

具体地，在本发明所述实施例中，针对所述流表项管理系统中包括的任一交换机，即所述第一交换机，所述配置点可通过以下方式配置与所述第一交换机相连接的各控制器相对于所述第一交换机的管理权限等级：

根据与所述第一交换机相连接的各控制器相对所述第一交换机的流表项操作权限的高低，将与所述第一交换机相连接的各控制器划分为多个权限等级；并

根据与所述第一交换机相连接的各控制器所对应的权限等级，为与所述第一交换机相连接的各控制器配置相应的相对于所述第一交换机的管理权限等级。

其中，所配置的与所述第一交换机相连接的各控制器相对于所述第一交换机的管理权限等级通常各不相同。当然，特殊地，也可存在所具备的相对于所述第一交换机的管理权限等级相同的两个或多个控制器，本发明实施例

对此不作任何限定。

另外需要说明的是，在本发明所述实施例中，针对任一控制器，所述控制器相对于与其相连接的不同的交换机的管理权限等级可相同或不同，具体可根据实际情况进行设定，本发明实施例对此也不作任何限定。

进一步地，在本发明所述实施例中，针对所述流表项管理系统中包括的任一交换机，即所述第一交换机，所述配置点在配置与所述第一交换机相连接的各控制器相对于所述第一交换机的管理权限等级的同时或之后，还可配置与所述第一交换机相连接的各控制器的网络协议地址（或各控制器的其他可用于唯一标识各控制器的标识信息）等信息。

进一步地，所述配置点在配置与所述第一交换机相连接的各控制器相对于所述第一交换机的管理权限等级、以及与所述第一交换机相连接的各控制器的网络协议地址等信息的同时或之后，可通过与所述第一交换机进行通信交互的方式，将所配置的与所述第一交换机相连接的各控制器相对于所述第一交换机的管理权限等级以及与所述第一交换机相连接的各控制器的网络协议地址等信息告知所述第一交换机，以使所述第一交换机根据接收到的来自所述配置点的上述信息，获知并存储与所述第一交换机相连接的各控制器相对于所述第一交换机的管理权限等级以及与所述第一交换机相连接的各控制器的网络协议地址等信息。

需要说明的是，在本发明所述实施例中，针对所述流表项管理系统中包括的任一交换机，即所述第一交换机，所述第一交换机在接收到与所述第一交换机相连接的各控制器相对于所述第一交换机的管理权限等级以及与所述第一交换机相连接的各控制器的网络协议地址等信息之后，可根据接收到的上述信息，建立与所述第一交换机相连接的各控制器相对所述第一交换机的管理权限等级和与所述第一交换机相连接的各控制器的网络协议地址（或各控制器的其他可用于唯一标识各控制器的标识信息）之间的关联关系，并通过在本地存储上述关联关系的方式，对接收到的与所述第一交换机相连接各控制器相对于所述第一交换机的管理权限等级以及与所述第一交换机相连接

接的各控制器的网络协议地址等信息进行相应的存储，本发明实施例对此不作任何限定。

相应地，在本发明所述实施例中，针对所述流表项管理系统中包括的任一交换机，即所述第一交换机，所述第一交换机在接收第一控制器发起的针对第一流表项的管理指令后，获取所述第一控制器相对所述第一交换机的管理权限等级，可以包括：

根据所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址以及预先建立的与所述第一交换机相连接的各控制器相对所述第一交换机的管理权限等级和与所述第一交换机相连接的各控制器的网络协议地址之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址相对应的管理权限等级，并将查询到的管理权限等级作为获取到的所述第一控制器相对所述第一交换机的管理权限等级。

进一步地，在本发明所述实施例中，针对所述流表项管理系统中包括的任一交换机，即所述第一交换机，在通过配置点在所述第一交换机上配置与所述第一交换机相连接的各控制器相对于所述第一交换机的管理权限等级以及与所述第一交换机相连接的各控制器的网络协议地址之后，还可将所配置的与所述第一交换机相连接的各控制器相对于所述第一交换机的管理权限等级以及与所述第一交换机相连接的各控制器的网络协议地址发送给相应的控制器，以便各控制器在本地保存与其相关的管理权限等级等配置信息。

具体地，在本发明所述实施例中，针对与所述第一交换机相连接的至少一个控制器中的任一控制器，即所述第一控制器，所述第一控制器可在与所述第一交换机建立相应的会话连接（如OpenFlow会话连接）后，通过向所述第一交换机发送权限获取请求消息（如authority_request消息）的方式，向所述第一交换机请求所述第一控制器相对于所述第一交换机的管理权限等级。相应地，所述第一交换机在接收到所述权限获取请求消息后，可根据所述第一控制器的网络协议地址，查找本地保存的与所述网络协议地址相对应的管理权限等级，并通过向所述第一控制器返回携带有相应管理权限等级的权限

应答消息（如authority_reply消息）的方式，向所述第一控制器返回相应的管理权限等级，本发明实施例对此不再赘述。

进一步地，在本发明所述实施例中，针对所述第一控制器发起的管理指令中携带的任一待创建流表项或所述第一交换机中存储的任一已创建流表项，即第一流表项，所述第一流表项对应不同的管理指令的安全等级通常可以由相应的控制器在下发针对所述第一流表项的创建指令时，由所述相应的控制器根据所述第一流表项的重要性以及私密性所预先配置的。

具体地，所述第一流表项的安全等级可包括所述第一流表项对应于内容修改管理指令的第一安全等级以及所述第一流表项对应于内容查看管理指令的第二安全等级。其中，所述内容修改管理指令至少可包括创建指令、修改指令以及删除指令中的一种或多种，所述内容查看管理指令至少可包括查看指令，本发明实施例对此不作任何限定。

另外需要说明的是，基于安全性的考虑，原则上，在进行所述第一流表项的安全等级的配置时，所配置的所述第一流表项对应于内容修改管理指令的第一安全等级应该不小于所配置的所述第一流表项对应于内容查看管理指令的第二安全等级，本发明实施例对此不作赘述。

进一步地，需要说明的是，在本发明所述实施例中，由于针对任意两个流表项，为其配置的安全等级通常互不相同，因此，为了便于区分各流表项的安全等级，通常可在为各流表项配置相应的安全等级的同时，由相应的控制器预先建立各流表项的安全等级与各流表项的匹配域（或各流表项的其他能够唯一表示各流表项的标识信息）之间的关联关系，以便后续可根据任一流表项的匹配域等信息，确定与其相对应的安全等级，本发明实施例对此不作赘述。

相应地，第一交换机在接收第一控制器发起的针对第一流表项的管理指令后，可通过以下方式获取所述第一流表项的安全等级：

根据所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域以及预先建立的各流表项的安全等级与各流表项的匹配域之间的关联关系，

查询与所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域相对应的安全等级，并将查询到的安全等级作为获取到的所述第一流表项的安全等级。

进一步地，需要说明的是，在本发明所述实施例中，当所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项时，所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系可携带在所述第一控制器发起的管理指令中。相应地，此时，所述第一交换机可根据所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域，查询所述第一控制器发起的管理指令中携带的、与所述第一流表项的匹配域相对应的方式，获取所述第一流表项的安全等级，本发明实施例对此不作赘述。

进一步地，需要说明的是，在本发明所述实施例中，当所述第一流表项为所述第一交换机中存储的任一已创建流表项时，所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系可存储在所述第一交换机中。相应地，此时，所述第一交换机可通过查询所述第一交换机中存储的、与所述第一流表项的匹配域相对应的方式，获取所述第一流表项的安全等级，本发明实施例对此也不作赘述。

步骤 102: 所述第一交换机将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级，则确定所述第一控制器具备对所述第一流表项进行相应管理的权限，并根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理。

具体地，所述第一交换机获取到的所述第一流表项的安全等级可包括所述第一流表项对应于内容修改管理指令的第一安全等级和/或所述第一流表项对应于内容查看管理指令的第二安全等级，具体可根据所述第一控制器发起的管理指令的性质来决定，本发明实施例对此不作任何限定。

例如，当所述第一控制器发起的管理指令为创建指令时，所述第一交换机获取到的所述第一流表项的安全等级通常可包括所述第一流表项的第一安全等级以及所述第一流表项的第二安全等级，即此时，所述第一交换机通常可获取所述第一流表项的所有安全等级。需要说明的是，此时，所述第一控制器发起的管理指令通常可以 flow_mod (OFPFC_ADD) 消息的形式发起，本发明实施例对此不作赘述。

另外需要说明的是，此时，所述第一流表项的第一安全等级以及所述第一流表项的第二安全等级通常可以是由所述第一控制器根据所述第一流表项的重要性和私密性预先配置的；并且，所述第一流表项的第一安全等级以及所述第一流表项的第二安全等级可同时携带在所述 flow_mod (OFPFC_ADD) 消息中发送给所述第一交换机，以使所述第一交换机通过查询所述 flow_mod (OFPFC_ADD) 消息中携带的与所述第一流表项的匹配域相对应的安全等级的方式获取相应的第一安全等级以及第二安全等级，本发明实施例对此也不作赘述。

相应地，当所述第一控制器发起的管理指令为创建指令时，将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级，则确定所述第一控制器具备对所述第一流表项进行相应管理的权限，可以包括：

将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项的第一安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第一安全等级，则确定所述第一控制器具备对所述第一流表项进行相应的创建的权限。

进一步地，当所述第一控制器发起的管理指令为创建指令时，在确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理，可以包括：

根据所述第一控制器发起的管理指令，在所述第一交换机本地创建所述第一流表项，并将所述第一控制器发起的管理指令中携带的所述第一流表项的安全等级填写入预先增加的所述第一流表项的流表项权限域中。其中，预先增加的所述第一流表项的流表项权限域可包括第一权限域和第二权限域。相应地，在进行所述第一流表项的安全等级的填写操作时，可将所述第一流表项的第一安全等级以及所述第一流表项的第二安全等级分别填写入所述流表项的第一权限域以及第二权限域中。

进一步地，需要说明的是，为了保证所创建的第一流表项本身的正确性，当所述第一控制器发起的管理指令为创建指令时，在确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第一安全等级的同时或之后，且在根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理之前，所述方法还可包括：

将所述第一流表项的第一安全等级与所述第一流表项的第二安全等级进行比对，并确定所述第一流表项的第一安全等级不低于所述第一流表项的第二安全等级。

也就是说，在进行第一流表项的创建操作时，除了要保证所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级之外，还需要保证所述第一流表项的第一安全等级不低于所述第一流表项的第二安全等级，以避免由于预先配置的第一流表项的安全等级不正确所导致的无法进行相应流表项的创建操作的目的。

另外，需要说明的是，当所述第一控制器发起的管理指令为针对多个流表项发起的创建指令时，针对每一流表项，均可以按照本发明实施例中所述的权限判断方式对所述第一控制器是否具备对所述流表项进行创建管理的权限进行判断，本发明实施例对此不作任何限定。进一步地，可在依次判断完所述第一控制器是否具备对上述多个流表项中的各流表项进行创建管理的权限之后，且确定所述第一控制器具备对上述多个流表项中的至少一个流表项

进行创建管理的权限时，根据所述第一控制器发起的管理指令，在本地创建相应的至少一个流表项；或者，也可在每次确定所述第一控制器具备对上述多个流表项中的任一流表项进行创建管理的权限时，根据所述第一控制器发起的管理指令，在本地创建相应的任一流表项，本发明实施例对此不作任何限定。

进一步地，当所述第一控制器发起的管理指令为修改指令或删除指令时，为了提高信息获取的便捷性以及节省信息获取资源，所述第一交换机获取到的所述第一流表项的安全等级可仅包括所述第一流表项的第一安全等级。需要说明的是，此时，所述修改指令或删除指令通常可分别以 flow_mod (OFPPC_MODIF) 消息或 flow_mod (OFPPC_DELETE) 消息的形式发起；并且，此时，所述第一流表项的第一安全等级通常可以是通过查询所述第一交换机本地保存的、与所述第一流表项的匹配域相对应的安全等级的方式获取到的，本发明实施例对此不作赘述。

相应地，当所述所述第一控制器发起的管理指令为修改指令或删除指令时，将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级，则确定所述第一控制器具备对所述第一流表项进行相应管理的权限，可以包括：

将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项的第一安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第一安全等级，则确定所述第一控制器具备对所述第一流表项进行相应的修改或删除的权限。

也就是说，在进行第一流表项的修改或删除等操作时，可仅保证所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于修改或删除等管理指令的安全等级即可。

进一步地，当所述第一控制器发起的管理指令为修改指令或删除指令时，

在确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理，可以包括：

根据所述第一控制器发起的管理指令，查找所述第一交换机本地存储的所述第一流表项，并对查找到的所述第一流表项进行相应的修改处理或删除处理。具体地，可通过所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域，查找相应的第一流表项，本发明实施例对此不作赘述。另外需要说明的是，在本发明所述实施例中，根据所述第一控制器发起的管理指令中携带的第一流表项的匹配域查找相应的流表项的操作还可在确定所述第一控制器是否具备对相应流表项进行管理的权限之前进行，本发明实施例对此不作任何限定。

再有需要说明的是，当所述第一控制器发起的管理指令为针对多个流表项发起的修改指令或删除指令时，针对每一流表项，均可以按照本发明实施例中所述的权限判断方式对所述第一控制器是否具备对所述流表项进行修改或删除管理的权限进行判断，本发明实施例对此不作任何限定。进一步地，可在每次确定所述第一控制器具备对上述多个流表项中的任一流表项进行修改或删除管理的权限时，根据所述第一控制器发起的管理指令，查找本地存储的所述任一流表项，并对查找到的所述任一流表项进行相应的修改处理或删除处理，本发明实施例对此不作任何限定。

进一步地，当所述第一控制器发起的管理指令为修改指令时，所述第一控制器发起的管理指令中通常还可携带有对相应流表项进行修改的修改内容信息，本发明实施例对此不作赘述。

进一步地，当所述第一控制器发起的管理指令为查看指令时，为了提高信息获取的便捷性以及节省信息获取资源，所述第一交换机获取到的所述第一流表项的安全等级可仅包括所述第一流表项的第二安全等级。当然，需要说明的是，由于第一流表项被创建后，其所对应的第一安全等级通常不小于其所对应的第二安全等级，因此，此时，所述第一交换机也可仅获取所述第一流表项的第一安全等级，或也可同时获取所述第一流表项的第一安全等级

以及所述第一流表项的第二安全等级，本发明实施例对此不作任何限定。另外需要说明的是，此时，所述查看指令通常可以 multipart (ofp_flow_stats_request) 消息的形式发起；并且，此时，所述第一流表项的第一安全等级或所述第一流表项的第二安全等级通常可以通过查询所述第一交换机本地保存的、与所述第一流表项的匹配域相对应的安全等级的方式获取到的，本发明实施例对此不作赘述。

相应地，当所述第一控制器发起的管理指令为查看指令时，将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级，则确定所述第一控制器具备对所述第一流表项进行相应管理的权限，可以包括：

将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项的第二安全等级（或所述第一流表项的第一安全等级）进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第二安全等级（或确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第一安全等级），则确定所述第一控制器具备对所述第一流表项进行查看的权限。

也就是说，在进行第一流表项的查看操作时，可仅保证所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第二安全等级（或所述第一流表项的第一安全等级）即可。

进一步地，当所述第一控制器发起的管理指令为查看指令时，在确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理，可以包括：

根据所述第一控制器发起的管理指令，查找所述第一交换机本地存储的所述第一流表项，并将查找到的所述第一流表项返回给所述第一控制器，以使所述第一控制器对所述第一流表项进行相应的查看处理。

需要说明的是，当所述第一控制器发起的管理指令为针对多个流表项发起的查看指令时，针对每一流表项，均可以按照本发明实施例中所述的权限判断方式对所述第一控制器是否具备对所述流表项进行查看管理的权限进行判断，本发明实施例对此不作任何限定。进一步地，可在依次判断完所述第一控制器是否具备对上述多个流表项中的各流表项进行查看管理的权限之后，且确定所述第一控制器具备对上述多个流表项中的至少一个流表项进行查看管理的权限时，根据所述第一控制器发起的管理指令，查找本地存储的所述至少一个流表项，并将查找到的所述至少一个流表项返回给所述第一控制器；具体地，此时，可通过将所述至少一个流表项组装成 ofp_multipart_reply (ofp_flow_stats) 消息的方式，返回给所述第一控制器。或者，也可在每次确定所述第一控制器具备对上述多个流表项中的任一流表项进行查看管理的权限时，根据所述第一控制器发起的管理指令，查找本地存储的所述任一流表项，并将查找到的所述任一流表项返回给所述第一控制器，本发明实施例对此不作任何限定。

另外需要说明的是，在本发明所述实施例中，在确定所述第一控制器具备对所述第一流表项进行管理的权限，且根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理之后，还可向所述第一控制器返回用于表示管理成功或管理失败的第一响应消息，本发明实施例对此不作任何限定。

进一步地，在本发明所述实施例中，所述方法还可包括以下步骤：

所述第一交换机若确定所述第一控制器相对所述第一交换机的管理权限等级低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级，则确定所述第一控制器不具备对所述第一流表项进行相应管理的权限，并拒绝执行根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理的操作。

具体地，所述第一交换机可通过向所述第一控制器返回用于表示所述第一控制器不具备对所述第一流表项进行管理的权限的第二响应消息的方式，拒绝执行根据所述第一控制器发起的管理指令对所述第一流表项进行相应管

理的操作，本发明实施例对此不作赘述。

本发明实施例一提供了一种流表项管理方法，在本发明实施例一所述技术方案中，由于任一交换机在接收到与其相连接的任一控制器发起的针对任一流表项的管理指令后，可首先根据获取到的所述任一控制器相对所述任一交换机的管理权限等级以及所述任一流表项的安全等级，判断所述任一控制器相对所述任一交换机的管理权限等级是否不低于所述任一流表项对应于所述任一控制器发起的管理指令的安全等级，并在确定判断结果为是时，确定所述任一控制器具备对所述任一流表项进行相应管理的权限，并根据所述任一控制器发起的管理指令对所述任一流表项进行相应管理，从而在避免了对流表项进行随意删除或修改等操作现象的基础上，达到了有效保护流表项、进而提高系统安全性的目的。

另外，在本发明实施例一所述技术方案中，通过控制器相对交换机的管理权限等级的配置以及权限的判断等操作，还可进一步达到隔离多个控制器在同一交换机上的流表项，以实现其他控制器无法操作本控制器所创建的流表项的效果。

实施例二：

本发明实施例二提供了一种可用于实现本发明实施例一所示方法的交换机，所述交换机可应用于流表项管理系统中，所述流表项管理系统可包括至少一个本发明实施例二所述的交换机以及至少一个控制器，其中，所述至少一个控制器中存在一个或多个控制器与所述交换机相连接，并且，与所述交换机相连接的一个或多个控制器中的每个控制器相对于所述交换机设置有相应的管理权限等级。

具体地，如图2所示，其为本发明实施例二所述交换机的结构示意图，所述交换机可包括指令接收模块11、权限获取模块12、权限比对模块13以及执行模块14，其中：

所述指令接收模块11可用于接收第一控制器发起的针对第一流表项的管理指令，所述第一控制器为与所述交换机相连接的一个或多个控制器中的任

一控制器，所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项或所述交换机中存储的任一已创建流表项；

所述权限获取模块 12 可用于在所述指令接收模块 11 接收到所述第一控制器发起的管理指令后，获取所述第一控制器相对所述交换机的管理权限等级，以及所述第一流表项的安全等级；其中，所述第一流表项对应不同的管理指令分别设置有相应的安全等级，所述安全等级用于表示对所述第一流表项进行管理的控制器所应具有的管理权限等级；

所述权限比对模块 13 可用于根据所述权限获取模块 12 获取到的所述第一控制器相对所述交换机的管理权限等级以及所述第一流表项的安全等级，将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，以确定所述第一控制器相对所述交换机的管理权限等级是否不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级；

所述执行模块 14 可用于在所述权限比对模块 13 确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时，确定所述第一控制器具备对所述第一流表项进行相应管理的权限，并根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理。

具体地，在本发明所述实施例中，所述指令接收模块 11 所接收到的所述第一控制器发起的管理指令可为创建指令、删除指令、修改指令或查看指令等，本发明实施例对此不作任何限定。并且，所述第一控制器发起的管理指令中通常可携带有所述第一控制器的网络协议地址以及所述第一控制器发起的管理指令所针对的第一流表项的匹配域等信息。另外需要说明的是，所述第一控制器发起的管理指令中还可携带有相应的掩码字符等信息、以进行流表项的模糊匹配等，本发明实施例对此也不作任何限定。

进一步地，需要说明的是，所述第一控制器发起的管理指令中所携带的流表项的匹配域可为一个或多个流表项的匹配域。也就是说，在本发明所述

实施例中，所述第一控制器发起的管理指令可为针对一个流表项或多个流表项的管理指令，本发明实施例对此不作任何限定。

进一步地，在本发明所述实施例中，所述交换机还可包括信息配置模块 15：

所述信息配置模块 15 可用于，通过与配置点进行通信交互的方式，获知所述配置点所配置的与所述交换机相连接的各控制器相对于所述交换机的管理权限等级以及与所述交换机相连接的各控制器的网络协议地址等信息。

其中，所配置的与所述交换机相连接的各控制器相对于所述交换机的管理权限等级通常各不相同。当然，特殊地，也可存在所具备的相对于所述交换机的管理权限等级相同的两个或多个控制器，本发明实施例对此不作任何限定。

另外需要说明的是，在本发明所述实施例中，针对任一控制器，所述控制器相对于与其相连接的不同的交换机的管理权限等级可相同或不同，具体可根据实际情况进行设定，本发明实施例对此也不作任何限定。

进一步地，所述信息配置模块 15 还可用于根据接收到的与所述交换机相连接的各控制器相对于所述交换机的管理权限等级以及与所述交换机相连接的各控制器的网络协议地址等信息，建立与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制器的网络协议地址之间的关联关系，并通过存储上述关联关系的方式，对接收到的与所述交换机相连接的各控制器相对于所述交换机的管理权限等级以及与所述交换机相连接的各控制器的网络协议地址等信息进行相应的存储。

相应地，所述权限获取模块 12 具体可用于在接收第一控制器发起的针对第一流表项的管理指令后，根据所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址，以及所述信息配置模块 15 预先建立的与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制器的网络协议地址之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址相对应的管理权限等

级，并将查询到的管理权限等级作为获取到的所述第一控制器相对所述交换机的管理权限等级。

进一步地，在本发明所述实施例中，所述第一流表项对应不同的管理指令的安全等级通常可以是由相应的控制器在下发针对所述第一流表项的创建指令时，由所述相应的控制器根据所述第一流表项的重要性以及私密性所预先配置的。具体地，所述第一流表项的安全等级可包括所述第一流表项对应于内容修改管理指令的第一安全等级以及所述第一流表项对应于内容查看管理指令的第二安全等级。其中，所述内容修改管理指令至少可包括创建指令、修改指令以及删除指令中的一种或多种，所述内容查看管理指令至少可包括查看指令，本发明实施例对此不作任何限定。

另外需要说明的是，基于安全性的考虑，原则上，在进行所述第一流表项的安全等级的配置时，所配置的所述第一流表项对应于内容修改管理指令的第一安全等级应该不小于所配置的所述第一流表项对应于内容查看管理指令的第二安全等级，本发明实施例对此不作赘述。

进一步地，在本发明所述实施例中，由于针对任意两个流表项，为其配置的安全等级通常互不相同，因此，为了便于区分各流表项的安全等级，通常可在为各流表项配置相应的安全等级的同时，建立各流表项的安全等级与各流表项的匹配域之间的关联关系；相应地，所述权限获取模块 12 具体可用于在接收第一控制器发起的针对第一流表项的管理指令后，根据所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域以及预先建立的各流表项的安全等级与各流表项的匹配域之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域相对应的安全等级，并将查询到的安全等级作为获取到的所述第一流表项的安全等级；其中，当所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系可携带在所述第一控制器发起的管理指令中，当所述第一流表项为所述交换机中存储的任一已创建流表项时，预先设置的所述第一流表项的

安全等级与所述第一流表项的匹配域之间的关联关系可存储在所述交换机中。

需要说明的是，所述权限获取模块12获取到的所述第一流表项的安全等级可包括所述第一流表项对应于内容修改管理指令的第一安全等级和/或所述第一流表项对应于内容查看管理指令的第二安全等级，具体可根据所述第一控制器发起的管理指令的性质来决定，本发明实施例对此不作任何限定。

例如，当所述第一控制器发起的管理指令为创建指令时，所述权限获取模块12获取到的所述第一流表项的安全等级通常可包括所述第一流表项的第一安全等级以及所述第一流表项的第二安全等级；当所述第一控制器发起的管理指令为修改指令或删除指令时，所述权限获取模块12获取到的所述第一流表项的安全等级可仅包括所述第一流表项的第一安全等级；当所述第一控制器发起的管理指令为查看指令时，所述权限获取模块12获取到的所述第一流表项的安全等级可仅包括所述第一流表项的第二安全等级，本发明实施例对此不作赘述。

进一步地，所述权限比对模块13具体可用于当所述第一控制器发起的管理指令为创建指令、修改指令或删除指令时，将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项的第一安全等级进行比对，若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等级，则确定所述第一控制器具备对所述第一流表项进行相应的创建、修改或删除的权限；或者，

具体可用于当所述第一控制器发起的管理指令为查看指令时，将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项的第二安全等级进行比对，若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第二安全等级，则确定所述第一控制器具备对所述第一流表项进行查看的权限。

进一步地，所述执行模块14具体可用于在所述权限比对模块13确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，若确定所述第

一控制器发起的管理指令为创建指令，则根据所述第一控制器发起的管理指令，在所述交换机的本地创建所述第一流表项，并将所述第一控制器发起的管理指令中携带的所述第一流表项的安全等级填写入预先增加的所述第一流表项的流表项权限域中；或者，

具体可用于在所述权限比对模块 13 确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，若确定所述第一控制器发起的管理指令为修改指令或删除指令，则根据所述第一控制器发起的管理指令，查找所述交换机的本地存储的所述第一流表项，并对查找到的所述第一流表项进行相应的修改或删除处理；或者，

具体可用于在所述权限比对模块 13 确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，若确定所述第一控制器发起的管理指令为查看指令，则根据所述第一控制器发起的管理指令，查找所述交换机本地存储的所述第一流表项，并将查找到的所述第一流表项返回给所述第一控制器。

具体地，预先增加的所述第一流表项的流表项权限域可包括第一权限域和第二权限域。相应地，所述执行模块 14 具体可用于在进行所述第一流表项的安全等级的填写操作时，将所述第一流表项的第一安全等级以及所述第一流表项的第二安全等级分别填写入所述流表项的第一权限域以及第二权限域中，本发明实施例对此不作赘述。

进一步地，需要说明的是，在本发明所述实施例中，为了保证所创建的第一流表项本身的正确性，所述权限比对模块 13 还可用于当所述第一控制器发起的管理指令为创建指令时，在确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等级的同时或之后，且在所述执行模块 14 根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理之前，将所述第一流表项的第一安全等级与所述第一流表项的第二安全等级进行比对，并确定所述第一流表项的第一安全等级不低于所述第一流表项的第二安全等级。

也就是说，在进行第一流表项的创建操作时，除了要保证所述第一控制

器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级之外，还需要保证所述第一流表项的第一安全等级不低于所述第一流表项的第二安全等级，以避免由于预先配置的第一流表项的安全等级不正确所导致的无法进行相应流表项的创建操作的目的。

进一步地，在本发明所述实施例中，所述执行模块 14 还可用于在所述权限比对模块 13 确定所述第一控制器相对所述交换机的管理权限等级低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时，确定所述第一控制器不具备对所述第一流表项进行相应管理的权限，并拒绝执行根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理的操作。

本发明实施例二提供了一种可用于实现本发明实施例一中所述流表项管理方法的交换机，在本发明实施例二所述技术方案中，由于所述交换机在接收到与其相连接的任一控制器发起的针对任一流表项的管理指令后，可首先根据获取到的所述任一控制器相对所述交换机的管理权限等级以及所述任一流表项的安全等级，判断所述任一控制器相对所述交换机的管理权限等级是否不低于所述任一流表项对应于所述任一控制器发起的管理指令的安全等级，并在确定判断结果为是时，确定所述任一控制器具备对所述任一流表项进行相应管理的权限，并根据所述任一控制器发起的管理指令对所述任一流表项进行相应管理，从而在避免了对流表项进行随意删除或修改等操作现象的基础上，达到了有效保护流表项、进而提高系统安全性的目的。

另外，在本发明实施例二所述技术方案中，通过控制器相对交换机的管理权限等级的配置以及权限的判断等操作，还可进一步达到隔离多个控制器在同一交换机上的流表项，以实现其他控制器无法操作本控制器所创建的流表项的效果。

实施例三：

本发明实施例三提供了一种可用于实现本发明实施例一所示方法的交换机，所述交换机可应用于流表项管理系统中，所述流表项管理系统可包括至

少一个本发明实施例三中所所述的交换机以及至少一个控制器，其中，所述至少一个控制器中存在一个或多个控制器与所述交换机相连接，并且，与所述交换机相连接的一个或多个控制器中的每个控制器相对于所述交换机设置有相应的管理权限等级。

具体地，如图 3 所示，其为本发明实施例三中所所述交换机的结构示意图，所述交换机可包括接收器 21 以及处理器 22 等部件。本领域技术人员可以理解，图 3 中示出的交换机的结构并不构成对交换机的限定，还可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置，本发明实施例对此不作任何限定。

具体地，下面结合图 3 对所述交换机的各个构成部件进行具体的介绍：

所述接收器 21 可用于接收第一控制器发起的针对第一流表项的管理指令，所述第一控制器为与所述交换机相连接的一个或多个控制器中的任一控制器，所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项或所述交换机中存储的任一已创建流表项；

所述处理器 22 可用于在所述接收器 21 接收到所述第一控制器发起的管理指令后，获取所述第一控制器相对所述交换机的管理权限等级以及所述第一流表项的安全等级，并将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，以及，在确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时，确定所述第一控制器具备对所述第一流表项进行相应管理的权限，并根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理；

其中，所述第一流表项对应不同的管理指令分别设置有相应的安全等级，所述安全等级用于表示对所述第一流表项进行管理的控制器所应具有的管理权限等级。

具体地，在本发明所述实施例中，所述接收器 21 所接收到的所述第一控制器发起的管理指令可为创建指令、删除指令、修改指令或查看指令等，本

发明实施例对此不作任何限定。并且，所述第一控制器发起的管理指令中通常可携带有所述第一控制器的网络协议地址以及所述第一控制器发起的管理指令所针对的第一流表项的匹配域等信息。另外需要说明的是，所述第一控制器发起的管理指令中还可携带有相应的掩码字符等信息，以进行流表项的模糊匹配等，本发明实施例对此也不作任何限定。

进一步地，需要说明的是，所述第一控制器发起的管理指令中所携带的流表项的匹配域可为一个或多个流表项的匹配域。也就是说，在本发明所述实施例中，所述第一控制器发起的管理指令可为针对一个流表项或多个流表项的管理指令，本发明实施例对此不作任何限定。

进一步地，在本发明所述实施例中，所述处理器 22 还可用于通过与配置点进行通信交互的方式，获知所述配置点所配置的与所述交换机相连接的各控制器相对于所述交换机的管理权限等级以及与所述交换机相连接的各控制器的网络协议地址等信息。

其中，所述配置点所配置的与所述交换机相连接的各控制器相对于所述交换机的管理权限等级通常各不相同。当然，特殊地，也可存在所具备的相对于所述交换机的管理权限等级相同的两个或多个控制器，本发明实施例对此不作任何限定。

另外需要说明的是，在本发明所述实施例中，针对任一控制器，所述控制器相对于与其相连接的不同的交换机的管理权限等级可相同或不同，具体可根据实际情况进行设定，本发明实施例对此也不作任何限定。

进一步地，所述处理器 22 还可用于根据接收到的与所述交换机相连接的各控制器相对于所述交换机的管理权限等级以及与所述交换机相连接的各控制器的网络协议地址等信息，建立与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制器的网络协议地址之间的关联关系，并通过将上述关联关系存储在所述交换机具备的存储器 23 中的方式，对接收到的与所述交换机相连接的各控制器相对于所述交换机的管理权限等级以及与所述交换机相连接的各控制器的网络协议地址等信息进

行相应的存储。

其中，所述存储器 23 可以是 ROM (read-only memory, 只读存储器) 或可存储静态信息和指令的其他类型的静态存储设备, RAM (random access memory, 随机存取存储器) 或者可存储信息和指令的其他类型的动态存储设备, 也可以是 EEPROM (Electrically Erasable Programmable Read-Only Memory, 电可擦可编程只读存储器), CD-ROM (Compact Disc Read-Only Memory, 只读光盘) 或其他光盘存储、光碟存储 (包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备, 或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质, 但不限于此。

进一步地, 所述处理器 22 具体可用于在接收第一控制器发起的针对第一流表项的管理指令后, 根据所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址, 以及预先建立的与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制器的网络协议地址之间的关联关系, 查询与所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址相对应的管理权限等级, 并将查询到的管理权限等级作为获取到的所述第一控制器相对所述交换机的管理权限等级。

进一步地, 在本发明所述实施例中, 所述第一流表项对应不同的管理指令的安全等级通常可以是由相应的控制器在下发针对所述第一流表项的创建指令时, 由所述相应的控制器根据所述第一流表项的重要性以及私密性所预先配置的。具体地, 所述第一流表项的安全等级可包括所述第一流表项对应于内容修改管理指令的第一安全等级以及所述第一流表项对应于内容查看管理指令的第二安全等级。其中, 所述内容修改管理指令至少可包括创建指令、修改指令以及删除指令中的一种或多种, 所述内容查看管理指令至少可包括查看指令, 本发明实施例对此不作任何限定。

另外需要说明的是, 基于安全性的考虑, 原则上, 在进行所述第一流表项的安全等级的配置时, 所配置的所述第一流表项对应于内容修改管理指令

的第一安全等级应该不小于所配置的所述第一流表项对应于内容查看管理指令的第二安全等级，本发明实施例对此不作赘述。

进一步地，在本发明所述实施例中，由于针对任意两个流表项，为其配置的安全等级通常互不相同，因此，为了便于区分各流表项的安全等级，通常可在为各流表项配置相应的安全等级的同时，建立各流表项的安全等级与各流表项的匹配域之间的关联关系。相应地，所述处理器 22 具体可用于在接收第一控制器发起的针对第一流表项的管理指令后，根据所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域以及预先建立的各流表项的安全等级与各流表项的匹配域之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域相对应的安全等级，并将查询到的安全等级作为获取到的所述第一流表项的安全等级。其中，当所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系可携带在所述第一控制器发起的管理指令中，当所述第一流表项为所述交换机中存储的任一已创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系可存储在所述交换机中。

需要说明的是，所述处理器 22 获取到的所述第一流表项的安全等级可包括所述第一流表项对应于内容修改管理指令的第一安全等级和/或所述第一流表项对应于内容查看管理指令的第二安全等级，具体可根据所述第一控制器发起的管理指令的性质来决定，本发明实施例对此不作任何限定。

例如，当所述第一控制器发起的管理指令为创建指令时，所述处理器 22 获取到的所述第一流表项的安全等级通常可包括所述第一流表项的第一安全等级以及所述第一流表项的第二安全等级；当所述第一控制器发起的管理指令为修改指令或删除指令时，所述处理器 22 获取到的所述第一流表项的安全等级可仅包括所述第一流表项的第一安全等级；当所述第一控制器发起的管理指令为查看指令时，所述处理器 22 获取到的所述第一流表项的安全等级可仅包括所述第一流表项的第二安全等级，本发明实施例对此不作赘述。

进一步地，所述处理器 22 具体可用于当所述第一控制器发起的管理指令为创建指令、修改指令或删除指令时，将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项的第一安全等级进行比对，若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等级，则确定所述第一控制器具备对所述第一流表项进行相应的创建、修改或删除的权限；或者，

具体可用于当所述第一控制器发起的管理指令为查看指令时，将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项的第二安全等级进行比对，若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第二安全等级，则确定所述第一控制器具备对所述第一流表项进行查看的权限。

进一步地，所述处理器 22 具体还可用于在确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，若确定所述第一控制器发起的管理指令为创建指令，则根据所述第一控制器发起的管理指令，在所述交换机的本地创建所述第一流表项，并将所述第一控制器发起的管理指令中携带的所述第一流表项的安全等级填写入预先增加的所述第一流表项的流表项权限域中；或者，

具体可用于在确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，若确定所述第一控制器发起的管理指令为修改指令或删除指令，则根据所述第一控制器发起的管理指令，查找所述交换机的本地存储的所述第一流表项，并对查找到的所述第一流表项进行相应的修改或删除处理；或者，

具体可用于在确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，若确定所述第一控制器发起的管理指令为查看指令，则根据所述第一控制器发起的管理指令，查找所述交换机本地存储的所述第一流表项，并将查找到的所述第一流表项返回给所述第一控制器。

具体地，预先增加的所述第一流表项的流表项权限域可包括第一权限域

和第二权限域。相应地，所述处理器 22 具体可用于在进行所述第一流表项的安全等级的填写操作时，将所述第一流表项的第一安全等级以及所述第一流表项的第二安全等级分别填写入所述流表项的第一权限域以及第二权限域中，本发明实施例对此不作赘述。

进一步地，需要说明的是，在本发明所述实施例中，为了保证所创建的第一流表项本身的正确性，所述处理器 22 还可用于当所述第一控制器发起的管理指令为创建指令时，在确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等级的同时或之后，且在根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理之前，将所述第一流表项的第一安全等级与所述第一流表项的第二安全等级进行比对，并确定所述第一流表项的第一安全等级不低于所述第一流表项的第二安全等级。

也就是说，在进行第一流表项的创建操作时，除了要保证所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级之外，还需要保证所述第一流表项的第一安全等级不低于所述第一流表项的第二安全等级，以避免由于预先配置的第一流表项的安全等级不正确所导致的无法进行相应流表项的创建操作的目的。

进一步地，在本发明所述实施例中，所述处理器 22 还可用于在确定所述第一控制器相对所述交换机的管理权限等级低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时，确定所述第一控制器不具备对所述第一流表项进行相应管理的权限，并拒绝执行根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理的操作。

本发明实施例三提供了一种可用于实现本发明实施例一中所述流表项管理方法的交换机，在本发明实施例三所述技术方案中，由于所述交换机在接收到与其相连接的任一控制器发起的针对任一流表项的管理指令后，可首先根据获取到的所述任一控制器相对所述交换机的管理权限等级以及所述任一流表项的安全等级，判断所述任一控制器相对所述交换机的管理权限等级是

否不低于所述任一流表项对应于所述任一控制器发起的管理指令的安全等级，并在确定判断结果为是时，确定所述任一控制器具备对所述任一流表项进行相应管理的权限，并根据所述任一控制器发起的管理指令对所述任一流表项进行相应管理，从而在避免了对流表项进行随意删除或修改等操作现象的基础上，达到了有效保护流表项、进而提高系统安全性的目的。

另外，在本发明实施例三所述技术方案中，通过控制器相对交换机的管理权限等级的配置以及权限的判断等操作，还可进一步达到隔离多个控制器在同一交换机上的流表项，以实现其他控制器无法操作本控制器所创建的流表项的效果。

本领域技术人员应明白，本发明的实施例可提供为方法、装置（设备）、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、装置（设备）和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的

处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种流表项管理方法，其特征在于，应用于流表项管理系统，所述流表项管理系统包括至少一个交换机以及至少一个控制器，其中，针对所述至少一个交换机中的任一交换机，所述至少一个控制器中存在一个或多个控制器与所述任一交换机相连接，并且，与所述任一交换机相连接的一个或多个控制器中的每个控制器相对于所述任一交换机设置有相应的管理权限等级，所述方法包括：

第一交换机在接收第一控制器发起的针对第一流表项的管理指令后，获取所述第一控制器相对所述第一交换机的管理权限等级，以及所述第一流表项的安全等级；其中，所述第一流表项对应不同的管理指令分别设置有相应的安全等级，所述安全等级用于表示对所述第一流表项进行管理的控制器所应具有的管理权限等级；所述第一交换机为所述至少一个交换机中的任一交换机，所述第一控制器为与所述第一交换机相连接的一个或多个控制器中的任一控制器，所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项或所述第一交换机中存储的任一已创建流表项；

所述第一交换机将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级，则确定所述第一控制器具备对所述第一流表项进行相应管理的权限，并根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理。

2、如权利要求1所述的流表项管理方法，其特征在于，所述方法还包括：

所述第一交换机若确定所述第一控制器相对所述第一交换机的管理权限等级低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级，则确定所述第一控制器不具备对所述第一流表项进行相应管理的权限，并拒绝执行根据所述第一控制器发起的管理指令对所述第一流表项进行相应

管理的操作。

3、如权利要求 1 或 2 所述的流表项管理方法，其特征在于，所述第一控制器发起的管理指令中携带有所述第一控制器的网络协议地址以及所述第一流表项的匹配域；

获取所述第一控制器相对所述第一交换机的管理权限等级，包括：

根据所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址以及预先设置的、与所述第一交换机相连接的各控制器相对所述第一交换机的管理权限等级和与所述第一交换机相连接的各控制器的网络协议地址之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址相对应的管理权限等级，并将查询到的管理权限等级作为获取到的所述第一控制器相对所述第一交换机的管理权限等级；其中，预先设置的、与所述第一交换机相连接的各控制器相对所述第一交换机的管理权限等级和与所述第一交换机相连接的各控制器的网络协议地址之间的关联关系存储在所述第一交换机中；

获取所述第一流表项的安全等级，包括：

根据所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域以及预先设置的各流表项的安全等级与各流表项的匹配域之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域相对应的安全等级，并将查询到的安全等级作为获取到的所述第一流表项的安全等级；其中，当所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系携带在所述第一控制器发起的管理指令中，当所述第一流表项为所述第一交换机中存储的任一已创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系存储在所述第一交换机中。

4、如权利要求 1 或 2 所述的流表项管理方法，其特征在于，

获取到的所述第一流表项的安全等级至少包括所述第一流表项对应于内

容修改管理指令的第一安全等级和/或所述第一流表项对应于内容查看管理指令的第二安全等级;

其中, 所述内容修改管理指令至少包括创建指令、修改指令以及删除指令中的一种或多种; 所述内容查看管理指令至少包括查看指令。

5、如权利要求 4 所述的流表项管理方法, 其特征在于, 将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对, 若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级, 则确定所述第一控制器具备对所述第一流表项进行相应管理的权限, 包括:

当所述第一控制器发起的管理指令为创建指令、修改指令或删除指令时, 将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项的第一安全等级进行比对, 若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第一安全等级, 则确定所述第一控制器具备对所述第一流表项进行相应的创建、修改或删除的权限; 或者,

当所述第一控制器发起的管理指令为查看指令时, 将所述第一控制器相对所述第一交换机的管理权限等级和所述第一流表项的第二安全等级进行比对, 若确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第二安全等级, 则确定所述第一控制器具备对所述第一流表项进行查看的权限。

6、如权利要求 4 所述的流表项管理方法, 其特征在于, 在确定所述第一控制器具备对所述第一流表项进行相应管理的权限时, 根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理, 包括:

若确定所述第一控制器发起的管理指令为创建指令, 则根据所述第一控制器发起的管理指令, 在所述第一交换机本地创建所述第一流表项, 并将所述第一控制器发起的管理指令中携带的所述第一流表项的安全等级填写入预先增加的所述第一流表项的流表项权限域中; 或者,

若确定所述第一控制器发起的管理指令为修改指令或删除指令，则根据所述第一控制器发起的管理指令，查找所述第一交换机本地存储的所述第一流表项，并对查找到的所述第一流表项进行相应的修改处理或删除处理；

或者，若确定所述第一控制器发起的管理指令为查看指令，则根据所述第一控制器发起的管理指令，查找所述第一交换机本地存储的所述第一流表项，并将查找到的所述第一流表项返回给所述第一控制器。

7、如权利要求5所述的流表项管理方法，其特征在于，当所述第一控制器发起的管理指令为创建指令时，在确定所述第一控制器相对所述第一交换机的管理权限等级不低于所述第一流表项的第一安全等级的同时或之后，且在根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理之前，所述方法还包括：

将所述第一流表项的第一安全等级与所述第一流表项的第二安全等级进行比对，并确定所述第一流表项的第一安全等级不低于所述第一流表项的第二安全等级。

8、一种交换机，其特征在于，应用于流表项管理系统，所述流表项管理系统包括至少一个所述交换机以及至少一个控制器，其中，所述至少一个控制器中存在一个或多个控制器与所述交换机相连接，并且，与所述交换机相连接的一个或多个控制器中的每个控制器相对于所述交换机设置有相应的管理权限等级，所述交换机包括：

指令接收模块，用于接收第一控制器发起的针对第一流表项的管理指令，所述第一控制器为与所述交换机相连接的一个或多个控制器中的任一控制器，所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项或所述交换机中存储的任一已创建流表项；

权限获取模块，用于在所述指令接收模块接收到所述第一控制器发起的管理指令后，获取所述第一控制器相对所述交换机的管理权限等级，以及所述第一流表项的安全等级；其中，所述第一流表项对应不同的管理指令分别设置有相应的安全等级，所述安全等级用于表示对所述第一流表项进行管理

的控制器所应具有的管理权限等级;

权限比对模块, 用于根据所述权限获取模块获取到的所述第一控制器相对所述交换机的管理权限等级, 以及所述第一流表项的安全等级, 将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对, 以确定所述第一控制器相对所述交换机的管理权限等级是否不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级;

执行模块, 用于在所述权限比对模块确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时, 确定所述第一控制器具备对所述第一流表项进行相应管理的权限, 并根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理。

9、如权利要求 8 所述的交换机, 其特征在于,

所述执行模块, 还用于在所述权限比对模块确定所述第一控制器相对所述交换机的管理权限等级低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时, 确定所述第一控制器不具备对所述第一流表项进行相应管理的权限, 并拒绝执行根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理的操作。

10、如权利要求 8 或 9 所述的交换机, 其特征在于, 所述指令接收模块接收到的所述第一控制器发起的管理指令中携带有所述第一控制器的网络协议地址以及所述第一流表项的匹配域;

所述权限获取模块, 具体用于根据所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址以及预先设置的、与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制器的网络协议地址之间的关联关系, 查询与所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址相对应的管理权限等级, 并将查询到的管理权限等级作为获取到的所述第一控制器相对所述交换机的管理权限

等级；其中，预先设置的、与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制器的网络协议地址之间的关联关系存储在所述交换机中；以及，

具体用于根据所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域以及预先设置的各流表项的安全等级与各流表项的匹配域之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域相对应的安全等级，并将查询到的安全等级作为获取到的所述第一流表项的安全等级；其中，当所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系携带在所述第一控制器发起的管理指令中，当所述第一流表项为所述交换机中存储的任一已创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系存储在所述交换机中。

11、如权利要求 8 或 9 所述的交换机，其特征在于，

所述权限获取模块获取到的所述第一流表项的安全等级至少包括所述第一流表项对应于内容修改管理指令的第一安全等级和/或所述第一流表项对应于内容查看管理指令的第二安全等级；

其中，所述内容修改管理指令至少包括创建指令、修改指令以及删除指令中的一种或多种；所述内容查看管理指令至少包括查看指令。

12、如权利要求 11 所述的交换机，其特征在于，

所述权限比对模块，具体用于当所述第一控制器发起的管理指令为创建指令、修改指令或删除指令时，将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项的第一安全等级进行比对，若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等级，则确定所述第一控制器具备对所述第一流表项进行相应的创建、修改或删除的权限；或者，

具体用于当所述第一控制器发起的管理指令为查看指令时，将所述第一

控制器相对所述交换机的管理权限等级和所述第一流表项的第二安全等级进行比对，若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第二安全等级，则确定所述第一控制器具备对所述第一流表项进行查看的权限。

13、如权利要求 11 所述的交换机，其特征在于，

所述执行模块，具体用于在所述权限比对模块确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，若确定所述第一控制器发起的管理指令为创建指令，则根据所述第一控制器发起的管理指令，在所述交换机的本地创建所述第一流表项，并将所述第一控制器发起的管理指令中携带的所述第一流表项的安全等级填写入预先增加的所述第一流表项的流表项权限域中；或者，

若确定所述第一控制器发起的管理指令为修改指令或删除指令，则根据所述第一控制器发起的管理指令，查找所述交换机的本地存储的所述第一流表项，并对查找到的所述第一流表项进行相应的修改或删除处理；或者，

若确定所述第一控制器发起的管理指令为查看指令，则根据所述第一控制器发起的管理指令，查找所述交换机本地存储的所述第一流表项，并将查找到的所述第一流表项返回给所述第一控制器。

14、如权利要求 12 所述的交换机，其特征在于，

所述权限比对模块，还用于当所述第一控制器发起的管理指令为创建指令时，在确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等级的同时或之后，且在所述执行模块根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理之前，将所述第一流表项的第一安全等级与所述第一流表项的第二安全等级进行比对，并确定所述第一流表项的第一安全等级不低于所述第一流表项的第二安全等级。

15、一种交换机，其特征在于，应用于流表项管理系统，所述流表项管理系统包括至少一个所述交换机以及至少一个控制器，其中，所述至少一个控制器中存在一个或多个控制器与所述交换机相连接，并且，与所述交换机

相连接的一个或多个控制器中的每个控制器相对于所述交换机设置有相应的管理权限等级，所述交换机包括：

接收器，用于接收第一控制器发起的针对第一流表项的管理指令，所述第一控制器为与所述交换机相连接的一个或多个控制器中的任一控制器，所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项或所述交换机中存储的任一已创建流表项；

处理器，用于在所述接收器接收到所述第一控制器发起的管理指令后，获取所述第一控制器相对所述交换机的管理权限等级，以及所述第一流表项的安全等级，并将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项对应于所述第一控制器发起的管理指令的安全等级进行比对，以及，在确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时，确定所述第一控制器具备对所述第一流表项进行相应管理的权限，并根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理；

其中，所述第一流表项对应不同的管理指令分别设置有相应的安全等级，所述安全等级用于表示对所述第一流表项进行管理的控制器所应具有的管理权限等级。

16、如权利要求 15 所述的交换机，其特征在于，

所述处理器，还用于在确定所述第一控制器相对所述交换机的管理权限等级低于所述第一流表项对应于所述第一控制器发起的管理指令的安全等级时，确定所述第一控制器不具备对所述第一流表项进行相应管理的权限，并拒绝执行根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理的操作。

17、如权利要求 15 或 16 所述的交换机，其特征在于，所述接收器接收到的所述第一控制器发起的管理指令中携带有所述第一控制器的网络协议地址以及所述第一流表项的匹配域；

所述处理器，具体用于根据所述第一控制器发起的管理指令中携带的所

述第一控制器的网络协议地址以及预先设置的、与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制器的网络协议地址之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一控制器的网络协议地址相对应的管理权限等级，并将查询到的管理权限等级作为获取到的所述第一控制器相对所述交换机的管理权限等级；其中，预先设置的、与所述交换机相连接的各控制器相对所述交换机的管理权限等级和与所述交换机相连接的各控制器的网络协议地址之间的关联关系存储在所述交换机中；以及，

具体用于根据所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域以及预先设置的各流表项的安全等级与各流表项的匹配域之间的关联关系，查询与所述第一控制器发起的管理指令中携带的所述第一流表项的匹配域相对应的安全等级，并将查询到的安全等级作为获取到的所述第一流表项的安全等级；其中，当所述第一流表项为所述第一控制器发起的管理指令中携带的任一待创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系携带在所述第一控制器发起的管理指令中，当所述第一流表项为所述交换机中存储的任一已创建流表项时，预先设置的所述第一流表项的安全等级与所述第一流表项的匹配域之间的关联关系存储在所述交换机中。

18、如权利要求 15 或 16 所述的交换机，其特征在于，

所述处理器获取到的所述第一流表项的安全等级至少包括所述第一流表项对应于内容修改管理指令的第一安全等级和/或所述第一流表项对应于内容查看管理指令的第二安全等级；

其中，所述内容修改管理指令至少包括创建指令、修改指令以及删除指令中的一种或多种；所述内容查看管理指令至少包括查看指令。

19、如权利要求 18 所述的交换机，其特征在于，

所述处理器，具体用于当所述第一控制器发起的管理指令为创建指令、修改指令或删除指令时，将所述第一控制器相对所述交换机的管理权限等级

和所述第一流表项的第一安全等级进行比对，若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等级，则确定所述第一控制器具备对所述第一流表项进行相应的创建、修改或删除的权限；或者，

具体用于当所述第一控制器发起的管理指令为查看指令时，将所述第一控制器相对所述交换机的管理权限等级和所述第一流表项的第二安全等级进行比对，若确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第二安全等级，则确定所述第一控制器具备对所述第一流表项进行查看的权限。

20、如权利要求 18 所述的交换机，其特征在于，

所述处理器，具体用于在确定所述第一控制器具备对所述第一流表项进行相应管理的权限时，若确定所述第一控制器发起的管理指令为创建指令，则根据所述第一控制器发起的管理指令，在所述交换机的本地创建所述第一流表项，并将所述第一控制器发起的管理指令中携带的所述第一流表项的安全等级填写入预先增加的所述第一流表项的流表项权限域中；或者，

若确定所述第一控制器发起的管理指令为修改指令或删除指令，则根据所述第一控制器发起的管理指令，查找所述交换机的本地存储的所述第一流表项，并对查找到的所述第一流表项进行相应的修改或删除处理；或者，

若确定所述第一控制器发起的管理指令为查看指令，则根据所述第一控制器发起的管理指令，查找所述交换机本地存储的所述第一流表项，并将查找到的所述第一流表项返回给所述第一控制器。

21、如权利要求 19 所述的交换机，其特征在于，

所述处理器，还用于当所述第一控制器发起的管理指令为创建指令时，在确定所述第一控制器相对所述交换机的管理权限等级不低于所述第一流表项的第一安全等级的同时或之后，且在根据所述第一控制器发起的管理指令对所述第一流表项进行相应管理之前，将所述第一流表项的第一安全等级与所述第一流表项的第二安全等级进行比对，并确定所述第一流表项的第一安

全等级不低于所述第一流表项的第二安全等级。

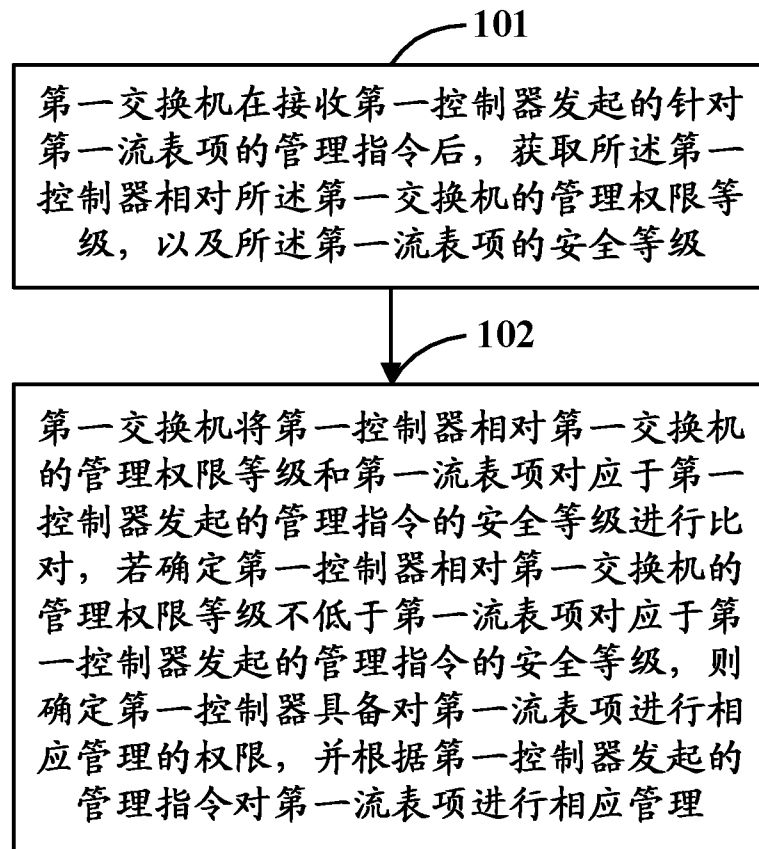


图 1

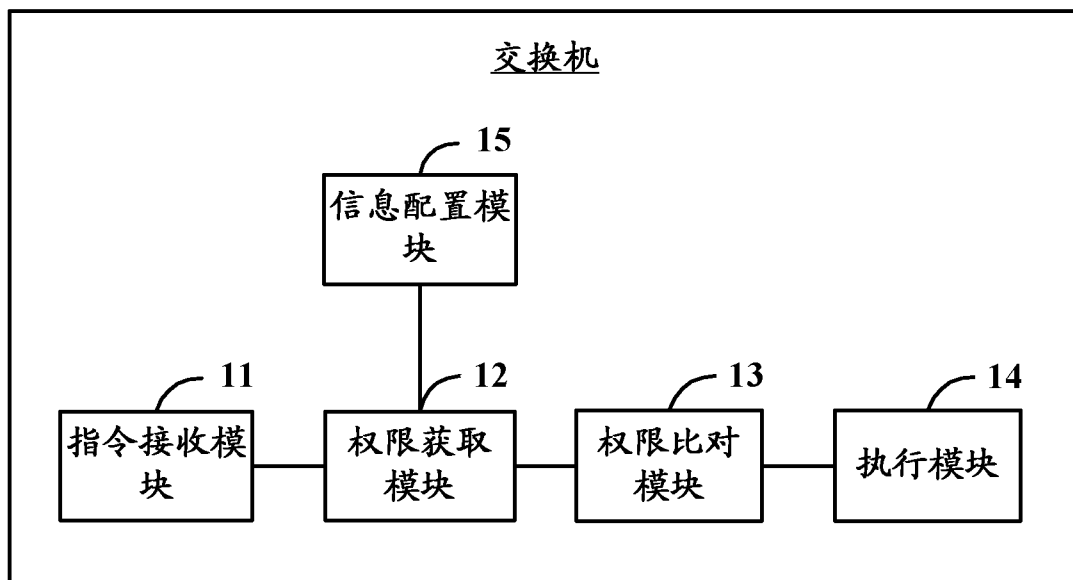


图 2

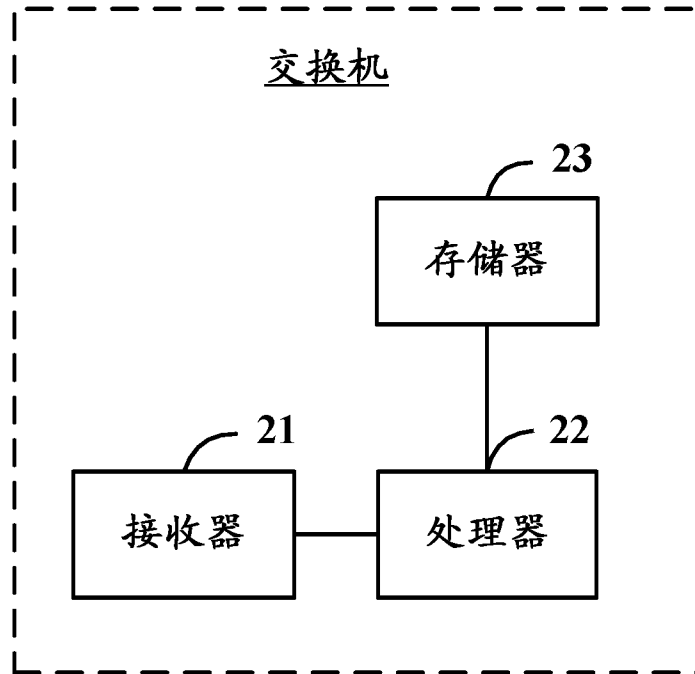


图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/075481

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/70 (2013.01) 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; G06F

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)

CPRSABS; CNTXT; CNKI: software defined network, SDN, SOFTWARE DEFINED, OPENFLOW, authority, authentication, class, safety, flow table, table entry, entry

VEN: SDN, SOFTWARE DEFINED, OPENFLOW, RIGHT, AUTHORI+, CLASS, SATETY, TABLE FLOW, ENTRY

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2011132568 A1 (NEC CORP. et al.), 27 October 2011 (27.10.2011), the whole document	1-21
A	CN 101631116 A (INSTITUTE OF GEOGRAPHIC SCIENCES AND NATURAL RESOURCES RESEARCH, CAS), 20 January 2010 (20.01.2010), the whole document	1-21
A	CN 1852261 A (HANGZHOU HUAWEI 3COM TECHNOLOGY CO., LTD.), 25 October 2006 (25.10.2006), the whole document	1-21
A	CN 103620616 A (HUAWEI TECHNOLOGIES CO., LTD.), 05 March 2014 (05.03.2014), the whole document	1-21

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 18 December 2014 (18.12.2014)	Date of mailing of the international search report 28 January 2015 (28.01.2015)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer WANG, Xiaoling Telephone No.: (86-10) 62412151

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/075481

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2011132568 A1	27 October 2011	EP 2562970 A1	27 February 2013
		US 2013114615 A1	09 May 2013
		CN 102859952 A	02 January 2013
		KR 20120139824 A	27 December 2012
		JP 5299856 B2	25 September 2013
		TW 201218692 A	01 May 2012
		KR 1422381 B1	22 July 2014
		WO 2011132568 S	18 July 2013
CN 101631116 A	20 January 2010	CN 101631116 B	17 October 2012
CN 1852261 A	25 October 2006	CN 100421427 C	24 September 2008
CN 103620616 A	05 March 2014	WO 2014153759 A1	02 October 2014

国际检索报告

国际申请号

PCT/CN2014/075481

A. 主题的分类

H04L 12/70(2013.01)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; G06F

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))

CPRSABS;CNTXT;CNKI:软件定义网络, SDN, SOFTWARE DEFINED, OPENFLOW, 权限, 鉴权, 等级, 安全, 流表, 表项, 条目 VEN: SDN, SOFTWARE DEFINED, OPENFLOW, RIGHT, AUTHORI+, CLASS, SATETY, TABLE FLOW, ENTRY

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
A	WO 2011132568 A1 (NEC CORP. 等) 2011年 10月 27日 (2011 - 10 - 27) 全文	1-21
A	CN 101631116 A (中国科学院地理科学与资源研究所) 2010年 1月 20日 (2010 - 01 - 20) 全文	1-21
A	CN 1852261 A (杭州华为三康技术有限公司) 2006年 10月 25日 (2006 - 10 - 25) 全文	1-21
A	CN 103620616 A (华为技术有限公司) 2014年 3月 05日 (2014 - 03 - 05) 全文	1-21

☐ 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

2014年 12月 18日

国际检索报告邮寄日期

2015年 1月 28日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
北京市海淀区蓟门桥西土城路6号
100088 中国

传真号 (86-10)62019451

授权官员

王晓玲

电话号码 (86-10)62412151

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2014/075481

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)
WO	2011132568	A1	2011年 10月 27日	EP	2562970	A1	2013年 2月 27日
				US	2013114615	A1	2013年 5月 09日
				CN	102859952	A	2013年 1月 02日
				KR	20120139824	A	2012年 12月 27日
				JP	5299856	B2	2013年 9月 25日
				TW	201218692	A	2012年 5月 01日
				KR	1422381	B1	2014年 7月 22日
				WO	2011132568	S	2013年 7月 18日
CN	101631116	A	2010年 1月 20日	CN	101631116	B	2012年 10月 17日
CN	1852261	A	2006年 10月 25日	CN	100421427	C	2008年 9月 24日
CN	103620616	A	2014年 3月 05日	WO	2014153759	A1	2014年 10月 02日

表 PCT/ISA/210 (同族专利附件) (2009年7月)