



(12) 发明专利申请

(10) 申请公布号 CN 113973101 A

(43) 申请公布日 2022.01.25

(21) 申请号 202011165160.3

H04L 45/247 (2022.01)

(22) 申请日 2020.10.27

H04L 9/40 (2022.01)

(66) 本国优先权数据

202010726603.5 2020.07.25 CN

(71) 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72) 发明人 朱筠 张耀坤 陈亮

(74) 专利代理机构 深圳市深佳知识产权代理事务所(普通合伙) 44285

代理人 常忠良

(51) Int. Cl.

H04L 61/5014 (2022.01)

H04L 12/46 (2006.01)

H04L 45/586 (2022.01)

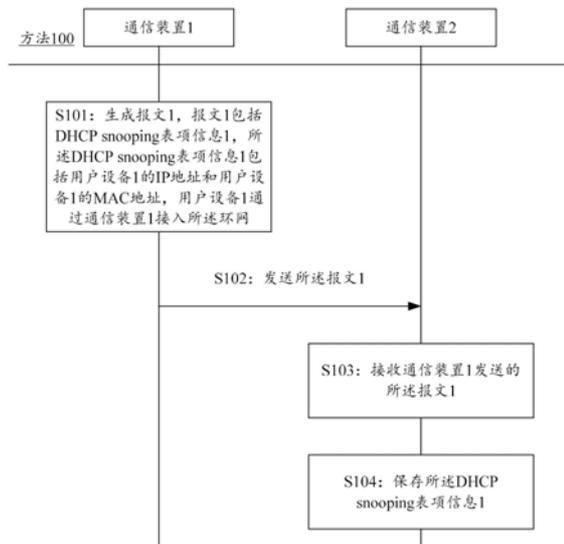
权利要求书2页 说明书21页 附图7页

(54) 发明名称

一种表项信息处理方法及装置

(57) 摘要

本申请提供了一种在环网中进行DHCP snooping表项信息处理的方法,该方法由环网上的第一通信装置执行。在一个示例中,第一通信装置可以获得DHCP snooping表项信息并将该DHCP snooping表项信息同步给环网上或与环网通信的其它一个或多个节点。该DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和第一用户设备的第一MAC地址。其中,第一用户设备通过所述第一通信装置接入所述环网。利用本方案,在报文传输路径发生变化后,新路径上的节点能够根据获取到的所述DHCP snooping表项信息,进行DHCP snooping,保证合法用户能够访问网络的同时,有效防范网络攻击。



1. 一种表项信息处理方法,其特征在于,由环网上的第一通信装置执行,所述方法包括:

生成第一报文,所述第一报文包括动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网;发送所述第一报文。

2. 根据权利要求1所述的方法,其特征在于,所述生成第一报文包括:

确定所述环网的拓扑发生变化后,生成所述第一报文。

3. 根据权利要求1或2所述的方法,其特征在于,所述发送所述第一报文,包括:

向所述环网的第一路径中的通信节点发送所述第一报文,所述第一路径用于在所述环网中的第二路径发生故障时,传输来自所述第一用户设备的报文,所述第一路径和所述第二路径为所述环网中传输方向相反的两条路径。

4. 根据权利要求3所述的方法,其特征在于,所述通信节点包括所述环网的根桥节点。

5. 根据权利要求1或2所述的方法,其特征在于,所述发送所述第一报文,包括:

向外部网络中的虚拟路由冗余协议VRRP组中的主节点发送所述第一报文,所述环网的根桥节点通过所述VRRP组接入所述外部网络。

6. 根据权利要求1-5任意一项所述的方法,其特征在于,在生成所述第一报文之前,所述方法还包括:

接收第二报文,所述第二报文用于向所述第一通信装置请求所述DHCP snooping表项信息。

7. 根据权利要求6所述的方法,其特征在于,所述接收第二报文,包括:

接收所述环网的根桥节点发送的所述第二报文。

8. 根据权利要求6所述的方法,其特征在于,所述接收第二报文包括:

接收外部网络中的虚拟路由冗余协议VRRP组中的主节点发送的所述第二报文,所述环网的根桥节点通过所述VRRP组接入所述外部网络。

9. 一种表项信息处理方法,其特征在于,由第二通信装置执行,所述方法包括:

接收环网上的第一通信装置发送的第一报文,所述第一报文包括动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网;

保存所述DHCP snooping表项信息。

10. 根据权利要求9所述的方法,其特征在于,所述第二通信装置为所述环网上的第一路径中的通信节点,所述第一路径用于在所述环网中的第二路径发生故障时,传输来自所述第一用户设备的报文,所述第一路径和所述第二路径为所述环网中传输方向相反的两条路径。

11. 根据权利要求10所述的方法,其特征在于,所述第二通信装置包括所述环网的根桥节点。

12. 根据权利要求9所述的方法,其特征在于,所述第二通信装置为外部网络中的虚拟路由冗余协议VRRP组中的主节点,所述环网的根桥节点通过所述VRRP组接入所述外部网

络。

13. 根据权利要求9-12任意一项所述的方法,其特征在于,所述方法还包括:

向所述第一通信装置发送第二报文,所述第二报文用于向所述第一通信装置请求所述DHCP snooping表项信息。

14. 根据权利要求9-13任意一项所述的方法,其特征在于,所述保存所述DHCP snooping表项信息,包括:

保存接收所述第一报文的接口和所述DHCP snooping表项信息的对应关系。

15. 根据权利要求1-14任意一项所述的方法,其特征在于,所述DHCP snooping表项信息还包括:

所述第一用户设备所属的虚拟局域网VLAN的标识,和/或,所述第一IP地址的租期。

16. 根据权利要求1-14任意一项所述的方法,其特征在于,所述第一报文为广播报文或者单播报文。

17. 根据权利要求1-16任意一项所述的方法,其特征在于,所述第一报文中还包括指示信息,所述指示信息用于指示所述环网上转发所述第一报文的通信节点获取所述DHCP snooping表项信息。

18. 根据权利要求1-17任意一项所述的方法,其特征在于,所述第一报文包括:

第一部分,用于携带包括所述DHCP snooping表项信息的至少一条DHCP snooping表项信息;

第二部分,用于指示所述第一部分中所携带的DHCP snooping表项信息的数量。

19. 根据权利要求1-18任意一项所述的方法,其特征在于,所述环网为二层环网或三层环网。

20. 一种表项信息处理方法,其特征在于,由第二通信装置执行,所述方法包括:

生成第二报文,所述第二报文用于向环网上的第一通信装置请求动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网;

向所述第一通信装置发送所述第二报文。

21. 一种第一通信装置,其特征在于,所述第一通信装置包括存储器和处理器;

所述存储器,用于存储程序代码;

所述处理器,用于运行所述程序代码中的指令,使得所述第一通信装置执行以上权利要求1-8任意一项或者15-19任意一项所述的方法。

22. 一种第二通信装置,其特征在于,所述第二通信装置包括存储器和处理器;

所述存储器,用于存储程序代码;

所述处理器,用于运行所述程序代码中的指令,使得所述第二通信装置执行以上权利要求9-20任意一项所述的方法。

23. 一种计算机可读存储介质,其特征在于,所述计算机可读存储介质中存储有指令,当其在计算机上运行时,使得所述计算机执行以上权利要求1-20任意一项所述的方法。

24. 一种通信系统,其特征在于,包括权利要求21所述的第一通信装置以及权利要求22所述的第二通信装置。

一种表项信息处理方法及装置

[0001] 本申请要求于2020年07月25日提交中国国家知识产权局、申请号为CN202010726603.5、发明名称为“一种通信方法和设备”的中国专利申请的优先权,其全部内容通过引用结合在本申请中。

技术领域

[0002] 本申请涉及通信领域,尤其涉及一种动态主机配置协议(Dynamic Host Configuration Protocol,DHCP)监听(snooping)表项信息的处理方法及装置。

背景技术

[0003] DHCP服务器(server)可以动态为DHCP客户端(client)分配互联网协议(Internet Protocol,IP)地址。但是DHCP服务器为DHCP客户端分配IP地址时,可能会存在安全隐患。例如,存在中间人攻击、IP仿冒(spoofing)攻击、媒体接入控制(media access control,MAC) spoofing攻击、续租报文攻击以及饿死攻击等。其中,DHCP客户端也可以被称为用户设备。

[0004] 为了降低安全隐患,可以在网络设备上部署DHCP snooping功能,DHCP snooping通过记录DHCP client的IP地址和MAC地址的对应关系,能够保证合法用户能访问网络,DHCP snooping还能够解决设备应用DHCP时遇到的例如续租报文攻击,非法IP报文攻击等问题。但是,在一些环网场景中,即使在网络设备上部署了DHCP snooping功能,仍然不能有效保证环网的网络安全。

发明内容

[0005] 本申请提供了一种表项信息处理方法,可以进一步提升网络安全。

[0006] 第一方面,本申请实施例提供了一种表项信息的处理方法,该方法可以由环网上的第一通信装置执行。在一个示例中,第一通信装置可以获取第一用户设备对应的DHCP snooping表项信息并将该DHCP snooping表项信息同步给环网上或者与环网通信的环网以外的其它装置,由此,当用于传输第一用户设备发送的报文的传输路径发生变化后,新的转发路径上的网络装置能够获取第一用户设备对应的DHCP snooping表项信息,从而在设备上进行DHCP snooping。具体来说,该第一用户设备对应的DHCP snooping表项信息包括第一用户设备的第一互联网协议(Internet Protocol,IP)地址和第一用户设备的第一媒体接入控制(media access control,MAC)地址。第一通信装置获取DHCP snooping表项信息之后,可以生成第一报文,所述第一报文中包括所述DHCP snooping表项信息。而后,第一通信装置可以发送所述第一报文。其中,第一用户设备通过所述第一通信装置接入所述环网。利用本方案,接收到所述第一报文的通信装置即可获取所述DHCP snooping表项信息,进而可以在设备中添加该DHCP snooping表项信息,保证合法用户能够访问网络的同时,有效防范网络攻击。在一个示例中,所述第一用户设备通过所述第一通信装置接入环网,并通过环网中的第二路径传输报文,当环网的网络拓扑发生改变,第一通信装置通过环网中的第一路径转发所述第一用户设备发送的报文时,通过本申请的方案,第一通信装置可以将第一

用户设备的DHCP snooping表项信息同步给第一路径上的通信装置。由此,可以在环网中使能DHCP snooping,在保证合法用户的正常业务的同时,有效降低了环网攻击,提升了环网的网络安全。

[0007] 在一种实现方式中,第一通信装置可以在所述环网的网络拓扑发生改变之后,执行前述获取DHCP snooping表项信息及其后续步骤。对于这种方式,第一通信装置在获取第一报文之前,还可以确定所述环网的拓扑发生变化。对于这种情况,第一通信装置可以在所述环网的网络拓扑发生改变之后,将所述DHCP snooping表项信息发送给其它通信装置,从而使得接收到所述第一报文的通信装置获取所述DHCP snooping表项信息,进而可以在设备中部署DHCP snooping功能,保证合法用户能够访问网络的同时,有效防范网络攻击。

[0008] 在一种实现方式中,所述DHCP snooping表项信息除了包括所述第一用户设备的第一IP地址和所述第一用户设备的MAC地址之外,还可以包括:所述第一用户设备所属的虚拟局域网VLAN的标识,和/或,所述第一IP地址的租期。

[0009] 在一种实现方式中,所述第一用户设备可以通过环网中的第二路径进行报文传输,当环网的网络拓扑发生改变,第一通信装置将通过第二路径进行传输的报文切换至第一路径上转发。其中,所述第一路径和所述第二路径为所述环网中传输方向相反的两条路径。对于这种情况,第一通信装置可以将第一报文发送给第一路径上的通信节点。由此,可以在环网中使能DHCP snooping,在保证合法用户的正常业务的同时,有效降低了环网攻击,提升了环网的网络安全。

[0010] 在一种实现方式中,考虑到对于环网而言,环网的根桥节点为环网与外部网络进行交互的节点,经过环网转发到外部网络的报文需要通过根桥节点进行转发。当环网的网络拓扑发生改变之后,用户设备发送的报文在环网中的转发路径发生改变,因此,根桥节点接收该报文的端口也会发生改变。在一个示例中,前述第一路径中的通信节点,可以为第一路径中的、所述环网的根桥节点。对于这种情况,即使环网的网络拓扑发生改变,则所述根桥节点也可以根据该DHCP snooping表项信息,对通过第一路径转发的报文进行校验,从而降低网络攻击,保证网络安全。

[0011] 在一种实现方式中,第一通信装置可以将第一报文发送给向外部网络中的虚拟路由冗余协议VRRP组中的主节点,其中,所述环网的根桥节点通过所述VRRP组接入所述外部网络。这样一来,所述主节点即可根据该DHCP snooping表项信息,对待转发的报文进行校验,从而避免网络攻击。在一个示例中,所述主节点例如可以为由备节点升级为主节点的节点,对于这种情况,即使所述VRRP组完成了主备切换,则新的主节点也可以获取该DHCP snooping表项信息,对待转发的报文进行校验,从而避免网络攻击。

[0012] 在一种实现方式中,所述第一报文为广播报文。在一个示例中,可以将该广播报文广播发送至所述第一路径中的各个通信节点,使得所述第一路径中的各个通信节点均可以根据该广播报文获取所述DHCP snooping表项信息,并基于该DHCP snooping表项信息对待转发的报文进行校验,从而有效避免环网攻击。

[0013] 在一种实现方式中,所述第一报文为单播报文。在一个示例中,第一通信装置可以将该单播报文发送给所述环网的根桥节点;在又一个示例中,第一通信装置可以将该单播报文发送给VRRP组的主节点;在又一个示例中,第一通信装置向所述第一路径中的各个通信节点分别发送一个单播报文。接收到所述第一报文的通信装置即可获取所述DHCP

snooping表项信息,进而可以在设备中部署DHCP snooping功能,保证合法用户能够访问网络的同时,有效防范网络攻击。

[0014] 在一种实现方式中,第一通信装置可以基于第二报文生成第一报文,并发送第一报文。在一个示例中,第一通信装置可以接收第二报文,所述第二报文用于向所述第一通信装置请求所述DHCP snooping表项信息。第一通信装置接收到第二报文之后,即可生成第一报文,并发送第一报文。从而使得接收到所述第一报文的通信装置即可获取所述DHCP snooping表项信息,进而可以在设备中部署DHCP snooping功能,保证合法用户能够访问网络的同时,有效防范网络攻击。

[0015] 在一种实现方式中,所述第二报文可以是所述环网的根桥节点发送给第一通信装置的。对于这种情况,第一通信装置可以将第一报文发送给所述环网的根桥节点。

[0016] 在一种实现方式中,所述第二报文可以是外部网络中的VRRP组中的主节点发送给第一通信装置的,其中,所述环网的根桥节点通过所述VRRP组接入所述外部网络。对于这种情况,所述第一通信装置可以将第一报文发送给所述VRRP组中的主节点。

[0017] 在一种实现方式中,所述第一报文中还包括指示信息,所述指示信息用于指示所述环网上转发所述第一报文的通信节点获取所述DHCP snooping表项信息。对于这种情况,所述环网上转发所述第一报文的通信节点即可获取所述DHCP snooping表项信息,进而可以在设备中部署DHCP snooping功能,保证合法用户能够访问网络的同时,有效防范网络攻击。

[0018] 在一种实现方式中,所述第一报文可以包括第一部分和第二部分,其中:第一部分,用于携带包括所述DHCP snooping表项信息的至少一条DHCP snooping表项信息;第二部分,用于指示所述第一部分中所携带的DHCP snooping表项信息的数量。

[0019] 在一种实现方式中,所述环网为二层环网或三层环网。当所述环网为二层环网时,利用本方案可以有效防止二层环网攻击,当所述环网为三层环网时,利用本方案可以有效防止三层环网攻击。

[0020] 第二方面,本申请提供了一种表项信息处理方法,该方法可以由第二通信装置执行,在一个示例中,第二通信装置可以接收环网上的第一通信装置发送的第一报文,所述第一报文包括动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网;第二通信装置接收到第一报文之后,可以保存所述DHCP snooping表项信息。进而第二通信装置可以利用该DHCP snooping表项信息保证合法用户能够访问网络的同时,有效防范网络攻击。

[0021] 在一种实现方式中,所述DHCP snooping表项信息还包括:所述第一用户设备所属的虚拟局域网VLAN的标识,和/或,所述第一IP地址的租期。

[0022] 在一种实现方式中,所述第二通信装置为所述环网上的第一路径中的通信节点,所述第一路径用于在所述环网中的第二路径发生故障时,传输来自所述第一用户设备的报文,所述第一路径和所述第二路径为所述环网中传输方向相反的两条路径。

[0023] 在一种实现方式中,所述第二通信装置包括所述环网的根桥节点。

[0024] 在一种实现方式中,所述第二通信装置为外部网络中的虚拟路由冗余协议VRRP组中的主节点,所述环网的根桥节点通过所述VRRP组接入所述外部网络。

- [0025] 在一种实现方式中,所述第一报文为广播报文。
- [0026] 在一种实现方式中,所述第一报文为单播报文。
- [0027] 在一种实现方式中,所述方法还包括:向所述第一通信装置发送第二报文,所述第二报文用于向所述第一通信装置请求所述DHCP snooping表项信息。
- [0028] 在一种实现方式中,所述第一报文中还包括指示信息,所述指示信息用于指示所述第二通信装置获取所述DHCP snooping表项信息。
- [0029] 在一种实现方式中,所述第一报文包括:第一部分,用于携带包括所述DHCP snooping表项信息的至少一条DHCP snooping表项信息;第二部分,用于指示所述第一部分中所携带的DHCP snooping表项信息的数量。
- [0030] 在一种实现方式中,所述环网为二层环网或三层环网。
- [0031] 在一种实现方式中,第二通信装置保存DHCP snooping表项信息在具体实现时,可以保存接收所述第一报文的接口和所述DHCP snooping表项信息的对应关系。
- [0032] 第三方面,本申请提供了一种表项信息处理方法,该方法可以由第二通信装置执行。在一个示例中,所述第二通信装置可以生成第二报文,并向第一通信装置发送所述第二报文。其中:所述第二报文用于向环网上的第一通信装置请求动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网。由此可见,利用本方案,第二通信装置可以向第一通信装置请求所述DHCP snooping表项信息,从而利用所述DHCP snooping表项信息对待转发的报文做校验,从而有效防止网络攻击。
- [0033] 在一种实现方式中,所述方法包括:接收所述第一通信装置发送的第一报文,所述第一报文包括所述DHCP snooping表项信息;保存所述DHCP snooping表项信息。
- [0034] 在一种实现方式中,在本申请中,保存所述DHCP snooping表项信息,包括生成DHCP snooping表,并在所述DHCP snooping表中保存所述DHCP snooping表项信息。在另一种实现方式中,保存所述DHCP snooping表项信息,包括将所述DHCP snooping表项信息保存到本地已有的DHCP snooping表中。
- [0035] 在一种实现方式中,所述DHCP snooping表项信息还包括:所述第一用户设备所属的虚拟局域网VLAN的标识,和/或,所述第一IP地址的租期。
- [0036] 在一种实现方式中,所述第二通信装置为所述环网上的第一路径中的通信节点,所述第一路径用于在所述环网中的第二路径发生故障时,传输来自所述第一用户设备的报文,所述第一路径和所述第二路径为所述环网中传输方向相反的两条路径。
- [0037] 在一种实现方式中,所述第二通信装置包括所述环网的根桥节点。
- [0038] 在一种实现方式中,所述第二通信装置为外部网络中的虚拟路由冗余协议VRRP组中的主节点,所述环网的根桥节点通过所述VRRP组接入所述外部网络。
- [0039] 在一种实现方式中,所述第一报文为广播报文。
- [0040] 在一种实现方式中,所述第一报文为单播报文。
- [0041] 在一种实现方式中,所述第一报文中还包括指示信息,所述指示信息用于指示所述第二通信装置获取所述DHCP snooping表项信息。
- [0042] 在一种实现方式中,所述第一报文包括:第一部分,用于携带包括所述DHCP

snooping表项信息的至少一条DHCP snooping表项信息;第二部分,用于指示所述第一部分中所携带的DHCP snooping表项信息的数量。

[0043] 在一种实现方式中,所述环网为二层环网或三层环网。

[0044] 在一种实现方式中,所述保存所述DHCP snooping表项信息,包括:保存接收所述第一报文的接口和所述DHCP snooping表项信息的对应关系。

[0045] 第四方面,本申请提供了一种第一通信装置,包括:收发单元和处理单元。所述收发单元用于执行以上第一方面以及第一方面任意一项所述的第一通信装置执行的收发操作,所述处理单元用于执行以上第一方面以及第一方面任意一项所述的第一通信装置执行的除收发操作之外的其它操作。

[0046] 第五方面,本申请提供了一种第一通信装置,所述第一通信装置包括存储器和处理器;所述存储器,用于存储程序代码;所述处理器,用于运行所述程序代码中的指令,使得所述第一通信装置执行以上第一方面以及第一方面任意一项所述的方法。

[0047] 第六方面,本申请提供了一种第一通信装置,所述第一通信装置包括通信接口和处理器,所述通信接口用于执行以上第一方面以及第一方面任意一项所述的第一通信装置执行的收发操作,所述处理器用于执行以上第一方面以及第一方面任意一项所述的第一通信装置执行的除收发操作之外的其它操作。

[0048] 第七方面,本申请提供了一种第二通信装置,包括:收发单元和处理单元。所述收发单元用于执行以上第二方面以及第二方面任意一项所述的第二通信装置执行的收发操作,所述处理单元用于执行以上第二方面以及第二方面任意一项所述的第二通信装置执行的除收发操作之外的其它操作;或者,所述收发单元用于执行以上第三方面以及第三方面任意一项所述的第二通信装置执行的收发操作,所述处理单元用于执行以上第三方面以及第三方面任意一项所述的第二通信装置执行的除收发操作之外的其它操作。

[0049] 第八方面,本申请提供了一种第二通信装置,所述第二通信装置包括存储器和处理器;所述存储器,用于存储程序代码;所述处理器,用于运行所述程序代码中的指令,使得所述第二通信装置执行以上第二方面以及第二方面任意一项所述的方法,或者,使得所述第二通信装置执行以上第三方面以及第三方面任意一项所述的方法。

[0050] 第九方面,本申请提供了一种第二通信装置,所述第二通信装置包括多个通信接口和至少一个处理器,所述多个通信接口用于执行以上第二方面以及第二方面任意一项所述的第二通信装置执行的收发操作,所述至少一个处理器用于执行以上第二方面以及第二方面任意一项所述的第二通信装置执行的除收发操作之外的其它操作;或者,所述多个通信接口用于执行以上第三方面以及第三方面任意一项所述的第二通信装置执行的收发操作,所述至少一个处理器用于执行以上第三方面以及第三方面任意一项所述的第二通信装置执行的除收发操作之外的其它操作。。

[0051] 第十方面,本申请提供了一种计算机可读存储介质,其特征在于,所述计算机可读存储介质中存储有指令,当其在计算机上运行时,使得所述计算机执行以上第一方面以及第一方面任意一项所述的方法,或者,使得所述计算机执行以上第二方面以及第二方面任意一项所述的方法,或者,使得所述计算机执行以上第三方面以及第三方面任意一项所述的方法。

[0052] 第十二方面,本申请提供了一种通信系统,该通信系统包括以上第四方面或者第

五方面或者第六方面所述的第一通信装置,以及以上第七方面或者第八方面或者第九方面所述的第二通信装置。

附图说明

[0053] 为了更清楚地说明本申请实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本申请中记载的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0054] 图1为本申请实施例提供的一种示例性应用场景示意图;

[0055] 图2为本申请实施例提供的又一个示例性应用场景示意图;

[0056] 图3为本申请实施例提供的一种表项信息处理方法的信令交互图;

[0057] 图4a为本申请实施例提供的一种报文1的结构示意图;

[0058] 图4b为本申请实施例提供的一种报文2的结构示意图;

[0059] 图5为本申请实施例提供的一种表项信息处理方法的流程示意图;

[0060] 图6为本申请实施例提供的一种表项信息处理方法的流程示意图;

[0061] 图7为本申请实施例提供的一种表项信息处理方法的流程示意图;

[0062] 图8为本申请实施例提供的一种通信装置的结构示意图;

[0063] 图9为本申请实施例提供的一种通信装置的结构示意图;

[0064] 图10为本申请实施例提供的一种通信装置的结构示意图。

具体实施方式

[0065] 本申请实施例提供了一种表项信息处理方法,用于提升网络安全。

[0066] 为方便理解,首先对本申请实施例可能的应用场景进行介绍。

[0067] 图1为本申请实施例提供的一种示例性应用场景示意图。

[0068] 在图1所示的场景中,用户设备101通过通信装置SW2接入环网100,并通过环网100与DHCP服务器102通信。本申请实施例中的环网100,可以是二层(layer 2,L2)环网,也可以是三层(layer 3,L3)环网,本申请实施例不做限定。

[0069] 如图1所示,环网100包括通信装置SW1、SW2、SW3、SW4、SW5和SW6。为了保证用户设备101和DHCP服务器102之间的通信安全,可以在环网100上的各个通信装置上部署DHCP snooping功能。在一个示例中,可以在通信装置SW2的用户侧端口上部署DHCP snooping功能。通信装置SW2可以保存DHCP snooping表。该DHCP snooping表可以包括部署了DHCP snooping功能的端口信息、和该部署了DHCP snooping功能的端口对应的DHCP snooping表项信息。在本申请中,DHCP snooping表还可以称为DHCP snooping绑定(binding)表。

[0070] 在本申请中,DHCP snooping表项信息包括至少一个用户设备的信息,用于指示来自合法用户设备的报文能够通过该端口进行转发。用户设备的信息包括用户的IP地址和MAC地址。用户设备的信息还可以包括IP地址的租期,和/或,用户设备101所属的虚拟局域网(virtual local area network,VLAN)的标识。举例说明:图1所示场景中,端口1部署了DHCP snooping功能,则通信装置SW2保存的DHCP snooping表项可以包括用户设备101的信息。进一步地,DHCP snooping表项可以包括用户设备101的信息和端口1的对应关系。该对

应关系用于指示来自用户设备101的报文被允许通过SW1的端口1进行转发。其中,用户设备101的信息,包括用户设备101的IP地址和MAC地址。在一些示例中,用户设备101的信息,还可以包括用户设备的IP地址的租期,和/或,用户设备101所属的VLAN的标识。

[0071] 关于通信装置SW2保存的DHCP snooping表项,可结合表1进行理解。

[0072] 表1

端口	IP地址	MAC地址	租期	VLAN
端口1	IP地址1	MAC地址1	租期1	VLAN1

[0074] 当通信装置SW2接收到报文时,根据报文中携带的用户设备的信息和DHCP snooping表进行匹配,若不完全匹配,则说明该报文为非法报文。通信装置SW2可以丢弃该报文,从而避免该报文对网络造成攻击。例如,通信装置SW2通过端口1接收到的报文中的IP地址为IP地址1,但是MAC地址不是MAC地址1,则说明该报文可能是网络黑客仿冒用户设备101的IP地址向通信装置SW2发送的报文,故而通信装置SW2可以丢弃该报文。在一些示例中,若所述提取的用户设备的信息以及接收该报文的端口和DHCP snooping表项完全匹配,则说明该报文是合法报文,故而通信装置SW2可以转发该报文。在又一些示例中,若所述提取的用户设备的信息和所述DHCP snooping表项中保存的IP地址和MAC地址完全不匹配,DHCP snooping表中没有保存用户设备的IP和MAC地址,则通信装置SW2无法判定该报文是否为攻击报文,此时,为了保证业务不中断,通信装置SW2可以转发该报文。

[0075] 在一个示例中,通信装置SW1可以是环网100的根桥节点;另外,通信装置SW6也可以是环网100的根桥节点。对于环网100而言,其可以部署生成树协议。根桥节点是指在生成树协议中,发布配置信息的节点。当环网100的网络拓扑发生改变时,可以由根桥节点来通知其它网络节点。

[0076] 当通信装置SW1和通信装置SW6均为环网100的根桥节点时,通信装置SW1和通信装置SW6其中一个为主根桥节点,另外一个为备根桥节点。另外,在一些实施例中,作为根桥节点的通信装置SW1和作为根桥节点的通信装置SW6还可以构成一个虚拟路由冗余协议(Virtual Router Redundancy Protocol, VRRP)组。

[0077] 图2为本申请实施例提供的又一个示例性应用场景示意图。

[0078] 如图2所示,用户设备101通过环网100以及外部网络200和DHCP服务器102通信。通信装置SW1通过通信装置R1接入外部网络200,通信装置SW6通过通信装置R2接入外部网络200。在一个示例中,通信装置R1和通信装置R2可以构成一个VRRP组。假设初始状态时通信装置R1为该VRRP组的主节点,通信装置R2为备节点,则环网100中的通信装置SW1可以通过通信装置R1接入外部网络200,而通信装置R2处于监听状态,环网100中的通信装置SW6不通过通信装置R2接入外部网络200。若通信装置R1发生故障,则通信装置R2切换为主节点,环网100中的通信装置SW6可以通过通信装置R2接入外部网络200。

[0079] 目前,环网中部署了DHCP snooping功能的通信装置所维护的DHCP snooping表项,是基于用户设备的上线报文得到的。未传输用户设备的上线报文的通信装置,则不会维护与该用户设备相对应的DHCP snooping表项。在一些情况下,如果未传输用户设备的上线报文的通信装置上没有使能DHCP snooping功能,则网络黑客可以仿冒用户设备发送攻击报文,进行网络攻击。为了有效防范上述网络攻击,一种可能的解决方案是将环网中所有的通信接口均使能DHCP snooping功能,即使如此,由于某些通信装置没有维护合法用户设备

所对应的DHCP snooping表项,导致若网络黑客仿冒该合法用户设备向所述没有维护合法用户设备所对应的DHCP snooping表项的通信接口发送报文,该报文也会在网络中继续转发。其中,用户设备的上线报文例如可以是指用户设备接入网络(也称为上线)时,在用户设备和DHCP服务器之间交互的报文。

[0080] 下面结合图1和图2的场景,对于上述问题场景进行示例性介绍。

[0081] 示例一:在图1所示的场景中,用户设备101上线时,用户设备101通过路径1与DHCP服务器102通信,路径1包括通信装置SW2和通信装置SW1。SW2的端口1和SW1的端口4均使能DHCP snooping,则用户设备101上线后,SW2和SW1可以分别保存用户设备101所对应的DHCP snooping表项,因此,合法的用户设备101发送的报文能够通过SW2和SW1验证。由此,通信装置SW2和通信装置SW1均可以利用前述用户设备101对应的DHCP snooping表项,对待转发的报文进行校验,从而有效避免网络黑客仿冒用户设备101(例如仿冒用户设备101的IP地址)向DHCP服务器102发送报文,从而对DHCP服务器102进行网络攻击。如上所述,部署了DHCP snooping功能的端口对应的DHCP snooping表项,是基于用户设备的上线报文生成的。对于未传输用户设备的上线报文的通信装置不会维护与用户设备对应的DHCP snooping表项。在一些情况下,如果该些通信装置的接收端口没有开启DHCP snooping功能,则网络黑客可以仿冒用户设备101向DHCP服务器102发送报文,从而对DHCP服务器102进行网络攻击。为了有效防范上述攻击,将环网中所有的通信接口均使能DHCP snooping功能。当通信装置SW2和通信装置SW1之间的路径1发生故障,导致环网100的网络拓扑发生改变。通信装置SW1将工作路径倒换到图1所示的路径2,以传输用户设备101发送的报文,但是路径2中的通信装置SW3等通信装置没有维护用户设备101对应的DHCP snooping表项,导致若网络黑客仿冒用户设备101(例如仿冒用户设备101的IP地址)向环网100中发送攻击报文,则由于路径2中的通信装置没有维护用户设备101对应的DHCP snooping表项,从而使得该攻击报文仍然可以在环网100中传输。

[0082] 示例二,在图2所示的场景中,通信装置R1上使能DHCP snooping功能。但是,如上文对于DHCP snooping表项生成方式的描述可知,通信装置R1上保存有用户设备101对应的DHCP snooping表项,但是通信装置R2上没有保存用户设备101对应的DHCP snooping表项。因此,即使通信装置R2使能了DHCP snooping功能,通信装置R2依旧无法正常识别网络黑客仿冒用户设备101发送的攻击报文。如果通信装置R2能够保存用户设备101对应的DHCP snooping表项,则通信装置R2即可识别网络黑客仿冒用户设备101发送的攻击报文,避免该攻击报文继续在网络中传输,从而提升网络安全。

[0083] 需要说明的是,本申请实施例中提及的通信装置,例如图1以及图2所示的通信装置SW1、SW2、SW3、SW4、SW5、SW6、R1和R2,可以是交换机、路由器等网络设备,也可以是网络设备上的一部分组件,例如是网络设备上的单板,线卡,还可以是网络设备上的一个功能模块,本申请实施例不做具体限定。通信装置之间例如可以通过以太网线或光缆直接连接。

[0084] 为了降低以上提及的安全隐患,本申请实施例提供了一种表项信息处理方法,以下结合附图介绍该方法。

[0085] 参见图3,该图为本申请实施例提供的一种表项信息处理方法的流程示意图。图3所示的表项信息处理方法100,方法100可以应用于图1或者图2所示的场景中。方法100例如可以包括如下S101-S103。

[0086] S101:环网上的通信装置1生成报文1,报文1包括DHCP snooping表项信息1,所述DHCP snooping表项信息1包括用户设备1的IP地址和用户设备1的MAC地址,用户设备1通过通信装置1接入所述环网。

[0087] 此处提及的环网,例如可以是图1或者图2所示的环网100,通信装置1可以是环网上的任一通信装置。例如,在图1或者图2所示的场景中,通信装置1可以是通信装置SW2, SW3, SW4, 或SW5。

[0088] 在一些实施例中,DHCP snooping表项信息1的信息还可以包括用户设备1的IP地址的租期,和/或,用户设备1所属的VLAN的标识。

[0089] 在一些实施例中,通信装置1获取的DHCP snooping表项信息1,除了包括用户设备1的信息之外,还可以包括其它通过所述通信装置1接入环网的用户设备的信息,本申请实施例不做具体限定。在一个示例中,通信装置1获取的DHCP snooping表项信息1,可以包括每个通过所述通信装置1接入环网的用户设备的信息。本申请实施例不做具体限定。例如,通信装置1获取的DHCP snooping表项信息1,还可以包括用户设备2的信息,其中,用户设备2的信息包括用户设备2的IP地址和用户设备2的MAC地址。在一些实施例中,用户设备2的信息还可以包括用户设备2的IP地址的租期,和/或,用户设备2所属的VLAN的标识。

[0090] 本申请实施例,报文1可以为广播报文,也可以为单播报文或组播报文。当报文1为广播报文时,报文1被广播发送至多个通信装置。如此,该多个通信装置均可以获得所述DHCP snooping表项信息1。当报文1为单播报文时,报文1可以被发送至某一特定的通信装置,由此,该特定的通信装置即可获得所述DHCP snooping表项信息1。通信装置1可以生成多个单播报文1,向环网中的其它多个通信装置分别发送该多个单播报文1,由此,环网中的其它多个通信装置可以分别从接收到报文1中获取对应的所述DHCP snooping表项信息1。当报文1是组播报文时,报文1可以被发送至组播组所对应的至少一个通信装置。

[0091] 在一个示例中,报文1中可以包括指示信息1,指示信息1用于指示环网上转发报文1的通信节点获取所述报文1中包括的DHCP snooping表项信息1。如此,环网上转发报文1的通信节点基于该指示信息1的指示,即可获得DHCP snooping表项信息1,并保存包括该DHCP snooping表项信息1的DHCP snooping表项,从而利用该DHCP snooping表项对接收到的报文进行校验,从而保证网络安全。

[0092] 可以理解的是,当报文1中包括前述指示信息1时,若报文1是单播报文,则除了报文1的目的接收节点之外,环网上转发报文1的通信节点也可以获得该DHCP snooping表项信息1。换言之,除了报文1的目的接收节点能够利用DHCP snooping表项信息1对接收到的报文进行校验之外,环网上转发报文1的通信节点也可以利用DHCP snooping表项信息1对接收到的报文进行校验,从而有效保证网络安全。

[0093] 本申请实施例不具体限定报文1的报文结构,在一个示例中,报文1可以包括第一部分和第二部分,其中:第一部分用于携带DHCP snooping表项信息1中的至少一条DHCP snooping表项信息;第二部分用于指示部分1所携带的DHCP snooping表项信息的数量。图4a为本申请实施例提供的一种报文1的结构示意图。如图4a所示,报文1可以包括类型(type)字段、校验和(checksum)字段、主机记录(host record)字段、主机记录数量(number of host record)字段以及预留(reserved)字段。其中:类型字段用于指示报文1的类型,在一个示例中,所述类型字段可以用于携带前文提及的指示信息1;校验和字段用于对报文1

进行完整性校验;主机记录字段可以对应前述第一部分,报文1可以包括一个或者多个主机记录字段。在一个示例中,一个主机记录字段用于携带一条DHCP snooping表项信息。主机记录数量字段可以对应前述第二部分。当然,所述指示信息1也可以携带在报文1的其它字段中,例如,携带在报文1的报文头的预留字段或者扩展字段中,本申请实施例不做具体限定。报文1可以基于DHCP或是其他协议,本申请不做具体限制。

[0094] S102:通信装置1发送所述报文1。

[0095] S103:通信装置2接收通信装置1发送的所述报文1。

[0096] 通信装置2接收报文1后,生成DHCP snooping表,用于保存与接入通信装置1的至少一个用户设备所对应DHCP snooping表项信息。

[0097] 在一些实施例中,例如在图1所示的场景中,通信装置1可以沿环网中的路径2发送报文1,其中,路径2用于在环网中的路径1发生故障时,传输来自于用户设备1的报文,路径1和路径2为环网中传输方向相反的两条路径。关于路径1和路径2,可以参考图1以及上文对于图1的描述部分,此处不做详述。

[0098] 采用方法100,路径2中包括的通信节点即可获取所述DHCP snooping表项信息1并生成对应的述DHCP snooping表项。这样一来,当路径1发生故障时,路径2中的通信节点也可以利用相应的述DHCP snooping表项对接收到的报文进行校验,从而有效保证网络安全的同时,能够保证合法用户的正常业务。在一个示例中,当报文1为广播报文时,通信装置2对应环网100的路径2中任意一个通信节点。当报文1是单播报文时,通信装置1可以向路径2中各个通信节点均发送该单播报文,通信装置2对应报文1的目的节点或者路径2中任一通信节点。当报文1是组播报文时,可以将路径2中的各个通信节点设置为一个组播组,此时,通信装置2对应组播组中的一个通信节点。

[0099] 在又一个示例中,对于环网而言,环网的根桥节点为环网与外部网络进行交互的节点,经过环网转发到外部网络的报文需要通过根桥节点进行转发。当环网的网络拓扑发生改变之后,用户设备发送的报文在环网中的转发路径发生改变,因此,根桥节点接收该报文的端口也会发生改变。以图1所示的场景为例,假设环网100网络拓扑发生改变之前,根桥节点SW1利用端口4接收来自于用户设备1的报文,端口4对应的DHCP snooping表中包括前述DHCP snooping表项信息1。环网100的网络拓扑发生改变之后,根桥节点SW1利用端口9接收来自于用户设备1的报文。此时,若根桥节点的端口9对应的DHCP snooping表能够包括DHCP snooping表项信息1,则环网100的网络拓扑发生改变之后,根桥节点SW1也可以利用相应的DHCP snooping表项对接收到的报文进行校验,从而避免网络黑客仿冒用户设备1所发送的报文被转发至外部网络,从而避免对DHCP服务器造成攻击。因此,前述路径2中的通信节点,可以为路径2中的、所述环网的根桥节点。对于这种情况,报文1可以是单播报文,报文1的目的接收节点为所述环网的根桥节点,例如为通信装置SW1。此时,通信装置2可以为所述环网的根桥节点。

[0100] 另外,若所述环网包括多个根桥节点,例如包括两个根桥节点,此时,这两个根桥节点可以组成一个VRRP组。对于这种情况,前述将报文1发送给环网的根桥节点,也可以认为是将报文1发送给VRRP组中的主节点。例如,将报文1发送给作为主节点的根桥节点SW1。又如,在通信装置SW6从备节点升级为主节点之后,通信装置1将报文1发送给所述通信装置SW6。

[0101] 在一些实施例中,通信装置2可以是外部网络中VRRP组中的主节点。例如在图2所示的场景中,通信装置1可以将报文1发送给外部网络中的VRRP组中的主节点。其中,所述主节点可以是完成备升主的通信节点。例如,在通信装置R2切换为主节点之后,通信装置1将报文1发送给通信装置R2。通信装置R2即可根据所述DHCP snooping表项信息1获取相应的所述DHCP snooping表项,从而利用该DHCP snooping表项对接收到的报文进行验证,有效防范了网络黑客仿冒用户设备1对DHCP服务器进行攻击。一个具体的示例中,通信装置R2切换为主节点之后,环网上每个通信装置都会将自身接入的用户设备的信息发送给R2,由此,R2可以通过DHCP snooping,有效防止攻击者仿冒用户设备进行网络攻击。

[0102] S104:通信装置2保存所述DHCP snooping表项信息1。

[0103] 通信装置2接收到报文1之后,可以保存所述DHCP snooping表项信息1。在一个示例中,通信装置2可以将所述DHCP snooping表项信息1保存至通信装置2的DHCP snooping表中。为了进一步提高DHCP snooping的性能,可以将用户端口与用户的IP地址和MAC地址绑定。示例性地,通信装置2可以将接收所述报文1的端口和所述DHCP snooping表项信息1之间的对应关系,保存至所述通信装置2的DHCP snooping表项中。现以通信装置2为图1所示的通信装置SW1为例进行说明。通信装置2通过端口9接收报文1之后,通信装置2保存所述DHCP snooping表项信息1之后得到的DHCP snooping表项,包括如下表2所示的内容。

[0104] 表2

端口	IP地址	MAC地址	租期	VLAN
端口9	IP地址1	MAC地址1	租期1	VLAN1
端口9	IP地址2	MAC地址2	租期2	VLAN1

[0106] 在本申请实施例的一种实现方式中,通信装置1可以在环网的网络拓扑发送改变之前执行前述S101-S102,从而实现将DHCP snooping表项信息1发送给其它通信装置。从而进一步使得在环网的网络拓扑发生改变之后,即使用户设备1和DHCP服务器之间的报文转发路径发生改变,其它通信装置也能基于DHCP snooping表项信息1对接收到的报文进行验证,从而避免网络黑客仿冒用户设备1对DHCP服务器进行攻击,并保证合法用户的正常业务。

[0107] 在本申请实施例的一种实现方式中,通信装置1也可以在环网的网络拓扑发送改变之后,执行前述S101-S102,本申请实施例不做具体限定。若通信装置1在环网的网络拓扑发送改变之后执行S101-S102,则通信装置在执行S101之前,还需要确定所述环网的网络拓扑发生改变。在一个示例中,通信装置1上可以部署环网破坏协议,通信装置1可以利用所述环网破坏协议确定环网的网络拓扑发生改变。其中,所述环网破坏协议例如可以为多生成树协议(Multiple Spanning Tree Protocol,MSTP)。此处提及的环网的网络拓扑发生改变,指的是报文在所述环网中的转发路径发生改变,例如,如前文所述,用户设备1发送的报文由环网上的路径2切换为环网上的路径1转发。关于路径2和路径1,可以参考前文的相关描述部分,此处不做详述。

[0108] 在本申请实施例中,若报文1为广播报文,则通信装置1可以主动发送该报文1,例如,通信装置1在确定环网的网络拓扑发生改变之后,主动将报文1广播发送至环网的第一路径中的各个通信节点。若报文1为单播报文,则在一个示例中,通信装置1可以在确定环网的网络拓扑发生改变之后,主动发送该报文1。在另一个示例中,通信装置1可以基于报文1

的目的接收节点的请求,向所述报文1的目的接收节点发送报文1。换言之,通信装置1在执行S101之前,还可以接收报文2,报文2用于向通信装置1请求所述DHCP snooping表项信息1。如前文,当报文1是单播报文时,报文1的目的接收节点,可以是所述环网的根桥节点,也可以外部网络中的VRRP组中的主节点。因此,此处提及的报文2,可以是前文提及的环网的根桥节点发送给通信装置1的,也可以是前文提及的外部网络中的VRRP组中的主节点发送给通信装置1的。在一些实施例中,若报文2是环网的根桥节点发送给通信装置1的,则所述根桥节点可以在所述环网的网络拓扑发生改变、并且所述环网的网络拓扑趋于稳定之后,将报文2发送给通信装置1。若报文2是外部网络中的VRRP组中的主节点发送给通信装置1的,则外部网络中的VRRP组中的节点可以在切换成主节点之后,将报文2发送给通信装置1。

[0109] 本申请实施例不具体限定所述报文2,在一个示例中,所述报文2可以为组播报文,该报文2中的目的接收节点为所述环网上的通信节点。本申请实施例不具体限定所述报文2的报文结构,在一个示例中,所述报文2可以包括类型字段,所述类型字段用于指示所述报文2用于请求所述DHCP snooping表项信息1。参见图4b,图4b为本申请实施例提供的一种报文2的结构示意图。如图4b所示,报文2包括类型(type)字段、最大响应延迟(Max Response delay)字段、校验和(checksum)字段和组播地址(Group Address)字段。需要说明的是,图4b指示为了方便理解报文2的报文结构而示出,其并不构成对报文2的报文结构的限定。

[0110] 关于报文2中各个字段的含义,可以参考下表3进行理解。

[0111] 表3

	字段	含义
[0112]	类型	指示报文用于请求 DHCP snooping 表项信
		息 1
[0113]	最大响应延迟	接收到报文 2 的通信装置针对报文 2 回复响应报文的最大时间间隔
	checksum	校验和。
	Group Address	组播地址, 从保留组播地址中挑选一个地址, 发给网段内所有通信节点

[0114] 图5为本申请实施例提供的一种表项信息处理方法的流程示意图。图5所示的表项信息处理方法200,可以由第一通信装置执行。第一通信装置可以为以上实施例中的通信装置1。用于执行以上方法100中通信装置1执行的步骤。所述方法200例如可以包括如下S201-S202。

[0115] S201:生成第一报文,所述第一报文包括动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网。

[0116] S202:发送所述第一报文。

[0117] 此处提及的第一报文,可以对应方法100中的报文1,此处提及的DHCP snooping表项信息,可以对应方法100中的DHCP snooping表项信息1。此处提及的第一用户设备,可以对应方法100中的用户设备1。

[0118] 在一种实现方式中,所述生成第一报文包括:

- [0119] 确定所述环网的拓扑发生变化后,生成所述第一报文。
- [0120] 在一种实现方式中,所述DHCP snooping表项信息还包括:
- [0121] 所述第一用户设备所属的虚拟局域网VLAN的标识,和/或,所述第一IP地址的租期。
- [0122] 在一种实现方式中,所述发送所述第一报文,包括:
- [0123] 向所述环网的第一路径中的通信节点发送所述第一报文,所述第一路径用于在所述环网中的第二路径发生故障时,传输来自所述第一用户设备的报文,所述第一路径和所述第二路径为所述环网中传输方向相反的两条路径。
- [0124] 此处提及的第一路径,可以对应方法100中的路径2,此处提及的第二路径,可以对应方法100中的路径1。
- [0125] 在一种实现方式中,所述通信节点包括所述环网的根桥节点。
- [0126] 在一种实现方式中,所述发送所述第一报文,包括:
- [0127] 向外部网络中的虚拟路由冗余协议VRRP组中的主节点发送所述第一报文,所述环网的根桥节点通过所述VRRP组接入所述外部网络。
- [0128] 在一种实现方式中,所述第一报文为广播报文。
- [0129] 在一种实现方式中,所述第一报文为单播报文。
- [0130] 在一种实现方式中,在生成所述第一报文之前,所述方法还包括:
- [0131] 接收第二报文,所述第二报文用于向所述第一通信装置请求所述DHCP snooping表项信息。
- [0132] 此处提及的第二报文,可以对应方法100中的报文2。
- [0133] 在一种实现方式中,所述接收第二报文,包括:
- [0134] 接收所述环网的根桥节点发送的所述第二报文。
- [0135] 在一种实现方式中,所述接收第二报文包括:
- [0136] 接收外部网络中的虚拟路由冗余协议VRRP组中的主节点发送的所述第二报文,所述环网的根桥节点通过所述VRRP组接入所述外部网络。
- [0137] 在一种实现方式中,所述第一报文中还包括指示信息,所述指示信息用于指示所述环网上转发所述第一报文的通信节点获取所述DHCP snooping表项信息。
- [0138] 此处提及的指示信息,可以对应方法100中的指示信息1。
- [0139] 在一种实现方式中,所述第一报文包括:
- [0140] 第一部分,用于携带包括所述DHCP snooping表项信息的至少一条DHCP snooping表项信息;
- [0141] 第二部分,用于指示所述第一部分中所携带的DHCP snooping表项信息的数量。
- [0142] 在一种实现方式中,所述环网为二层环网或三层环网。
- [0143] 图6为本申请实施例提供的一种表项信息处理方法的流程示意图。图6所示的表项信息处理方法300,可以由第二通信装置执行。第二通信装置可以为以上实施例中的通信装置2。用于执行以上方法100中通信装置2执行的步骤。在方法300中,第一通信装置可以对应以上实施例中的通信装置1。所述方法300例如可以包括如下S301-S302。
- [0144] S301:接收环网上的第一通信装置发送的第一报文,所述第一报文包括动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的

第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网。

[0145] S302:保存所述DHCP snooping表项信息。

[0146] 在一个示例中,在本申请中,保存所述DHCP snooping表项信息包括:生成DHCP snooping表,在所述DHCP snooping表中保存所述DHCP snooping表项信息。在一个示例中,本申请中的DHCP snooping表包括接口、用户设备的IP地址以及用户设备的MAC地址的对应关系。此处提及的第一报文,可以对应方法100中的报文1。此处提及的第一用户设备,可以对应方法100中的用户设备1,此处提及的DHCP snooping表项信息,可以对应方法100中的DHCP snooping表项信息1。

[0147] 在一种实现方式中,所述DHCP snooping表项信息还包括:

[0148] 所述第一用户设备所属的虚拟局域网VLAN的标识,和/或,所述第一IP地址的租期。

[0149] 在一种实现方式中,所述第二通信装置为所述环网上的第一路径中的通信节点,所述第一路径用于在所述环网中的第二路径发生故障时,传输来自所述第一用户设备的报文,所述第一路径和所述第二路径为所述环网中传输方向相反的两条路径。

[0150] 此处提及的第一路径,可以对应方法100中的路径2,此处提及的第二路径,可以对应方法100中路径1。

[0151] 在一种实现方式中,所述第二通信装置包括所述环网的根桥节点。

[0152] 在一种实现方式中,所述第二通信装置为外部网络中的虚拟路由冗余协议VRRP组中的主节点,所述环网的根桥节点通过所述VRRP组接入所述外部网络。

[0153] 在一种实现方式中,所述第一报文为广播报文。

[0154] 在一种实现方式中,所述第一报文为单播报文。

[0155] 在一种实现方式中,所述方法还包括:

[0156] 向所述第一通信装置发送第二报文,所述第二报文用于向所述第一通信装置请求所述DHCP snooping表项信息。

[0157] 此处提及的第二报文,可以对应方法100中的报文2。

[0158] 在一种实现方式中,所述第一报文中还包括指示信息,所述指示信息用于指示所述第二通信装置获取所述DHCP snooping表项信息。

[0159] 此处提及的指示信息,可以对应方法100中的指示信息1。

[0160] 在一种实现方式中,所述第一报文包括:

[0161] 第一部分,用于携带包括所述DHCP snooping表项信息的至少一条DHCP snooping表项信息;

[0162] 第二部分,用于指示所述第一部分中所携带的DHCP snooping表项信息的数量。

[0163] 在一种实现方式中,所述环网为二层环网或三层环网。

[0164] 在一种实现方式中,所述保存所述DHCP snooping表项信息,包括:

[0165] 保存接收所述第一报文的接口和所述DHCP snooping表项信息的对应关系。

[0166] 图7为本申请实施例提供的一种表项信息处理方法的流程示意图。图7所示的表项信息处理方法400,可以由第二通信装置执行。第二通信装置可以为以上实施例中的通信装置2。用于执行以上方法100中通信装置2执行的步骤。在方法400中,第一通信装置可以对应

以上实施例中的通信装置1。所述方法400例如可以包括如下S401-S402。

[0167] S401:生成第二报文,所述第二报文用于向环网上的第一通信装置请求动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网。

[0168] S402:向所述第一通信装置发送所述第二报文。

[0169] 此处提及的第二报文,可以对应方法100中的报文2,此处提及的DHCP snooping表项信息,可以对应方法100中的DHCP snooping表项信息1,此处提及的第一用户设备,可以对应方法100中的用户设备1。

[0170] 在一种实现方式中,所述方法包括:

[0171] 接收所述第一通信装置发送的第一报文,所述第一报文包括所述DHCP snooping表项信息;

[0172] 保存所述DHCP snooping表项信息。

[0173] 此处提及的第一报文,可以对应方法100中的报文1。

[0174] 在一种实现方式中,所述DHCP snooping表项信息还包括:

[0175] 所述第一用户设备所属的虚拟局域网VLAN的标识,和/或,所述第一IP地址的租期。

[0176] 在一种实现方式中,所述第二通信装置为所述环网上的第一路径中的通信节点,所述第一路径用于在所述环网中的第二路径发生故障时,传输来自所述第一用户设备的报文,所述第一路径和所述第二路径为所述环网中传输方向相反的两条路径。

[0177] 此处提及的第一路径,可以对应方法100中的路径2,此处提及的第二路径,可以对应方法100中的路径1。

[0178] 在一种实现方式中,所述第二通信装置包括所述环网的根桥节点。

[0179] 在一种实现方式中,所述第二通信装置为外部网络中的虚拟路由冗余协议VRRP组中的主节点,所述环网的根桥节点通过所述VRRP组接入所述外部网络。

[0180] 在一种实现方式中,所述第一报文为广播报文。

[0181] 在一种实现方式中,所述第一报文为单播报文。

[0182] 在一种实现方式中,所述第一报文中还包括指示信息,所述指示信息用于指示所述第二通信装置获取所述DHCP snooping表项信息。

[0183] 此处提及的指示信息,可以对应方法100中的指示信息1。

[0184] 在一种实现方式中,所述第一报文包括:

[0185] 第一部分,用于携带包括所述DHCP snooping表项信息的至少一条DHCP snooping表项信息;

[0186] 第二部分,用于指示所述第一部分中所携带的DHCP snooping表项信息的数量。

[0187] 在一种实现方式中,所述环网为二层环网或三层环网。

[0188] 在一种实现方式中,所述保存所述DHCP snooping表项信息,包括:

[0189] 保存接收所述第一报文的接口和所述DHCP snooping表项信息的对应关系。

[0190] 关于以上方法200、方法300以及方法400的具体实现,可以参考上文对于方法100的描述部分,此处不做详述。

[0191] 此外,本申请实施例还提供了一种通信装置800,参见图8所示。图8为本申请实施例提供的一种通信装置的结构示意图。该通信装置800包括收发单元801和处理单元802。该通信装置800可以用于执行以上实施例中的方法100、方法200、方法300或者方法400。

[0192] 在一个示例中,所述通信装置800可以执行以上实施例中的方法100,当通信装置800用于执行以上实施例中的方法100时,通信装置800相当于方法100中的通信装置1。收发单元801用于执行方法100中通信装置1执行的收发操作。处理单元802用于执行方法100中通信装置1执行的除收发操作之外的操作。例如:处理单元802用于生成报文1,报文1包括DHCP snooping表项信息1,所述DHCP snooping表项信息1包括用户设备1的IP地址和用户设备1的MAC地址,用户设备1通过通信装置1接入所述环网;收发单元801用于发送所述报文1。

[0193] 在一个示例中,所述通信装置800可以执行以上实施例中的方法100,当通信装置800用于执行以上实施例中的方法100时,通信装置800相当于方法100中的通信装置2。收发单元801用于执行方法100中通信装置2执行的收发操作。处理单元802用于执行方法100中通信装置2执行的除收发操作之外的操作。例如:收发单元801用于接收通信装置1发送的报文1,报文1中包括DHCP snooping表项信息1,所述DHCP snooping表项信息1包括用户设备1的IP地址和用户设备1的MAC地址,用户设备1通过通信装置1接入所述环网;处理单元802用于保存所述DHCP snooping表项信息1。

[0194] 在一个示例中,所述通信装置800可以执行以上实施例中的方法100,当通信装置800用于执行以上实施例中的方法100时,通信装置800相当于方法100中的通信装置2。收发单元801用于执行方法100中通信装置2执行的收发操作。处理单元802用于执行方法100中通信装置2执行的除收发操作之外的操作。例如:处理单元802用于生成报文2,所述报文2用于向环网上的通信装置1请求动态主机配置协议DHCP监听snooping表项信息1,所述DHCP snooping表项信息包括用户设备1的IP地址和所述用户设备1的MAC地址,所述用户设备1通过所述通信装置1接入所述环网;所述收发单元801用于将所述报文2发送给通信装置1。

[0195] 在一个示例中,所述通信装置800可以执行以上实施例中的方法200,当通信装置800用于执行以上实施例中的方法200时,通信装置800相当于方法200中的第一通信装置。收发单元801用于执行方法200中第一通信装置执行的收发操作。处理单元802用于执行方法200中第一通信装置执行的除收发操作之外的操作。例如:处理单元802用于生成第一报文,所述第一报文包括动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网;收发单元801用于发送所述第一报文。

[0196] 在一个示例中,所述通信装置800可以执行以上实施例中的方法300,当通信装置800用于执行以上实施例中的方法300时,通信装置800相当于方法300中的第二通信装置。收发单元801用于执行方法300中第二通信装置执行的收发操作。处理单元802用于执行方法300中第二通信装置执行的除收发操作之外的操作。例如:收发单元801用于接收环网上的第一通信装置发送的第一报文,所述第一报文包括动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置

接入所述环网;处理单元802用于保存所述DHCP snooping表项信息。

[0197] 在一个示例中,所述通信装置800可以执行以上实施例中的方法400,当通信装置800用于执行以上实施例中的方法400时,通信装置800相当于方法400中的第二通信装置。收发单元801用于执行方法400中第二通信装置执行的收发操作。处理单元802用于执行方法400中第二通信装置执行的除收发操作之外的操作。例如:处理单元802用于生成第二报文,所述第二报文用于向环网上的第一通信装置请求动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网;收发单元801用于向所述第一通信装置发送所述第二报文。

[0198] 此外,本申请实施例还提供了一种通信装置900,参见图9所示,图9为本申请实施例提供的一种通信装置的结构示意图。该通信装置900包括通信接口901和与通信接口901连接的处理器902。该通信装置900可以用于执行以上实施例中的方法100、方法200、方法300或者方法400。

[0199] 在一个示例中,所述通信装置900可以执行以上实施例中的方法100,当通信装置900用于执行以上实施例中的方法100时,通信装置900相当于方法100中的通信装置1。通信接口901用于执行方法100中通信装置1执行的收发操作。处理器902用于执行方法100中通信装置1执行的除收发操作之外的操作。例如:处理器902用于生成报文1,报文1包括DHCP snooping表项信息1,所述DHCP snooping表项信息1包括用户设备1的IP地址和用户设备1的MAC地址,用户设备1通过通信装置1接入所述环网;通信接口901用于发送所述报文1。

[0200] 在一个示例中,所述通信装置900可以执行以上实施例中的方法100,当通信装置900用于执行以上实施例中的方法100时,通信装置900相当于方法100中的通信装置2。通信接口901用于执行方法100中通信装置2执行的收发操作。处理器902用于执行方法100中通信装置2执行的除收发操作之外的操作。例如:通信接口901用于接收通信装置1发送的报文1,报文1中包括DHCP snooping表项信息1,所述DHCP snooping表项信息1包括用户设备1的IP地址和用户设备1的MAC地址,用户设备1通过通信装置1接入所述环网;处理器902用于保存所述DHCP snooping表项信息1。

[0201] 在一个示例中,所述通信装置900可以执行以上实施例中的方法100,当通信装置900用于执行以上实施例中的方法100时,通信装置900相当于方法100中的通信装置2。通信接口901用于执行方法100中通信装置2执行的收发操作。处理器902用于执行方法100中通信装置2执行的除收发操作之外的操作。例如:处理器902用于生成报文2,所述报文2用于向环网上的通信装置1请求动态主机配置协议DHCP监听snooping表项信息1,所述DHCP snooping表项信息包括用户设备1的IP地址和所述用户设备1的MAC地址,所述用户设备1通过所述通信装置1接入所述环网;所述通信接口901用于将所述报文2发送给通信装置1。

[0202] 在一个示例中,所述通信装置900可以执行以上实施例中的方法200,当通信装置900用于执行以上实施例中的方法200时,通信装置900相当于方法200中的第一通信装置。通信接口901用于执行方法200中第一通信装置执行的收发操作。处理器902用于执行方法200中第一通信装置执行的除收发操作之外的操作。例如:处理器902用于生成第一报文,所述第一报文包括动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控

制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网;通信接口901用于发送所述第一报文。

[0203] 在一个示例中,所述通信装置900可以执行以上实施例中的方法300,当通信装置900用于执行以上实施例中的方法300时,通信装置900相当于方法300中的第二通信装置。通信接口901用于执行方法300中第二通信装置执行的收发操作。处理器902用于执行方法300中第二通信装置执行的除收发操作之外的操作。例如:通信接口901用于接收环网上的第一通信装置发送的第一报文,所述第一报文包括动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网;处理器902用于保存所述DHCP snooping表项信息。

[0204] 在一个示例中,所述通信装置900可以执行以上实施例中的方法400,当通信装置900用于执行以上实施例中的方法400时,通信装置900相当于方法400中的第二通信装置。通信接口901用于执行方法400中第二通信装置执行的收发操作。处理器902用于执行方法400中第二通信装置执行的除收发操作之外的操作。例如:处理器902用于生成第二报文,所述第二报文用于向环网上的第一通信装置请求动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网;通信接口901用于向所述第一通信装置发送所述第二报文。

[0205] 此外,本申请实施例还提供了一种通信装置1000,参见图10所示,图10为本申请实施例提供的一种通信装置的结构示意图。

[0206] 该通信装置1000可以用于执行以上实施例中的方法100、方法200、300或者方法400。

[0207] 如图10所示,通信装置1000可以包括处理器1010,与所述处理器1010耦合连接的存储器1020,收发器1030。收发器1030例如可以是通信接口,光模块等。处理器1010可以是中央处理器(英文:central processing unit,缩写:CPU),网络处理器(英文:network processor,缩写:NP)或者CPU和NP的组合。处理器还可以是专用集成电路(英文:application-specific integrated circuit,缩写:ASIC),可编程逻辑器件(英文:programmable logic device,缩写:PLD)或其组合。上述PLD可以是复杂可编程逻辑器件(英文:complex programmable logic device,缩写:CPLD),现场可编程逻辑门阵列(英文:field-programmable gate array,缩写:FPGA),通用阵列逻辑(英文:generic array logic,缩写:GAL)或其任意组合。处理器1010可以是指一个处理器,也可以包括多个处理器。存储器1020可以包括易失性存储器(英文:volatile memory),例如随机存取存储器(英文:random-access memory,缩写:RAM);存储器也可以包括非易失性存储器(英文:non-volatile memory),例如只读存储器(英文:read-only memory,缩写:ROM),快闪存储器(英文:flash memory),硬盘(英文:hard disk drive,缩写:HDD)或固态硬盘(英文:solid-state drive,缩写:SSD);存储器1020还可以包括上述种类的存储器的组合。存储器1020可以是指一个存储器,也可以包括多个存储器。在一个实施方式中,存储器1020中存储有计算机可读指令,所述计算机可读指令包括多个软件模块,例如发送模块1021,处理模块1022和接收模块1023。处理器1010执行各个软件模块后可以按照各个软件模块的指示进行相应的

操作。在本实施例中，一个软件模块所执行的操作实际上是指处理器1010根据所述软件模块的指示而执行的操作。

[0208] 在一个示例中，所述通信装置1000可以执行以上实施例中的方法100，当通信装置1000用于执行以上实施例中的方法100时，通信装置1000相当于方法100中的通信装置1。收发器1030用于执行方法100中通信装置1执行的收发操作。处理器1010用于执行方法100中通信装置1执行的除收发操作之外的操作。例如：处理器1010用于生成报文1，报文1包括DHCP snooping表项信息1，所述DHCP snooping表项信息1包括用户设备1的IP地址和用户设备1的MAC地址，用户设备1通过通信装置1接入所述环网；收发器1030用于发送所述报文1。

[0209] 在一个示例中，所述通信装置1000可以执行以上实施例中的方法100，当通信装置1000用于执行以上实施例中的方法100时，通信装置1000相当于方法100中的通信装置2。收发器1030用于执行方法100中通信装置2执行的收发操作。处理器1010用于执行方法100中通信装置2执行的除收发操作之外的操作。例如：收发器1030用于接收通信装置1发送的报文1，报文1中包括DHCP snooping表项信息1，所述DHCP snooping表项信息1包括用户设备1的IP地址和用户设备1的MAC地址，用户设备1通过通信装置1接入所述环网；处理器1010用于保存所述DHCP snooping表项信息1。

[0210] 在一个示例中，所述通信装置1000可以执行以上实施例中的方法100，当通信装置1000用于执行以上实施例中的方法100时，通信装置1000相当于方法100中的通信装置2。收发器1030用于执行方法100中通信装置2执行的收发操作。处理器1010用于执行方法100中通信装置2执行的除收发操作之外的操作。例如：处理器1010用于生成报文2，所述报文2用于向环网上的通信装置1请求动态主机配置协议DHCP监听snooping表项信息1，所述DHCP snooping表项信息包括用户设备1的IP地址和所述用户设备1的MAC地址，所述用户设备1通过所述通信装置1接入所述环网；所述收发器1030用于将所述报文2发送给通信装置1。

[0211] 在一个示例中，所述通信装置1000可以执行以上实施例中的方法200，当通信装置1000用于执行以上实施例中的方法200时，通信装置1000相当于方法200中的第一通信装置。收发器1030用于执行方法200中第一通信装置执行的收发操作。处理器1010用于执行方法200中第一通信装置执行的除收发操作之外的操作。例如：处理器1010用于生成第一报文，所述第一报文包括动态主机配置协议DHCP监听snooping表项信息，所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址，所述第一用户设备通过所述第一通信装置接入所述环网；收发器1030用于发送所述第一报文。

[0212] 在一个示例中，所述通信装置1000可以执行以上实施例中的方法300，当通信装置1000用于执行以上实施例中的方法300时，通信装置1000相当于方法300中的第二通信装置。收发器1030用于执行方法300中第二通信装置执行的收发操作。处理器1010用于执行方法300中第二通信装置执行的除收发操作之外的操作。例如：收发器1030用于接收环网上的第一通信装置发送的第一报文，所述第一报文包括动态主机配置协议DHCP监听snooping表项信息，所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址，所述第一用户设备通过所述第一通信装置接入所述环网；处理器1010用于保存所述DHCP snooping表项信息。

[0213] 在一个示例中,所述通信装置1000可以执行以上实施例中的方法400,当通信装置1000用于执行以上实施例中的方法400时,通信装置1000相当于方法400中的第二通信装置。收发器1030用于执行方法400中第二通信装置执行的收发操作。处理器1010用于执行方法400中第二通信装置执行的除收发操作之外的操作。例如:处理器1010用于生成第二报文,所述第二报文用于向环网上的第一通信装置请求动态主机配置协议DHCP监听snooping表项信息,所述DHCP snooping表项信息包括第一用户设备的第一互联网协议IP地址和所述第一用户设备的第一媒体接入控制MAC地址,所述第一用户设备通过所述第一通信装置接入所述环网;收发器1030用于向所述第一通信装置发送所述第二报文。

[0214] 本申请实施例还提供了一种计算机可读存储介质,所述计算机可读存储介质中存储有指令,当其在计算机上运行时,使得所述计算机执行以上实施例中由第一通信装置执行的步骤。

[0215] 本申请实施例还提供了一种计算机可读存储介质,所述计算机可读存储介质中存储有指令,当其在计算机上运行时,使得所述计算机执行以上实施例中由第二通信装置执行的步骤。

[0216] 本申请实施例还提供了一种通信系统,包括以上实施例提及的任一种第一通信装置和任一种第二通信装置。

[0217] 本申请实施例还提供了一种通信系统,包括至少一个存储器和至少一个处理器,该至少一个存储器存储有指令,该至少一个处理器执行所述指令,使得所述通信系统执行本申请前述实施例中任一实施例所述的方法(例如,方法100,方法200和方法300)中任意一个或多个操作。

[0218] 本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”等(如果存在)是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外,术语“包括”和“具有”以及他们的任何变形,意图在于覆盖不排他的包含,例如,包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元,而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0219] 所属领域的技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的系统,装置和单元的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0220] 在本申请所提供的几个实施例中,应该理解到,所揭露的系统,装置和方法,可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,单元的划分,仅仅为一种逻辑业务划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0221] 作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0222] 另外,在本申请各个实施例中的各业务单元可以集成在一个处理单元中,也可以

是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件业务单元的形式实现。

[0223] 集成的单元如果以软件业务单元的形式实现并作为独立的产品销售或使用,可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备)执行本申请各个实施例方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0224] 本领域技术人员应该可以意识到,在上述一个或多个示例中,本发明所描述的业务可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时,可以将这些业务存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质,其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是通用或专用计算机能够存取的任何可用介质。

[0225] 以上的具体实施方式,对本发明的目的、技术方案和有益效果进行了进一步详细说明,所应理解的是,以上仅为本发明的具体实施方式而已。

[0226] 以上,以上实施例仅用以说明本申请的技术方案,而非对其限制;尽管参照前述实施例对本申请进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本申请各实施例技术方案的范围。

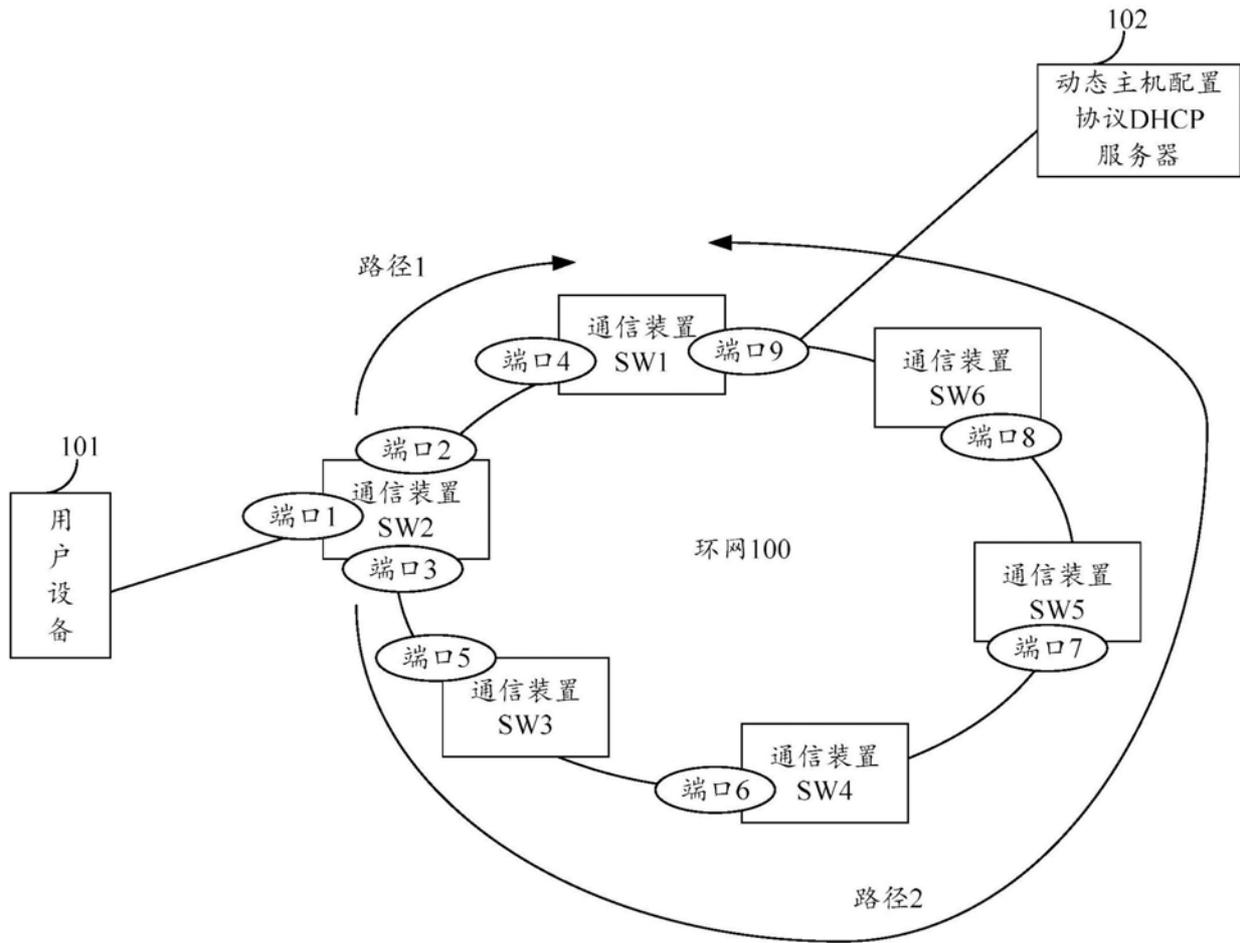


图1

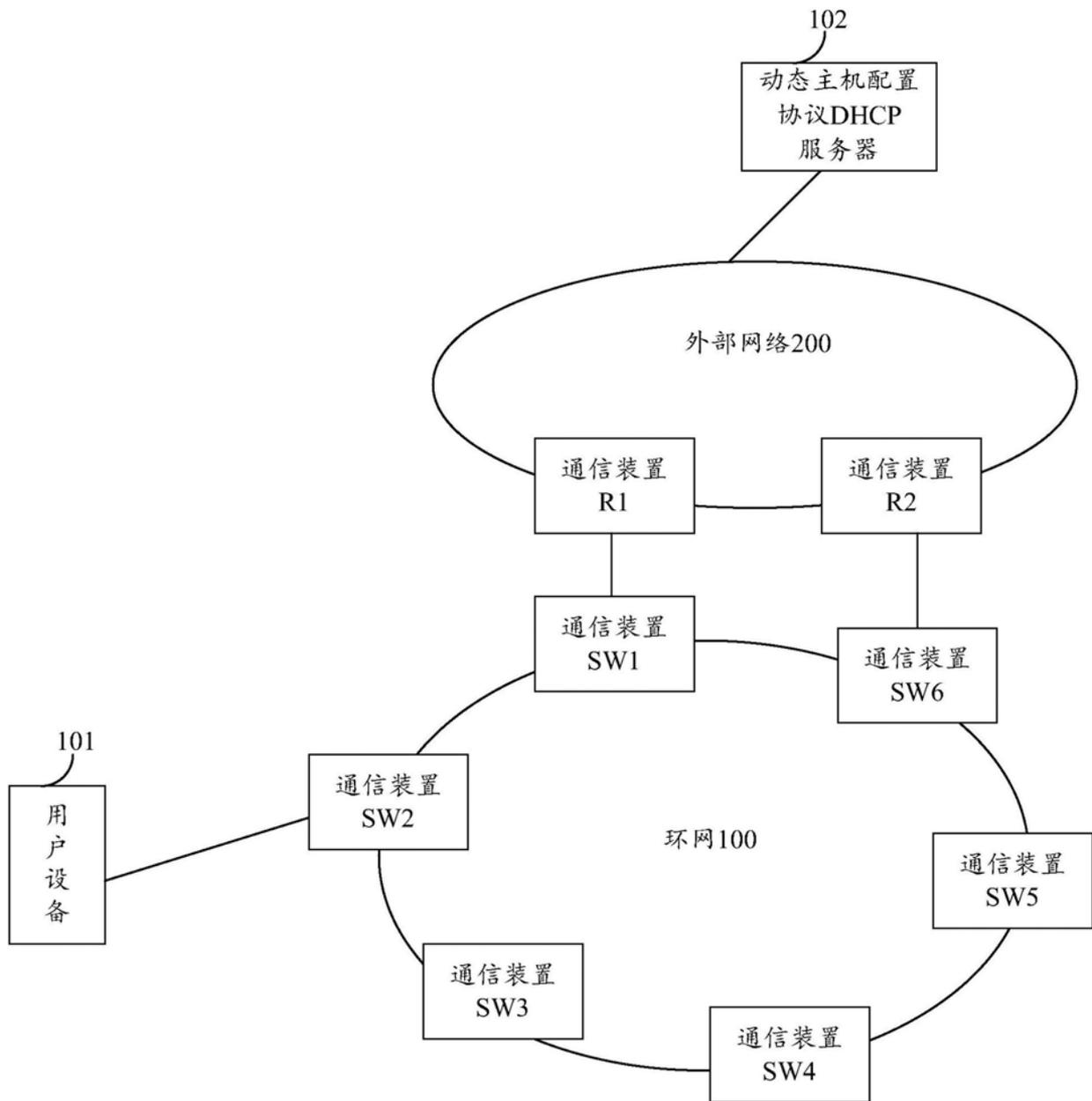


图2

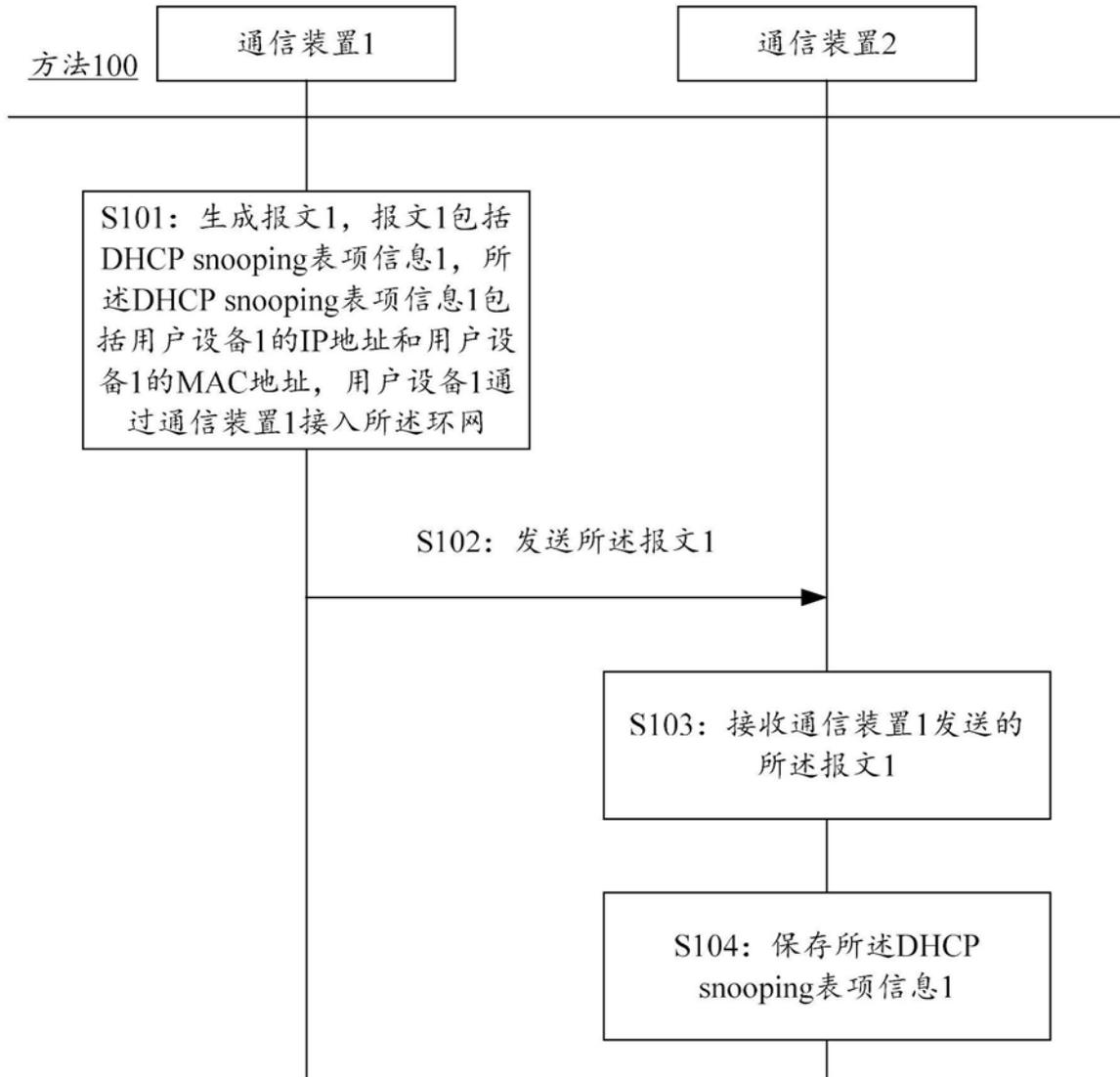


图3

类型 type	预留 reserved	校验和 checksum
预留 reserved		主机记录数量 number of host record
		主机记录 host record
		主机记录 host record
	

图4a

类型 type	最大响应延迟 Max Response delay	校验和 checksum
组播地址 Group Address		

图4b

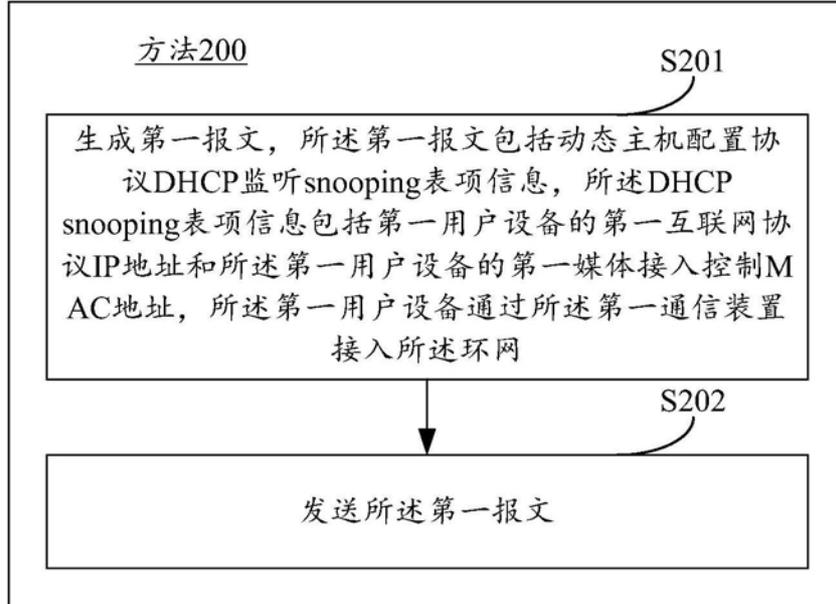


图5

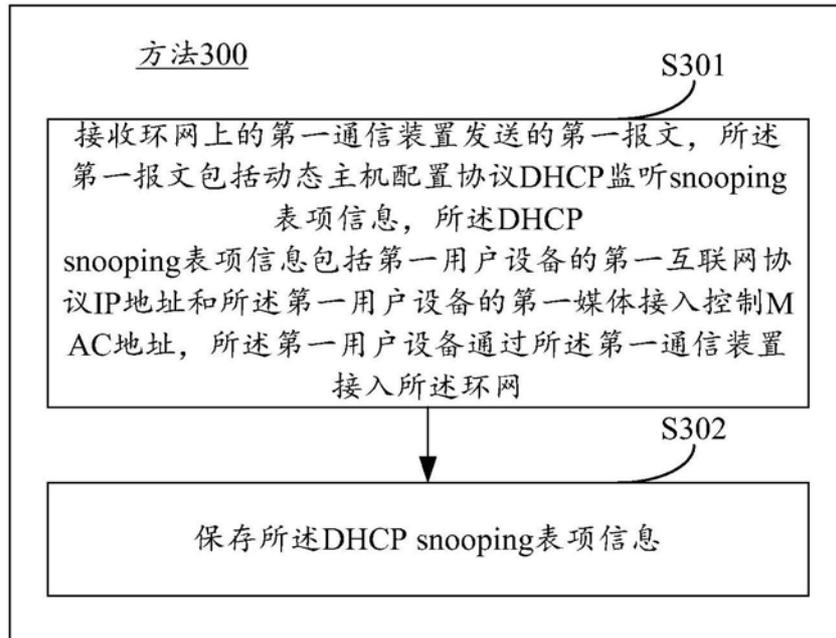


图6

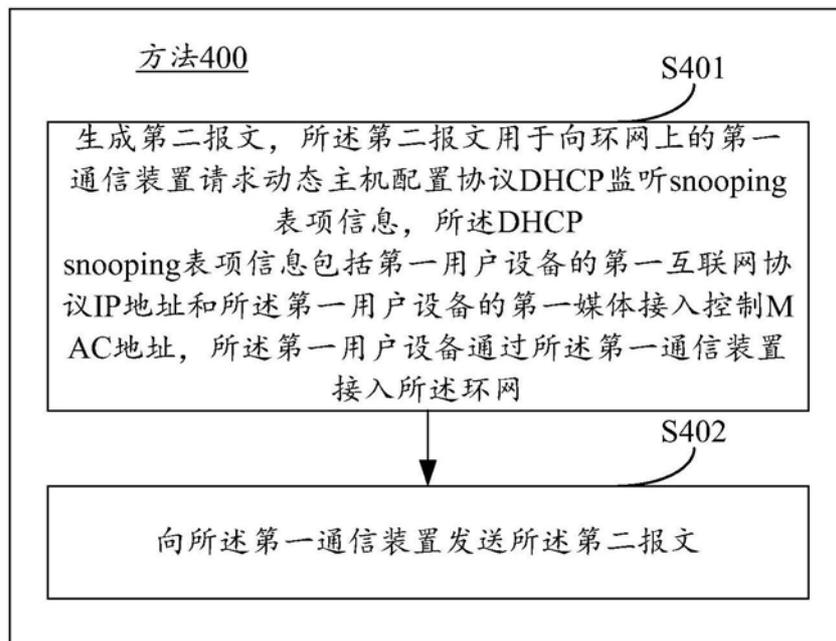


图7

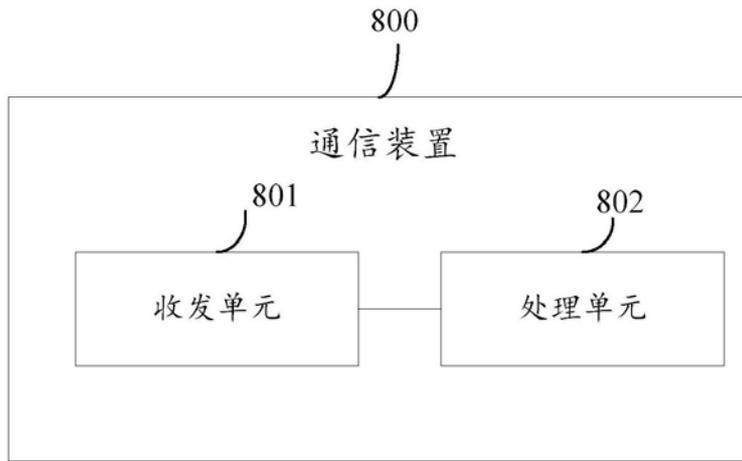


图8

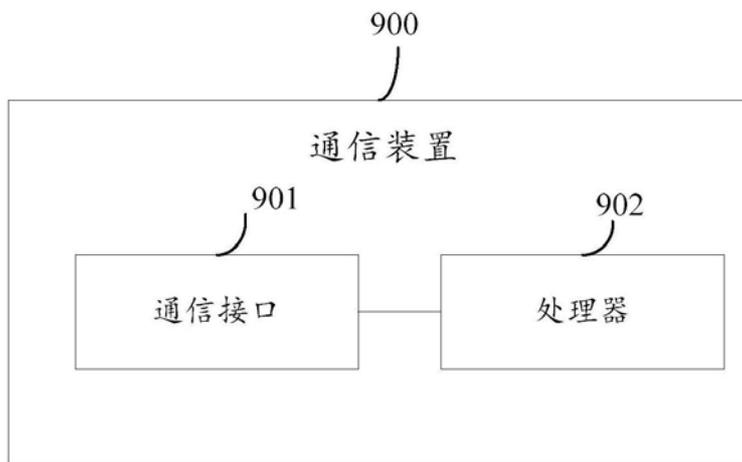


图9

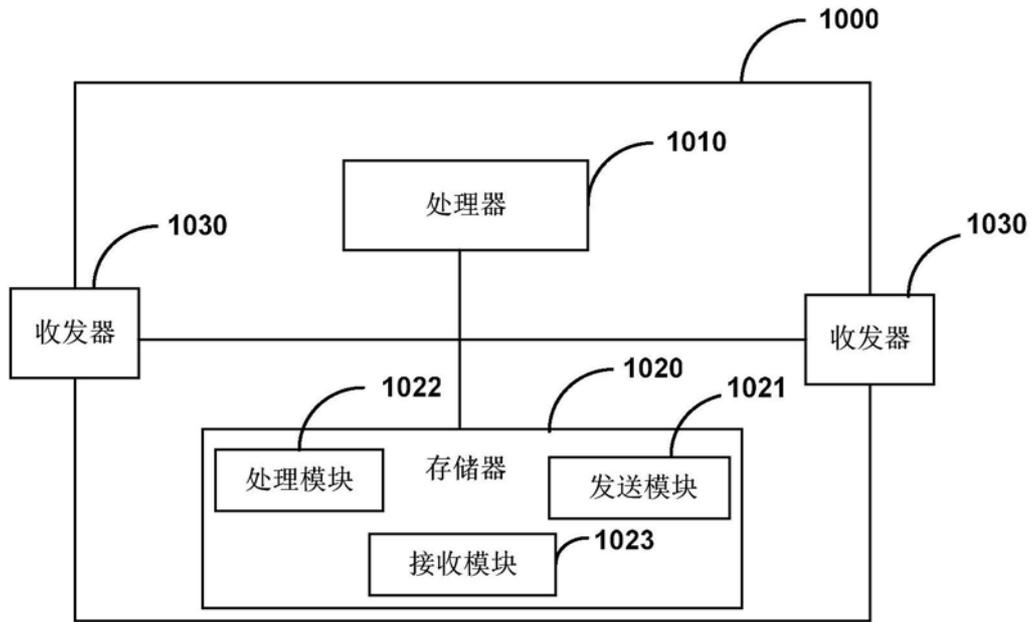


图10