(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102546666 B
(45)授权公告日 2016.04.27

(21)申请号 201210048874.5
(22)申请日 2012.02.28
(73)专利权人 神州数码网络（北京）有限公司
地址 100085 北京市海淀区上地九街9号数码科技广场一段三层A区
(72)发明人 梁小冰
(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 宋松
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/12(2006.01)
H04L 12/741(2013.01)
H04L 12/761(2013.01)

(56)对比文件
CN 101227287 A,2008.07.23,
CN 101001249 A,2007.07.18,
CN 10116084 A,2008.04.23,
CN 101478542 A,2009.07.08,
CN 101022340 A,2007.08.22,

审查员 刘永辉

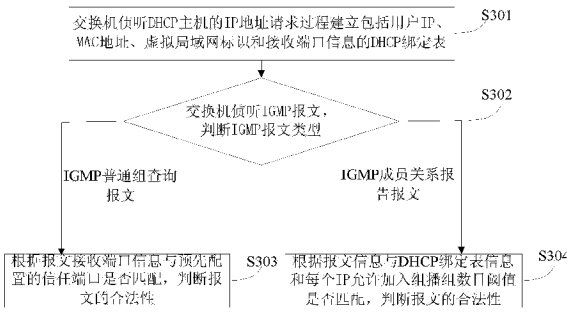
权利要求书2页 说明书6页 附图4页

(54)发明名称

防止IGMP欺骗和攻击的方法及装置

(57)摘要

本发明公开一种防止IGMP欺骗和攻击的方法及装置，包括：S1：交换机侦听DHCP主机的IP地址请求过程建立包括用户IP、MAC地址、虚拟局域网标识和接收端口信息的DHCP绑定表；S2：交换机侦听IGMP报文，判断报文类型，如是普通组查询报文，则执行步骤S3，如是成员关系报告报文，则执行步骤S4；S3：根据接收端口信息与预先配置的信任端口是否匹配，判断报文的合法性；S4：根据报文信息与DHCP绑定表信息和每个IP允许加入的组播组数目阈值是否匹配，判断报文的合法性。本发明有效解决了IGMP普遍组查询欺骗、IGMP源地址欺骗以及IGMP成员报告报文攻击问题，该方法简单易实现，有利于网络的安全运行。



CN 102546666 B

1.一种防止IGMP欺骗和攻击的方法，其特征在于，该方法包括：

S1：交换机侦听DHCP主机的IP地址请求过程建立包括用户IP、MAC地址、虚拟局域网标识和接收端口信息的DHCP绑定表；

S2：交换机侦听IGMP报文，判断报文类型，如是IGMP普通组查询报文，则执行步骤S3；如是IGMP成员关系报告报文，则执行步骤S4；

S3：根据报文接收端口信息与预先配置的信任端口是否匹配，判断报文的合法性；

S4：根据报文信息与DHCP绑定表信息和每个IP允许加入组播组数目阈值是否匹配，判断报文的合法性。

2.根据权利要求1所述的防止IGMP欺骗和攻击的方法，其特征在于，所述步骤S1中交换机侦听DHCP主机的IP地址请求过程建立DHCP绑定表的步骤包括：

交换机侦听用户的DHCP请求报文，根据所述报文中源MAC地址查询绑定表，如果绑定表中存在该MAC地址，将报文从可信端口转发出去；如绑定表中不存在该MAC地址，交换机创建一个临时的REQUEST绑定，记录用户的MAC地址、端口信息和虚拟局域网标识信息，将报文从可信端口转发出去；

交换机侦听服务器返回的DHCP应答报文，根据报文中的目的MAC地址查询REQUEST绑定表，如果存在相同用户MAC地址，创建一个包括用户IP、MAC地址、虚拟局域网标识和接收端口信息的绑定信息。

3.根据权利要求1所述的防止IGMP欺骗和攻击的方法，其特征在于，所述交换机上配置的IGMP信任端口为上联组播路由器的端口。

4.根据权利要求1所述的防止IGMP欺骗和攻击的方法，其特征在于，所述步骤S3中交换机接收IGMP普通组查询报文并解析，如报文接收端口与预先配置的信任端口不一致，则判断报文为非法报文，将所述报文丢弃；如报文接收端口与预先配置的信任端口一致，则将所述报文向其所在虚拟局域网内除接收端口外的所有端口转发。

5.根据权利要求1所述的防止IGMP欺骗和攻击的方法，其特征在于，所述步骤S4中交换机接收IGMP成员关系报告报文并解析，判断报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息是否匹配，同时，根据报文源主机IP查询所述主机IP已请求加入的组播组列表，判断该主机IP已请求加入的组播组数目是否超过预先配置的阈值，如报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息匹配且该主机IP已请求加入的组播组数目未超过预先配置的阈值，则将所述报文通过其所在虚拟局域网内的所有信任端口转发出去；否则，将所述报文丢弃。

6.根据权利要求5所述的防止IGMP欺骗和攻击的方法，其特征在于，所述步骤S4中如报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息匹配且该主机IP已请求加入的组播组数目未超过预先配置的阈值，查询所述报文的组播组地址是否已加入到该主机IP已请求加入的组播组列表中，如在列表中，则通过其所在虚拟局域网内的所有信任端口转发出去；如果不在，则将此组播组地址加入到该IP请求加入的组播组地址列表中，通过其所在虚拟局域网内的所有信任端口转发出去。

7.一种防止IGMP欺骗和攻击的装置，所述装置包括收发模块、重定向模块、绑定表生成模块和判断模块；

所述收发模块用于接收来自主机和服务器的报文并对报文进行转发；

重定向模块用于将收发模块接收到的DHCP报文重定向到绑定表生成模块进行解析，将IGMP报文重定向至判断模块进行解析；

绑定表生成模块用于将DHCP主机的IP地址请求过程中解析出的用户IP、MAC地址、虚拟局域网标识和接收端口信息生成DHCP绑定表；

判断模块用于对重定向的IGMP报文进行解析并判断IGMP报文的解析结果与交换机上配置的IGMP信任端口、每个主机IP允许请求的组播组阈值和DHCP绑定表信息是否匹配，从而判断报文的合法性；

其中，所述判断模块具体用于：在接收到IGMP普通组查询报文时，根据接收端口信息与预先配置的信任端口是否匹配，判断报文的合法性，在接收到IGMP成员关系报告报文时，根据报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息是否匹配，以及该主机IP已请求加入的组播组数目是否超过预先配置的阈值，判断报文的合法性。

8.根据权利要求7所述的防止IGMP欺骗和攻击的装置，其特征在于，在报文类型为IGMP普通组查询报文时，所述判断模块用于：如报文接收端口与预先配置的信任端口不一致，则判断报文为非法报文，将所述报文丢弃；如报文接收端口与预先配置的信任端口一致，则将所述报文向其所在虚拟局域网内除接收端口外的所有端口转发。

9.根据权利要求7所述的防止IGMP欺骗和攻击的装置，其特征在于，在报文类型为IGMP成员关系报告报文时，所述判断模块还用于：根据报文源主机IP查询所述主机IP已请求加入的组播组列表，判断该主机IP已请求加入的组播组数目是否超过预先配置的阈值，如报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息匹配且该主机IP已请求加入的组播组数目未超过预先配置的阈值，则将所述报文通过其所在虚拟局域网内的所有信任端口转发出去；否则，将所述报文丢弃。

10.根据权利要求7所述的防止IGMP欺骗和攻击的装置，其特征在于，所述装置上配置的IGMP信任端口为上联组播路由器的端口。

防止IGMP欺骗和攻击的方法及装置

技术领域

[0001] 本发明涉及计算机数据通信领域，尤其涉及一种防止IGMP欺骗和攻击的方法及装置。

背景技术

[0002] 随着网络宽带技术的不断发展，流媒体数据以其直观性、实用性、互动性等特点广泛应用于视频点播、网络教学、网络直播等诸多业务，这些业务都具有点对多点的特性，对于类似点对多点的业务模式如采用点对点的单播模式进行数据传输，会浪费了大量的网络资源。为了节省网络资源的占用，IP组播技术应时而生，通过IP组播技术，一个系统可以将相同的数据包同时发送到同一组播组内的多个主机上。IGMP(Internet Group Management Protocol，互联网组管理协议)是TCP/IP协议族中负责IP组播成员管理的协议，用来在IP主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。

[0003] 在现有网络环境中，通过动态主机分配协议(Dynamic Host Configuration Protocol，DHCP)来完成用户IP的分配。为了防止DHCP攻击及私设DHCP服务器，一般在交换机中开启DHCP侦听(DHCP SNOOPING)功能，监测DHCP客户端通过DHCP协议获取IP的过程，从而保证用户终端获得合法的IP地址。

[0004] IGMP SNOOPING(Internet Group Management Protocol Snooping，互联网组管理协议侦听)是运行在二层设备上的组播约束机制，用于管理和控制组播组。运行IGMP SNOOPING的二层设备通过对收到的IGMP报文进行分析，为端口和MAC组播地址建立起映射关系，并根据这样的映射关系转发组播数据。IGMP SNOOPING通过二层组播将信息只转发给有需要的接收者，减少了二层网络中的广播报文，节约了网络带宽并增强了组播信息的安全性。

[0005] 在IGMP查询器选择中，如果网路上存在多个查询器，则选择IP较小者为网路上唯一的IGMP查询器。如果有非法主机伪造一个源IP较小的IGMP查询器，则根据IGMP协议，此非法主机会被选为合法查询器。如果非法用户伪造的IGMP查询器主机的IGMP离开消息，则在主机离开后，还会有组播流量流向离组播组的主机，造成带宽的浪费；如果有非法主机伪造源IP发送IGMP成员报告报文，将增加网路上组播路由器的CPU负担。此外，即使是拥有合法IP的主机，也可能发动IGMP攻击，该主机发送大量的IGMP成员报告报文，增加网路上组播路由器的CPU负担，占用大量的软件和硬件资源。

[0006] 针对上述IGMP普遍组查询欺骗、IGMP源地址欺骗以及IGMP成员报告报文攻击问题，需要采用一种机制来防止IGMP欺骗和攻击。

发明内容

[0007] 为了克服现有技术的缺陷和不足，本发明提出一种能够有效拦截和阻止IGMP欺骗和攻击的方法及装置。

[0008] 本发明公开一种防止IGMP欺骗和攻击的方法，该方法包括：

[0009] S1：交换机侦听DHCP主机的IP地址请求过程建立包括用户IP、MAC地址、虚拟局域网标识和接收端口信息的DHCP绑定表；

[0010] S2：交换机侦听IGMP报文，判断报文类型，如是IGMP普通组查询报文，则执行步骤S3；如是IGMP成员关系报告报文，则执行步骤S4；

[0011] S3：根据报文接收端口信息与预先配置的信任端口是否匹配，判断报文的合法性；

[0012] S4：根据报文信息与DHCP绑定表信息和每个IP允许加入组播组数目阈值是否匹配，判断报文的合法性。

[0013] 进一步地，所述步骤S1中交换机侦听DHCP主机的IP地址请求过程建立DHCP绑定表的步骤包括：

[0014] 交换机侦听用户的DHCP请求报文，根据所述报文中源MAC地址查询绑定表，如果绑定表中存在该MAC地址，将报文从可信口端转发出去；如绑定表中不存在该MAC地址，交换机创建一个临时的REQUEST绑定，记录用户的MAC地址、端口信息和虚拟局域网标识信息，将报文从可信端口转发出去；

[0015] 交换机侦听服务器返回的DHCP应答报文，根据报文中的目的MAC地址查询REQUEST绑定表，如果存在相同用户MAC地址，创建一个包括用户IP、MAC地址、虚拟局域网标识和接收端口信息的绑定信息。

[0016] 进一步地，所述交换机上配置的IGMP信任端口为上联组播路由器的端口。

[0017] 进一步地，所述步骤S3中交换机接收IGMP普通组查询报文并解析，如报文接收端口与预先配置的信任端口不一致，则判断报文为非法报文，将所述报文丢弃；如报文接收端口与预先配置的信任端口一致，则将所述报文向其所在虚拟局域网内除接收端口外的所有端口转发。

[0018] 进一步地，所述步骤S4中交换机接收IGMP成员关系报告报文并解析，判断报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息是否匹配，同时，根据报文源主机IP查询所述主机IP已请求加入的组播组列表，判断该主机IP已请求加入的组播组数目是否超过预先配置的阈值，如报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息匹配且该主机IP已请求加入的组播组数目未超过预先配置的阈值，则将所述报文通过其所在虚拟局域网内的所有信任端口转发出去；否则，将所述报文丢弃。

[0019] 进一步地，所述步骤S4中如报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息匹配且该主机IP已请求加入的组播组数目未超过预先配置的阈值，查询所述报文的组播组地址是否已加入到该主机IP已请求加入的组播组列表中，如在列表中，则通过其所在虚拟局域网内的所有信任端口转发出去；如果不在，则将此组播组地址加入到该IP请求加入的组播组地址列表中，通过其所在虚拟局域网内的所有信任端口转发出去。

[0020] 本发明还公开一种防止IGMP欺骗和攻击的装置，所述装置包括收发模块、重定向模块、绑定表生成模块和判断模块；

[0021] 所述收发模块用于接收来自主机和服务器的报文并对报文进行转发；

[0022] 重定向模块用于将交换机接收到的DHCP报文重定向到绑定表生成模块进行解析，将IGMP报文重定向至判断模块进行解析；

[0023] 绑定表生成模块用于将DHCP主机的IP地址请求过程中解析出的用户IP、MAC地址、虚拟局域网标识和接收端口信息生成DHCP绑定表；

[0024] 判断模块用于对重定向的IGMP报文进行解析并判断IGMP报文的解析结果与交换机上配置的IGMP信任端口、每个主机IP允许请求的组播组阈值和DHCP绑定表信息是否匹配，从而判断报文的合法性。

[0025] 进一步地，交换机接收IGMP普通组查询报文，判断模块根据接收端口信息与预先配置的信任端口是否匹配，判断报文的合法性：如报文接收端口与预先配置的信任端口不一致，则判断报文为非法报文，将所述报文丢弃；如报文接收端口与预先配置的信任端口一致，则将所述报文向其所在虚拟局域网内除接收端口外的所有端口转发。

[0026] 进一步地，交换机接收IGMP成员关系报告报文，交换机接收IGMP成员关系报告报文并解析，判断报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息是否匹配，同时，根据报文源主机IP查询所述主机IP已请求加入的组播组列表，判断该主机IP已请求加入的组播组数目是否超过预先配置的阈值，如报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息匹配且该主机IP已请求加入的组播组数目未超过预先配置的阈值，则将所述报文通过其所在虚拟局域网内的所有信任端口转发出去；否则，将所述报文丢弃。

[0027] 进一步地，交换机上配置的IGMP信任端口为上联组播路由器的端口。

[0028] 本发明的技术方案有效解决了IGMP普遍组查询欺骗、IGMP源地址欺骗以及IGMP成员报告报文攻击问题，该方法简单易实现，有利于网络的安全运行。

附图说明

[0029] 图1为本发明实施例的防止IGMP欺骗和攻击的系统框图；

[0030] 图2为本发明实施例的交换机的结构框图；

[0031] 图3为本发明实施例的DHCP环境下防止IGMP欺骗和攻击的方法流程图；

[0032] 图4为本发明实施例的步骤S3中防止IGMP普通组查询报文欺骗的方法流程图；

[0033] 图5为本发明一实施例的步骤S4中防止IGMP成员关系报告报文欺骗和攻击的方法流程图；

[0034] 图6为本发明另一实施例的步骤S4中防止IGMP成员关系报告报文欺骗和攻击的方法流程图。

具体实施方式

[0035] 为详细说明本发明的技术内容、所实现目的及效果，以下结合实施方式并配合附图予以详细说明。

[0036] 图1为本发明实施例的DHCP环境下防止IGMP欺骗和攻击的系统框图。该系统包括DHCP主机、交换机、组播路由器、DHCP服务器和组播源，DHCP主机通过交换机与组播路由器连接，组播路由器与组播源连接，组播路由器上联DHCP服务器；其中，所述组播路由器用于发起IGMP成员查询并让有需要的节点做出回应；交换机用于侦听DHCP主机的IP地址请求过程建立包括用户IP、MAC地址、虚拟局域网标识和接收端口信息的DHCP绑定表；所述交换机通过侦听IGMP报文，将IGMP报文重定向到判断模块进行解析，根据报文的解析结果与预先

配置的信任端口、每个主机IP允许请求的组播组阈值和DHCP绑定表是否匹配，判断IGMP报文的合法性，如报文为非法报文，则将报文丢弃；如报文为合法报文，则将报文进行转发，有效解决了IGMP普遍组查询欺骗、IGMP源地址欺骗以及IGMP成员报告报文攻击问题。

[0037] 图2为本发明实施例的交换机的结构框图。交换机基于图1所示系统实现防止IGMP欺骗和攻击的功能。

[0038] 所述交换机包括收发模块、重定向模块、绑定表生成模块和判断模块；所述收发模块用于接收来自主机和服务器的报文并对报文进行转发；重定向模块用于将交换机接收到的DHCP报文重定向到绑定表生成模块进行解析，将IGMP报文重定向至判断模块进行解析；绑定表生成模块用于将DHCP主机的IP地址请求过程中解析出的用户IP、MAC地址、虚拟局域网标识和接收端口信息生成DHCP绑定表；判断模块用于对重定向的IGMP报文进行解析并判断IGMP报文的解析结果与交换机上配置的IGMP信任端口、每个主机IP允许请求的组播组阈值和DHCP绑定表信息是否匹配，从而判断报文的合法性。

[0039] 交换机侦听IGMP报文，判断报文类型并通过重定向模块将IGMP报文重定向到判断模块进行解析，如交换机接收到IGMP普通组查询报文，判断模块则根据接收端口信息与预先配置的信任端口是否匹配，判断报文的合法性：如报文接收端口与预先配置的信任端口不一致，则判断报文为非法报文，将所述报文丢弃；如报文接收端口与预先配置的信任端口一致，则将所述报文向其所在虚拟局域网内除接收端口外的所有端口转发；如交换机接收到IGMP成员关系报告报文，则根据报文信息与DHCP绑定表信息和每个IP允许请求加入的组播组数目阈值是否匹配，判断报文的合法性：如报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息一致且该主机IP已请求加入的组播组数目未超过预先配置的阈值，则将所述报文通过其所在虚拟局域网内的所有信任端口转发出去；否则，将所述报文丢弃。

[0040] 其中，交换机接收IGMP成员关系报告报文并解析，如报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息匹配且该主机IP已请求加入的组播组数目未超过预先配置的阈值，查询所述报文的组播组地址是否已加入到该主机IP已请求加入的组播组列表中，如在列表中，则通过其所在虚拟局域网内的所有信任端口转发出去；如果不在，则将此组播组地址加入到该IP请求加入的组播组地址列表中，通过其所在虚拟局域网内的所有信任端口转发出去，从而防止了IGMP成员关系报告报文的欺骗和攻击。

[0041] 交换机上配置的IGMP信任端口为上联组播路由器的端口，可以为交换机的二层物理端口或者汇聚端口。交换机启用DHCP SNOOPING功能和IGMP SNOOPING功能，侦听DHCP报文和IGMP报文，下发重定向规则，不执行硬件转发行为，将接收到的DHCP报文重定向到绑定表生成模块进行解析，将IGMP报文重定向至判断模块进行解析；绑定表生成模块根据DHCP请求报文及其回应报文的解析结果生成DHCP绑定表，所述DHCP绑定表中每一个绑定信息包括用户IP、MAC地址、虚拟局域网标识和接收端口信息。

[0042] 图3为本发明实施例的DHCP环境下防止IGMP欺骗和攻击的方法流程图。参见图3，该方法包括如下步骤：

[0043] 步骤S301：交换机侦听DHCP主机的IP地址请求过程建立包括用户IP、MAC地址、虚拟局域网标识和接收端口信息的DHCP绑定表。

[0044] 交换机使能DHCP SNOOPING功能，侦听用户的DHCP请求报文，下发重定向规则，重

定向模块将所述DHCP请求报文重定向到绑定表生成模块进行解析，根据报文中源MAC地址查询绑定表，如果绑定表中存在该MAC地址，将所述报文从可信端口转发出去；如绑定表中不存在该MAC地址，交换机创建一个临时的REQUEST绑定，记录用户的MAC地址、接收端口信息和虚拟局域网标识信息，将报文从可信端口转发出去；交换机侦听服务器返回的DHCP应答报文，根据报文中的目的MAC地址查询REQUEST绑定表，如果存在相同用户MAC地址，则创建一个绑定信息，记录DHCP主机的MAC地址、IP地址、租期、虚拟局域网标识和接收端口信息等，绑定表生成模块根据其中的用户IP、MAC地址、虚拟局域网标识和接收端口信息生成DHCP绑定表。

[0045] 步骤S302：交换机侦听IGMP报文，判断IGMP报文类型，如是IGMP普通组查询报文，则执行步骤S303；如是IGMP成员关系报告报文，则执行步骤S304。

[0046] 步骤S303：根据报文接收端口信息与预先配置的信任端口是否匹配，判断报文的合法性。

[0047] 图4为本发明实施例的所述步骤S303中防止IGMP普通组查询报文欺骗的方法流程图。具体步骤为：交换机接收到IGMP普通组查询报文，通过解析得到报文的接收端口信息，由判断模块判断报文接收端口与预先配置的信任端口是否一致，如否，则将所述报文丢弃；如是，则将报文向其所在虚拟局域网内除接收端口外的所有端口转发。

[0048] 其中，预先配置的信任端口为交换机上联组播路由器的端口，所述信任端口可以为交换机的二层物理端口或汇聚端口。

[0049] 步骤S304：根据报文信息与DHCP绑定表信息和每个IP允许加入组播组数目阈值是否匹配，判断报文的合法性。

[0050] 图5为本发明一实施例的所述步骤S304中防止IGMP成员关系报告报文欺骗和攻击的方法流程图。具体步骤为：交换机接收IGMP成员关系报告报文，通过对报文解析，从报文的IP首部获取源IP地址，从以太网头获取源MAC地址，并记录接收报文的虚拟局域网标识和接收端口信息，由判断模块判断报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息是否匹配，同时，判断模块根据报文源主机IP查询所述主机IP已请求加入的组播组列表，判断该主机IP已请求加入的组播组数目是否超过预先配置的阈值，如报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息匹配且该主机IP已请求加入的组播组数目未超过预先配置的阈值，则将所述报文通过其所在虚拟局域网内的所有信任端口转发出去；否则，将所述报文丢弃，从而有效防止IGMP成员关系报告报文的欺骗和攻击行为。

[0051] 其中，如报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息匹配且该主机IP已请求加入的组播组数目未超过预先配置的阈值时，查询所述报文的组播组地址是否已加入到该主机IP已请求加入的组播组列表中，如在列表中，则通过其所在虚拟局域网内的所有信任端口转发出去；如果不在，则将此组播组地址加入到该IP请求加入的组播组地址列表中，通过其所在虚拟局域网内的所有信任端口转发出去。

[0052] 图6为本发明另一实施例的所述步骤S304中防止IGMP成员关系报告报文欺骗和攻击的方法流程图。该实施例按照先后顺序判断IGMP成员关系报告报文的合法性，具体步骤为：交换机接收IGMP成员关系报告报文，通过对报文解析，从报文的IP首部获取源IP地址，从以太网头获取源MAC地址，并记录接收报文的虚拟局域网标识和接收端口信息，由判断模

块判断报文源主机IP、源MAC地址、虚拟局域网标识和接收端口信息与DHCP绑定表中信息是否匹配，如否，则将所述报文丢弃；如是，则查询所述IP已请求加入的组播组列表，判断该IP已请求加入的组播组数目是否超过预先配置的阈值，如是，则将所述报文丢弃；如否，则根据报文源IP地址查询所述报文的组播组地址是否已加入到该主机IP已请求加入的组播组列表中，如在列表中，则通过其所在虚拟局域网内的所有信任端口转发出去；如果不在，则将此组播组地址加入到该IP请求加入的组播组地址列表中，通过其所在虚拟局域网内的所有信任端口转发出去，有效防止了IGMP成员关系报告报文的欺骗和攻击。

[0053] 其中，每个主机IP允许请求的组播组阈值在交换机上预先配置，所述阈值可根据组播系统的复杂程度或具体情况进行设置，如设阈值为K，K值可选，如5、10等。

[0054] 本发明的技术方案有效解决了IGMP普遍组查询欺骗、IGMP源地址欺骗以及IGMP成员报告报文攻击问题，该方法简单易实现，有利于网络的安全运行。

[0055] 上述仅为本发明的较佳实施例及所运用技术原理，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围内。

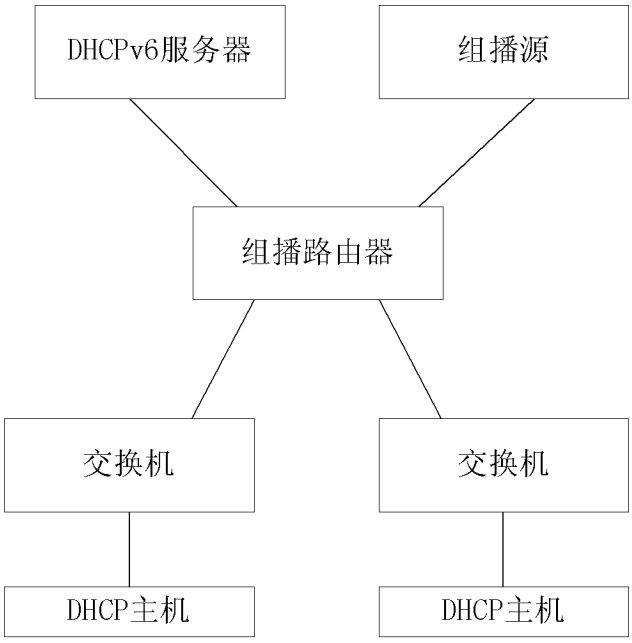

DHCPv6服务器
组播源
组播路由器
交换机
交换机
DHCP主机
DHCP主机

图1

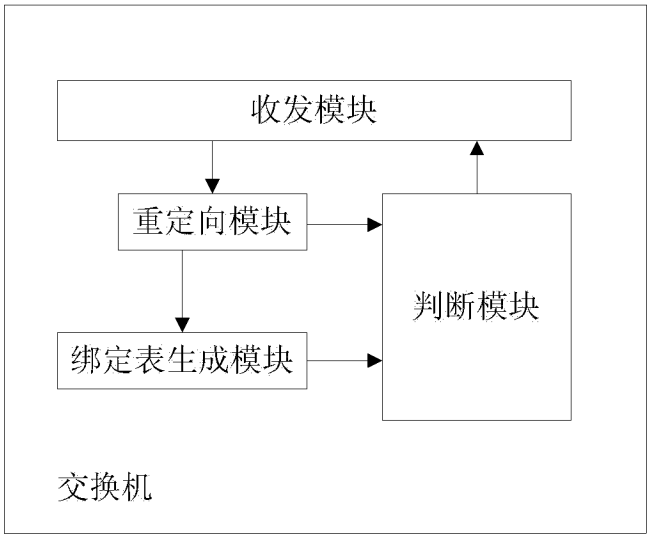

收发模块
重定向模块
判断模块
绑定表生成模块
交换机

图2

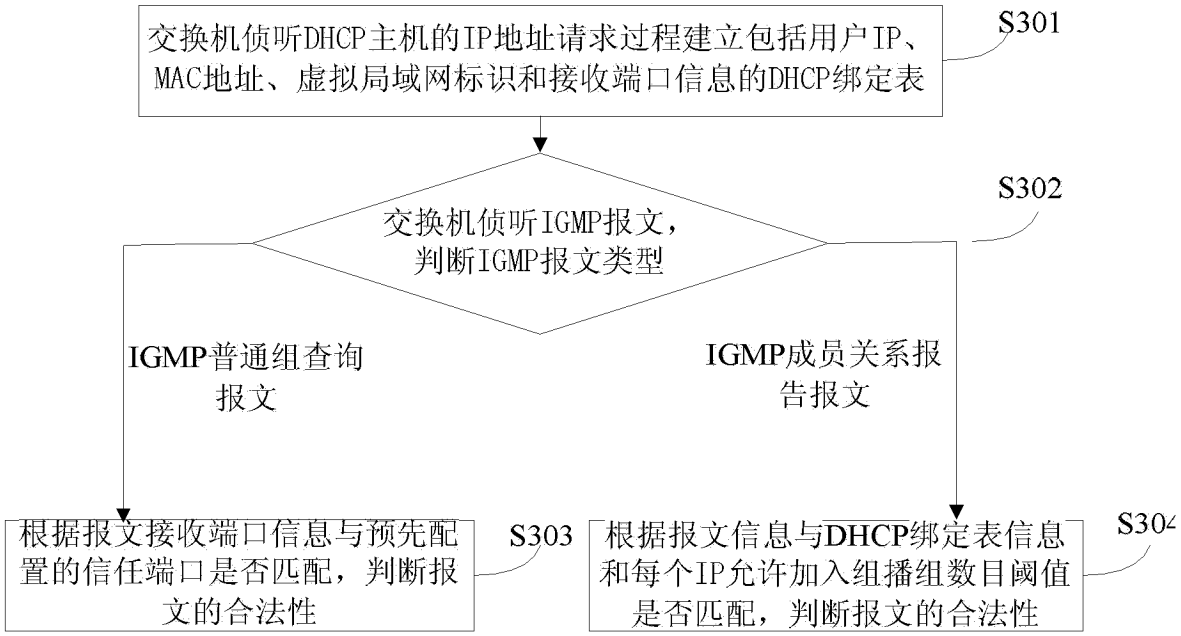

交换机侦听DHCP主机的IP地址请求过程建立包括用户IP、MAC地址、虚拟局域网标识和接收端口信息的DHCP绑定表
S301
交换机侦听IGMP报文，判断IGMP报文类型
S302
IGMP普通组查询报文
IGMP成员关系报告报文
根据报文接收端口信息与预先配置的信任端口是否匹配，判断报文的合法性
S303
根据报文信息与DHCP绑定表信息和每个IP允许加入组播组数目阈值是否匹配，判断报文的合法性
S304

图3

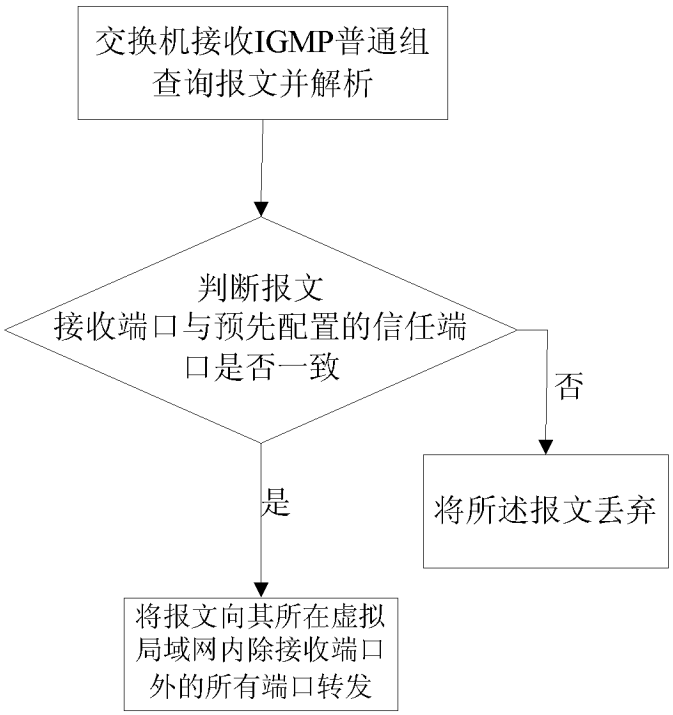

交换机接收IGMP普通组查询报文并解析
判断报文接收端口与预先配置的信任端口是否一致
否
是
将所述报文丢弃
将报文向其所在虚拟局域网内除接收端口外的所有端口转发

图4

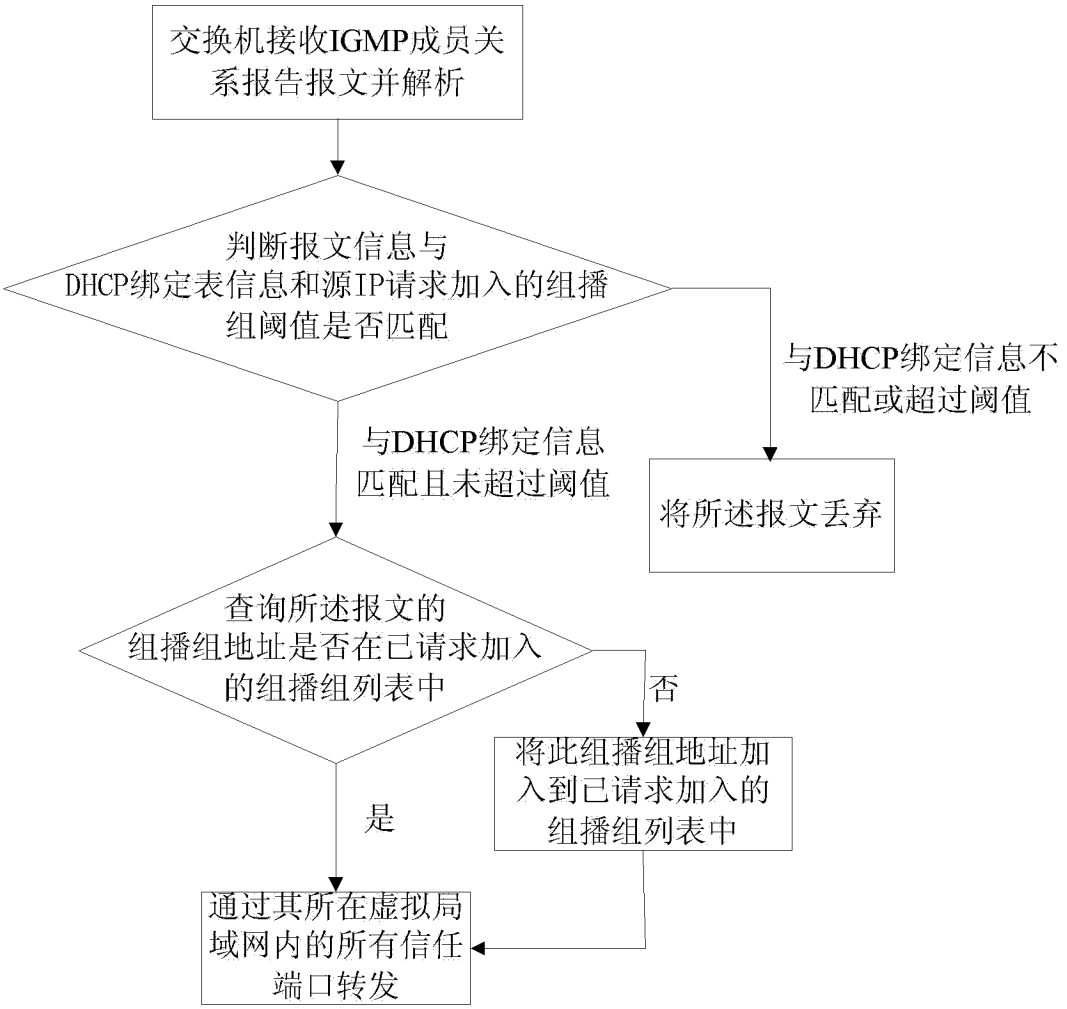

交换机接收IGMP成员关系报告报文并解析
判断报文信息与DHCP绑定表信息和源IP请求加入的组播组阈值是否匹配
与DHCP绑定信息不匹配或超过阈值
将所述报文丢弃
与DHCP绑定信息匹配且未超过阈值
查询所述报文的组播组地址是否在已请求加入的组播组列表中
否
将此组播组地址加入到已请求加入的组播组列表中
是
通过其所在虚拟局域网内的所有信任端口转发

图5

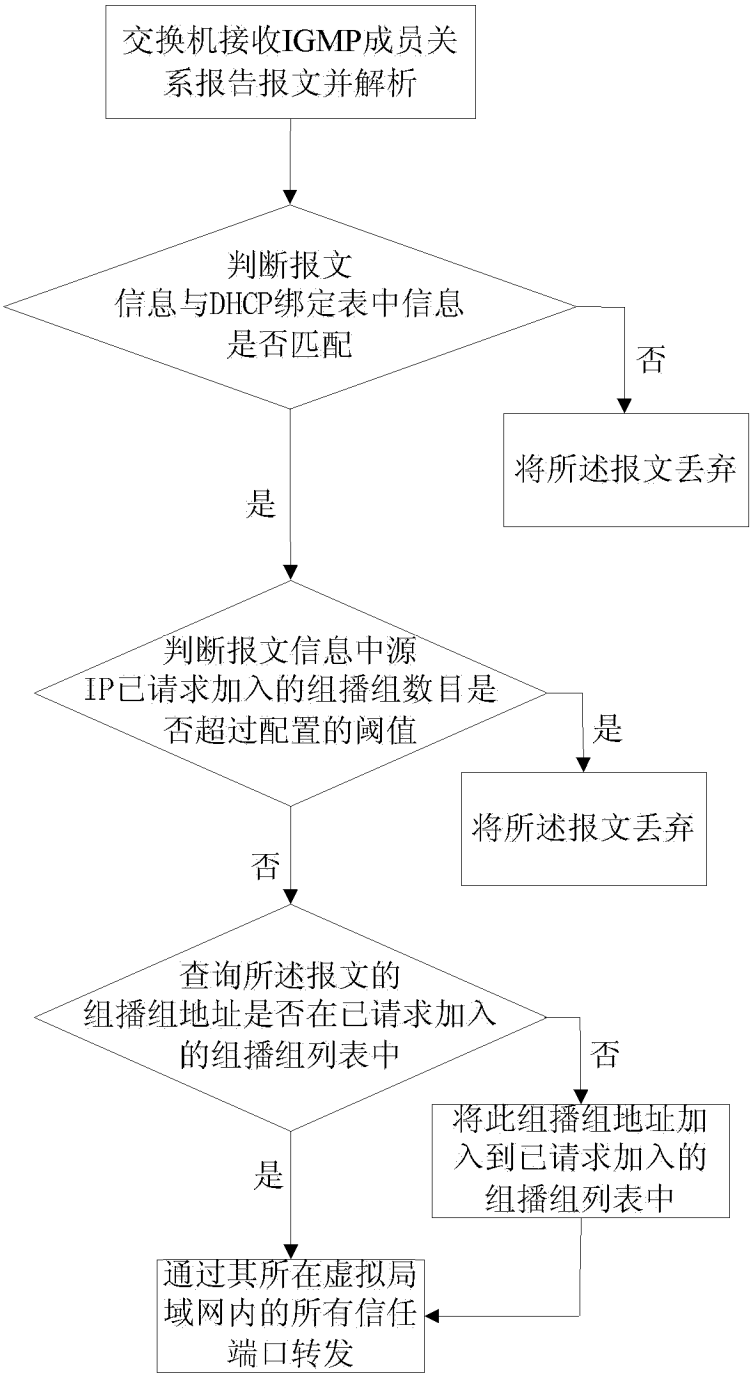

交换机接收IGMP成员关系报告报文并解析
判断报文信息与DHCP绑定表中信息是否匹配
否
将所述报文丢弃
是
判断报文信息中源IP已请求加入的组播组数目是否超过配置的阈值
是
将所述报文丢弃
否
查询所述报文的组播组地址是否在已请求加入的组播组列表中
否
将此组播组地址加入到已请求加入的组播组列表中
是
通过其所在虚拟局域网内的所有信任端口转发

图6