

一种安全表项生成方法、装置、网络设备及存储介质

技术领域

本申请涉及网络通信技术领域，尤其涉及一种安全表项生成方法、装置、网络设备及存储介质。

5 背景技术

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，但攻击者可能通过伪造源地址对网络进行攻击，产生了大量网络安全问题。

如图 1 所示，各主机可以通过接入网访问互联网。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，导致监管平台无法对非法网络行为进行溯源。再例如，攻击主机 H 可以仿冒合法主机 G 的源地址盗用合法主机 G 的网络资源，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。

发明内容

15 本申请实施例的目的在于提供一种安全表项生成方法、装置、网络设备及存储介质，用于提升网络安全性。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生成方法，所述方法应用于第一网络设备，所述第一网络设备包括第一接口，所述第一接口作为接收目标链路状态信息的入接口，所述方法包括：

20 从链路状态数据库中获取所述目标链路状态信息，所述目标链路状态信息包括第一源前缀；
为所述入接口生成安全表项，所述安全表项包括所述入接口的标识和所述第一源前缀。

在一种可能的实现方式中，所述从链路状态数据库中获取所述目标链路状态信息，包括：

从所述链路状态数据库中查找所述第一网络设备的第一链路状态信息，所述第一链路状态信息包括所述第一网络设备与至少一个下一层级网络设备之间的连接关系；

25 将所述下一层级作为当前遍历层级，针对当前遍历层级的每个网络设备，从所述链路状态数据库中查找该网络设备的第二链路状态信息；

若所述第二链路状态信息包括源前缀，则将所述第二链路状态信息作为所述目标链路状态信息；

若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将所述下一层级作为当前遍历层级；

30 重复执行所述针对当前遍历层级的每个网络设备，从所述链路状态数据库中查找该网络设备的第二链路状态信息，若所述第二链路状态信息包括源前缀，则将所述第二链路状态信息作为所述目标链路状态信息，若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将所述下一层级作为当前遍历层级的步骤，直至确定当前遍历层级的网络设备不具有下一层级网络设备。

在一种可能的实现方式中，所述下一层级网络设备为 AS 域内除所述第一网络设备之外的其他网络设备。

35 在一种可能的实现方式中，所述目标链路状态信息还包括所述第一源前缀对应的接入标签；在为所述入接口生成安全表项之后，所述方法还包括：

从所述链路状态数据库中查找包括所述接入标签的第三链路状态信息，所述第三链路状态信息包括所述接入标签对应的第二源前缀；

将所述第二源前缀加入所述安全表项。

在一种可能的实现方式中，所述入接口上配置有接入标签；所述方法还包括：

从所述链路状态数据库中查找包括所述接入标签的第四链路状态信息，所述第四链路状态信息包括所述接入标签对应的第三源前缀；

5 为所述入接口生成包括所述入接口的标识和所述第三源前缀的安全表项。

在一种可能的实现方式中，在所述从链路状态数据库中获取所述目标链路状态信息之前，所述方法还包括：

接收 AS 域内的网络设备发送的第一报文，所述第一报文包括所述目标链路状态信息；

将所述目标链路状态信息存入所述链路状态数据库。

10 在一种可能的实现方式中，

所述第一报文包括第一 TLV，所述第一 TLV 包括第一标志位和地址前缀，所述第一标志位用于指示所述地址前缀为所述第一源前缀；或者，

所述第一报文包括第二 TLV，所述第二 TLV 包括地址前缀，所述第二 TLV 包括第一子 TLV，所述第一子 TLV 包括所述第二标志位，所述第二标志位用于指示所述第二 TLV 包括的地址前缀为所述第一源前缀；或者，

15 所述第一报文包括第三 TLV，所述第三 TLV 包括所述第一源前缀。

在一种可能的实现方式中，所述第一 TLV、所述第二 TLV 和所述第三 TLV 均包括第二子 TLV，所述第二子 TLV 包括标签字段，所述标签字段用于承载所述第一源前缀对应的接入标签；或者，

20 所述第三 TLV 包括所述第一源前缀对应的接入标签，且所述接入标签位于所述第一源前缀之前与
所述第一源前缀相邻的标签字段。

第二方面，本申请实施例提供一种安全表项生成装置，所述装置应用于第一网络设备，所述第一网络设备包括第一接口，所述第一接口作为接收目标链路状态信息的入接口，所述装置包括：

获取模块，用于从链路状态数据库中获取所述目标链路状态信息，所述目标链路状态信息包括第一源前缀；

25 生成模块，用于为所述入接口生成安全表项，所述安全表项包括所述入接口的标识和所述第一源前缀。

在一种可能的实现方式中，所述获取模块，具体用于：

从所述链路状态数据库中查找所述第一网络设备的第一链路状态信息，所述第一链路状态信息包括所述第一网络设备与至少一个下一层级网络设备之间的连接关系；

30 将所述下一层级作为当前遍历层级，针对当前遍历层级的每个网络设备，从所述链路状态数据库中查找该网络设备的第二链路状态信息；

若所述第二链路状态信息包括源前缀，则将所述第二链路状态信息作为所述目标链路状态信息；

若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将所述下一层级作为当前遍历层级；

35 重复执行所述针对当前遍历层级的每个网络设备，从所述链路状态数据库中查找该网络设备的第二链路状态信息，若所述第二链路状态信息包括源前缀，则将所述第二链路状态信息作为所述目标链路状态信息，若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将所述下一层级作为当前遍历层级的步骤，直至确定当前遍历层级的网络设备不具有下一层级网络设备。

在一种可能的实现方式中,所述下一层级网络设备为AS域内除所述第一网络设备之外的其他网络设备。

在一种可能的实现方式中,所述目标链路状态信息还包括所述第一源前缀对应的接入标签;

所述获取模块,还用于从所述链路状态数据库中查找包括所述接入标签的第三链路状态信息,所述
5 第三链路状态信息包括所述接入标签对应的第二源前缀;

所述生成模块,还用于将所述第二源前缀加入所述安全表项。

在一种可能的实现方式中,所述入接口上配置有接入标签;

所述获取模块,还用于从所述链路状态数据库中查找包括所述接入标签的第四链路状态信息,所述
第四链路状态信息包括所述接入标签对应的第三源前缀;

10 所述生成模块,还用于为所述入接口生成包括所述入接口的标识和所述第三源前缀的安全表项。

在一种可能的实现方式中,所述装置还包括:

接收模块,用于接收AS域内的网络设备发送的第一报文,所述第一报文包括所述目标链路状态信息;

存储模块,用于将所述目标链路状态信息存入所述链路状态数据库。

15 在一种可能的实现方式中,所述第一报文包括第一TLV,所述第一TLV包括第一标志位和地址前缀,所述第一标志位用于指示所述地址前缀为所述第一源前缀;或者,

所述第一报文包括第二TLV,所述第二TLV包括地址前缀,所述第二TLV包括第一子TLV,所述
第一子TLV包括所述第二标志位,所述第二标志位用于指示所述第二TLV包括的地址前缀为所述第一
源前缀;或者,

20 所述第一报文包括第三TLV,所述第三TLV包括所述第一源前缀。

在一种可能的实现方式中,所述第一TLV、所述第二TLV和所述第三TLV均包括第二子TLV,所述
第二子TLV包括标签字段,所述标签字段用于承载所述第一源前缀对应的接入标签;或者,

所述第三TLV包括所述第一源前缀对应的接入标签,且所述接入标签位于所述第一源前缀之前与
所述第一源前缀相邻的标签字段。

25 第三方面,本申请实施例提供一种第一网络设备,所述第一网络设备包括第一接口,所述第一接口
作为接收目标链路状态信息的入接口,所述第一网络设备包括:

处理器;

收发器;

30 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:

从链路状态数据库中获取所述目标链路状态信息,所述目标链路状态信息包括第一源前缀;

为所述入接口生成安全表项,所述安全表项包括所述入接口的标识和所述第一源前缀。

在一种可能的实现方式中,所述机器可执行指令还促使所述处理器执行以下步骤:

35 从所述链路状态数据库中查找所述第一网络设备的第一链路状态信息,所述第一链路状态信息包括
所述第一网络设备与至少一个下一层级网络设备之间的连接关系;

将所述下一层级作为当前遍历层级,针对当前遍历层级的每个网络设备,从所述链路状态数据库中
查找该网络设备的第二链路状态信息;

若所述第二链路状态信息包括源前缀,则将所述第二链路状态信息作为所述目标链路状态信息;

若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系,则将所述下一层级作为当前遍历层级;

重复执行所述针对当前遍历层级的每个网络设备,从所述链路状态数据库中查找该网络设备的第二链路状态信息,若所述第二链路状态信息包括源前缀,则将所述第二链路状态信息作为所述目标链路状态信息,若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系,则将所述下一层级作为当前遍历层级的步骤,直至确定当前遍历层级的网络设备不具有下一层级网络设备。

在一种可能的实现方式中,所述下一层级网络设备为AS域内除所述第一网络设备之外的其他网络设备。

在一种可能的实现方式中,所述目标链路状态信息还包括所述第一源前缀对应的接入标签;
所述机器可执行指令还促使所述处理器执行以下步骤:

从所述链路状态数据库中查找包括所述接入标签的第三链路状态信息,所述第三链路状态信息包括所述接入标签对应的第二源前缀;

将所述第二源前缀加入所述安全表项。

在一种可能的实现方式中,所述入接口上配置有接入标签;所述机器可执行指令还促使所述处理器执行以下步骤:

从所述链路状态数据库中查找包括所述接入标签的第四链路状态信息,所述第四链路状态信息包括所述接入标签对应的第三源前缀;

为所述入接口生成包括所述入接口的标识和所述第三源前缀的安全表项。

在一种可能的实现方式中,所述机器可执行指令还促使所述处理器执行以下步骤:

接收AS域内的网络设备发送的第一报文,所述第一报文包括所述目标链路状态信息;

将所述目标链路状态信息存入所述链路状态数据库。

在一种可能的实现方式中,所述第一报文包括第一TLV,所述第一TLV包括第一标志位和地址前缀,所述第一标志位用于指示所述地址前缀为所述第一源前缀;或者,

所述第一报文包括第二TLV,所述第二TLV包括地址前缀,所述第二TLV包括第一子TLV,所述第一子TLV包括所述第二标志位,所述第二标志位用于指示所述第二TLV包括的地址前缀为所述第一源前缀;或者,

所述第一报文包括第三TLV,所述第三TLV包括所述第一源前缀。

在一种可能的实现方式中,所述第一TLV、所述第二TLV和所述第三TLV均包括第二子TLV,所述第二子TLV包括标签字段,所述标签字段用于承载所述第一源前缀对应的接入标签;或者,

所述第三TLV包括所述第一源前缀对应的接入标签,且所述接入标签位于所述第一源前缀之前与所述第一源前缀相邻的标签字段。

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: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,第一网络设备可以从链路状态数据库中获取目标链路状态信息,因第一接口作为接收目标链路状态信息的入接口,代表着携带该第一源前缀的报文后续将通过该入接进入第一网络设备。因此,第一网络设备可以生成包括该入接口的标识和该第一源前缀的安全表项,后续基于该安全表

项可以对报文的入接口和源前缀进行验证，如此可以识别出仿冒源 IP 地址的报文，能够避免网络资源被盗用，提升了网络安全性。

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安全表项生成方法的流程图；
图 3 为本申请实施例提供的一种 AS 域内的网络拓扑结构图；
图 4 为本申请实施例提供的域内出口流量的安全校验场景的示例性示意图；
图 5 为本申请实施例提供的域外攻击流量的安全校验场景的示例性示意图；
图 6 为本申请实施例提供的另一种 AS 域内的网络拓扑结构图；
图 7 为本申请实施例提供的一种 ISIS 前缀 TLV 的示意图；
图 8 为本申请实施例提供的一种 OSPFv2 的扩展前缀 TLV 的示意图；
图 9 为本申请实施例提供的一种子 TLV 的示意图；
图 10 为本申请实施例提供的另一种子 TLV 的示意图；
图 11 为本申请实施例提供的 IS-IS 协议中第三 TLV 的示意图；
图 12 为本申请实施例提供的 OSPFv2 协议中 LSA 的示意图；
图 13 为本申请实施例提供的 OSPFv2 协议中第三 TLV 的示意图；
图 14 为本申请实施例提供的 OSPFv3 协议中 LSA 的示意图；
图 15 为本申请实施例提供的 OSPFv3 协议中第三 TLV 的示意图；
图 16 为本申请实施例提供的一种安全表项生成装置的结构示意图；
图 17 为本申请实施例提供的一种电子设备的结构示意图。

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。

为提升网络安全性，本申请实施例提供了一种安全表项生成方法，该方法应用于第一网络设备，第一网络设备可以为自治系统（Autonomous system，AS）域内的任意使能域内域间源地址验证架构协议（Source Address Validation in Intra-domain and Inter-domain Networks，SAVNET）的网络设备，第一网络设备包括第一接口，第一接口作为接收目标链路状态信息的入接口，如图 2 所示，该方法包括：

S201、从链路状态数据库中获取目标链路状态信息，目标链路状态信息包括第一源前缀。
可以理解的是，发布目标链路状态信息的网络设备与第一网络设备的该入接口之间具有连通路经。
其中，该链路状态数据库为第一网络设备中的链路状态数据库（Link State Data Base，LSDB），链路状态数据库中存储有 AS 域内的每个网络设备通过内部网关协议（Interior Gateway Protocol，IGP）通告的链路状态信息。

在 IGP 为中间系统到中间系统(Intermediate system to intermediate system，IS-IS)协议的情况下，链路状态信息为 LSP；在 IGP 为开放式最短路径优先（Open Shortest Path First，OSPF）协议的情况下，链路状态信息为 LSA。

S202、为入接口生成安全表项，安全表项包括入接口的标识和第一源前缀。

其中，该安全表项用于对从该入接口接收到的报文进行安全验证。

若从该入接口接收到的报文的源 IP 地址与该安全表项中的第一源前缀匹配，则可确定该报文为合法报文，可放行该报文；

5 若从该入接口接收到的报文的源 IP 地址与该安全表项中的第一源前缀不匹配，则可确定该报文为
10 仿冒其他源 IP 地址的报文，则拦截该报文。

需要说明的是，若第一网络设备查找到多个目标链路状态信息，则第一网络设备可以将各目标链路
状态信息包括的源前缀加入该安全表项。

10 其中，步骤 S201-S202 具体可以由第一网络设备中的 SAVNET AGENT(代理)模块执行，即 SAVNET
AGENT 可以利用 SAVNET 的 LSDB 信息生成安全表项。

采用该方法，第一网络设备可以从链路状态数据库中获取目标链路状态信息，因第一接口作为接收
目标链路状态信息的入接口，代表着携带该第一源前缀的报文后续将通过该入接进入第一网络设备。因
此，第一网络设备可以生成包括该入接口的标识和该第一源前缀的安全表项，后续基于该安全表项可以
对报文的入接口和源前缀进行验证，如此可以识别出仿冒源 IP 地址的报文，能够避免网络资源被盗用，
15 提升了网络安全性。

在本申请实施例中，上述 S201、从链路状态数据库中获取目标链路状态信息，具体可以实现为：

步骤 1、从链路状态数据库中查找第一网络设备的第一链路状态信息。

其中，第一链路状态信息包括第一网络设备与至少一个下一层级网络设备之间的连接关系。

20 本申请实施例中的各网络设备均为 IGP 节点，可通过 IGP ID 对网络设备进行标识。对于 IS-IS 协
议，IGP ID 为网络设备的 system（系统）ID 和 level（级别），对于 OSPF 协议，IGP ID 为路由 ID 和网
络设备所在的区域。

网络设备之间的连接关系，可以通过本端地址、对端地址、本地 IGP ID 和对端 IGP ID 进行标识。

需要说明的是，第一网络设备基于第一链路状态信息确定下一层级网络设备后，还需反向查找下一
层级网络设备是否具有指向第一网络设备的链路，即查找下一层级网络设备的链路状态信息是否包括与
25 第一网络设备之间的连接关系。在第一网络设备与下一层级网络设备之间具有双向链路时，能够确定第
一网络设备与下一层级网络设备之间连通，进而可对下一层级网络设备进行遍历。

在不同协议中，该连接关系在链路状态信息的表现形式不同，具体表现形式可遵循相关协议规定，
本申请实施例对此不作限定。

30 假设第一网络设备的两个入接口分别连接网络设备 A 和 B，则设备 A 和设备 B 为第一网络设备的
下一层级网络设备。

步骤 2、将下一层级作为当前遍历层级。

步骤 3、针对当前遍历层级的每个网络设备，从链路状态数据库中查找该网络设备的第二链路状态
信息。

35 步骤 4、若第二链路状态信息包括源前缀，则将第二链路状态信息作为目标链路状态信息。

其中，若第二链路状态信息包括源前缀，则后续可生成包括该源前缀与入接口的标识的安全表项。

作为示例，若当前层级的网络设备包括网络设备 A 和 B，且网络设备 A 的第二链路状态信息包括
源前缀 P1，网络设备 B 的第二链路状态信息包括源前缀 P2。

若网络设备 A 和 B 均与第一网络设备的接口 1 具有连通路径，则后续可生成包括接口 1 与源前缀

P1 和 P2 的安全表项。

或者，若网络设备 A 与第一网络设备的接口 1 具有连通路径，网络设备 B 与第一网络设备的接口 2 具有连通路径，则后续可为接口 1 生成包括接口 1 与源前缀 P1 的安全表项，为接口 2 生成包括接口 2 与源前缀 P2 的安全表项。

5 步骤 5、若第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将下一层级作为当前遍历层级。

步骤 6、重复执行步骤 3 至步骤 5，直至确定当前遍历层级的网络设备不具有下一层级网络设备。

需要说明的是，上述步骤中每一次确定的下一层级网络设备均为除第一网络设备之外的网络设备，以避免重复遍历。

10 其中，对于 AS 域内与第一网络设备具有连通路径的每一层级的网络设备，均可按照步骤 3-步骤 5 的方式进行遍历，从而可以查找到 AS 域内的网络设备学习到的每个源前缀在第一网络设备对应的入接口，如此能够为每个入接口生成安全表项，提升网络安全性。

并且，采用该方法，各网络设备可以基于链路状态数据库自动生成安全表项，相比于人工 ACL 规则的方式，本申请实施例生成安全表项的过程无需人工参与，且网络设备可根据网络拓扑变化及时调整安全表项，从而高效地实现域内源地址的安全防护。

15 以下结合具体例子对生成安全表项的过程进行说明，如图 3 所示，图 3 中示例性地示出了一个 AS 域内包括的 6 个网络设备，分别为网络设备 A 至 F。

其中，网络设备 A 具有入接口 A1 和 A2 以及连接域外的域外接口，网络设备 B 具有入接口 B1 和 B2，网络设备 E 具有入接口 E1。

20 网络设备 C 学习到了源前缀 P1，网络设备 D 学习到了源前缀 P2，网络设备 F 学习到了源前缀 P3。
假设网络设备 A、B 和 E 均已使能 SAVNET 功能，以下分别对设网络设备 A、B 和 E 生成安全表项的方法进行介绍。

对于网络设备 A，网络设备 A 从 LSDB 中查找到自身的 LSA1。LSA1 包括网络设备 A 与网络设备 B 的连接信息，以及网络设备 A 与网络设备 E 的连接信息。即下一层级网络设备包括网络设备 B 和 E。

25 然后，网络设备 A 从 LSDB 中查找网络设备 B 的 LSA2，并查找到网络设备 E 的 LSA3。LSA2 包括网络设备 B 与网络设备 C 的连接信息，以及网络设备 B 与网络设备 D 的连接信息。LSA3 包括网络设备 E 与网络设备 F 的连接信息。并且，LSA2 和 LSA3 均不包括源前缀。可见下一级网络设备包括网络设备 C、D 和 F。

然后，网络设备从 LSDB 中查找网络设备 C 的 LSA4、网络设备 D 的 LSA5 以及网络设备 F 的 LSA6。

30 其中，LSA4 包括源前缀 P1，进而网络设备 A 根据连通链路 C->B->A，可确定源前缀 P1 在网络设备 A 中对应的入接口为 A1，进而生成包括 P1 和 A1 的安全表项。

LSA5 包括源前缀 P2，进而网络设备 A 根据连通链路 D->B->A，可确定源前缀 P2 在网络设备 A 中对应的入接口为 A1，进而生成包括 P2 和 A1 的安全表项。

35 LSA6 包括源前缀 P3，进而网络设备 A 根据连通链路 F->E->A，可确定源前缀 P2 在网络设备 A 中对应的入接口为 A2，进而生成包括 P2 和 A2 的安全表项。

由于网络设备 C、D、F 均不具有下一级网络设备，所以遍历结束，网络设备 A 生成的安全表项如表 1 所示。

表 1

源前缀	入接口
P1, P2	A1
P3	A2

网络设备 B 和 E 也按照相同的方式生成安全表项，网络设备 B 生成的安全表项如表 2 所示，网络设备 E 生成的安全表项如表 3 所示。

表 2

源前缀	入接口
P1	B1
P2	B2

表 3

源前缀	入接口
P3	E1

5 上述安全表项可以应用于域内出口流量的安全校验场景中。如图 4 所示，图 4 中示出了两个 AS 域，分别为 AS X 和 AS Y，若子网 2 向 AS X 发送仿冒子网 1 的源地址的报文，该报文的目的地子网 3 的地址。按照目前的基于目的地址进行报文转发的原理，该报文将被 AS X 转发至 AS Y，相当于子网 2 仿冒了子网 1 的源地址。采用本申请实施例的方式，能够 AS X 中的网络设备能够基于安全表项对该报
10 文进行校验，并拦截该报文，避免该报文被转发至 AS Y。

具体的，若 AS 域内的最底层网络设备发送仿冒源地址的报文，该报文将被该最底层网络设备的上层最靠近的网络设备拦截。

以图 3 为例，若网络设备 B 通过接口 B1 接收到网络设备 C 发送的报文，则获取该报文的源地址，基于表 2，若该报文的源地址与源前缀 P1 不匹配，则拦截该报文。

15 同理，若网络设备 B 通过接口 B2 接收到网络设备 C 发送的报文，基于表 2，若该报文的源地址与源前缀 P2 不匹配，则拦截该报文。

如此，实现了对源地址的真实性的验证，避免了网络设备向外转发仿冒源地址的报文，能够提升网络安全
20 安全性。

上述安全表项可以应用于域外攻击流量的安全校验场景中。如图 5 所示，图 5 中示出了两个 AS 域，分别为 AS X 和 AS Y，若 AS X 接收到 AS Y 发送的仿冒 AS X 内的源地址的报文，采用本申请实施例的方法，该报文将被 AS X 拦截。

仍以图 3 为例，若网络设备 A 从连接域外的一个接口接收到报文，假设该报文的源地址的地址前缀为源前缀 P1，则网络设备可从表 1 所示的安全表项中查找是否存在包括该接口和源前缀 P1 的安全表项，若不存在，则说明该报文是仿冒域内源地址的攻击报文，则拦截该报文。

25 在本申请的一些实施例中，上述目标链路状态信息还包括第一源前缀对应的接入接入标签，在上述 S202、为入接口生成安全表项之后，该方法还包括：

从链路状态数据库中查找包括该接入标签的第三链路状态信息，第三链路状态信息包括该接入标签对应的第二源前缀，将第三链路状态信息包括的第二源前缀加入安全表项。

其中，对于一个子网多归属接入 AS 域的场景，一个子网可以包括多个源前缀，在本申请实施例中，
30 可以为同一子网的源前缀设置相同的接入标签，从而将同一子网的多个源前缀加入第一网络设备的同一

入接口对应的安全表项，可以避免对多归属接入的子网流量进行错误拦截。

如图 6 所示，图 6 中示例性地示出了一个 AS 域内包括的 5 个网络设备，分别为网络设备 A 至 E。

其中，网络设备 C 具有入接口 C1 和 C2，网络设备 B 具有入接口 B1，网络设备 A 具有入接口 A1，网络设备 D 具有入接口 D1。

5 网络设备 A 学习到了源前缀 P1，网络设备 D 学习到了源前缀 P2，且源前缀 P1 和源前缀 P2 为同一子网中的源前缀。

假设网络设备 A、B、C 和 D 均已使能 SAVNET 功能，以下分别对设网络设备 A、B、C 和 D 生成安全表项的方法进行介绍。。

10 对于网络设备 A，网络设备 A 从 LSDB 中查找到自身的 LSA1，LSA1 包括源前缀 P1 和源前缀 P1 对应的接入标签 100。由于源前缀 P1 所在的子网接入网络设备 A 的入接口 A1，则网络设备 A 生成包括源前缀 P1 和入接口 A1 的安全表项。进而网络设备 A 从 LSDB 中查找包括接入标签 100 的其他 LSA，假设 LSA2 中包括源前缀 P2 和源前缀 P2 对应的接入标签 100，则将 P2 也加入入接口 A1 对应的安全表项中。网络设备 A 生成的安全表项如表 4 所示。

表 4

源前缀	入接口
P1, P2	A1

15 对于网络设备 D，网络设备 D 从 LSDB 中查找到自身的 LSA3，LSA3 包括源前缀 P2 和源前缀 P2 对应的接入标签 100。由于源前缀 P2 所在的子网接入网络设备 D 的入接口 D1，则网络设备 D 生成包括源前缀 P2 和入接口 D1 的安全表项。进而网络设备 D 从 LSDB 中查找包括接入标签 100 的其他 LSA，假设 LSA4 中包括源前缀 P1 和源前缀 P1 对应的接入标签 100，则将 P1 也加入入接口 D1 对应的安全表项中。网络设备 D 生成的安全表项如表 5 所示。

表 5

源前缀	入接口
P1, P2	D1

对于网络设备 B，网络设备 B 从 LSDB 中查找到自身的 LSA5，LSA5 包括网络设备 B 与网络设备 A 的连接信息。然后网络设备 B 从 LSDB 中查找网络设备 A 的 LSA1，LSA1 包括源前缀 P1 和源前缀 P1 对应的接入标签 100。由于网络设备 A 接入网络设备 B 的入接口 B1，则网络设备 B 生成包括源前缀 P1 和入接口 B1 的安全表项。

25 进而网络设备 B 从 LSDB 中查找包括接入标签 100 的其他 LSA，假设 LSA2 中包括源前缀 P2 和源前缀 P2 对应的接入标签 100，则将 P2 也加入入接口 B1 对应的安全表项中。网络设备 B 生成的安全表项如表 6 所示。

表 6

源前缀	入接口
P1, P2	B1

网络设备 C 也可按照相同的方法分别为入接口 C1 和入接口 C2 生成安全表项，网络设备 C 生成的安全表项如表 7 所示。

30

源前缀	入接口
P1, P2	C1

P1, P2	C2
--------	----

基于上述安全表项，若网络设备 A 通过入接口 A1 接收到报文，且该报文的源地址的源前缀为 P2，网络设备 A 基于表 4 的安全表项可放行该报文，可以避免在子网多归属接入一个 AS 域的情况下出现错误拦截的问题，可以避免在非对称路由场景下的错误拦截。

需要说明的是，在上述实施例的例子中，均以 OSPF 协议中的 P2P 通信场景为例进行说明，即以链路状态信息为 LSA 为例进行说明。在其他 IGP 协议的场景中，链路状态信息的表现形式不同，具体可参考相关协议规定，比如在 IS-IS 协议中，链路状态信息可以为 LSP。或者，本申请实施例中的链路状态信息可以为基于 LSDB 数据库整理出的每个网络设备的连接关系信息，本申请实施例对此不作限定。

在本申请的一些实施例中，第一网络设备的入接口上配置有接入标签。在此基础上，该方法还包括：从链路状态数据库中查找包括该接入标签的第四链路状态信息，第四链路状态信息包括该接入标签对应的第三源前缀，为该入接口生成包括入接口的标识和第三源前缀的安全表项。

该入接口可以为第一网络设备的任一被配置有接入标签的入接口。作为示例，假设子网中包括一个源前缀 P3，该子网可以双归属接入第一网络设备，其中，第一网络设备从自身的接口 1 接收到包括源前缀 P3 的链路状态信息，这种情况下第一网络设备可为接口 1 生成包括接口 1 和源前缀 P3 的安全表项。若该链路状态信息还包括源前缀 P3 对应的接入标签 200，且第一网络设备的接口 2 也被配置了接入标签 200，则第一网络设备还可为接口 2 生成包括接口 2 和源前缀 P3 的安全表项。

在本申请实施例中，在从链路状态数据库获取目标链路状态信息之前，第一网络设备可以接收 AS 域内的网络设备发送的第一报文，第一报文包括目标链路状态信息，进而第一网络设备将目标链路状态信息存入链路状态数据库。

可以理解的是，第一网络设备可以学习到 AS 域内的每个网络设备的链路状态信息，并将各网络设备的链路状态信息存入链路状态数据库。进而第一网络设备根据链路状态数据库得到路径连通性信息，即第一网络设备与 AS 域内的其他网络设备之间的连接关系，并基于连接关系查找到目标链路状态信息，以生成安全表项。

其中，第一报文为用于通告链路状态信息的报文。比如可以为 IGP 协议中的 LSP 或 LSA，利用第一报文可以实现源前缀的泛洪。

在一种实施方式中，第一报文包括第一 TLV，第一 TLV 包括第一标志位和地址前缀，第一标志位用于指示该地址前缀为第一源前缀。

其中，第一 TLV 为第一报文中用于承载地址前缀的前缀 TLV，本申请实施例中，可以占用第一 TLV 的 Flags 字段的 1 个比特位承载第一标志位。相当于对前缀 TLV 包括的 Flags 字段进行了扩展，以表明前缀 TLV 包括的地址前缀是否为用于实现 SAVNET 的源前缀。

在另一种实施方式中，第一报文包括第二 TLV，第二 TLV 包括第一子 TLV，第一子 TLV 包括第二标志位，第二标志位用于指示所述第二 TLV 包括的地址前缀为所述第一源前缀。

其中，第二 TLV 为第一报文中用于承载地址前缀的前缀 TLV，本申请实施例中，对于 OSPF 协议，可以在第二 TLV 中新增一个第一子 TLV，该第一子 TLV 的 value 字段用于承载第二标志位。对于 IS-IS 协议，第一子 TLV 为前缀 TLV 包括的前缀属性标志子 TLV，可以占用该前缀属性标志子 TLV 的 Flags 字段的 1 个比特位承载第二标志位，相当于对该 Flags 字段进行了扩展，以表明前缀 TLV 包括的地址前缀是否为用于实现 SAVNET 的源前缀。在后续实施例中用于实现 SAVNET 的源前缀简称为 SAVNET 源前缀。

在本申请实施例中，第一标志位和第二标志位均为 SAVNET Flag，在下文中简称为 S-Flag。

在子网多归属接入 AS 域的情况下，第一 TLV 和第二 TLV 均包括第二子 TLV，第二子 TLV 包括标签字段，所述标签字段用于承载第一源前缀对应的接入标签。在本申请实施例中，接入标签可表示为 SAVNET access tag，也可表示为 SAVNET access interface tag。

5 以下结合具体的 IGP 协议进行举例说明。

以 IS-IS 协议为例，可以占用前缀属性标志子 TLV 的 Flags 字段的一个暂未被占用的比特位，用于承载 S-Flag，当 S-Flag 取值为 1 时，表示前缀 TLV 中的地址前缀为 SAVNET 源前缀。

其中，前缀属性标志子 TLV 为 RFC7794 标准定义的用于承载 IPv4/IPv6 扩展可达性属性标志的子 TLV。

10 如图 7 所示，前缀属性标志子 TLV 包括 Type（类型）、Length（长度）以及 Value（值）。其中，Type 的取值可以为 4，Length 的值为 Value 的字节数，Value 的大小为 (Length * 8) bits。Value 用于承载 Flags 字段，目前，Flags 字段包括 X、R 和 N，本申请实施例可以在 Flags 字段中新增 S-Flag，在图 7 中可表示为“S”。图 7 中的“X”表示 X-Flag，X-Flag 为外部前缀标志，用于表示源前缀已按照其他协议重新分配。图 7 中的“R”表示 R-Flag，R-Flag 为重新通告标志位。图 7 中的“N”表示 N-Flag，N-Flag 为节点标志位。

或者，可以在前缀 TLV 中扩展子 TLV，该子 TLV 用于承载 S-Flag，当 S-Flag 取值为 1 时，表示前缀 TLV 中的地址前缀为 SAVNET 源前缀。

在子网多归属接入 AS 域的情况下，可以在前缀 TLV 中扩展另一个子 TLV，该子 TLV 用于承载接入标签。其中，该子 TLV 的 Type 和 Length 的长度均为 1 字节，Value 部分为接入标签。

20 以 OSPFv2 为例，OSPFv2 的扩展前缀 TLV 如图 8 所示，该扩展前缀 TLV 中包括 Type、Length、Route Type（路由类型）、Prefix Length（前缀长度）、AF（address family，地址族）、Flags（标志位）、Address Prefix（地址前缀）以及 Sub-TLVs（子 TLV）。其中，Address Prefix 和 Sub-TLVs 均为可变的（variable）。

一种实施方式中，可以占用 Flags 字段的一个暂未被占用的比特位，用于承载 S-Flags，当 S-Flags 25 取值为 1 时，表示扩展前缀 TLV 中的地址前缀为 SAVNET 源前缀。

另一种实施方式中，在扩展前缀 TLV 中扩展一个子 TLV，该子 TLV 用于承载 S-Flags，当 S-Flags 取值为 1 时，表示扩展前缀 TLV 中的地址前缀为 SAVNET 源前缀。

在子网多归属接入 AS 域的情况下，可以在扩展前缀 TLV 中扩展另一个子 TLV，该子 TLV 用于承载接入标签。

30 其中，其中，该子 TLV 的 Type 和 Length 的长度均为 2 字节，Value 部分为接入标签。

以 OSPFv3 为例，可以在 OSPFv3 的 Intra-Area Prefix TLV（域间前缀 TLV）、Inter-Area Prefix TLV（域内前缀 TLV）以及 External Prefix TLV（扩展前缀 TLV）中增加一个子 TLV，如图 9 所示，该子 TLV 包括 Type、Length 和 Value，Value 用于承载 Prefix Attribute Flags（前缀属性标志位），该前缀属性标志位包括 S-Flag，当 S-Flag 取值为 1 时，该子 TLV 所属的前缀 TLV 中的地址前缀为 SAVNET 源前缀。 35

在子网多归属接入 AS 域的情况下，可以在 Intra-Area Prefix TLV（域间前缀 TLV）、Inter-Area Prefix TLV（域内前缀 TLV）以及 External Prefix TLV（扩展前缀 TLV）中扩展另一个子 TLV，如图 10 所示，该 TLV 包括 Type、Length 和 Value，Value 用于承载接入标签。

需要说明的是，本申请实施例介绍的各子 TLV 均适用于 TLV 135、235、236 和 237。

在另一种实施方式中，第一报文包括第三 TLV，第三 TLV 包括第一源前缀。

其中，第三 TLV 为本申请实施例中的在第一报文中新增加的一个用于携带 SAVNET 源前缀的 TLV。

在子网多归属接入 AS 域的情况下，第三 TLV 包括第二子 TLV，第二子 TLV 包括标签字段，标签
5 字段用于承载第一源前缀对应的接入标签；或者第三 TLV 包括第一源前缀对应的接入标签，且该接入
标签位于第一源前缀之前与该第一源前缀相邻的标签字段。

在 IGP 协议为 IS-IS 协议的情况下，如图 11 所示，第三 TLV 中包括 Type、Length、Reserved（保
留位）、接入标签、Flags（标志位）、Algorithm（算法）、SAVNET SrcSize（源前缀尺寸）、SAVNET Src
（源前缀）、Sub-TLV-len（子 TLV 长度）和 Sub-TLVs（子 TLV）。其中，该子 TLV 是可变的（variable）。

10 其中，SAVNET SrcSize 用于表示第三 TLV 中携带的 SAVNET Src 的长度，SAVNET Src 为需要通
告的用于 SAVNET 的源前缀，SAVNET Src 占用 SAVNET SrcSize 之后与 SAVNET Src 相邻的比特位，
且 SAVNET Src 是连续的可变的（continued, variable），接入标签为该 SAVNET Src 对应的接入标签。第
三 TLV 包括的其他字段的定义遵循 IS-IS 协议的规定，此处不再赘述。

在 IGP 协议为 OSPFv2 协议的情况下，若第一报文包括第三 TLV，则还需对 LSA 进行扩展，如图
15 12 所示，LSA 包括 LS age（链路状态时限）、Options（选项）、LS Type（链路状态类型）、Opaque Type
（隐含类型）、Opaque ID（隐含 ID）、Advertising Router（通告路由）、LS sequence number（链路状态序
号）、LS checksum（链路状态校验和）和 Length（长度）以及 TLVs（类型-长度-值）。各字段的含义遵从
OSPFv2 协议的规定，本申请实施例中，可以占用 Opaque Type 中的空闲比特位，指示 LSA 包括一个新
增的第三 TLV。

20 第三 TLV 的格式如图 13 所示，包括 Type、Length、Route Type、Algorithm、Prefix Length、Prefix
Options（前缀选项）、接入标签、SAVNET src 以及子 TLV。其中，SAVNET src 的长度为 4 octets。该子
TLV 是可变的（variable）。

在 IGP 协议为 OSPFv3 协议的情况下，若第一报文包括第三 TLV，则还需对 LSA 进行扩展，如图
14 所示，LSA 包括 LS age（链路状态时限）、U、S12、Function Code（功能码）、Link State ID（链路
25 状态 ID）、Advertising Router（通告路由）、LS sequence number（链路状态序号）、LS checksum（链路
状态校验和）和 Length（长度）字段以及 TLVs（类型-长度-值）。各字段的含义遵从 OSPFv3 协议的规定，
本申请实施例中，可以占用 Function Code 中的空闲比特位，指示 LSA 包括一个新增的第三 TLV。

该第三 TLV 的格式如图 15 所示，包括 Type、Length、Route Type、Algorithm、Prefix Length、Prefix
Options（前缀选项）、接入标签、SAVNET src 以及子 TLV。其中，SAVNET src 占用连续的 16 octets。

30 对应于上述方法实施例，本申请实施例还提供一种安全表项生成装置，该装置应用于第一网络设备，
第一网络设备包括第一接口，第一接口作为接收目标链路状态信息的入接口，如图 16 所示，该装置包
括：

获取模块 1601，用于从链路状态数据库中获取目标链路状态信息，目标链路状态信息包括第一源
前缀；

35 生成模块 1602，用于为入接口生成安全表项，安全表项包括入接口的标识和第一源前缀。

可选地，获取模块 1601，具体用于：

从链路状态数据库中查找第一网络设备的第一链路状态信息，第一链路状态信息包括第一网络设备
与至少一个下一层级网络设备之间的连接关系；

将下一层级作为当前遍历层级，针对当前遍历层级的每个网络设备，从链路状态数据库中查找该网络设备的第二链路状态信息；

若第二链路状态信息包括源前缀，则将第二链路状态信息作为目标链路状态信息；

5 若第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将下一层级作为当前遍历层级；

重复执行针对当前遍历层级的每个网络设备，从链路状态数据库中查找该网络设备的第二链路状态信息，若第二链路状态信息包括源前缀，则将第二链路状态信息作为目标链路状态信息，若第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将下一层级作为当前遍历层级的步骤，直至确定当前遍历层级的网络设备不具有下一层级网络设备。

10 可选地，下一层级网络设备为 AS 域内除第一网络设备之外的其他网络设备。

可选地，目标链路状态信息还包括第一源前缀对应的接入标签；

获取模块 1601，还用于从链路状态数据库中查找包括接入标签的第三链路状态信息，第三链路状态信息包括接入标签对应的第二源前缀；

生成模块 1602，还用于将第二源前缀加入安全表项。

15 可选地，入接口上配置有接入标签；

获取模块 1601，还用于从链路状态数据库中查找包括接入标签的第四链路状态信息，第四链路状态信息包括接入标签对应的第三源前缀；

生成模块 1602，还用于为入接口生成包括入接口的标识和第三源前缀的安全表项。

可选地，该装置还包括：

20 接收模块，用于接收 AS 域内的网络设备发送的第一报文，第一报文包括目标链路状态信息；

存储模块，用于将目标链路状态信息存入链路状态数据库。

可选地，第一报文包括第一 TLV，第一 TLV 包括第一标志位和地址前缀，第一标志位用于指示地址前缀为第一源前缀；或者，

25 第一报文包括第二 TLV，第二 TLV 包括地址前缀，第二 TLV 包括第一子 TLV，第一子 TLV 包括第二标志位，第二标志位用于指示第二 TLV 包括的地址前缀为第一源前缀；或者，

第一报文包括第三 TLV，第三 TLV 包括第一源前缀。

可选地，第一 TLV、第二 TLV 和第三 TLV 均包括第二子 TLV，第二子 TLV 包括标签字段，标签字段用于承载第一源前缀对应的接入标签；或者，

30 第三 TLV 包括第一源前缀对应的接入标签，且接入标签位于第一源前缀之前与第一源前缀相邻的标签字段。

对应于上述方法实施例，本申请实施例还提供一种第一网络设备，第一网络设备包括第一接口，第一接口作为接收目标链路状态信息的入接口，如图 17 所示，该第一网络设备包括：

处理器 1701；

收发器 1704；

35 机器可读存储介质 1702，机器可读存储介质 1702 存储有能够被处理器 1701 执行的机器可执行指令；机器可执行指令促使处理器 1701 执行以下步骤：

从链路状态数据库中获取目标链路状态信息，目标链路状态信息包括第一源前缀；

为入接口生成安全表项，安全表项包括入接口的标识和第一源前缀。

可选地，机器可执行指令还促使处理器 1701 执行以下步骤：

从链路状态数据库中查找第一网络设备的第一链路状态信息，第一链路状态信息包括第一网络设备与至少一个下一层级网络设备之间的连接关系；

5 将下一层级作为当前遍历层级，针对当前遍历层级的每个网络设备，从链路状态数据库中查找该网络设备的第二链路状态信息；

若第二链路状态信息包括源前缀，则将第二链路状态信息作为目标链路状态信息；

若第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将下一层级作为当前遍历层级；

10 重复执行针对当前遍历层级的每个网络设备，从链路状态数据库中查找该网络设备的第二链路状态信息，若第二链路状态信息包括源前缀，则将第二链路状态信息作为目标链路状态信息，若第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将下一层级作为当前遍历层级的步骤，直至确定当前遍历层级的网络设备不具有下一层级网络设备。

可选地，下一层级网络设备为 AS 域内除第一网络设备之外的其他网络设备。

可选地，目标链路状态信息还包括第一源前缀对应的接入标签；

15 机器可执行指令还促使处理器 1701 执行以下步骤：

从链路状态数据库中查找包括接入标签的第三链路状态信息，第三链路状态信息包括接入标签对应的第二源前缀；

将第二源前缀加入安全表项。

可选地，入接口上配置有接入标签；机器可执行指令还促使处理器 1701 执行以下步骤：

20 从链路状态数据库中查找包括接入标签的第四链路状态信息，第四链路状态信息包括接入标签对应的第三源前缀；

为入接口生成包括入接口的标识和第三源前缀的安全表项。

可选地，机器可执行指令还促使处理器 1701 执行以下步骤：

接收 AS 域内的网络设备发送的第一报文，第一报文包括目标链路状态信息；

25 将目标链路状态信息存入链路状态数据库。

可选地，第一报文包括第一 TLV，第一 TLV 包括第一标志位和地址前缀，第一标志位用于指示地址前缀为第一源前缀；或者，

第一报文包括第二 TLV，第二 TLV 包括地址前缀，第二 TLV 包括第一子 TLV，第一子 TLV 包括第二标志位，第二标志位用于指示第二 TLV 包括的地址前缀为第一源前缀；或者，

30 第一报文包括第三 TLV，第三 TLV 包括第一源前缀。

可选地，第一 TLV、第二 TLV 和第三 TLV 均包括第二子 TLV，第二子 TLV 包括标签字段，标签字段用于承载第一源前缀对应的接入标签；或者，

第三 TLV 包括第一源前缀对应的接入标签，且接入标签位于第一源前缀之前与第一源前缀相邻的标签字段。

35 如图 17 所示，第一网络设备还可以包括通信总线 1703。处理器 1701、机器可读存储介质 1702 及收发器 1704 之间通过通信总线 1703 完成相互间的通信，通信总线 1703 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 1703 可以分为地址总线、数据总线、控制总线等。

收发器 1704 可以为无线通信模块，收发器 1704 在处理器 1701 的控制下，与其他设备进行数据交互。

5 机器可读存储介质 1702 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 1702 还可以是至少一个位于远离前述处理器的存储装置。

处理器 1701 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。

10 基于同一种发明构思，根据上述本申请实施例提供的安全表项生成方法，本申请实施例还提供了一种机器可读存储介质，机器可读存储介质存储有能够被处理器执行的机器可执行指令。处理器被机器可执行指令促使实现上述安全表项生成方法的步骤。

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安全表项生成方法的步骤。

15 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。

20 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。

25 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、一种安全表项生成方法，其特征在于，所述方法应用于第一网络设备，所述第一网络设备包括第一接口，所述第一接口作为接收目标链路状态信息的入接口，所述方法包括：
- 5 从链路状态数据库中获取所述目标链路状态信息，所述目标链路状态信息包括第一源前缀；
- 为所述入接口生成安全表项，所述安全表项包括所述入接口的标识和所述第一源前缀。
- 2、根据权利要求 1 所述的方法，其特征在于，所述从链路状态数据库中获取所述目标链路状态信息，包括：
- 从所述链路状态数据库中查找所述第一网络设备的第一链路状态信息，所述第一链路状态信息包括所述所述第一网络设备与至少一个下一层级网络设备之间的连接关系；
- 10 将所述下一层级作为当前遍历层级，针对当前遍历层级的每个网络设备，从所述链路状态数据库中查找该网络设备的第二链路状态信息；
- 若所述第二链路状态信息包括源前缀，则将所述第二链路状态信息作为所述目标链路状态信息；
- 若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将所述下一层级作为当前遍历层级；
- 15 重复执行所述针对当前遍历层级的每个网络设备，从所述链路状态数据库中查找该网络设备的第二链路状态信息，若所述第二链路状态信息包括源前缀，则将所述第二链路状态信息作为所述目标链路状态信息，若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将所述下一层级作为当前遍历层级的步骤，直至确定当前遍历层级的网络设备不具有下一层级网络设备。
- 3、根据权利要求 2 所述的方法，其特征在于，所述下一层级网络设备为 AS 域内除所述第一网络设备之外的其他网络设备。
- 20 4、根据权利要求 1 所述的方法，其特征在于，所述目标链路状态信息还包括所述第一源前缀对应的接入标签；在为所述入接口生成安全表项之后，所述方法还包括：
- 从所述链路状态数据库中查找包括所述接入标签的第三链路状态信息，所述第三链路状态信息包括所述接入标签对应的第二源前缀；
- 25 将所述第二源前缀加入所述安全表项。
- 5、根据权利要求 1 所述的方法，其特征在于，所述入接口上配置有接入标签；所述方法还包括：
- 从所述链路状态数据库中查找包括所述接入标签的第四链路状态信息，所述第四链路状态信息包括所述接入标签对应的第三源前缀；
- 为所述入接口生成包括所述入接口的标识和所述第三源前缀的安全表项。
- 30 6、根据权利要求 1 所述的方法，其特征在于，在所述从链路状态数据库中获取所述目标链路状态信息之前，所述方法还包括：
- 接收 AS 域内的网络设备发送的第一报文，所述第一报文包括所述目标链路状态信息；
- 将所述目标链路状态信息存入所述链路状态数据库。
- 7、根据权利要求 6 所述的方法，其特征在于，
- 35 所述第一报文包括第一 TLV，所述第一 TLV 包括第一标志位和地址前缀，所述第一标志位用于指示所述地址前缀为所述第一源前缀；或者，
- 所述第一报文包括第二 TLV，所述第二 TLV 包括地址前缀，所述第二 TLV 包括第一子 TLV，所述第一子 TLV 包括所述第二标志位，所述第二标志位用于指示所述第二 TLV 包括的地址前缀为所述第一

源前缀；或者，

所述第一报文包括第三 TLV，所述第三 TLV 包括所述第一源前缀。

8、根据权利要求 7 所述的方法，其特征在于，

5 所述第一 TLV、所述第二 TLV 和所述第三 TLV 均包括第二子 TLV，所述第二子 TLV 包括标签字段，所述标签字段用于承载所述第一源前缀对应的接入标签；或者，

所述第三 TLV 包括所述第一源前缀对应的接入标签，且所述接入标签位于所述第一源前缀之前与
所述第一源前缀相邻的标签字段。

9、一种安全表项生成装置，其特征在于，所述装置应用于第一网络设备，所述第一网络设备包括
第一接口，所述第一接口作为接收目标链路状态信息的入接口，所述装置包括：

10 获取模块，用于从链路状态数据库中获取所述目标链路状态信息，所述目标链路状态信息包括第一
源前缀；

生成模块，用于为所述入接口生成安全表项，所述安全表项包括所述入接口的标识和所述第一源前
缀。

10、根据权利要求 9 所述的装置，其特征在于，所述获取模块，具体用于：

15 从所述链路状态数据库中查找所述第一网络设备的第一链路状态信息，所述第一链路状态信息包括
所述第一网络设备与至少一个下一层级网络设备之间的连接关系；

将所述下一层级作为当前遍历层级，针对当前遍历层级的每个网络设备，从所述链路状态数据库中
查找该网络设备的第二链路状态信息；

若所述第二链路状态信息包括源前缀，则将所述第二链路状态信息作为所述目标链路状态信息；

20 若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将所述
下一层级作为当前遍历层级；

重复执行所述针对当前遍历层级的每个网络设备，从所述链路状态数据库中查找该网络设备的第二
链路状态信息，若所述第二链路状态信息包括源前缀，则将所述第二链路状态信息作为所述目标链路状
态信息，若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将
25 所述下一层级作为当前遍历层级的步骤，直至确定当前遍历层级的网络设备不具有下一层级网络设备。

11、根据权利要求 10 所述的装置，其特征在于，所述下一层级网络设备为 AS 域内除所述第一网
络设备之外的其他网络设备。

12、根据权利要求 9 所述的装置，其特征在于，所述目标链路状态信息还包括所述第一源前缀对应
的接入标签；

30 所述获取模块，还用于从所述链路状态数据库中查找包括所述接入标签的第三链路状态信息，所述
第三链路状态信息包括所述接入标签对应的第二源前缀；

所述生成模块，还用于将所述第二源前缀加入所述安全表项。

13、根据权利要求 9 所述的装置，其特征在于，所述入接口上配置有接入标签；

35 所述获取模块，还用于从所述链路状态数据库中查找包括所述接入标签的第四链路状态信息，所述
第四链路状态信息包括所述接入标签对应的第三源前缀；

所述生成模块，还用于为所述入接口生成包括所述入接口的标识和所述第三源前缀的安全表项。

14、根据权利要求 9 所述的装置，其特征在于，所述装置还包括：

接收模块，用于接收 AS 域内的网络设备发送的第一报文，所述第一报文包括所述目标链路状态信

息；

存储模块，用于将所述目标链路状态信息存入所述链路状态数据库。

15、根据权利要求 14 所述的装置，其特征在于，

5 所述第一报文包括第一 TLV，所述第一 TLV 包括第一标志位和地址前缀，所述第一标志位用于指示所述地址前缀为所述第一源前缀；或者，

所述第一报文包括第二 TLV，所述第二 TLV 包括地址前缀，所述第二 TLV 包括第一子 TLV，所述第一子 TLV 包括所述第二标志位，所述第二标志位用于指示所述第二 TLV 包括的地址前缀为所述第一源前缀；或者，

所述第一报文包括第三 TLV，所述第三 TLV 包括所述第一源前缀。

10 16、根据权利要求 15 所述的装置，其特征在于，

所述第一 TLV、所述第二 TLV 和所述第三 TLV 均包括第二子 TLV，所述第二子 TLV 包括标签字段，所述标签字段用于承载所述第一源前缀对应的接入标签；或者，

所述第三 TLV 包括所述第一源前缀对应的接入标签，且所述接入标签位于所述第一源前缀之前与所述第一源前缀相邻的标签字段。

15 17、一种第一网络设备，其特征在于，所述第一网络设备包括第一接口，所述第一接口作为接收目标链路状态信息的入接口，所述第一网络设备包括：

处理器；

收发器；

20 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：

从链路状态数据库中获取所述目标链路状态信息，所述目标链路状态信息包括第一源前缀；

为所述入接口生成安全表项，所述安全表项包括所述入接口的标识和所述第一源前缀。

18、根据权利要求 17 所述的第一网络设备，其特征在于，所述机器可执行指令还促使所述处理器执行以下步骤：

25 从所述链路状态数据库中查找所述第一网络设备的第一链路状态信息，所述第一链路状态信息包括所述第一网络设备与至少一个下一层级网络设备之间的连接关系；

将所述下一层级作为当前遍历层级，针对当前遍历层级的每个网络设备，从所述链路状态数据库中查找该网络设备的第二链路状态信息；

若所述第二链路状态信息包括源前缀，则将所述第二链路状态信息作为所述目标链路状态信息；

30 若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将所述下一层级作为当前遍历层级；

35 重复执行所述针对当前遍历层级的每个网络设备，从所述链路状态数据库中查找该网络设备的第二链路状态信息，若所述第二链路状态信息包括源前缀，则将所述第二链路状态信息作为所述目标链路状态信息，若所述第二链路状态信息包括该网络设备与至少一个下一层级网络设备之间的连接关系，则将所述下一层级作为当前遍历层级的步骤，直至确定当前遍历层级的网络设备不具有下一层级网络设备。

19、根据权利要求 18 所述的第一网络设备，其特征在于，所述下一层级网络设备为 AS 域内除所述第一网络设备之外的其他网络设备。

20、根据权利要求 17 所述的第一网络设备，其特征在于，所述目标链路状态信息还包括所述第一

源前缀对应的接入标签；

所述机器可执行指令还促使所述处理器执行以下步骤：

从所述链路状态数据库中查找包括所述接入标签的第三链路状态信息，所述第三链路状态信息包括所述接入标签对应的第二源前缀；

5 将所述第二源前缀加入所述安全表项。

21、根据权利要求 17 所述的第一网络设备，其特征在于，所述入接口上配置有接入标签；所述机器可执行指令还促使所述处理器执行以下步骤：

从所述链路状态数据库中查找包括所述接入标签的第四链路状态信息，所述第四链路状态信息包括所述接入标签对应的第三源前缀；

10 为所述入接口生成包括所述入接口的标识和所述第三源前缀的安全表项。

22、根据权利要求 17 所述的第一网络设备，其特征在于，所述机器可执行指令还促使所述处理器执行以下步骤：

接收 AS 域内的网络设备发送的第一报文，所述第一报文包括所述目标链路状态信息；

将所述目标链路状态信息存入所述链路状态数据库。

15 23、根据权利要求 22 所述的第一网络设备，其特征在于，

所述第一报文包括第一 TLV，所述第一 TLV 包括第一标志位和地址前缀，所述第一标志位用于指示所述地址前缀为所述第一源前缀；或者，

所述第一报文包括第二 TLV，所述第二 TLV 包括地址前缀，所述第二 TLV 包括第一子 TLV，所述第一子 TLV 包括所述第二标志位，所述第二标志位用于指示所述第二 TLV 包括的地址前缀为所述第一源前缀；或者，

20 所述第一报文包括第三 TLV，所述第三 TLV 包括所述第一源前缀。

24、根据权利要求 23 所述的第一网络设备，其特征在于，

所述第一 TLV、所述第二 TLV 和所述第三 TLV 均包括第二子 TLV，所述第二子 TLV 包括标签字段，所述标签字段用于承载所述第一源前缀对应的接入标签；或者，

25 所述第三 TLV 包括所述第一源前缀对应的接入标签，且所述接入标签位于所述第一源前缀之前与所述第一源前缀相邻的标签字段。

25、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 1-8 任一所述的方法。

30 26、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 1-8 任一所述的方法。