

一种安全表项切换方法、装置、网络设备及存储介质

技术领域

本申请涉及通信技术领域，尤其涉及一种安全表项切换方法、装置、网络设备及存储介质。

背景技术

在源地址验证网络（Source Address Validation Networks，SAVNET）中，各节点接收到报文后，可以利用源地址验证（Source Address Validation，SAV）表项对报文合法性进行校验。如果存在该报文的源地址和入接口对应的 SAV 表项，则确定该报文为合法报文，正常处理该报文；否则，确定该报文为非法报文，丢弃该报文。

在两个节点之间存在主用路径和备用路径的情况下，备用路径对应的 SAV 表项默认处于未生效状态，即不被用于报文合法性校验。在快速重路由（Fast Reroute，FRR）场景中，当需要进行主备路径切换时，若备用路径对应的 SAV 表项未及时生效，将导致 FRR 的切换收敛性能下降；若备用路径对应的 SAV 表项过早生效，将导致备用路径存在安全漏洞。

发明内容

本申请实施例的目的在于提供一种安全表项切换方法、装置、网络设备及存储介质，以在防止安全漏洞的前提下提高 FRR 收敛速度。具体技术方案如下：

第一方面，本申请实施例提供一种安全表项切换方法，应用于网络设备的数据面，所述网络设备包括第一安全表项，所述第一安全表项包括第一接口的标识和第一源前缀，所述第一安全表项与到达目的端的备用路径对应，所述第一安全表项的状态为备用状态；所述方法包括：

若通过所述第一接口接收到具有所述第一源前缀的报文，则将所述第一安全表项的状态变更为临时主用状态；

若在第一预设时长内未接收到控制面的更新指令，则将所述第一安全表项变的状态更为备用状态；

若在第一预设时长内接收到控制面的更新指令，则根据所述更新指令将所述第一安全表项的状态变更为主用状态。

在一种可能的实现方式中，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；在所述若通过所述第一接口接收到具有所述第一源前缀的报文，则将所述第一安全表项的状态变更为临时主用状态之前，所述方法还包括：

监测所述第二接口是否接收到具有所述第二源前缀的报文；

若所述第二接口持续第二预设时长未接收到具有所述第二源前缀的报文，则监测所述第一接口是否接收到具有所述第一源前缀的报文；

其中，所述第二源前缀与所述第一源前缀相同或不同。

10 在一种可能的实现方式中，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；所述方法还包括：

若检测到所述第二接口与所述主路径上的上一跳网络设备之间存在链路故障，则将所述第一安全表项的状态变更为主用状态，将所述第二安全表项的状态变更为备用状态。

在一种可能的实现方式中，所述第一安全表项包括主备状态字段，所述第一安全表项的主备状态字段的值默认为第一值，所述第一值用于表示备用状态。

20 在一种可能的实现方式中，所述第二安全表项包括主备状态字段，所述第二安全表项的主备状态字段的值默认为第二值，所述第二值用于表示主用状态。

第二方面，本申请实施例提供一种安全表项切换装置，应用于网络设备的数据面，所述网络设备包括第一安全表项，所述第一安全表项包括第一接口的标识和第一源前缀，所述第一安全表项与到达目的端的备用路径对应，所述装置包括：

变更模块，用于若通过所述第一接口接收到具有所述第一源前缀的报文，则将所述第一安全表项的状态变更为临时主用状态；

所述变更模块，还用于若在第一预设时长内未接收到控制面的更新指令，则将所述第一安全表项的状态变更为备用状态；

所述变更模块，还用于若在第一预设时长内接收到控制面的更新指令，则根据所述更新指令将所述第一安全表项的状态变更为主用状态。

在一种可能的实现方式中，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；所述装置还包括监测模块；

所述监测模块，用于监测所述第二接口是否接收到具有所述第二源前缀的报文；以及若所述第二接口持续第二预设时长未接收到具有所述第二源前缀的报文，则监测所述第一接口是否接收到具有所述第一源前缀的报文；

10 其中，所述第二源前缀与所述第一源前缀相同或不同。

在一种可能的实现方式中，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；

所述变更模块，还用于若检测到所述第二接口与所述主路径上的上一跳网络设备之间存在链路故障，则将所述第一安全表项的状态变更为主用状态，
15 将所述第二安全表项的状态变更为备用状态。

在一种可能的实现方式中，所述第一安全表项包括主备状态字段，所述第一安全表项的主备状态字段的值默认为第一值，所述第一值用于表示备用状态。

20 在一种可能的实现方式中，所述第二安全表项包括主备状态字段，所述第二安全表项的主备状态字段的值默认为第二值，所述第二值用于表示主用状态。

第三方面，本申请实施例提供一种网络设备，所述网络设备包括第一安全表项，所述第一安全表项包括第一接口的标识和第一源前缀，所述第一安全表项与到达目的端的备用路径对应，所述第一安全表项的状态为备用状态，
25 所述网络设备包括：

处理器；

收发器；

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；所述机器可执行指令促使所述处理器执行以下步骤：
30

若通过所述第一接口接收到具有所述第一源前缀的报文，则将所述第一安全表项的状态变更为临时主用状态；

若在第一预设时长内未接收到控制面的更新指令，则将所述第一安全表项的状态变更为备用状态；

5 若在第一预设时长内接收到控制面的更新指令，则根据所述更新指令将所述第一安全表项的状态变更为主用状态。

在一种可能的实现方式中，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；所述机器可执行指令还促使所述处理器执行以下步骤：

10

监测所述第二接口是否接收到具有所述第二源前缀的报文；

若所述第二接口持续第二预设时长未接收到具有所述第二源前缀的报文，则监测所述第一接口是否接收到具有所述第一源前缀的报文；

其中，所述第二源前缀与所述第一源前缀相同或不同。

15 在一种可能的实现方式中，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；所述机器可执行指令还促使所述处理器执行以下步骤：

若检测到所述第二接口与所述主路径上的上一跳网络设备之间存在链路故障，则将所述第一安全表项的状态变更为主用状态，将所述第二安全表项的状态变更为备用状态。

20

在一种可能的实现方式中，所述第一安全表项包括主备状态字段，所述第一安全表项的主备状态字段的值默认为第一值，所述第一值用于表示备用状态。

25 在一种可能的实现方式中，所述第二安全表项包括主备状态字段，所述第二安全表项的主备状态字段的值默认为第二值，所述第二值用于表示主用状态。

第四方面，本申请实施例提供一种机器可读存储介质，存储有机器可执行指令，在被处理器调用和执行时，所述机器可执行指令促使所述处理器：

30 实现第一方面所述的方法。

第五方面，本申请实施例提供一种计算机程序产品，所述计算机程序产品促使所述处理器：实现第一方面所述的方法。

采用上述技术方案，若通过第一接口接收到具有第一源前缀的报文，说明可能是因为主用路径故障导致流量被切换至备用路径，因此将第一安全表项的状态变更为临时主用状态，可以防止备用路径对应的安全表项未及时生效而导致流量被误拦截，在进行主备切换的情况下可使得 FRR 快速收敛。后续若在第一预设时长内未接收到控制面的更新指令，则将第一安全表项的状态变更为备用状态，可以防止备用路径对应的安全表项长期处于生效状态而出现的安全漏洞。若在第一预设时长内接收到更新指令，即可按照更新指令将第一安全表项的状态变更为主用状态。如此，既实现在主备路径切换时提前使得备用路径对应的第一安全表项生效，提升 FRR 的切换收敛效率，又可避免备用路径对应的安全表项长期处于生效状态而出现安全漏洞，兼顾了 FRR 效率和网络安全性。

附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。

- 图 1 为现有技术中攻击主机对网络攻击的过程的示例性示意图；
- 图 2 为本申请实施例提供的一种 SANET 技术实现流程的示意图；
- 图 3 为本申请实施例提供的一种源前缀通告方法的示例性示意图；
- 图 4 为本申请实施例提供的一种路径探测方法的示例性示意图；
- 图 5 为本申请实施例提供的一种应用场景的示例性示意图；
- 图 6 为本申请实施例提供的一种安全表项切换方法的流程图；
- 图 7 为本申请实施例提供的一种安全表项切换装置的结构示意图；
- 图 8 为本申请实施例提供的一种网络设备的结构示意图。

具体实施方式

为使本申请的目的、技术方案、及优点更加清楚明白，以下参照附图并举实施例，对本申请进一步详细说明。显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员所获得的所有其他实施例，都属于本申请保护的范围。

在通信网络中，网络设备基于报文的目的地址对报文进行转发，并不会对转发报文的源地址的真实性进行验证，使得攻击者通过伪造源地址对网络进行攻击，产生了大量的网络安全问题。

如图 1 所示，各主机可以通过接入网络访问互联网。例如，攻击主机 A 可以仿冒合法主机 B 的源地址，对重要网站进行恶意攻击，导致重要网站无法正常访问，干扰合法用户使用重要业务。攻击主机 E 可以仿冒合法主机 D 的源地址访问互联网进行非法网络行为，且攻击者可以隐匿自己的真实身份和位置，导致监管平台对非法网络行为无法网络溯源。再例如，攻击主机 H 可以仿冒合法主机 G 的源地址盗用网络资源，从而干扰计费系统对真实源地址的计费、管理和安全认证等，造成大量网络资源被盗用。

为了解决基于源地址的非法攻击，提出了 SAVNET 技术，如图 2 所示，SANET 技术的实现方法包括：

S201、合法源前缀通告。

其中，连接用户侧网络的始发节点可以将自身连接的用户侧网络的网络前缀作为合法源前缀，然后将合法源前缀封装在源前缀通告（Source Prefix Advertisement, SPA）报文中以泛洪的形式通告给域内的其他节点，使得域内的各节点均能学习到用户侧网络的合法源前缀。

如图 3 所示，图 3 中示例性地示出了节点 A 至节点 D，其中节点 A 连接的用户侧网络的网络前缀为源前缀 P1 和 P2，节点 B 连接的用户侧网络的网络前缀为源前缀 P3，节点 C 连接的用户侧网络的网络前缀为源前缀 P4，节点 D 连接的用户侧网络的网络前缀为源前缀 P5。其中，始发节点 A 确定的合法源前缀为 P1 和 P2，始发节点 A 将合法源前缀封装在 SPA 报文中，进而在域内泛洪通告给域内的中继节点，即节点 B、节点 C 和节点 D。在图 3 中，该 SPA 报文表示为 SPA（A：P1，P2）。

S202、目的前缀路径探测。

其中，始发节点和各中继节点通过传递目的前缀探测（Destination Prefix Probing, DPP）报文，能够完成到达指定目的前缀的转发路径探测。

以始发节点 A 为例，始发节点 A 根据本地记录的路由表信息，生成 DPP 报文并通过出接口发送给下一跳节点，下一跳节点为路由表中目的前缀对应的下一跳节点。DPP 报文中包括始发节点的路由标识（Router ID）和该出接

口能到达的所有目的前缀集合。

如图 4 所示，始发节点 A 连接的用户侧网络的网络前缀为 P1 和 P2，始发节点 A 确定网络前缀 P1 和 P2 为合法前缀。中继节点 B 连接的用户侧网络的网络前缀为 P3，中继节点 C 连接的用户侧网络的网络前缀为 P4。中继节点 D 连接的用户侧网络的网络前缀为 P5。其中，始发节点 A 具有接口 A1 和 A2，中继节点 B 具有接口 B1、B2 和 B3，中继节点 C 具有接口 C1，中继节点 D 具有接口 D1。

如表 1-1 所示，表 1-1 为始发节点 A 中的路由表：

表 1-1

始发节点 A 的路由表（Router Table for A）		
目的前缀	出接口	下一跳
P3	A1	B
P4	A1	B
P5	A2	D

如表 1-2 所示，表 1-2 为中继节点 B 中的路由表：

表 1-2

中继节点 B 的路由表（Router Table for B）		
目的前缀	出接口	下一跳
P4	B2	C
P5	B3	D

始发节点可以查找路由表，即上表 1-1，基于路由表确定出接口 A1 可达的目的前缀为 P3 和 P4，A1 对应的下一跳为中继节点 B。假设始发节点 A 的 Router ID 为 A，则始发节点 A 生成的 DPP 报文可以表示为 DPP（A：P3，P4），始发节点 A 将生成的 DPP 报文通过出接口 A1 发送给中继节点 B。

并且，始发节点 A 通过上表 1-1 确定出接口 A2 可达的目的前缀为 P5，A2 对应的下一跳为中继节点 D。假设始发节点 A 的 Router ID 为 A，则始发节点 A 生成的 DPP 报文可以表示为 DPP（A：P5），始发节点 A 将生成的 DPP 报文通过出接口 A2 发送给中继节点 D。

中继节点 B 接收到始发节点 A 发送的 DPP 报文后，根据该 DPP 报文中

的携带的目的前缀 P4，在上述表 1-2 所示的路由表中查找目的前缀 P4 对应的出接口和下一跳，查找到的出接口为 B2，下一跳为中继节点 C。然后中继节点 B 基于接收到的 DPP 报文中的 Router ID 和查找到的出接口以及下一跳，生成 DPP 报文，该 DPP 报文可以表示为 DPP (A: P4)，中继节点 B 将生成
5 的 DPP 报文通过出接口 B2 发送给中继节点 C。

S203、安全表项生成。

其中，各中继节点在本地查找和接收到的 DPP 报文具有相同 Router ID 的 SPA 报文，将查找到的 SPA 报文中的合法源前缀与接收 DPP 报文的入接口进行绑定，生成各中继节点对应的安全表项，即 SAV 表项。SAV 表项包括合法
10 源前缀与入接口之间的对应关系。

以图 4 为例，中继节点 B、中继节点 C 和中继节点 D 接收到始发节点 A 发送的 DPP 报文后，对比本地记录的接收到的 SPA 报文中，是否存在和接收到的 DPP 报文具有相同 Router ID 的 SPA 报文，若存在，则绑定 SPA 报文中的合法源前缀和接收该 DPP 报文的入接口，生成 SAV 表项。SAV 表项即为上
15 述安全表项。

中继节点 B、C、D 生成的 SAV 表项如表 2-1 至 2-3 所示所示：

表 2-1

中继节点 B 的源地址验证表项 (SAVNET Table for B)	
合法源前缀	入接口
P1、P2	B1

表 2-2

中继节点 C 的源地址验证表项 (SAVNET Table for C)	
合法源前缀	入接口
P1、P2	C1

表 2-3

中继节点 D 的源地址验证表项 (SAVNET Table for D)	
合法源前缀	入接口
P1、P2	D1

20 S204、报文合法性验证。

可以理解的，当各中继节点接收到报文后，可以基于 SAV 表项对报文的

合法性进行校验。中继节点可以确定接收该报文的入接口以及该报文的源 IP 地址所属的源前缀,若 SAV 表项中存在该入接口和该源前缀之间的对应关系,则该中继节点判定该报文合法,对该报文进行转发,反之,判定该报文为非法报文,将该报文丢弃。

5 在节点之间存在主用路径和备用路径的场景中,如图 5 所示,图 5 示例性示出了始发节点 A 和三个中继节点,三个中继节点分别为中继节点 B、中继节点 C 和中继节点 D。

始发节点 A 连接的用户侧网络的网络前缀为 P1,中继节点 C 连接的用户侧网络的网络前缀为 P2。中继节点 B 具有接口 B1 和 B2,中继节点 C 具有接口 C1 和 C2,中继节点 D 具有接口 D1 和 D2。

其中,主用路径(Main)为始发节点 A、中继节点 B 和中继节点 C 之间的转发路径,备用路径(Backup)为始发节点 A、中继节点 D 和中继节点 C 之间的转发路径。

其中,始发节点 A 和中继节点 B 的接口 B1 之间的路径属于主用路径,该路径在图 5 中可以利用网络前缀和接口表示为 Main (P1, B1);中继节点 B 的接口 B2 与中继节点 C 的接口 C1 之间的路径也为主用路径,该路径在图 5 中可以利用网络前缀和接口表示为 Main (P1, C1)。

始发节点 A 和中继节点 D 接口 D1 之间的路径为备用路径,该路径在图 5 中可以利用网络前缀和接口表示为 Backup (P1, D1);中继节点 D 的接口 D2 和中继节点 C 的接口 C2 之间的路径为备用路径,该路径在图 5 中可以利用网络前缀和接口表示为 Backup (P1, C2)。

在使用主用路径进行通信的过程中,中继节点 C 中的备用路径对应的 SAV 表项以及中继节点 D 中的备用路径对应的 SACNET 表项均处于未生效状态。

25 若中继节点 C 通过接口 C2 接收到源前缀 P1 的报文,则会将该报文确定为非法报文,同理,若中继节点 D 通过接口 D1 接收到源前缀 P1 的报文,则会将该报文确定为非法报文。

然而,若主用路径出现故障,在 FRR 场景中如何在保证网络安全性的前提下使得 FRR 快速收敛,是目前亟需解决的问题。

30 为了解决上述问题,本申请实施例提供了一种安全表项切换方法,该方

法应用于网络设备的数据面，网络设备包括第一安全表项，第一安全表项包括第一接口标识和第一源前缀，第一安全表项与到达目的端的备用路径对应，第一安全表项的状态为备用状态。如图 6 所示，该方法包括：

5 S601、若通过第一接口接收到具有第一源前缀的报文，则将第一安全表项的状态变更为临时主用状态。

其中，第一安全表项可以包括一个或多个源前缀，若通过第一接口接收的报文的源地址与第一安全表项包括的任一源前缀匹配，说明通过第一接口接收到了来自备用路径的报文，则将第一安全表项的状态变更为临时主用状态。

10 可以理解的是，第一安全表项为备用路径对应的安全表项，所以默认处于未生效的状态。在将第一安全表项的状态变更为临时主用状态后，第一安全表项被激活，即处于生效的状态，进而网络设备可以将与第一安全表项匹配的报文识别为合法报文。

15 S602、若在第一预设时长内未接收到控制面的更新指令，则将第一安全表项的状态变更为备用状态。

其中，第一预设时长为预先配置的临时主用状态的超时时长，具体取值可根据经验配置。

20 在将第一安全表项的状态变更为临时主用状态后开始计时。若计时时长达到第一预设时长，且未接收到网络设备的控制面的更新指令，说明网络设备未进行主备路径的切换，则将第一安全表项的状态恢复为备用状态，从而使得第一安全表项恢复为不生效的状态。

S603、若在第一预设时长内接收到控制面的更新指令，则根据更新指令将第一安全表项的状态变更为主用状态。

25 其中，更新指令用于指示主备切换，若在第一预设时长内接收到控制面的更新指令，说明控制面已确定需要进行主备切换，进而可按照更新指令将第一安全表项变更为主用状态。

控制面进行主备切换的方式可参考 FRR 技术的实现，本申请实施例对此不作限定。

30 采用该方法，若通过第一接口接收到具有第一源前缀的报文，说明可能是因为主用路径故障导致流量被切换至备用路径，因此将第一安全表项的状

态变更为临时主用状态，可以防止备用路径对应的安全表项未及时生效而导致流量被误拦截，在需要进行主备切换的情况下可使得 FRR 快速收敛。后续若在第一预设时长内未接收到控制面的更新指令，则将第一安全表项的状态变更为备用状态，可以防止备用路径对应的安全表项长期处于生效状态而出现的漏洞。若在第一预设时长内接收到更新指令，即可按照更新指令将第一安全表项的状态变更为主用状态。如此，既实现在主备路径切换时提前使得备用路径对应的第一安全表项生效，提升 FRR 的切换收敛效率，又可避免备用路径对应的安全表项长期处于生效状态而出现安全漏洞，兼顾了 FRR 效率和网络安全性。

10 在本申请的一些实施例中，网络设备还包括第二安全表项，第二安全表项包括第二接口的接口标识和第二源前缀，第二安全表项与到达目的端的主用路径对应，第二安全表项的状态为主用状态。在此基础上，在 S601、若通过第一接口接收到具有第一源前缀的报文，则将第一安全表项的状态变更为临时主用状态之前，该方法还包括：

15 监测第二接口是否接收到具有第二源前缀的报文，若第二接口持续第二预设时长未接收到具有第二源前缀的报文，则监测第一接口是否接收到具有第一源前缀的报文。

其中，第二安全表项可以包括一个或多个源前缀，若持续第二预设时长未接收到任意一个具有第二安全表项包括的源前缀的报文，说明主用路径可能存在故障。第二安全表项与第一安全表项包括的源前缀相同，例如，第一安全表项和第二安全表项均包括源前缀 P1 和 P2。

20 第一源前缀与第二源前缀相同或不同，可以理解为，在主用路径故障前后，主用路径和备用路径接收到的报文的源前缀相同或不同。

例如，在主用路径故障前，主用路径接收具有源前缀 P1 的报文；在主用路径故障后，备用路径接收具有源前缀 P1 的报文。这种情况下第一源前缀和第二源前缀不同。

再例如，在主用路径故障前，主用路径接收具有源前缀 P1 的报文；在主用路径故障后，备用路径接收具有源前缀 P2 的报文。这种情况下第一源前缀和第二源前缀不同。

30 第二预设时长可以根据经验预先设置，例如可以为 30 毫秒。

若第二接口持续第二预设时长未接收到具有第二源前缀的报文，说明主用路径可能存在远端故障，所以网络设备可以进一步监测第一接口是否接收到具有第一源前缀的报文。若此时第一接口接收到具有第一源前缀的报文，则说明当前可能正在进行 FRR，即主路径上的远端设备已经将流量切换至备用路径，但第一接口所在的网络设备还未完成主备切换，此时可以先将第一安全表项的状态设置为临时主用状态，以避免对业务流量的误拦截。

例如，第一安全表项包括源前缀 P1 以及接口 1，第二安全表项包括源前缀 P1 以及接口 2。

若网络设备持续第二预设时长未通过接口 2 接收到具有源前缀 P1 的报文，但通过接口 1 接收到具有源前缀 P1 的报文，则将第一安全表项的状态变更为临时主用状态。

再例如，第一安全表项包括源前缀 P1、P2 以及接口 1，第二安全表项包括源前缀 P1、P2 以及接口 2。

若网络设备持续第二预设时长未通过接口 2 接收到具有源前缀 P1 的报文，也未接收到具有源前缀 P2 的报文，但通过接口 1 接收到具有源前缀 P1 或 P2 的报文，则将第一安全表项的状态变更为临时主用状态。

在本申请的一些实施例中，在网络设备包括第二安全表项的情况下，该方法还包括：

若检测到第二接口与主路径上的上一跳网络设备之间存在链路故障，则将第一安全表项的状态更新为主用状态，将第二安全表项的状态变更为备用状态。

其中，网络设备可以通过直连故障检测技术检测主路径上与上一跳设备之间的链路是否存在直连故障。作为示例，该直连故障检测技术可以为双向转发检测（Bidirectional Forwarding Detection, BFD）。若网络设备与上一跳设备之间的链路存在直连故障，说明后续会进行 FRR，所以网络设备可以直接将第一安全表项的状态更新为主用状态，使得第一安全表项立即生效，可以避免对业务流量的误拦截，也可提高 FRR 的收敛速度。

在本申请实施例中，第一安全表项包括主备状态字段，第一安全表项的主备状态字段的值默认为第一值，第一值用于表示备用状态。

第二安全表项包括主备状态，第二安全表项的主备状态字段的值默认为

第二值，第二值用于表示主用状态。

也就是说，本申请实施例中在原有 SAV 表项的基础上，新增了主备状态字段，使得 SAV 表项包括源前缀字段、入接口字段以及主备状态字段。

以图 5 为例进行说明，上述实施例中的网络设备可以为图 5 中的节点 C 或节点 D。

图 5 中节点 C 的 SAV 表项如表 3-1 所示，节点 B 的 SAV 表项如表 3-2 所示，节点 D 的 SAV 表项如表 3-3 所示。以下 3 个表格中的字段值仅为示例，本申请实施例对各个字段值的表现形式不作限定。例如，在以下三个表格中将第一值示例性地表示为“备”，将第二值示例性地表示为“主”。在实际实现中，也可以使用二进制数区分主备状态，例如“0”表示备用状态，“1”表示主用状态。

表 3-1

节点 C 的源地址验证表项（SAV ENTRY for C）		
源前缀	入接口	主备状态
P1	C1	主
P1	C2	备

表 3-2

节点 B 的源地址验证表项（SAV ENTRY for B）		
源前缀	入接口	主备状态
P1	B1	主

表 3-3

节点 D 的源地址验证表项（SAV ENTRY for D）		
源前缀	入接口	主备状态
P1	D1	备

从表 3-1 可以看出，节点 C 同时存在主备 SAV 表项，节点 C 可以启动故障检测，该故障检测包括利用直连故障检测技术检测与节点 B 之间是否存在链路故障，以及启动定时器检测接口 C1 的接口流量。

如果节点 C 检测到与节点 B 之间存在直连故障，则可将表 3-1 中的第二条表项更新为主用状态，将表 3-1 中第一条表项更新为备用状态。进而若节点 C 通过接口 C2 接收到源前缀为 P1 的报文，则可放行该报文。

如果节点 C 未检测到直连故障，但监测到接口 C1 在 30ms 内均未接收到源前缀 P1 的流量，并且在接口 C2 接收到源前缀 P1 的流量，则节点 C 可确定主用路径可能存在远端故障，可以将表 3-1 中的第二条表项变更为临时主用状态，即先将该表项激活一段时间，保证流量不被拦截。

5 在将表 3-1 中的第二条表项变更为临时主用状态之后，若激活时间超时，且未接收到指示主备切换的更新指令，则将第二条表项变更为备用状态，停止放行通过接口 C2 接收到的源前缀 P1 的流量，以避免安全漏洞。若激活时间超时前接收到指示主备切换的更新指令，则将表 3-1 中的第二条表项更新为主用状态，将表 3-1 中第一条表项更新为备用状态。

10 另外，从表 3-3 中可以看出，节点 D 只配置有备 SAV 表项，若节点 D 在接口 D1 接收到源前缀 P1 的报文，则将表 3-3 中的表项更新为临时主用状态，即先将该表项激活一段时间，保证流量不被拦截。

 在将该表项变更为临时主用状态之后，若激活时间超时，且未接收到指示主备切换的更新指令，则将该表项变更为备用状态，停止放行通过接口 D1
15 接收到的源前缀 P1 的流量，以避免安全漏洞。若激活时间超时前接收到指示主备切换的更新指令，则将表该表项更新为主用状态。

图 5 中以域内通信为例进行说明，本申请实施例提供的方法也适用于域间通信。

 基于相同的构思，本申请实施例提供一种安全表项切换装置，应用于网
20 络设备的数据面，网络设备包括第一安全表项，第一安全表项包括第一接口的标识和第一源前缀，第一安全表项与到达目的端的备用路径对应，第一安全表项的状态为备用状态；如图 7 所示，该装置包括：

 变更模块 701，用于若通过第一接口接收到具有第一源前缀的报文，则将第一安全表项的状态变更为临时主用状态；

25 变更模块 701，还用于若在第一预设时长内未接收到控制面的更新指令，则将第一安全表项的状态变更为备用状态；

 变更模块 701，还用于若在第一预设时长内接收到控制面的更新指令，则根据更新指令将第一安全表项的状态更新为主用状态。

 可选的，网络设备还包括第二安全表项，第二安全表项包括第二接口的
30 标识和第二源前缀，第二安全表项与到达目的端的主用路径对应，第二安全

表项的状态为主用状态；如图 7 所示，该装置还包括监测模块 702；

监测模块 702，用于监测第二接口是否接收到具有第二源前缀的报文；以及若第二接口持续第二预设时长未接收到具有第二源前缀的报文，则监测第一接口是否接收到具有第一源前缀的报文；

5 其中，所述第二源前缀与所述第一源前缀相同或不同。

可选的，网络设备还包括第二安全表项，第二安全表项包括第二接口的标识和第二源前缀，第二安全表项与到达目的端的主用路径对应，第二安全表项的状态为主用状态；变更模块 701，还用于若检测到第二接口与主路径上的上一跳网络设备之间存在链路故障，则将第一安全表项的状态变更为主用
10 状态，将第二安全表项的状态变更为备用状态。

可选的，第一安全表项包括主备状态字段，第一安全表项的主备状态字段的值默认为第一值，第一值用于表示备用状态。

可选的，第二安全表项包括主备状态字段，第二安全表项的主备状态字段的值默认为第二值，第二值用于表示主用状态。

15 基于相同的构思，本申请实施例还提供一种网络设备，网络设备包括第一安全表项，第一安全表项包括第一接口的标识和第一源前缀，第一安全表项与到达目的端的备用路径对应，第一安全表项的状态为备用状态，如图 8 所示，该网络设备包括：

处理器 801；收发器 804；机器可读存储介质 802，机器可读存储介质 802
20 存储有能够被处理器 801 执行的机器可执行指令；机器可执行指令促使处理器 801 执行以下步骤：

若通过第一接口接收到具有第一源前缀的报文，则将第一安全表项的状态变更为临时主用状态；

若在第一预设时长内未接收到控制面的更新指令，则将第一安全表项的
25 状态变更为备用状态；

若在第一预设时长内接收到控制面的更新指令，则根据更新指令将第一安全表项的状态变更为主用状态。

可选的，网络设备还包括第二安全表项，第二安全表项包括第二接口的标识和第二源前缀，第二安全表项与到达目的端的主用路径对应，第二安全
30 表项的状态为主用状态；机器可执行指令还促使处理器 801 执行以下步骤：

监测第二接口是否接收到具有第二源前缀的报文；

若第二接口持续第二预设时长未接收到具有第二源前缀的报文，则监测第一接口是否接收到具有第一源前缀的报文；

其中，所述第二源前缀与所述第一源前缀相同或不同。

- 5 可选的，网络设备还包括第二安全表项，第二安全表项包括第二接口的标识和第二源前缀，第二安全表项与到达目的端的主用路径对应，第二安全表项的状态为主用状态；机器可执行指令还促使处理器 801 执行以下步骤：

若检测到第二接口与主路径上的上一跳网络设备之间存在链路故障，则将第一安全表项的状态变更为主用状态，将第二安全表项的状态变更为备用状态。

- 10 可选的，第一安全表项包括主备状态字段，第一安全表项的主备状态字段的值默认为第一值，第一值用于表示备用状态。

可选的，第二安全表项包括主备状态字段，第二安全表项的主备状态字段的值默认为第二值，第二值用于表示主用状态。

- 15 在图 8 中，还可以包括通信总线 803。处理器 801、机器可读存储介质 802 及收发器 804 之间通过通信总线 803 完成相互间的通信，通信总线 803 可以是外设部件互连标准（Peripheral Component Interconnect, PCI）总线或扩展工业标准结构（Extended Industry Standard Architecture, EISA）总线等。该通信总线可以分为地址总线、数据总线、控制总线等。

- 20 收发器 804 可以为无线通信模块，收发器 804 在处理器 801 的控制下，与其他设备进行数据交互。

- 机器可读存储介质 802 可以包括随机存取存储器（Random Access Memory, RAM），也可以包括非易失性存储器（Non-Volatile Memory, NVM），例如至少一个磁盘存储器。另外，机器可读存储介质 802 还可以是至少一个
25 位于远离前述处理器的存储装置。

- 处理器 801 可以是通用处理器，包括中央处理器（Central Processing Unit, CPU）、网络处理器（Network Processor, NP）等；还可以是数字信号处理器（Digital Signal Processing, DSP）、专用集成电路（Application Specific Integrated Circuit, ASIC）、现场可编程门阵列（Field-Programmable Gate Array, FPGA）或其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。

在本申请提供的又一实施例中，还提供了一种计算机可读存储介质，该计算机可读存储介质内存储有计算机程序，所述计算机程序被处理器执行时实现上述任一安全表项切换方法的步骤。

在本申请提供的又一实施例中，还提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述实施例中任一安全表项切换方法。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘 Solid State Disk (SSD)）等。

需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

本说明书中的各个实施例均采用相关的方式描述，各个实施例之间相同

相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

- 5 以上所述仅为本申请的较佳实施例，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

权 利 要 求

1、一种安全表项切换方法，其特征在于，应用于网络设备的数据面，所述网络设备包括第一安全表项，所述第一安全表项包括第一接口的标识和第一源前缀，所述第一安全表项与到达目的端的备用路径对应，所述第一安全表项的状态为备用状态；所述方法包括：

若通过所述第一接口接收到具有所述第一源前缀的报文，则将所述第一安全表项的状态变更为临时主用状态；

若在第一预设时长内未接收到控制面的更新指令，则将所述第一安全表项变的状态更为备用状态；

10 若在第一预设时长内接收到控制面的更新指令，则根据所述更新指令将所述第一安全表项的状态变更为主用状态。

2、根据权利要求1所述的方法，其特征在于，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；在所述若通过所述第一接口接收到具有所述第一源前缀的报文，则将所述第一安全表项的状态变更为临时主用状态之前，所述方法还包括：

监测所述第二接口是否接收到具有所述第二源前缀的报文；
若所述第二接口持续第二预设时长未接收到具有所述第二源前缀的报文，则监测所述第一接口是否接收到具有所述第一源前缀的报文；

20 其中，所述第二源前缀与所述第一源前缀相同或不同。

3、根据权利要求1所述的方法，其特征在于，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；所述方法还包括：

25 若检测到所述第二接口与所述主路径上的上一跳网络设备之间存在链路故障，则将所述第一安全表项的状态变更为主用状态，将所述第二安全表项的状态变更为备用状态。

4、根据权利要求1所述的方法，其特征在于，所述第一安全表项包括主备状态字段，所述第一安全表项的主备状态字段的值默认为第一值，所述第一值用于表示备用状态。

30

5、根据权利要求 2 或 3 所述的方法，其特征在于，所述第二安全表项包括主备状态字段，所述第二安全表项的主备状态字段的值默认为第二值，所述第二值用于表示主用状态。

6、一种安全表项切换装置，其特征在于，应用于网络设备的数据面，所述网络设备包括第一安全表项，所述第一安全表项包括第一接口的标识和第一源前缀，所述第一安全表项与到达目的端的备用路径对应，所述第一安全表项的状态为备用状态；所述装置包括：

变更模块，用于若通过所述第一接口接收到具有所述第一源前缀的报文，则将所述第一安全表项的状态变更为临时主用状态；

10 所述变更模块，还用于若在第一预设时长内未接收到控制面的更新指令，则将所述第一安全表项的状态变更为备用状态；

所述变更模块，还用于若在第一预设时长内接收到控制面的更新指令，则根据所述更新指令将所述第一安全表项的状态变更为主用状态。

7、根据权利要求 6 所述的装置，其特征在于，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；所述装置还包括监测模块；

20 所述监测模块，用于监测所述第二接口是否接收到具有所述第二源前缀的报文；以及若所述第二接口持续第二预设时长未接收到具有所述第二源前缀的报文，则监测所述第一接口是否接收到具有所述第一源前缀的报文；

其中，所述第二源前缀与所述第一源前缀相同或不同。

8、根据权利要求 6 所述的装置，其特征在于，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；

25 所述变更模块，还用于若检测到所述第二接口与所述主路径上的上一跳网络设备之间存在链路故障，则将所述第一安全表项的状态变更为主用状态，将所述第二安全表项的状态变更为备用状态。

9、根据权利要求 6 所述的装置，其特征在于，所述第一安全表项包括主备状态字段，所述第一安全表项的主备状态字段的值默认为第一值，所述第

一值用于表示备用状态。

10、根据权利要求 7 或 8 所述的装置，其特征在于，所述第二安全表项包括主备状态字段，所述第二安全表项的主备状态字段的值默认为第二值，所述第二值用于表示主用状态。

- 5 11、一种网络设备，其特征在于，所述网络设备包括第一安全表项，所述第一安全表项包括第一接口的标识和第一源前缀，所述第一安全表项与到达目的端的备用路径对应，所述第一安全表项的状态为备用状态，所述网络设备包括：

处理器；

- 10 收发器；

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；所述机器可执行指令促使所述处理器执行以下步骤：

若通过所述第一接口接收到具有所述第一源前缀的报文，则将所述第一安全表项的状态变更为临时主用状态；

- 15 若在第一预设时长内未接收到控制面的更新指令，则将所述第一安全表项的状态变更为备用状态；

若在第一预设时长内接收到控制面的更新指令，则根据所述更新指令将所述第一安全表项的状态变更为主用状态。

- 20 12、根据权利要求 11 所述的网络设备，其特征在于，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；所述机器可执行指令还促使所述处理器执行以下步骤：

监测所述第二接口是否接收到具有所述第二源前缀的报文；

- 25 若所述第二接口持续第二预设时长未接收到具有所述第二源前缀的报文，则监测所述第一接口是否接收到具有所述第一源前缀的报文；

其中，所述第二源前缀与所述第一源前缀相同或不同。

- 30 13、根据权利要求 11 所述的网络设备，其特征在于，所述网络设备还包括第二安全表项，所述第二安全表项包括第二接口的标识和第二源前缀，所述第二安全表项与到达目的端的主用路径对应，所述第二安全表项的状态为主用状态；所述机器可执行指令还促使所述处理器执行以下步骤：

若检测到所述第二接口与所述主路径上的上一跳网络设备之间存在链路故障，则将所述第一安全表项的状态变更为主用状态，将所述第二安全表项的状态变更为备用状态。

- 14、根据权利要求 11 所述的网络设备，其特征在于，所述第一安全表项
5 包括主备状态字段，所述第一安全表项的主备状态字段的值默认为第一值，
所述第一值用于表示备用状态。

15、根据权利要求 12 或 13 所述的网络设备，其特征在于，所述第二安全表项包括主备状态字段，所述第二安全表项的主备状态字段的值默认为第二值，所述第二值用于表示主用状态。

- 10 16、一种机器可读存储介质，其特征在于，存储有机器可执行指令，在被处理器调用和执行时，所述机器可执行指令促使所述处理器：实现权利要求 1-5 任一所述的方法。

17、一种计算机程序产品，其特征在于，所述计算机程序产品促使所述处理器：实现权利要求 1-5 任一所述的方法。