一种安全表项维护方法、装置、网络设备和存储介质

技术领域

本申请涉及通信技术领域，特别涉及一种安全表项维护方法、装置、网络设备和存储介质。

背景技术

为了提高网络安全性，可以在接入设备上部署源地址安全检查机制，接入设备可以基于媒体访问控制地址-互联网协议地址（Media Access Control address- Internet Protocol address，MAC-IP）表项对接收到的报文进行合法性检查，从而避免非法报文通过。

接入设备 1 为终端生成 MAC-IP 表项后，可通过协议连接将 MAC-IP 表项通告给汇聚设备，进而汇聚设备将该 MAC-IP 表项通告给其他接入设备。如此，当终端从接入设备 1 下挂的接入点（Access Point，AP）移动到接入设备 2 下挂的 AP 后，接入设备 2 可以基于该 MAC-IP 表项对该终端进行合法性检查。

若接入设备 2 只与一个汇聚设备连接，在接入设备 2 与汇聚设备之间的协议连接中断的情况下，接入设备 2 可以将来自该协议连接的 MAC-IP 表项删除。这种情况下，如果使能源地址安全检查机制，则接入设备 2 无法基于该 MAC-IP 表项进行合法性检查，导致合法报文被丢弃；如果不使能源地址安全检查机制，则非法报文也可以进入网络，导致网络安全性降低。

若接入设备 2 不删除来自该协议连接的 MAC-IP 表项，若后续协议连接一直未恢复，将导致该 MAC-IP 表项长时间占用硬件资源，造成资源浪费。所以，在协议连接中断的情况下，MAC-IP 表项如何保持是亟需解决的问题。

发明内容

本申请实施例的目的在于提供一种安全表项维护方法、装置、网络设备和存储介质，能够避免资源浪费和合法报文被丢弃，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维护方法，应用于第一网络设备，所述第一网络设备包括远端 MAC-IP 表，所述远端 MAC-IP 表包括所述第二网络设备通告的至少一个远端 MAC-IP 表项，所述方法包括：

当与所述第二网络设备之间的协议连接 中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，所述有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 表项。

在一种可能的实现方式中，所述方法还包括：

当所述第一网络设备生成 DHCP 中继表项时，基于所述 DHCP 中继表项建立本地 MAC-IP 表项，并向硬件资源下发所述本地 MAC-IP 表项对应的转发 MAC-IP 表项，所述本地 MAC-IP 表项包括第一 IP 地址的第一有效生命周期值；

向第三网络设备发送第一 MAC-IP 通告消息，以使得所述第三网络设备建立第一远端 MAC-IP 表项；

其中，所述第一 MAC-IP 通告消息包括第一序列号以及所述第一有效生命周期值，所述第一远端 MAC-IP 表项包括所述第一序列号以及所述第一有效生命周期值；

所述第一序列号为与所述本地 MAC-IP 表项匹配的远端 MAC-IP 表项中的最大序列号与 1 的和值。

在一种可能的实现方式中，在所述向硬件资源下发所述本地 MAC-IP 表项对应的转发 MAC-IP 表项

之后，所述方法还包括：

当所述本地 MAC-IP 表项匹配的接入表项被删除时，删除所述转发 MAC-IP 表项。

在一种可能的实现方式中，在所述当与所述第二网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值之前，所述方法还包括：

接收所述第二网络设备发送的第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括第二 IP 地址的第二有效生命周期值以及第二序列号；

建立第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项包括所述第二有效生命周期值以及所述第二序列号。

在一种可能的实现方式中，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括至少一个本地 MAC-IP 表项；

在所述建立第二远端 MAC-IP 表项之后，所述方法还包括：

接收终端发送的第一报文，所述第一报文包括所述终端的 MAC 地址和 IP 地址；

若所述本地 MAC-IP 表中未存在与所述终端的 MAC 地址和 IP 地址匹配的本地 MAC-IP 表项，且所述终端的 MAC 地址和 IP 地址与所述第二远端 MAC-IP 表项匹配，则对所述终端进行接入探测；

若接收到所述终端发送的接入响应，则生成合成 MAC-IP 表项，所述合成 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址、端口标识以及 VLAN 标识；

根据所述合成 MAC-IP 表项生成转发 MAC-IP 表项，所述转发 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址；

将所述转发 MAC-IP 表项下发至硬件资源中。

在一种可能的实现方式中，在所述将所述转发 MAC-IP 表项下发至硬件资源中之后，所述方法还包括：

当所述终端接入表项被删除时，删除所述合成 MAC-IP 表项和所述转发 MAC-IP 表项。

在一种可能的实现方式中，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括第一本地 MAC-IP 表项，所述第一本地 MAC-IP 表项包括第三序列号；在所述建立第二远端 MAC-IP 表项之后，所述方法还包括：

若所述第二远端 MAC-IP 表项与所述第一本地 MAC-IP 表项匹配，且所述第二序列号大于所述第三序列号，则将所述第一本地 MAC-IP 表项删除，并将所述第一本地 MAC-IP 表项对应的 DHCP 中继表项删除。

在一种可能的实现方式中，所述第一网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

在一种可能的实现方式中，所述第一网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

第二方面，本申请实施例提供一种安全表项维护方法，应用于第二网络设备，所述第二网络设备包括第一远端 MAC-IP 表，所述第一远端 MAC-IP 表包括第四网络设备通告的至少一个远端 MAC-IP 表项，所述方法包括：

当与所述第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，

所述有效生命周期值用于指示所述远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 表项。

在一种可能的实现方式中，在所述当与第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值之前，所述方法还包括：

接收所述第四网络设备发送的第一 MAC-IP 通告消息，所述第一 MAC-IP 通告消息包括第一 IP 地址的第一有效生命周期值以及第一序列号；

建立第一远端 MAC-IP 表项，所述第一远端 MAC 表项包括所述第一有效生命周期值以及所述第一序列号。

在一种可能的实现方式中，所述第二网络设备还包括至少一个第二远端 MAC-IP 表，所述至少一个第二远端表包括第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项与所述第一远端 MAC-IP 表项匹配，所述第二远端 MAC-IP 表项包括第二序列号；在所述建立第一远端 MAC-IP 表项之后，所述方法还包括：

若所述第一序列号大于所述第二序列号，则向除所述第四网络设备之外的其他网络设备发送第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括所述第一有效生命周期值以及所述第一序列号。

在一种可能的实现方式中，所述第二远端设备还包括至少一个第三远端 MAC-IP 表，每个第三远端 MAC-IP 表包括至少一个远端 MAC-IP 表项；在所述删除所述至少一个远端 MAC-IP 表项之后，所述方法还包括：

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中未存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则向除所述第四网络设备之外的其他网络设备发送第一 MAC-IP 撤销消息，所述第一 MAC-IP 撤销消息包括该远端 MAC-IP 表项中的 MAC 地址和 IP 地址；或者，

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则从匹配的远端 MAC-IP 表项中选择序列号最大的第三远端 MAC-IP 表项，所述第三远端 MAC-IP 表项包括第二有效生命周期值以及第三序列号；向除第五网络设备之外的其他网络设备发送第三 MAC-IP 通告消息，所述第三 MAC-IP 通告消息包括所述第二有效生命周期值和所述第三序列号，所述第五网络设备为所述第三远端 MAC-IP 表项的来源设备。

在一种可能的实现方式中，所述第二网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

在一种可能的实现方式中，所述第二网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

第三方面，本申请实施例提供一种安全表项维护装置，应用于第一网络设备，所述第一网络设备包括远端 MAC-IP 表，所述远端 MAC-IP 表包括所述第二网络设备通告的至少一个远端 MAC-IP 表项，所述装置包括：

获取模块，用于当与所述第二网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，所述有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

删除模块，用于若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 表项。

在一种可能的实现方式中，所述装置还包括：

建立模块，用于当所述第一网络设备生成 DHCP 中继表项时，基于所述 DHCP 中继表项建立本地 MAC-IP 表项，并向硬件资源下发所述本地 MAC-IP 表项对应的转发 MAC-IP 表项，所述本地 MAC-IP 表项包括第一 IP 地址的第一有效生命周期值；

发送模块，用于向第三网络设备发送第一 MAC-IP 通告消息，以使得所述第三网络设备建立第一远端 MAC-IP 表项；

其中，所述第一 MAC-IP 通告消息包括第一序列号以及所述第一有效生命周期值，所述第一远端 MAC-IP 表项包括所述第一序列号以及所述第一有效生命周期值；

所述第一序列号为与所述本地 MAC-IP 表项匹配的远端 MAC-IP 表项中的最大序列号与 1 的和值。

在一种可能的实现方式中，所述删除模块，还用于当所述本地 MAC-IP 表项匹配的接入表项被删除时，删除所述转发 MAC-IP 表项。

在一种可能的实现方式中，所述装置还包括：

接收模块，用于接收所述第二网络设备发送的第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括第二 IP 地址的第二有效生命周期值以及第二序列号；

建立模块，用于建立第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项包括所述第二有效生命周期值以及所述第二序列号。

在一种可能的实现方式中，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括至少一个本地 MAC-IP 表项；

所述装置还包括：探测模块、生成模块和下发模块；

所述接收模块，还用于接收终端发送的第一报文，所述第一报文包括所述终端的 MAC 地址和 IP 地址；

所述探测模块，用于若所述本地 MAC-IP 表中未存在与所述终端的 MAC 地址和 IP 地址匹配的本地 MAC-IP 表项，且所述终端的 MAC 地址和 IP 地址与所述第二远端 MAC-IP 表项匹配，则对所述终端进行接入探测；

所述生成模块，用于若接收到所述终端发送的接入响应，则生成合成 MAC-IP 表项，所述合成 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址、端口标识以及 VLAN 标识；

所述生成模块，还用于根据所述合成 MAC-IP 表项生成转发 MAC-IP 表项，所述转发 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址；

所述下发模块，用于将所述转发 MAC-IP 表项下发至硬件资源中。

在一种可能的实现方式中，所述删除模块，还用于当所述终端的接入表项被删除时，删除所述合成 MAC-IP 表项和所述转发 MAC-IP 表项。

在一种可能的实现方式中，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括第一本地 MAC-IP 表项，所述第一本地 MAC-IP 表项包括第三序列号；

所述删除模块，还用于若所述第二远端 MAC-IP 表项与所述第一本地 MAC-IP 表项匹配，且所述第二序列号大于所述第三序列号，则将所述第一本地 MAC-IP 表项删除，并将所述第一本地 MAC-IP 表项对应的 DHCP 中继表项删除。

在一种可能的实现方式中，所述第一网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，

所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

在一种可能的实现方式中，所述第一网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

第四方面，本申请实施例提供一种安全表项维护装置，应用于第二网络设备，所述第二网络设备包括第一远端 MAC-IP 表，所述第一远端 MAC-IP 表包括第四网络设备通告的至少一个远端 MAC-IP 表项，所述装置包括：

获取模块，用于当与所述第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，所述有效生命周期值用于指示所述远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

删除模块，用于若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 表项。

在一种可能的实现方式中，所述装置还包括：

接收模块，用于接收所述第四网络设备发送的第一 MAC-IP 通告消息，所述第一 MAC-IP 通告消息包括第一 IP 地址的第一有效生命周期值以及第一序列号；

建立模块，用于建立第一远端 MAC-IP 表项，所述第一远端 MAC 表项包括所述第一有效生命周期值以及所述第一序列号。

在一种可能的实现方式中，所述第二网络设备还包括至少一个第二远端 MAC-IP 表，所述至少一个第二远端表包括第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项与所述第一远端 MAC-IP 表项匹配，所述第二远端 MAC-IP 表项包括第二序列号；所述装置还包括：

发送模块，用于若所述第一序列号大于所述第二序列号，则向除所述第四网络设备之外的其他网络设备发送第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括所述第一有效生命周期值以及所述第一序列号。

在一种可能的实现方式中，所述第二远端设备还包括至少一个第三远端 MAC-IP 表，每个第三远端 MAC-IP 表包括至少一个远端 MAC-IP 表项；所述装置还包括发送模块；

所述发送模块，用于：

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中未存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则向除所述第四网络设备之外的其他网络设备发送第一 MAC-IP 撤销消息，所述第一 MAC-IP 撤销消息包括该远端 MAC-IP 表项中的 MAC 地址和 IP 地址；或者，

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则从匹配的远端 MAC-IP 表项中选择序列号最大的第三远端 MAC-IP 表项，所述第三远端 MAC-IP 表项包括第二有效生命周期值以及第三序列号；向除第五网络设备之外的其他网络设备发送第三 MAC-IP 通告消息，所述第三 MAC-IP 通告消息包括所述第二有效生命周期值和所述第三序列号，所述第五网络设备为所述第三远端 MAC-IP 表项的来源设备。

在一种可能的实现方式中，所述第二网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

在一种可能的实现方式中，所述第二网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

第五方面，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远端 MAC-IP 表，所述远端 MAC-IP 表包括所述第二网络设备通告的至少一个远端 MAC-IP 表项；所述第一网络设备包括：

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：

当与所述第二网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，所述有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 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：

当所述第一网络设备生成 DHCP 中继表项时，基于所述 DHCP 中继表项建立本地 MAC-IP 表项，并向硬件资源下发所述本地 MAC-IP 表项对应的转发 MAC-IP 表项，所述本地 MAC-IP 表项包括第一 IP 地址的第一有效生命周期值；

通过所述收发器向第三网络设备发送第一 MAC-IP 通告消息，以使得所述第三网络设备建立第一远端 MAC-IP 表项；

其中，所述第一 MAC-IP 通告消息包括第一序列号以及所述第一有效生命周期值，所述第一远端 MAC-IP 表项包括所述第一序列号以及所述第一有效生命周期值；

所述第一序列号为与所述本地 MAC-IP 表项匹配的远端 MAC-IP 表项中的最大序列号与 1 的和值。

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：

当所述本地 MAC-IP 表项匹配的接入表项被删除时，删除所述转发 MAC-IP 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：

通过所述收发器接收所述第二网络设备发送的第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括第二 IP 地址的第二有效生命周期值以及第二序列号；

建立第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项包括所述第二有效生命周期值以及所述第二序列号。

在一种可能的实现方式中，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括至少一个本地 MAC-IP 表项；

所述机器可执行指令还促使所述处理器执行以下步骤：

通过收发器接收终端发送的第一报文，所述第一报文包括所述终端的 MAC 地址和 IP 地址；

若所述本地 MAC-IP 表中未存在与所述终端的 MAC 地址和 IP 地址匹配的本地 MAC-IP 表项，且所述终端的 MAC 地址和 IP 地址与所述第二远端 MAC-IP 表项匹配，则对所述终端进行接入探测；

若接收到所述终端发送的接入响应，则生成合成 MAC-IP 表项，所述合成 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址、端口标识以及 VLAN 标识；

根据所述合成 MAC-IP 表项生成转发 MAC-IP 表项，所述转发 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址；

将所述转发 MAC-IP 表项下发至硬件资源中。

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：

当所述终端的接入表项被删除时，删除所述合成 MAC-IP 表项和所述转发 MAC-IP 表项。

在一种可能的实现方式中，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括第一本地 MAC-IP 表项，所述第一本地 MAC-IP 表项包括第三序列号；所述机器可执行指令还促使所述处理器执行以下步骤：

若所述第二远端 MAC-IP 表项与所述第一本地 MAC-IP 表项匹配，且所述第二序列号大于所述第三序列号，则将所述第一本地 MAC-IP 表项删除，并将所述第一本地 MAC-IP 表项对应的 DHCP 中继表项删除。

在一种可能的实现方式中，所述第一网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

在一种可能的实现方式中，所述第一网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

第六方面，本申请实施例提供一种第二网络设备，所述第二网络设备包括第一远端 MAC-IP 表，所述第一远端 MAC-IP 表包括第四网络设备通告的至少一个远端 MAC-IP 表项，所述第二网络设备包括：

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：

当与所述第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，所述有效生命周期值用于指示所述远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 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：

通过所述收发器接收所述第四网络设备发送的第一 MAC-IP 通告消息，所述第一 MAC-IP 通告消息包括第一 IP 地址的第一有效生命周期值以及第一序列号；

建立第一远端 MAC-IP 表项，所述第一远端 MAC 表项包括所述第一有效生命周期值以及所述第一序列号。

在一种可能的实现方式中，所述第二网络设备还包括至少一个第二远端 MAC-IP 表，所述至少一个第二远端表包括第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项与所述第一远端 MAC-IP 表项匹配，所述第二远端 MAC-IP 表项包括第二序列号；所述机器可执行指令促使所述处理器执行以下步骤：

若所述第一序列号大于所述第二序列号，则向除所述第四网络设备之外的其他网络设备发送第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括所述第一有效生命周期值以及所述第一序列号。

在一种可能的实现方式中，所述第二远端设备还包括至少一个第三远端 MAC-IP 表，每个第三远端 MAC-IP 表包括至少一个远端 MAC-IP 表项；所述机器可执行指令促使所述处理器执行以下步骤：

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中未存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则向除所述第四网络设备之外的其他网络设备发送第一 MAC-IP 撤销消息，所述第一 MAC-IP 撤销消息包括该远端 MAC-IP 表项中的 MAC 地址和 IP 地址；或者，

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则从匹配的远端 MAC-IP 表项中选择序列号最大的第三远端 MAC-IP 表项，所述第三远端 MAC-IP 表项包括第二有效生命周期值以及第三序列号；向除第五网络设备之外的其他网络设备发送第三 MAC-IP 通告消息，所述第三 MAC-IP 通告消息包括所述第二有效生命周期值和所述第三序列号，所述第五网络设备为所述第三远端 MAC-IP 表项的来源设备。

在一种可能的实现方式中，所述第二网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

在一种可能的实现方式中，所述第二网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

第七方面，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：实现第一方面或第二方面所述的方法。

第八方面，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：实现第一方面或第二方面所述的方法。

采用上述技术方案，第一网络设备中的远端 MAC-IP 表项中包括有效生命期值，且该有效生命期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命期，若协议连接中断的持续时长达到有效生命周期值，说明 MAC-IP 表项包括的 IP 地址已经无效。即原本申请到该 IP 地址的终端已经无法继续使用该 IP 地址，此时将远端 MAC-IP 表项删除也不会影响到后续对该终端的合法性校验，不会影响网络安全，且可避免该远端 MAC-IP 表项继续占用第一网络设备的资源。在协议连接中断的持续时长达到有效生命周期值之前，第一网络设备不会将该远端 MAC-IP 表项删除，因此在使能源地址安全检查机制的情况下，也不会导致与该远端 MAC-IP 表项匹配的合法报文被丢弃，且能防止非法报文进入网络，能够提升网络安全性。

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 为本申请实施例提供的一种 Spine-Leaf 组网系统结构示意图；

图 2 为本申请实施例提供的一种安全表项维护方法流程图；

图 3 为本申请实施例提供的一种 MAC-IP NLRI 的格式的示例性示意图；

图 4 为本申请实施例提供的一种 Route Type 的格式的示例性示意图；

图 5 为本申请实施例提供的一种第一扩展团体属性格式的示例性示意图；

图 6 为本申请实施例提供的一种第二扩展团体属性格式的示例性示意图；

图 7 为本申请实施例提供的另一种安全表项维护方法流程图；

图 8 为本申请实施例提供的另一种 Spine-Leaf 组网系统结构示意图；

图 9 为本申请实施例提供的又一种 Spine-Leaf 组网系统结构示意图；

图 10 为本申请实施例提供的再一种 Spine-Leaf 组网系统结构示意图；

图 11 为本申请实施例提供的一种安全表项维护装置结构示意图；

图 12 为本申请实施例提供的另一种安全表项维护装置结构示意图；

图 13 为本申请实施例提供的一种第一网络设备的结构示意图；

图 14 为本申请实施例提供的一种第二网络设备的结构示意图。

具体实施方式

为使本发明的目的、技术方案、及优点更加清楚明白，以下参照附图并举实施例，对本发明进一步详细说明。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所获得的所有其他实施例，都属于本发明保护的范围。

本申请实施例所应用的组网系统可以为脊（Spine）-叶（Leaf）组网，如图 1 所示，该组网系统中包括两级汇聚设备，其中 Spine3 为区域 1 中的 Spine1 和区域 2 中的 Spine2 的上级汇聚设备。

Spine3 与互联网协议第六版动态主机配置协议（Dynamic Host Configuration Protocol Version 6，DHCPv6）服务器和接入控制器（Access Controller，AC）相连，DHCPv6 服务器用于为终端分配互联网协议第 6 版（Internet Protocol Version 6，IPv6）地址。

Spine1 位于区域 1 中，区域 1 中还包括三个接入设备，分别为 Leaf1、Leaf2 和 Leaf3，Leaf1、Leaf2 和 Leaf3 均与 Spine1 相连。

AP1 与 Leaf1 相连，AP2 与 Leaf2 相连，AP3 与 Leaf3 相连，终端可以与 AP 进行通信，图 1 中示例性地示出了终端接入 AP1。

需要说明的是，图 1 中的各设备数量仅为示例，实际实现中，图 1 中的各设备数量不限于此。

接入设备上部署有安全检查机制，该安全检查机制包括控制平面检查机制和数据平面检查机制。

其中，控制平面检查机制是指对接收到的协议报文进行合法性检查，例如对邻居发现（Neighbor Discovery，ND）和地址解析协议（Address Resolution Protocol，ARP）探测报文的发送者的媒体访问控制（Media Access Control，MAC）地址和互联网协议（Internet Protocol，IP）地址进行过滤，防止生成非法 ND 表项和 ARP 表项。

数据平面检查机制是指对接收到的业务报文的源 MAC 地址和源 IP 地址进行过滤控制，防止非法业务报文通过。

控制平面检查机制和数据平面检查机制均依赖于预先生成的 MAC-IP 表项，目前动态生成 MAC-IP 表项的方式有：基于动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）中继表项生成 MAC-IP 表项以及通过 DHCP 侦听（snooping）生成 MAC-IP 表项。本申请实施例对接入设备生成本地安全表项的方式不作限定。

需要说明的是，若用户私自为终端设置 IP 地址，不会触发接入设备生成 MAC-IP 表项，则接入设备会将来自该终端的报文丢弃。

本申请实施例中的 IP 地址可以为互联网协议第 4 版（Internet Protocol Version 4，IPv4）地址或者 IPv6 地址。

本申请实施例提供一种安全表项维护方法，该方法应用于第一网络设备，该第一网络设备可以为接入设备，例如可以为 Spine-Leaf 结构中的 Leaf 设备。第一网络设备包括远端 MAC-IP 表，远端 MAC-IP 表包括第二网络设备通告的至少一个远端 MAC-IP 表项。如图 2 所示，该方法包括：

S201、当与第二网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值。

其中，有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期。

第二网络设备可以为汇聚设备。以图 1 所示的组网系统为例，第一网络设备可以为图 1 中的为 Leaf1、Leaf2 或 Leaf3，第二网络设备可以为 Spine1。第一网络设备与第二网络设备之间的协议连接可以为边界网关协议（Border Gateway Protocol，BGP）连接；或者该第一网络设备与第二网络设备之间的协议连接也可以为自定义的私有协议连接，在该协议连接为私有协议连接的情况下，各网络设备之间通过私有协议通告 MAC-IP 表项。

S202、若协议连接中断的持续时长达到有效生命周期值，则删除至少一个远端 MAC-IP 表项。

可以理解的是，在远端 MAC-IP 表包括一个 MAC-IP 表项的情况下，第一网络设备可获取该 MAC-IP 表项包括的有效生命周期值。第一网络设备以检测到协议连接中断的时刻为起始时刻，将远端 MAC-IP 表项保存有效生命期值，即第一网络设备在检测到协议连接中断后，将该远端 MAC-IP 表项保持有效生命周期值，在到达有效生命周期值之前，不会将该远端 MAC-IP 表项删除。

若距离起始时刻的时长达到有效生命周期值时，该协议连接仍未恢复，则删除该远端 MAC-IP 表项。

例如有效生命期值为 100000 秒，则第一网络设备检测到协议连接中断后开始计时，将该远端 MAC-IP 表项保持 100000 秒。若 100000 秒后，协议连接仍未恢复，则第一网络设备将该远端 MAC-IP 表项删除。

在远端 MAC-IP 表包括多个 MAC-IP 表项的情况下，第一网络设备可以获取到多个远端 MAC-IP 表项的有效生命周期值。

一种实施方式中，在协议连接中断的持续时长达到获取到的所有有效生命周期值后，也就是协议连接中断的持续时长达到获取的各有效生命周期值中的最大生命周期值后，一次性删除该远端 MAC-IP 表包括多个 MAC-IP 表项。

另一种实施方式中，针对每个有效生命周期值，若协议连接中断的持续时长达到该有效生命周期值，则将该有效生命周期值所属的 MAC-IP 表项删除。

采用上述方法，第一网络设备中的远端 MAC-IP 表项中包括有效生命期值，且该有效生命期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命期，若协议连接中断的持续时长达到有效生命周期值，说明 MAC-IP 表项包括的 IP 地址已经无效。即原本申请到该 IP 地址的终端已经无法继续使用该 IP 地址，此时将远端 MAC-IP 表项删除也不会影响到后续对该终端的合法性校验，不会影响网络安全，且可避免该远端 MAC-IP 表项继续占用第一网络设备的资源。在协议连接中断的持续时长达到有效生命周期值之前，第一网络设备不会将该远端 MAC-IP 表项删除，因此在使能源地址安全检查机制的情况下，也不会导致与该远端 MAC-IP 表项匹配的合法报文被丢弃，且能防止非法报文进入网络，能够提升网络安全性。

以下结合具体例子进行说明，结合图 1，以第一网络设备为 Leaf1，第二网络设备为 Spine1 为例，Leaf1 接收到 Spine1 通告的 MAC-IP 表项 1 和 MAC-IP 表项 2，并保存为远端 MAC-IP 表项 1 和远端 MAC-IP 表项 2。假设远端 MAC-IP 表项 1 中的 IP 地址的有效生周期为 90000 秒，远端 MAC-IP 表项 2 中的 IP 地址的有效生命周期值为 100000 秒。

一种实施方式中，若 Leaf1 检测到和 Spine1 之间的协议连接中断，则 Leaf1 以检测到协议连接中断的时刻为起始时刻，将远端 MAC-IP 表项 1 和远端 MAC-IP 表项 2 保持 100000 秒。若在 100000 秒后，

Leaf1 和 Spine1 之间的协议连接仍未恢复，则 Leaf1 将远端 MAC-IP 表项 1 和远端 MAC-IP 表项 2 删除。

如此，第一网络设备可以一次性删除多个远端 MAC-IP 表项，在不影响网络安全的前提下，避免资源浪费，且可以节省第一网络设备删除远端表项过程的处理开销。

另一实施方式中，仍以 leaf1 中包括上述远端 MAC-IP 表项 1 和远端 MAC-IP 表项 2 为例，若 Leaf1 检测到和 Spine1 之间的协议连接中断，则 Leaf1 以检测到协议连接中断的时刻为起始时刻，将远端 MAC-IP 表项 1 保持 90000 秒，若 90000 秒后该协议连接未恢复，则将远端 MAC-IP 表项 1 删除。Leaf1 以检测到协议连接中断的时刻为起始时刻，将远端 MAC-IP 表项 2 保持 100000 秒，若 100000 秒后该协议连接仍未恢复，则将远端 MAC-IP 表项 2 删除。

如此，可以及时准确地删除每条已经失效的远端 MAC-IP 表项，在不影响网络安全的前提下，避免已经失效的远端 MAC-IP 表项占用资源。

本申请实施例中的第一网络设备还可以生成本地 MAC-IP 表项，并向其他网络设备通告本地 MAC-IP 表项，该过程具体包括：

当第一网络设备生成 DHCP 中继表项时，基于 DHCP 中继表项建立本地 MAC-IP 表项，并向硬件资源下发本地 MAC-IP 表项对应的转发 MAC-IP 表项，本地 MAC-IP 表项中包括第一 IP 地址的第一有效生命周期值。

本申请实施例中，第一网络设备可以作为 DHCP 中继设备，DHCP 中继设备在为终端向 DHCP 服务器申请 IP 地址后，可以获取 DHCP 服务器为终端分配的第一 IP 地址，以及该第一 IP 地址的首选生命周期值和有效生命周期值。本申请实施例中，第一网络设备可以将第一 IP 地址的第一有效生命周期值加入本地 MAC-IP 表项，可选地，还可以将第一 IP 地址的首选生命周期值加入本地 MAC-IP 表项。

以 IPv6 网络为例，本地 MAC-IP 表项中至少包括表 1 中示出的字段：

表 1

字段	描述
IPv6 address	DHCPv6 终端的 IPv6 地址
MAC Address	DHCPv6 终端的 MAC 地址
Port index	DHCPv6 中继收到 DHCPv6 请求报文的二层端口信息
Interface	DHCPv6 中继接口
Inner VLAN	DHCPv6 中继用户地址表项的内层虚拟局域网标识（Virtual Local Area Network Tag，VLAN Tag）
Outer VLAN	DHCPv6 中继用户地址表项的外层 VLAN Tag
Preferred lifetime	IPv6 地址的首选生命期值，单位为秒
Valid lifetime	IPv6 地址的有效生命期值，单位为秒

其中，本地 MAC-IP 表项为控制 MAC-IP 表项，控制 MAC-IP 表项由网络设备的软件维护，可以存

储于网络设备的内存中。控制平面可以基于控制 MAC-IP 表项进行控制平面的协议报文合法性检查，例如对 ND 报文进行合法性检查。

本地 MAC-IP 表项对应的转发 MAC-IP 表项包括上述 MAC 地址和 IPv6 地址字段，存储于硬件转发芯片的硬件资源中，需消耗硬件转发芯片中的 MAC-IP 表项资源，用于对转发平面的业务报文进行合法性检查。其中，硬件转发芯片中的 MAC-IP 表项资源是较为紧缺的资源。

第一网络设备生成上述本地 MAC-IP 表项后，可以向第三网络设备发送第一 MAC-IP 通告消息，以使得第三网络设备建立第一远端 MAC-IP 表项。

其中，第一 MAC-IP 通告消息包括第一序列号以及第一有效生命周期值，且第一远端 MAC-IP 表项包括第一序列号以及第一有效生命周期值。第一序列号为与本地 MAC-IP 表项匹配的远端 MAC-IP 表项中的最大序列号与 1 的和值。

可以理解的是，第一 MAC-IP 通告消息还包括本地 MAC-IP 表项中的 MAC 地址和第一 IP 地址，相应地，第一远端 MAC-IP 表项也包括该 MAC 地址和第一 IP 地址。

其中，第三网络设备为汇聚设备，第三网络设备和第二网络设备可以是同一汇聚设备，也可以是不同的汇聚设备。

与本地 MAC-IP 表项匹配的远端 MAC-IP 表项是指与本地 MAC-IP 表项中的 MAC 地址和 IP 地址均相同的远端 MAC-IP 表项。若第一网络设备中存储有与本地 MAC-IP 表项匹配的远端 MAC-IP 表项，则说明该终端是从其他接入设备迁移而来的，每个远端 MAC-IP 表项中均包括序列号。远端 MAC-IP 表项中携带的序列号越大，代表该远端 MAC-IP 表项的生成时间越晚。

以 IPv6 网络为例，第一 MAC-IP 通告消息中可以包括表 2 中示出的字段：

表 2

字段	描述
IPv6 address	DHCPv6 终端的 IPv6 地址
MAC Address	DHCPv6 终端的 MAC 地址
Preferred lifetime	IPv6 地址的首选生命期值，单位为秒
Valid lifetime	IPv6 地址的有效生命期值，单位为秒
Sequence Number	序列号

在上述实施例的基础上，第一网络设备可能会删除 ARP 表项或 ND 表项。例如，以 IPv6 场景为例，有些终端在锁屏等状态下，对第一网络设备发起的 ND 表项老化探测消息不回应，会导致第一网络设备中该终端对应的 ND 表项被老化删除。或者，若接入设备检测到终端的接入接口断开，则接入设备可以将从该接入接口上线的终端的 ND 表项删除。

第一网络设备向硬件资源下发本地 MAC-IP 表项对应的转发 MAC-IP 表项后，当该本地 MAC-IP 表项匹配的接入表项被删除时，删除该转发 MAC-IP 表项。

其中，接入表项是 ND 表项或 ARP 表项。

本申请实施例中，将硬件资源中转发 MAC-IP 表项删除，可以节约硬件资源。并且由于此时并未删除内存中存储的本地 MAC-IP 表项，所以若终端再次接入，再次学习到该终端的接入表项后，还可以基于本地 MAC-IP 表项再次向硬件资源下发转发 MAC-IP 表项，不会因该转发 MAC-IP 表项被删除而导致合法报文被丢弃，可以提高网络安全性。

此外，ND 表项或 ARP 表项被删除不代表着终端申请的 IP 地址租约到期，所以删除 ND 表项或 ARP 表项后，不会删除该终端对应的 DHCP 中继表项。

在本申请实施例中，第一网络设备也可以接收到其他网络设备通告的 MAC-IP 表项，基于此，在上述 S201、当与第二网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值之前，该方法还包括：

接收第二网络设备发送的第二 MAC-IP 通告消息，并建立第二远端 MAC-IP 表项。其中，第二 MAC-IP 通告消息包括第二 IP 地址的第二有效生命周期值以及第二序列号；第二远端表项包括第二 IP 地址的第二有效生命周期值以及第二序列号。可以理解的是，第二 MAC-IP 通告消息还包括：MAC 地址和第二 IP 地址。相应的，第二远端 MAC-IP 表项也包括 MAC 地址和第二 IP 地址。

可选地，第二 MAC-IP 通告消息中还可以包括第二 IP 地址的首选生命周期值，相应地，远端 MAC-IP 表项中也包括第二 IP 地址的首选生命周期值。

可以理解的，第二网络设备将从第一网络设备之外的其他网络设备接收到的 MAC-IP 表项通告给该第一网络设备，使得终端从其他接入设备迁入第一网络设备后，第一网络设备可以利用第二远端 MAC-IP 表项对该终端的报文进行合法性检查，拒绝非法报文进入网络，提高了网络安全性。且由于第二 MAC-IP 通告消息中包括第二序列号，若后续终端迁移至第一网络设备，第一网络设备可以基于序列号获知该终端的迁移情况。

第一网络设备可以将该第二远端 MAC-IP 表项存储于内存中，此时该第二远端 MAC-IP 表项不占用内存中的控制 MAC-IP 表项资源，即第一网络设备可以利用内存中除控制 MAC-IP 表项资源之外的空闲资源存储该第二远端 MAC-IP 表项，并且此时该远端 MAC-IP 表项不占用硬件资源。第一网络设备可以为第二网络设备维护一个远端 MAC-IP 表项，第二远端 MAC-IP 表项存储于该远端 MAC-IP 表中。

以 IPv6 应用场景为例，第二远端 MAC-IP 表项包括的字段如表 3 所示：

表 3

字段	描述
IPv6 address	DHCPv6 终端的 IPv6 地址
MAC Address	DHCPv6 终端的 MAC 地址
Preferred lifetime	IPv6 地址的首选生命期值，单位为秒
Valid lifetime	IPv6 地址的有效生命期值，单位为秒
Sequence Number	序列号

在本申请实施例中，第一网络设备还包括本地 MAC-IP 表，本地 MAC-IP 表包括第一本地 MAC-IP

表项，第一本地 MAC-IP 表项包括第三序列号。

在建立第二远端 MAC-IP 表项后，若第二远端 MAC-IP 表项与第一本地 MAC-IP 表项匹配，且第二序列号大于第三序列号，则将第一本地 MAC-IP 表项删除，并将第一本地 MAC-IP 表项对应的 DHCP 中继表项删除。

其中，第二远端 MAC-IP 表项与第一本地 MAC-IP 表项匹配是指：第二远端 MAC-IP 表项包括的 MAC 地址和 IP 地址，与第一本地 MAC-IP 表项包括的 MAC 地址和 IP 地址相同。

可以理解的，若第二序列号大于第三序列号，说明该第一本地 MAC-IP 表项对应的终端已迁移至其他接入设备，即在该终端再次迁回之前，第一网络设备不会接收到该终端发送的业务报文。相应地，第一网络设备不会继续利用第一本地 MAC-IP 表项对该终端的业务报文进行合法性检查，所以可将该第一本地 MAC-IP 表项删除，并将第一本地 MAC-IP 表项对应的 DHCP 中继表项删除。

其中，第一网络设备可以将第一本地 MAC-IP 表项从内存中删除，并将硬件转发芯片的硬件资源中存储的与该第一本地 MAC-IP 表项对应的转发 MAC-IP 表项删除。如此，可以在不影响网络安全性的前提下，节约第一网络设备的内存资源和硬件资源。

需要说明的是，由于第一网络设备在生成第一本地 MAC-IP 表项后，会将该第一本地 MAC-IP 表项通告给其他网络设备。相应的，在第一网络设备将第一本地 MAC-IP 表项删除后，第一网络设备需要向其他网络设备发送 MAC-IP 撤销消息，以使得其他网络设备将与第一本地 MAC-IP 表项对应的远端 MAC-IP 表项删除。

此外，当第一网络设备因终端释放 IP 地址或者 IP 地址租约老化等原因删除 DHCP 中继表项时，可以同步删除 DHCP 中继表项对应的本地 MAC-IP 表项。

在本申请另一实施例中，第一网络设备包括本地 MAC-IP 表，本地 MAC-IP 表包括至少一个本地 MAC-IP 表项。在建立第二远端 MAC-IP 表项之后，该方法还包括：

步骤 A、接收终端发送的第一报文，第一报文包括终端的 MAC 地址和 IP 地址。

步骤 B、若本地 MAC-IP 表中未存在与终端的 MAC 地址和 IP 地址匹配的本地 MAC-IP 表项，且终端的 MAC 地址和 IP 地址与第二远端 MAC-IP 表项匹配，则对终端进行接入探测。

可以理解的是，若本地 MAC-IP 表中未存在与终端的 MAC 地址和 IP 地址匹配的本地 MAC-IP 表项，但终端的 MAC 地址和 IP 地址与第二远端 MAC-IP 表项匹配，则说明该终端是从其他接入设备迁移而来。

可选地，终端迁移至第一网络设备下挂的 AP 后，若终端未立即进行 IP 地址的租约更新，第一网络设备可以接收到来自该终端的第一报文，该第一报文可以为协议报文或者业务报文。

第一网络设备接收到该第一报文后，第一网络设备的转发平面会生成一个该第一报文的源 MAC 地址的首包事件。在 IPv6 场景下，该首包事件会触发一次 ND 探测，在 IPv4 场景下，该首包事件会触发一次 ARP 探测。

步骤 C、若接收到终端发送的接入响应，则生成合成 MAC-IP 表项。合成 MAC-IP 表项包括终端的 MAC 地址和 IP 地址、端口标识以及 VLAN 标识。

在 IPv4 场景下，第一网络设备进行 ARP 探测后，若接收到终端发送的接入响应，则可生成 ARP 表项，ARP 表项包括终端接入的端口标识以及 VLAN 标识，进而第一网络设备可以基于第二远端

MAC-IP 表项和 ARP 表项生成合成 MAC-IP 表项。

在 IPv6 场景下，第一网络设备进行 ND 探测后，若接收到终端发送的接入响应，则可生成 ND 表项，ND 表项包括终端接入的端口标识以及 VLAN 标识，进而第一网络设备可以基于第二远端 MAC-IP 表项和 ND 表项生成合成 MAC-IP 表项。

以 IPv6 场景为例，合成 MAC-IP 表项包括的字段如表 4 所示：

表 4

字段	描述
IPv6 address	DHCPv6 终端的 IPv6 地址（来自远端 MAC-IP 表项）
MAC Address	DHCPv6 终端的 MAC 地址（来自远端 MAC-IP 表项和携带该 MAC 地址的第一报文）
Port index	DHCPv6 中继设备收到 DHCPv6 终端请求报文的二层端口信息 （来自 ND 表项）
Interface	DHCPv6 中继接口（来自 ND 表项）
Inner VLAN	DHCPv6 中继用户地址表项的内层 VLAN Tag （来自 ND 表项）
Outer VLAN	DHCPv6 中继用户地址表项的外层 VLAN Tag （来自 ND 表项）
Preferred lifetime	IPv6 地址的首选生命期值，单位为秒（来自远端 MAC-IP 表项）
Valid lifetime	IPv6 地址的有效生命期值，单位为秒（来自远端 MAC-IP 表项）

需要说明的是，合成 MAC-IP 表项仅在生成该合成 MAC-IP 表项的第一网络设备中使用，第一网络设备不会向其他网络设备通告合成 MAC-IP 表项。

其中，该合成 MAC-IP 表项占用第一网络设备的内存中用于存储控制 MAC-IP 表项的资源。

步骤 D、根据合成 MAC-IP 表项生成转发 MAC-IP 表项，转发 MAC-IP 表项包括终端的 MAC 地址和 IP 地址。

步骤 E、将转发 MAC-IP 表项存下发至硬件资源中。

其中，硬件资源为硬件转发芯片中，用于存储转发 MAC-IP 表项的硬件资源。

采用上述方法，第一网络设备生成第二远端 MAC-IP 表项后，此时终端可能未迁移至该第一网络设备下挂的终端，因此无需利用该第二远端 MAC-IP 表项进行安全性检查，进而无需将该第二远端 MAC-IP 表项对应的转发 MAC-IP 表项下发到硬件资源，可以避免占用紧缺的硬件资源。当第一网络设备确定该第二远端 MAC-IP 表项对应的终端接入该第一网络设备后，生成合成 MAC-IP 表项，并将合成 MAC-IP 表项对应的转发 MAC-IP 表项下发至硬件资源中，进而可以实现对该终端的报文进行控制面检查和转发面检查，拒绝非法报文进入网络，提高网络安全性。

在上述实施例的基础上，第一网络设备可能会删除 ARP 表项或 ND 表项。例如，以 IPv6 场景为例，有些终端在锁屏等状态下，对第一网络设备发起的 ND 表项老化探测消息不回应，会导致第一网络设备

中该终端对应的ND表项被老化删除。或者，若接入设备检测到终端的接入接口断开，则接入设备可以将从该接入接口上线的终端的ND表项删除。

当终端的接入表项被删除时，第一网络设备可以删除上述合成MAC-IP表项和转发MAC-IP表项。

其中，终端的接入表项是该终端对应的ND表项或ARP表项。

由于第一网络设备在认为终端已经断开的情况下，才会删除ND表项或ARP表项，进而暂时无需对来自该终端的报文进行合法性检查，所以可以删除内存中存储的合成MAC-IP表项，并删除该合成MAC-IP表项对应的转发MAC-IP表项。如此可以减少对第一网络设备的内存资源和硬件资源的占用。由于第一网络设备中该合成MAC-IP表项对应的第二远端MAC-IP表项未被删除，所以若该终端再次接入，第一网络设备仍可基于该第二远端MAC-IP表项再次生成合成MAC-IP表项，不会导致来自该终端的合法报文被丢弃，第一网络设备利用合成MAC-IP表项对报文进行安全性检查，可以提高网络安全性。

以下对第一网络设备发送的MAC-IP通告消息进行介绍。

MAC-IP通告消息中包括第一扩展团体属性，第一扩展团体属性中包括IP地址的有效生命周期值。

可选地，MAC-IP通告消息中包括第二扩展团体属性，第二扩展团体属性中包括MAC-IP表项的序列号。

第一网络设备可以基于BGP协议发送MAC-IP通告消息和MAC-IP撤销消息，且MAC-IP通告消息和MAC-IP撤销消息均可以为BGP更新（Update）报文。

其中，MAC-IP通告消息可以为携带多协议可达网络层可达性信息（Multiprotocol_ Reachable_ Network Layer Reachability Information，MP_ REACH_ NLRI）属性的BGP更新（Update）报文，MP_REACH_NLRI属性表示MAC-IP表项对应的终端对于发送该MAC-IP通告消息的设备可达。

MAC-IP撤销消息可以为携带多协议不可达网络层可达性信息（Multiprotocol_ UNReachable_ Network Layer Reachability Information，MP_ UNREACH_ NLRI）属性的BGP Update报文，MP_UNREACH_NLRI属性表示MAC-IP表项对应的终端对于发送该MAC-IP撤销消息的设备不可达。

MP_REACH_NLRI属性和MP_UNREACH_NLRI属性中均包括MAC-IP NLRI，MAC-IP NLRI的格式如图3所示，包括：路由类型（Route Type）、长度（Length）和路由类型明细（Route Type specific）。

其中，Route Type表示MAC-IP NLRI的类型，占用1八位组（octet），本申请实施例中，可以定义该路由类型为用于传输MAC-IP表项的路由类型。

Length表示MAC-IP NLRI的长度，占用1 octet；

Route Type specific表示MAC-IP NLRI的路由类型，占用的比特数是可变的（variable）。

如图4所示，Route Type specific中包括：路由区分符（Route Distinguisher，RD）、以太网段标识符（Ethernet Segment Identifier），以太网标志（Ethernet Tag ID），MAC地址长度（MAC Address Length）、MAC地址（MAC Address）、IP地址长度（IP Address Length）和IP地址（IP Address）。

其中，RD，占用8 octets；

Ethernet Segment Identifier为标识以太网段的唯一非零标识符，占用10 octets；

Ethernet Tag ID用于储存终端所在VLAN的VLAN标识，占用4 octets；

MAC Address Length用于记录终端的MAC地址长度，占用1 octet；

MAC Address用于记录终端的MAC地址，占用6 octets；

IP Address Length 用于记录终端的 IP 地址长度，占用 1 octet；

IP Address 用于记录终端的 IP 地址，占用 0、4 或 16 octets。

为了在 BGP Update 报文中携带 MAC-IP 表项中的 IP 地址的有效生命期值，可以对 BGP 协议进行扩展，在 BGP 协议中引入 MAC-IP 表项的第一扩展团体属性，该第一扩展团体属性的长度可以为 16 个字节，结构如图 5 所示。

其中，Type 表示第一扩展团体属性的类型，长度为 1 字节；作为示例，Type 的取值可以为 0x8d，Type 的取值可以根据实际情况设置，本申请实施例对此不作限定。

Sub-Type 表示第一扩展团体属性的子类型，长度为 1 字节；作为示例，Sub-Type 的取值可以为 0x01，Sub-Type 的取值可以根据实际情况设置，本申请实施例对此不作限定。

Reserved 为预留位，长度为 2 字节，作为示例，Reserved 的取值可以为 0，Reserved 的取值可以根据实际情况设置，本申请实施例对此不作限定。

Preferred lifetime 为本地 MAC-IP 表项中的 IP 地址的首选生命期值，长度为 4 字节，本申请实施例中暂未使用该参数。

Valid lifetime 为本地 MAC-IP 表项中的 IP 地址的有效生命期值，长度为 4 字节。

同理，为了在 BGP Update 报文中携带序列号，可以对 BGP 协议进行扩展，在 BGP 协议中引入 MAC-IP 表项对应的第二扩展团体属性，该第二扩展团体属性长度可以为 8 个字节，结构如图 6 所示。

其中，Type 表示第二扩展团体属性的类型，长度为 1 字节；作为示例，Type 的取值可以为 0x8e，Type 的取值可以根据实际情况设置，本申请实施例对此不作限定。

Sub-Type 表示第二扩展团体属性的子类型，长度为 1 字节；作为示例，Sub-Type 的取值可以为 0x01，Sub-Type 的取值可以根据实际情况设置，本申请实施例对此不作限定。

Reserved 为预留位，长度为 2 字节，作为示例，Reserved 的取值可以为 0，Reserved 的取值可以根据实际情况设置，本申请实施例对此不作限定。

Sequence Number 为 MAC-IP 表项对应的序列号，长度为 4 字节。

对应于上述实施例，本申请实施例还提供一种安全表项维护方法，该方法应用于第二网络设备，第二网络设备可以为图 1 中的 Spine1、Spine2 或 Spine3。第二网络设备包括第一远端 MAC-IP 表，第一远端 MAC-IP 表包括第四网络设备通告的至少一个远端 MAC-IP 表项，如图 7 所示，该方法包括：

S701、当与第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值。

其中，有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期。

第二网络设备可以为汇聚设备。第四网络设备可以为与第二网络设备之间存在协议连接的接入设备或汇聚设备。

以图 1 所示的组网系统为例，在第二网络设备为图 1 中的 Spine1 的情况下，第四网络设备可以为 Leaf1、Leaf2 或 Leaf3，也可以为 Spine3。

或者，在第二网络设备为图 1 中的 Spine3 的情况下，第四网络设备可以为 Spine1 或 Spine2。

第二网络设备与第四网络设备之间的协议连接可以为 BGP 协议连接。或者第二网络设备与第四网络设备之间的协议连接也可以为自定义的私有协议连接，在该协议连接为私有协议连接的情况下，各网

络设备之间通过私有协议通告 MAC-IP 表项。

S702、若协议连接中断的持续时长达到有效生命周期值，则删除至少一个远端 MAC-IP 表项。

可以理解的是，在第一远端 MAC-IP 表包括一个 MAC-IP 表项的情况下，第二网络设备可获取该 MAC-IP 表项包括的有效生命周期值。第二网络设备以检测到协议连接中断的时刻为起始时刻，将远端 MAC-IP 表项保存有效生命期值，即第二网络设备在检测到协议连接中断后，将远端 MAC-IP 表项保持有效生命周期值，在到达有效生命周期值之前，不会将该远端 MAC-IP 表项删除。

若距离起始时刻的时长达到有效生命周期值时，该协议连接仍未恢复，则删除该远端 MAC-IP 表项。

例如有效生命期为 100000 秒，则第二网络设备检测到协议连接中断后开始计时，将该远端 MAC-IP 表项保持 100000 秒。若 100000 秒后，协议连接仍未恢复，则第二网络设备将该远端 MAC-IP 表项删除。

在第一远端 MAC-IP 表包括多个 MAC-IP 表项的情况下，第二网络设备可以获取到多个远端 MAC-IP 表项的有效生命周期值。

一种实施方式中，在协议连接中断的持续时长达到获取到的所有有效生命周期值后，也就是协议连接中断的持续时长达到获取的各有效生命周期值中的最大生命周期值后，一次性删除第二远端 MAC-IP 表包括多个 MAC-IP 表项。

另一种实施方式中，针对每个有效生命周期值，若协议连接中断的持续时长达到该有效生命周期值，则将该有效生命周期值所属的 MAC-IP 表项删除。

采用上述方法，第二网络设备中的远端 MAC-IP 表项中包括有效生命期值，且该有效生命期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命期，若协议连接中断的持续时长达到有效生命周期值，说明该 MAC-IP 表项包括的 IP 地址已经无效。即原本申请到该 IP 地址的终端已经无法继续使用该 IP 地址，此时将该远端 MAC-IP 表项删除也不会影响到后续对该终端的合法性校验，不会影响网络安全，且可避免该远端 MAC-IP 表项继续占用第二网络设备的资源。在协议连接中断的持续时长达到有效生命周期值之前，第二网络设备不会将该远端 MAC-IP 表项删除，因此在使能源地址安全检查机制的情况下，也不会导致与该远端 MAC-IP 表项匹配的合法报文被丢弃，且能防止非法报文进入网络，能够提升网络安全性。

在本申请另一实施例中，第二网络设备可以接收到其他网络设备通告的 MAC-IP 表项，基于此，在上述 S701、当与第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项中的有效生命周期值之前，该方法还包括：

接收第四网络设备发送的第一 MAC-IP 通告消息，建立第一远端 MAC-IP 表项。

其中，第一 MAC-IP 通告消息包括第一 IP 地址的第一有效生命周期值以及第一序列号。相应地，第一远端 MAC-IP 表项包括第一有效生命周期值以及第一序列号。

可以理解的是，第一 MAC-IP 通告消息还包括 MAC 地址和第一 IP 地址，第一远端 MAC-IP 表项也包括该 MAC 地址和第一 IP 地址。

可选地，第一 MAC-IP 通告消息中还可以包括第一 IP 地址的首选生命周期值，相应地，第一远端 MAC-IP 表项中也包括第一 IP 地址的首选生命周期值。

可以理解的是，网络设备之间可以互相进行 MAC-IP 表项的通告，可以使得终端发生迁移后，终端接入的接入设备仍能够基于远端 MAC-IP 表项对终端的报文进行合法性检查，拒绝非法报文进入网络，

提高网络安全性。

在本申请的一个实施例中，第二网络设备还包括至少一个第二远端 MAC-IP 表，至少一个第二远端 MAC-IP 表包括第二远端 MAC-IP 表项，第二远端 MAC-IP 表项包括第二序列号。第二网络设备在建立远端 MAC-IP 表项之后，该方法还包括：

若第一序列号大于第二序列号，则向除第四网络设备之外的其他网络设备发送第二 MAC-IP 通告消息，第二 MAC-IP 通告消息包括第一有效生命周期值以及第一序列号。

其中，第一序列号大于第二序列号，则说明第二网络设备存储的各远端 MAC-IP 表中，不存在与第一远端 MAC-IP 表项匹配，且包括的序列号大于第一序列号的远端表项。

可以理解的，针对 IP 地址和 MAC 地址相同的远端 MAC-IP 表项，序列号越大，则该序列号对应的远端 MAC-IP 表项生成时间越晚。因此，若第一序列号大于第二序列号，则说明第一远端 MAC-IP 表项是最新生成的 MAC-IP 表项，进而需向除第四网络设备之外的其他网络设备通告该第一远端 MAC-IP 表项。

采用上述方法，由于序列号用于表示同一终端对应的 MAC-IP 表项的生成顺序，序列号越大，则该序列号对应的 MAC-IP 表项生成时间越晚。因此，序列号小的远端 MAC-IP 表项可能不再适用于该远端 MAC-IP 表项对应的终端。若第一序列号大于第二序列号，则向除第四网络设备之外的其他网络设备发送第二 MAC-IP 通告消息。如此，可以提高 MAC-IP 通告的及时性和准确性。

在本申请的另一实施例中，在图 7 对应的实施例的基础上，第二网络设备还包括至少一个第三远端 MAC-IP 表，每个第三远端 MAC-IP 表包括至少一个远端 MAC-IP 表项。

可以理解的是，由于第二网络设备在生成远端 MAC-IP 表项后，会将生成的远端 MAC-IP 表项通告给除第四网络设备之外的其他网络设备。相应地，在删除远端 MAC-IP 表项之后，第二网络设备还需要基于删除的远端 MAC-IP 表项发送 MAC-IP 撤销消息或 MAC-IP 通告消息。在第二网络设备删除至少一个远端 MAC-IP 表项后，具体包括以下两种情况：

情况一、针对删除的每个远端 MAC-IP 表项，若至少一个第三远端 MAC-IP 表中未存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则向除第四网络设备之外的其他网络设备发送第一 MAC-IP 撤销消息。

其中，第一 MAC-IP 撤销消息中包括该远端 MAC-IP 表项中的 MAC 地址和 IP 地址。

进而，除第四网络设备之外的其他网络设备接收到该第一 MAC-IP 撤销消息后，可以及时更新自身存储的远端 MAC-IP 表项，避免继续使用失效的远端 MAC-IP 表项，可以提高网络安全性。

情况二、针对删除的每个远端 MAC-IP 表项，若至少一个第三 MAC-IP 表中存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则从匹配的其他 MAC-IP 表项中选择序列号最大的第三远端 MAC-IP 表项，向除第五网络设备之外的其他网络设备发送第五 MAC-IP 通告消息。

其中，第三远端 MAC-IP 表项包括第二有效生命周期值以及第三序列号，相应地，第三 MAC-IP 通告消息中包该第二有效生命周期值以及第三序列号，第五网络设备为第三远端 MAC-IP 表项的来源设备。第五网络设备可以为接入设备，也可以为汇聚设备的上级汇聚设备。

也就是说，若第二网络设备中存在与删除的远端 MAC-IP 表项匹配的其他远端 MAC-IP 表项，则第二网络设备需要重新通告一个与删除的远端 MAC-IP 表项中 IP 地址和 MAC 地址相同的，且序列号最

大的远端 MAC-IP 表项。

需要说明的是，在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项中，可能存在多个序列号最大的远端 MAC-IP 表项，即多个远端 MAC-IP 表项的序列号相同，并列最大。则第二网络设备可以在多个序列号最大的远端 MAC-IP 表项中随机选择一个，并将选择的一个序列号最大的远端 MAC-IP 表项作为上述第三远端 MAC-IP 表项，并通告给除第五网络设备之外的其他网络设备。

例如，第二网络设备中存储有:

来自网络设备 A 的远端 MAC-IP 表项 1，序列号为 3；

来自网络设备 B 的远端 MAC-IP 表项 2，序列号为 2；

来自网络设备 C 的远端 MAC-IP 表项 3，序列号为 1；

以及来自网络设备 D 的远端 MAC-IP 表项 4，序列号为 2。

上述 4 个远端表项中的 MAC 地址和 IP 地址均相同，在第二网络设备与网络设备 A 之间的协议连接中断后，且按照上述实施例介绍的方法将远端 MAC-IP 表项 1 删除后，可以确定远端 MAC-IP 表项 2 和远端 MAC-IP 表项 4 的序列号最大，第二网络设备在远端 MAC-IP 表项 2 和远端 MAC-IP 表项 4 中随机选择远端 MAC-IP 表项 2，则第二网络设备向网络设备 C 和网络设备 D 通告远端 MAC-IP 表项 2。

网络设备 C 接收到第二网络设备通告的远端 MAC-IP 表项 2 后，将查找到第二网络设备上次通告的远端 MAC-IP 表项 1，并将自身存储的远端 MAC-IP 表项 1 修改为远端 MAC-IP 表项 2。

网络设备 D 接收到第二网络设备通告的远端 MAC-IP 表项 2 后，将查找到第二网络设备上次通告的远端 MAC-IP 表项 1，并将自身存储的远端 MAC-IP 表项 1 修改为远端 MAC-IP 表项 2。

如此，第二网络设备在删除远端 MAC-IP 表项后，若还存储有 MAC 地址和 IP 地址相同的其他远端 MAC-IP 表项，可以及时向其他网络设备重新通告远端 MAC-IP 表项，可以避免其他网络设备继续使用失效的远端 MAC-IP 表项，保证各网络设备中存储的远端 MAC-IP 表项的准确性，提高网络安全性。

以下对第二网络设备发送的 MAC-IP 通告消息进行说明：

第二网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，第一扩展团体属性中包括 IP 地址的有效生命周期值。

第二网络设备发送的 MAC-IP 通告消息中包括第二扩展团体属性，第二扩展团体属性中包括 MAC-IP 表项的序列号。

MAC-IP 通告消息的格式可以参考上述实施例中的相关描述。

以下，结合具体的应用场景对本申请实施例提供的安全表项维持方法进行介绍。

如图 8 所示，如 8 的结构与图 1 相同，其中，Leaf1、Leaf2 和 Leaf3 为接入设备，Spine1 和 Spine2 汇聚设备，Spine3 为 Spine1 和 Spine2 的上级汇聚设备。

区域 1 内的 Leaf1 生成新的本地 MAC-IP 表项后，通过协议连接向 Spine1 发送 MAC-IP 通告消息，MAC-IP 通告消息中包括本地 MAC-IP 表项中的 IP 地址、MAC 地址、序列号（Sequence Number，SN）和该 IP 地址的有效生命周期值。其中，该 MAC-IP 通告消息中的序列号为 1。

Spine1 接收 Leaf1 发送的 MAC-IP 通告消息后，生成远端 MAC-IP 表项，该远端 MAC-IP 表项中包括 MAC-IP 通告消息中的 IP 地址、MAC 地址、SN 和该 IP 地址的有效生命周期值。

此时，Spine1 中只存储有该终端对应的一个序列号为 1 的远端 MAC-IP 表项，Spine1 可以向 Leaf2、

Leaf3 以及 Spine3 发送 MAC-IP 通告消息，该 MAC-IP 通告消息中包括该远端 MAC-IP 表项中的内容。

Leaf2、Leaf3 以及 Spine3 接收到 MAC-IP 通告消息后，也可生成远端 MAC-IP 表项。

进而，假设 Spine3 中不存在与该远端 MAC-IP 表项匹配的其他远端 MAC-IP 表项，则 Spine3 向区域 2 的 spine2 发送 MAC-IP 通告消息，该 MAC-IP 通告消息中包括该远端 MAC-IP 表项中的内容。

spine2 接收到 MAC-IP 通告消息后，也可生成远端 MAC-IP 表项。

进而，在图 8 的基础上，若该终端迁移到 Leaf2 下联的 AP2，则如图 9 所示，在一种实现方式中，若终端立即向 DHCPv6 服务器发起 IPv6 地址租约更新，则 Leaf2 可以生成 DHCP 中继表项，并基于 DHCP 中继表项生成本地 MAC-IP 表项。

然后，Leaf2 可以向 Spine1 发送 MAC-IP 通告消息，该 MAC-IP 通告消息中携带的序列号为 2，Spine1 接收到该 MAC-IP 通告消息后，基于该 MAC-IP 通告消息生成远端 MAC-IP 表项，该远端 MAC-IP 表项中包括的序列号为 2。

此时 Spine1 确定本地还存储有序列号为 1，且与该新生成的远端 MAC-IP 表项中的 MAC 地址和 IP 地址均相同的远端 MAC-IP。

因新生成的远端 MAC-IP 表项中的序列号较大，因此 Spine1 将序列号为 2 的远端 MAC-IP 表项通告给 Spine3、Leaf1 和 Leaf3。

Spine3、Leaf1 和 Leaf3 接收到 MAC-IP 通告消息后，Leaf1 生成序列号为 2 的远端 MAC-IP 表项，Spine3 和 Leaf3 中此时均存储有来自 Spine1 的序列号为 1 的远端 MAC-IP 表项，且该远端 MAC-IP 表项中的 MAC 地址和 IP 地址为此次接收到的 MAC-IP 通告消息中的 MAC 地址和 IP 地址相同，则 Spine3 和 Leaf3 将该序列号为 1 的远端 MAC-IP 表项修改为序列号为 2 的远端 MAC-IP 表项。

Spine3 还会向 Spine2 发送 MAC-IP 通告消息，进而 Spine2 将对应的序列号为 1 的远端 MAC-IP 表项修改为序列号为 2 的远端 MAC-IP 表项。

若终端采用另一种实现方式，在图 8 的基础上，若该终端迁移到 Leaf2 下联的 AP2，则如图 10 所示，若终端未立即向 DHCPv6 服务器发起 IPv6 地址租约更新，若 Leaf2 接收到该终端发送的报文，该报文可以是协议报文或者业务报文，将通过首包事件触发 Leaf2 对该终端进行 ND 探测，Leaf2 学习该终端对应的 ND 表项，并基于 ND 表项和 Leaf2 上存储的该终端对应的远端 MAC-IP 表项，生成合成 MAC-IP 表项。

需要说明的是，在图 10 实施例的基础上，在 Leaf2 生成终端对应的合成 MAC-IP 表项后，若后续接终端向 DHCPv6 服务器发起 IPv6 地址租约更新时，该接入设备可以执行图 9 中介绍的流程，即 Leaf2 还可以为该终端生成本地 MAC-IP 表项。

基于相同的构思，本申请实施例提供一种安全表项维护装置，应用于第一网络设备，第一网络设备包括远端 MAC-IP 表，远端 MAC-IP 表包括第二网络设备通告的至少一个远端 MAC-IP 表项，如图 11 所示，该装置包括：

获取模块 1101，用于当与第二网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

删除模块 1102，用于若协议连接中断的持续时长达到有效生命周期值，则删除至少一个远端 MAC-IP 表项。

可选地，该装置还包括：

建立模块，用于当第一网络设备生成 DHCP 中继表项时，基于 DHCP 中继表项建立本地 MAC-IP 表项，并向硬件资源下发本地 MAC-IP 表项对应的转发 MAC-IP 表项，本地 MAC-IP 表项包括第一 IP 地址的第一有效生命周期值；

发送模块，用于向第三网络设备发送第一 MAC-IP 通告消息，以使得第三网络设备建立第一远端 MAC-IP 表项；

其中，第一 MAC-IP 通告消息包括第一序列号以及第一有效生命周期值，第一远端 MAC-IP 表项包括第一序列号以及第一有效生命周期值；

第一序列号为与本地 MAC-IP 表项匹配的远端 MAC-IP 表项中的最大序列号与 1 的和值。

可选地，删除模块 1102，还用于当本地 MAC-IP 表项匹配的接入表项被删除时，删除转发 MAC-IP 表项。

可选地，该装置还包括：

接收模块，用于接收第二网络设备发送的第二 MAC-IP 通告消息，第二 MAC-IP 通告消息包括第二 IP 地址的第二有效生命周期值以及第二序列号；

建立模块，用于建立第二远端 MAC-IP 表项，第二远端 MAC-IP 表项包括第二有效生命周期值以及第二序列号。

可选地，第一网络设备包括本地 MAC-IP 表，本地 MAC-IP 表包括至少一个本地 MAC-IP 表项；

该装置还包括：探测模块、生成模块和下发模块；

接收模块，还用于接收终端发送的第一报文，第一报文包括终端的 MAC 地址和 IP 地址；

探测模块，用于若本地 MAC-IP 表中未存在与终端的 MAC 地址和 IP 地址匹配的本地 MAC-IP 表项，且终端的 MAC 地址和 IP 地址与第二远端 MAC-IP 表项匹配，则对终端进行接入探测；

生成模块，用于若接收到终端发送的接入响应，则生成合成 MAC-IP 表项，合成 MAC-IP 表项包括终端的 MAC 地址和 IP 地址、端口标识以及 VLAN 标识；

生成模块，还用于根据合成 MAC-IP 表项生成转发 MAC-IP 表项，转发 MAC-IP 表项包括终端的 MAC 地址和 IP 地址；

下发模块，用于将转发 MAC-IP 表项下发至硬件资源中。

可选地，删除模块 1102，还用于当终端的接入表项被删除时，删除合成 MAC-IP 表项和转发 MAC-IP 表项。

可选地，第一网络设备包括本地 MAC-IP 表，本地 MAC-IP 表包括第一本地 MAC-IP 表项，第一本地 MAC-IP 表项包括第三序列号；

删除模块 1102，还用于若第二远端 MAC-IP 表项与第一本地 MAC-IP 表项匹配，且第二序列号大于第三序列号，则将第一本地 MAC-IP 表项删除，并将第一本地 MAC-IP 表项对应的 DHCP 中继表项删除。

可选地，第一网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，第一扩展团体属性中包括 IP 地址的有效生命周期值。

可选地，第一网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，第二扩展团体属性中

包括 MAC-IP 表项的序列号。

基于相同的构思，本申请实施例还提供一种安全表项维护装置，应用于第二网络设备，第二网络设备包括第一远端 MAC-IP 表，第一远端 MAC-IP 表包括第四网络设备通告的至少一个远端 MAC-IP 表项，如图 12 所示，该装置包括：

获取模块 1201，用于当与第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

删除模块 1202，用于若协议连接中断的持续时长达到有效生命周期值，则删除至少一个远端 MAC-IP 表项。

可选地，该装置还包括：

接收模块，用于接收第四网络设备发送的第一 MAC-IP 通告消息，第一 MAC-IP 通告消息包括第一 IP 地址的第一有效生命周期值以及第一序列号；

建立模块，用于建立第一远端 MAC-IP 表项，第一远端 MAC 表项包括第一有效生命周期值以及第一序列号。

可选地，第二网络设备还包括至少一个第二远端 MAC-IP 表，至少一个第二远端表包括第二远端 MAC-IP 表项，第二远端 MAC-IP 表项与第一远端 MAC-IP 表项匹配，第二远端 MAC-IP 表项包括第二序列号；该装置还包括：

发送模块，用于若第一序列号大于第二序列号，则向除第四网络设备之外的其他网络设备发送第二 MAC-IP 通告消息，第二 MAC-IP 通告消息包括第一有效生命周期值以及第一序列号。

可选地，第二远端设备还包括至少一个第三远端 MAC-IP 表，每个第三远端 MAC-IP 表包括至少一个远端 MAC-IP 表项；该装置还包括发送模块；

发送模块，用于：

针对删除的每个远端 MAC-IP 表项，若至少一个第三远端 MAC-IP 表中未存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则向除第四网络设备之外的其他网络设备发送第一 MAC-IP 撤销消息，第一 MAC-IP 撤销消息包括该远端 MAC-IP 表项中的 MAC 地址和 IP 地址；或者，

针对删除的每个远端 MAC-IP 表项，若至少一个第三远端 MAC-IP 表中存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则从匹配的远端 MAC-IP 表项中选择序列号最大的第三远端 MAC-IP 表项，第三远端 MAC-IP 表项包括第二有效生命周期值以及第三序列号；向除第五网络设备之外的其他网络设备发送第三 MAC-IP 通告消息，第三 MAC-IP 通告消息包括第二有效生命周期值和第三序列号，第五网络设备为第三远端 MAC-IP 表项的来源设备。

可选地，第二网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，第一扩展团体属性中包括 IP 地址的有效生命周期值。

可选地，第二网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，第二扩展团体属性中包括 MAC-IP 表项的序列号。

基于相同的构思，本申请实施例还提供一种第一网络设备，第一网络设备包括远端 MAC-IP 表，远端 MAC-IP 表包括第二网络设备通告的至少一个远端 MAC-IP 表项；如图 13 所示，该第一网络设备包括：

处理器 1301；

收发器 1304；

机器可读存储介质 1302，机器可读存储介质 1302 存储有能够被处理器 1301 执行的机器可执行指令；机器可执行指令促使处理器 1301 执行以下步骤：

当与第二网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

若协议连接中断的持续时长达到有效生命周期值，则删除至少一个远端 MAC-IP 表项。

可选地，机器可执行指令还促使处理器 1301 执行以下步骤：

当第一网络设备生成 DHCP 中继表项时，基于 DHCP 中继表项建立本地 MAC-IP 表项，并向硬件资源下发本地 MAC-IP 表项对应的转发 MAC-IP 表项，本地 MAC-IP 表项包括第一 IP 地址的第一有效生命周期值；

通过收发器 1304 向第三网络设备发送第一 MAC-IP 通告消息，以使得第三网络设备建立第一远端 MAC-IP 表项；

其中，第一 MAC-IP 通告消息包括第一序列号以及第一有效生命周期值，第一远端 MAC-IP 表项包括第一序列号以及第一有效生命周期值；

第一序列号为与本地 MAC-IP 表项匹配的远端 MAC-IP 表项中的最大序列号与 1 的和值。

可选地，机器可执行指令还促使处理器 1301 执行以下步骤：

当本地 MAC-IP 表项匹配的接入表项被删除时，删除转发 MAC-IP 表项。

可选地，机器可执行指令还促使处理器 1301 执行以下步骤：

通过收发器 1304 接收第二网络设备发送的第二 MAC-IP 通告消息，第二 MAC-IP 通告消息包括第二 IP 地址的第二有效生命周期值以及第二序列号；

建立第二远端 MAC-IP 表项，第二远端 MAC-IP 表项包括第二有效生命周期值以及第二序列号。

可选地，第一网络设备包括本地 MAC-IP 表，本地 MAC-IP 表包括至少一个本地 MAC-IP 表项；

机器可执行指令还促使处理器 1301 执行以下步骤：

通过收发器 1304 接收终端发送的第一报文，第一报文包括终端的 MAC 地址和 IP 地址；

若本地 MAC-IP 表中未存在与终端的 MAC 地址和 IP 地址匹配的本地 MAC-IP 表项，且终端的 MAC 地址和 IP 地址与第二远端 MAC-IP 表项匹配，则对终端进行接入探测；

若接收到终端发送的接入响应，则生成合成 MAC-IP 表项，合成 MAC-IP 表项包括终端的 MAC 地址和 IP 地址、端口标识以及 VLAN 标识；

根据合成 MAC-IP 表项生成转发 MAC-IP 表项，转发 MAC-IP 表项包括终端的 MAC 地址和 IP 地址；

将转发 MAC-IP 表项下发至硬件资源中。

可选地，机器可执行指令还促使处理器 1301 执行以下步骤：

当终端的接入表项被删除时，删除合成 MAC-IP 表项和转发 MAC-IP 表项。

可选地，第一网络设备包括本地 MAC-IP 表，本地 MAC-IP 表包括第一本地 MAC-IP 表项，第一本地 MAC-IP 表项包括第三序列号；机器可执行指令还促使处理器 1301 执行以下步骤：

若第二远端 MAC-IP 表项与第一本地 MAC-IP 表项匹配，且第二序列号大于第三序列号，则将第一本地 MAC-IP 表项删除，并将第一本地 MAC-IP 表项对应的 DHCP 中继表项删除。

可选地，第一网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，第一扩展团体属性中包括 IP 地址的有效生命周期值。

可选地，第一网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，第二扩展团体属性中包括 MAC-IP 表项的序列号。

在图 13 中，还可以包括通信总线 1303。处理器 1301、机器可读存储介质 1302 及收发器 1304 之间通过通信总线 1303 完成相互间的通信，通信总线 1303 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。

收发器 1304 可以为无线通信模块，收发器 1304 在处理器 1301 的控制下，与其他设备进行数据交互。

机器可读存储介质 1302 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 1301 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。

基于相同的构思，本申请实施例还提供一种第二网络设备，第二网络设备包括第一远端 MAC-IP 表，第一远端 MAC-IP 表包括第四网络设备通告的至少一个远端 MAC-IP 表项，如图 14 所示，该第二网络设备包括：

处理器 1401；

收发器 1404；

机器可读存储介质 1402，机器可读存储介质 1402 存储有能够被处理器 1401 执行的机器可执行指令；机器可执行指令促使处理器 1401 执行以下步骤：

当与第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

若协议连接中断的持续时长达到有效生命周期值，则删除至少一个远端 MAC-IP 表项。

可选地，机器可执行指令还促使处理器 1401 执行以下步骤：

通过收发器 1404 接收第四网络设备发送的第一 MAC-IP 通告消息，第一 MAC-IP 通告消息包括第一 IP 地址的第一有效生命周期值以及第一序列号；

建立第一远端 MAC-IP 表项，第一远端 MAC 表项包括第一有效生命周期值以及第一序列号。

可选地，第二网络设备还包括至少一个第二远端 MAC-IP 表，至少一个第二远端表包括第二远端 MAC-IP 表项，第二远端 MAC-IP 表项与第一远端 MAC-IP 表项匹配，第二远端 MAC-IP 表项包括第二序列号；机器可执行指令促使处理器 1401 执行以下步骤：

若第一序列号大于第二序列号，则向除第四网络设备之外的其他网络设备发送第二 MAC-IP 通告消息，第二 MAC-IP 通告消息包括第一有效生命周期值以及第一序列号。

可选地，第二远端设备还包括至少一个第三远端 MAC-IP 表，每个第三远端 MAC-IP 表包括至少一个远端 MAC-IP 表项；机器可执行指令促使处理器 1401 执行以下步骤：

针对删除的每个远端 MAC-IP 表项，若至少一个第三远端 MAC-IP 表中未存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则向除第四网络设备之外的其他网络设备发送第一 MAC-IP 撤销消息，第一 MAC-IP 撤销消息包括该远端 MAC-IP 表项中的 MAC 地址和 IP 地址；或者，

针对删除的每个远端 MAC-IP 表项，若至少一个第三远端 MAC-IP 表中存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则从匹配的远端 MAC-IP 表项中选择序列号最大的第三远端 MAC-IP 表项，第三远端 MAC-IP 表项包括第二有效生命周期值以及第三序列号；向除第五网络设备之外的其他网络设备发送第三 MAC-IP 通告消息，第三 MAC-IP 通告消息包括第二有效生命周期值和第三序列号，第五网络设备为第三远端 MAC-IP 表项的来源设备。

可选地，第二网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，第一扩展团体属性中包括 IP 地址的有效生命周期值。

可选地，第二网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，第二扩展团体属性中包括 MAC-IP 表项的序列号。

在图 14 中，还可以包括通信总线 1403。处理器 1401、机器可读存储介质 1402 及收发器 1404 之间通过通信总线 1403 完成相互间的通信，通信总线 1303 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。

收发器 1404 可以为无线通信模块，收发器 1404 在处理器 1401 的控制下，与其他设备进行数据交互。

机器可读存储介质 1402 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 1401 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。

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维护方法，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任一安全表项维护方法的步骤。

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维护方法的步骤。

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。

以上所述仅为本发明的较佳实施例，并不用以限制本发明，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、一种安全表项维护方法，其特征在于，应用于第一网络设备，所述第一网络设备包括远端 MAC-IP 表，所述远端 MAC-IP 表包括所述第二网络设备通告的至少一个远端 MAC-IP 表项，所述方法包括：

当与所述第二网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，所述有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 表项。

2、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

当所述第一网络设备生成 DHCP 中继表项时，基于所述 DHCP 中继表项建立本地 MAC-IP 表项，并向硬件资源下发所述本地 MAC-IP 表项对应的转发 MAC-IP 表项，所述本地 MAC-IP 表项包括第一 IP 地址的第一有效生命周期值；

向第三网络设备发送第一 MAC-IP 通告消息，以使得所述第三网络设备建立第一远端 MAC-IP 表项；

其中，所述第一 MAC-IP 通告消息包括第一序列号以及所述第一有效生命周期值，所述第一远端 MAC-IP 表项包括所述第一序列号以及所述第一有效生命周期值；

所述第一序列号为与所述本地 MAC-IP 表项匹配的远端 MAC-IP 表项中的最大序列号与 1 的和值。

3、根据权利要求 2 所述的方法，其特征在于，在所述向硬件资源下发所述本地 MAC-IP 表项对应的转发 MAC-IP 表项之后，所述方法还包括：

当所述本地 MAC-IP 表项匹配的接入表项被删除时，删除所述转发 MAC-IP 表项。

4、根据权利要求 1 所述的方法，其特征在于，在所述当与所述第二网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值之前，所述方法还包括：

接收所述第二网络设备发送的第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括第二 IP 地址的第二有效生命周期值以及第二序列号；

建立第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项包括所述第二有效生命周期值以及所述第二序列号。

5、根据权利要求 4 所述的方法，其特征在于，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括至少一个本地 MAC-IP 表项；

在所述建立第二远端 MAC-IP 表项之后，所述方法还包括：

接收终端发送的第一报文，所述第一报文包括所述终端的 MAC 地址和 IP 地址；

若所述本地 MAC-IP 表中未存在与所述终端的 MAC 地址和 IP 地址匹配的本地 MAC-IP 表项，且所述终端的 MAC 地址和 IP 地址与所述第二远端 MAC-IP 表项匹配，则对所述终端进行接入探测；

若接收到所述终端发送的接入响应，则生成合成 MAC-IP 表项，所述合成 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址、端口标识以及 VLAN 标识；

根据所述合成 MAC-IP 表项生成转发 MAC-IP 表项，所述转发 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址；

将所述转发 MAC-IP 表项下发至硬件资源中。

6、根据权利要求 5 所述的方法，其特征在于，在所述将所述转发 MAC-IP 表项下发至硬件资源中之后，所述方法还包括：

当所述终端的接入表项被删除时，删除所述合成 MAC-IP 表项和所述转发 MAC-IP 表项。

7、根据权利要求 4 所述的方法，其特征在于，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括第一本地 MAC-IP 表项，所述第一本地 MAC-IP 表项包括第三序列号；在所述建立第二远端 MAC-IP 表项之后，所述方法还包括：

若所述第二远端 MAC-IP 表项与所述第一本地 MAC-IP 表项匹配，且所述第二序列号大于所述第三序列号，则将所述第一本地 MAC-IP 表项删除，并将所述第一本地 MAC-IP 表项对应的 DHCP 中继表项删除。

8、根据权利要求 1-7 任一项所述的方法，其特征在于，所述第一网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

9、根据权利要求 8 所述的方法，其特征在于，所述第一网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

10、一种安全表项维护方法，其特征在于，应用于第二网络设备，所述第二网络设备包括第一远端 MAC-IP 表，所述第一远端 MAC-IP 表包括第四网络设备通告的至少一个远端 MAC-IP 表项，所述方法包括：

当与所述第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，所述有效生命周期值用于指示所述远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 表项。

11、根据权利要求 10 所述的方法，其特征在于，在所述当与第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值之前，所述方法还包括：

接收所述第四网络设备发送的第一 MAC-IP 通告消息，所述第一 MAC-IP 通告消息包括第一 IP 地址的第一有效生命周期值以及第一序列号；

建立第一远端 MAC-IP 表项，所述第一远端 MAC 表项包括所述第一有效生命周期值以及所述第一序列号。

12、根据权利要求 11 所述的方法，其特征在于，所述第二网络设备还包括至少一个第二远端 MAC-IP 表，所述至少一个第二远端表包括第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项与所述第一远端 MAC-IP 表项匹配，所述第二远端 MAC-IP 表项包括第二序列号；在所述建立第一远端 MAC-IP 表项之后，所述方法还包括：

若所述第一序列号大于所述第二序列号，则向除所述第四网络设备之外的其他网络设备发送第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括所述第一有效生命周期值以及所述第一序列号。

13、根据权利要求 10 所述的方法，其特征在于，所述第二远端设备还包括至少一个第三远端 MAC-IP 表，每个第三远端 MAC-IP 表包括至少一个远端 MAC-IP 表项；在所述删除所述至少一个远端 MAC-IP 表项之后，所述方法还包括：

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中未存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则向除所述第四网络设备之外的其他网络设备发送第一 MAC-IP 撤销消息，所述第一 MAC-IP 撤销消息包括该远端 MAC-IP 表项中的 MAC 地址和 IP 地址；或者，

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中存在与该远端 MAC-IP

表项匹配的远端 MAC-IP 表项，则从匹配的远端 MAC-IP 表项中选择序列号最大的第三远端 MAC-IP 表项，所述第三远端 MAC-IP 表项包括第二有效生命周期值以及第三序列号；向除第五网络设备之外的其他网络设备发送第三 MAC-IP 通告消息，所述第三 MAC-IP 通告消息包括所述第二有效生命周期值和所述第三序列号，所述第五网络设备为所述第三远端 MAC-IP 表项的来源设备。

14、根据权利要求 10-13 任一项所述的方法，其特征在于，所述第二网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

15、根据权利要求 14 所述的方法，其特征在于，所述第二网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

16、一种安全表项维护装置，其特征在于，应用于第一网络设备，所述第一网络设备包括远端 MAC-IP 表，所述远端 MAC-IP 表包括所述第二网络设备通告的至少一个远端 MAC-IP 表项，所述装置包括：

获取模块，用于当与所述第二网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，所述有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

删除模块，用于若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 表项。

17、根据权利要求 16 所述的装置，其特征在于，所述装置还包括：

建立模块，用于当所述第一网络设备生成 DHCP 中继表项时，基于所述 DHCP 中继表项建立本地 MAC-IP 表项，并向硬件资源下发所述本地 MAC-IP 表项对应的转发 MAC-IP 表项，所述本地 MAC-IP 表项包括第一 IP 地址的第一有效生命周期值；

发送模块，用于向第三网络设备发送第一 MAC-IP 通告消息，以使得所述第三网络设备建立第一远端 MAC-IP 表项；

其中，所述第一 MAC-IP 通告消息包括第一序列号以及所述第一有效生命周期值，所述第一远端 MAC-IP 表项包括所述第一序列号以及所述第一有效生命周期值；

所述第一序列号为与所述本地 MAC-IP 表项匹配的远端 MAC-IP 表项中的最大序列号与 1 的和值。

18、根据权利要求 17 所述的装置，其特征在于，

所述删除模块，还用于当所述本地 MAC-IP 表项匹配的接入表项被删除时，删除所述转发 MAC-IP 表项。

19、根据权利要求 16 所述的装置，其特征在于，所述装置还包括：

接收模块，用于接收所述第二网络设备发送的第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括第二 IP 地址的第二有效生命周期值以及第二序列号；

建立模块，用于建立第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项包括所述第二有效生命周期值以及所述第二序列号。

20、根据权利要求 19 所述的装置，其特征在于，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括至少一个本地 MAC-IP 表项；

所述装置还包括：探测模块、生成模块和下发模块；

所述接收模块，还用于接收终端发送的第一报文，所述第一报文包括所述终端的 MAC 地址和 IP

地址；

所述探测模块，用于若所述本地 MAC-IP 表中未存在与所述终端的 MAC 地址和 IP 地址匹配的本地 MAC-IP 表项，且所述终端的 MAC 地址和 IP 地址与所述第二远端 MAC-IP 表项匹配，则对所述终端进行接入探测；

所述生成模块，用于若接收到所述终端发送的接入响应，则生成合成 MAC-IP 表项，所述合成 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址、端口标识以及 VLAN 标识；

所述生成模块，还用于根据所述合成 MAC-IP 表项生成转发 MAC-IP 表项，所述转发 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址；

所述下发模块，用于将所述转发 MAC-IP 表项下发至硬件资源中。

21、 根据权利要求 20 所述的装置，其特征在于，

所述删除模块，还用于当所述终端的接入表项被删除时，删除所述合成 MAC-IP 表项和所述转发 MAC-IP 表项。

22、根据权利要求 19 所述的装置，其特征在于，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括第一本地 MAC-IP 表项，所述第一本地 MAC-IP 表项包括第三序列号；

所述删除模块，还用于若所述第二远端 MAC-IP 表项与所述第一本地 MAC-IP 表项匹配，且所述第二序列号大于所述第三序列号，则将所述第一本地 MAC-IP 表项删除，并将所述第一本地 MAC-IP 表项对应的 DHCP 中继表项删除。

23、根据权利要求 16-22 任一项所述的装置，其特征在于，所述第一网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

24、根据权利要求 23 所述的装置，其特征在于，所述第一网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

25、一种安全表项维护装置，其特征在于，应用于第二网络设备，所述第二网络设备包括第一远端 MAC-IP 表，所述第一远端 MAC-IP 表包括第四网络设备通告的至少一个远端 MAC-IP 表项，所述装置包括：

获取模块，用于当与所述第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，所述有效生命周期值用于指示所述远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

删除模块，用于若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 表项。

26、根据权利要求 25 所述的装置，其特征在于，所述装置还包括：

接收模块，用于接收所述第四网络设备发送的第一 MAC-IP 通告消息，所述第一 MAC-IP 通告消息包括第一 IP 地址的第一有效生命周期值以及第一序列号；

建立模块，用于建立第一远端 MAC-IP 表项，所述第一远端 MAC 表项包括所述第一有效生命周期值以及所述第一序列号。

27、根据权利要求 26 所述的装置，其特征在于，所述第二网络设备还包括至少一个第二远端 MAC-IP 表，所述至少一个第二远端表包括第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项与所述第一远端 MAC-IP 表项匹配，所述第二远端 MAC-IP 表项包括第二序列号；所述装置还包括：

发送模块，用于若所述第一序列号大于所述第二序列号，则向除所述第四网络设备之外的其他网络设备发送第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括所述第一有效生命周期值以及所述第一序列号。

28、根据权利要求 25 所述的装置，其特征在于，所述第二远端设备还包括至少一个第三远端 MAC-IP 表，每个第三远端 MAC-IP 表包括至少一个远端 MAC-IP 表项；所述装置还包括发送模块；

所述发送模块，用于：

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中未存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则向除所述第四网络设备之外的其他网络设备发送第一 MAC-IP 撤销消息，所述第一 MAC-IP 撤销消息包括该远端 MAC-IP 表项中的 MAC 地址和 IP 地址；或者，

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则从匹配的远端 MAC-IP 表项中选择序列号最大的第三远端 MAC-IP 表项，所述第三远端 MAC-IP 表项包括第二有效生命周期值以及第三序列号；向除第五网络设备之外的其他网络设备发送第三 MAC-IP 通告消息，所述第三 MAC-IP 通告消息包括所述第二有效生命周期值和所述第三序列号，所述第五网络设备为所述第三远端 MAC-IP 表项的来源设备。

29、根据权利要求 25-28 任一项所述的装置，其特征在于，所述第二网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

30、根据权利要求 29 所述的装置，其特征在于，所述第二网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

31、一种第一网络设备，其特征在于，所述第一网络设备包括远端 MAC-IP 表，所述远端 MAC-IP 表包括所述第二网络设备通告的至少一个远端 MAC-IP 表项；所述第一网络设备包括：

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：

当与所述第二网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，所述有效生命周期值用于指示远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 表项。

32、根据权利要求 31 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：

当所述第一网络设备生成 DHCP 中继表项时，基于所述 DHCP 中继表项建立本地 MAC-IP 表项，并向硬件资源下发所述本地 MAC-IP 表项对应的转发 MAC-IP 表项，所述本地 MAC-IP 表项包括第一 IP 地址的第一有效生命周期值；

通过所述收发器向第三网络设备发送第一 MAC-IP 通告消息，以使得所述第三网络设备建立第一远端 MAC-IP 表项；

其中，所述第一 MAC-IP 通告消息包括第一序列号以及所述第一有效生命周期值，所述第一远端 MAC-IP 表项包括所述第一序列号以及所述第一有效生命周期值；

所述第一序列号为与所述本地 MAC-IP 表项匹配的远端 MAC-IP 表项中的最大序列号与 1 的和值。

33、根据权利要求 32 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：

当所述本地 MAC-IP 表项匹配的接入表项被删除时，删除所述转发 MAC-IP 表项。

34、根据权利要求 31 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：

通过所述收发器接收所述第二网络设备发送的第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括第二 IP 地址的第二有效生命周期值以及第二序列号；

建立第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项包括所述第二有效生命周期值以及所述第二序列号。

35、根据权利要求 34 所述的第一网络设备，其特征在于，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括至少一个本地 MAC-IP 表项；

所述机器可执行指令还促使所述处理器执行以下步骤：

通过收发器接收终端发送的第一报文，所述第一报文包括所述终端的 MAC 地址和 IP 地址；

若所述本地 MAC-IP 表中未存在与所述终端的 MAC 地址和 IP 地址匹配的本地 MAC-IP 表项，且所述终端的 MAC 地址和 IP 地址与所述第二远端 MAC-IP 表项匹配，则对所述终端进行接入探测；

若接收到所述终端发送的接入响应，则生成合成 MAC-IP 表项，所述合成 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址、端口标识以及 VLAN 标识；

根据所述合成 MAC-IP 表项生成转发 MAC-IP 表项，所述转发 MAC-IP 表项包括所述终端的 MAC 地址和 IP 地址；

将所述转发 MAC-IP 表项下发至硬件资源中。

36、根据权利要求 35 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：

当所述终端的接入表项被删除时，删除所述合成 MAC-IP 表项和所述转发 MAC-IP 表项。

37、根据权利要求 34 所述的第一网络设备，其特征在于，所述第一网络设备包括本地 MAC-IP 表，所述本地 MAC-IP 表包括第一本地 MAC-IP 表项，所述第一本地 MAC-IP 表项包括第三序列号；所述机器可执行指令还促使所述处理器执行以下步骤：

若所述第二远端 MAC-IP 表项与所述第一本地 MAC-IP 表项匹配，且所述第二序列号大于所述第三序列号，则将所述第一本地 MAC-IP 表项删除，并将所述第一本地 MAC-IP 表项对应的 DHCP 中继表项删除。

38、根据权利要求 31-37 任一项所述的第一网络设备，其特征在于，所述第一网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

39、根据权利要求 38 所述的第一网络设备，其特征在于，所述第一网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

40、一种第二网络设备，其特征在于，所述第二网络设备包括第一远端 MAC-IP 表，所述第一远端 MAC-IP 表包括第四网络设备通告的至少一个远端 MAC-IP 表项，所述第二网络设备包括：

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：

当与所述第四网络设备之间的协议连接中断时，获取每个远端 MAC-IP 表项包括的有效生命周期值，所述有效生命周期值用于指示所述远端 MAC-IP 表项包括的 IP 地址的有效生命周期；

若所述协议连接中断的持续时长达到所述有效生命周期值，则删除所述至少一个远端 MAC-IP 表项。

41、根据权利要求 40 所述的第二网络设备，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：

通过所述收发器接收所述第四网络设备发送的第一 MAC-IP 通告消息，所述第一 MAC-IP 通告消息包括第一 IP 地址的第一有效生命周期值以及第一序列号；

建立第一远端 MAC-IP 表项，所述第一远端 MAC 表项包括所述第一有效生命周期值以及所述第一序列号。

42、根据权利要求 41 所述的第二网络设备，其特征在于，所述第二网络设备还包括至少一个第二远端 MAC-IP 表，所述至少一个第二远端表包括第二远端 MAC-IP 表项，所述第二远端 MAC-IP 表项与所述第一远端 MAC-IP 表项匹配，所述第二远端 MAC-IP 表项包括第二序列号；所述机器可执行指令促使所述处理器执行以下步骤：

若所述第一序列号大于所述第二序列号，则向除所述第四网络设备之外的其他网络设备发送第二 MAC-IP 通告消息，所述第二 MAC-IP 通告消息包括所述第一有效生命周期值以及所述第一序列号。

43、根据权利要求 40 所述的第二网络设备，其特征在于，所述第二远端设备还包括至少一个第三远端 MAC-IP 表，每个第三远端 MAC-IP 表包括至少一个远端 MAC-IP 表项；所述机器可执行指令促使所述处理器执行以下步骤：

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中未存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则向除所述第四网络设备之外的其他网络设备发送第一 MAC-IP 撤销消息，所述第一 MAC-IP 撤销消息包括该远端 MAC-IP 表项中的 MAC 地址和 IP 地址；或者，

针对删除的每个远端 MAC-IP 表项，若所述至少一个第三远端 MAC-IP 表中存在与该远端 MAC-IP 表项匹配的远端 MAC-IP 表项，则从匹配的远端 MAC-IP 表项中选择序列号最大的第三远端 MAC-IP 表项，所述第三远端 MAC-IP 表项包括第二有效生命周期值以及第三序列号；向除第五网络设备之外的其他网络设备发送第三 MAC-IP 通告消息，所述第三 MAC-IP 通告消息包括所述第二有效生命周期值和所述第三序列号，所述第五网络设备为所述第三远端 MAC-IP 表项的来源设备。

44、根据权利要求 40-43 任一项所述的第二网络设备，其特征在于，所述第二网络设备发送的 MAC-IP 通告消息中包括第一扩展团体属性，所述第一扩展团体属性中包括 IP 地址的有效生命周期值。

45、根据权利要求 44 所述的第二网络设备，其特征在于，所述第二网络设备发送的 MAC-IP 通告消息中还包括第二扩展团体属性，所述第二扩展团体属性中包括 MAC-IP 表项的序列号。

46、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 1-9 或 10-15 任一所述的方法。

47、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 1-9 或 10-15 任一所述的方法。