(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 102594834 B
(45)授权公告日 2014.09.10

(21)申请号 201210062417.1
(22)申请日 2012.03.09
(73)专利权人 北京星网锐捷网络技术有限公司
地址 100036 北京市海淀区复兴路29号中意鹏奥大厦东楼11层
(72)发明人 赖鹏飞
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 黄志华
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
CN 101415002 A,2009.04.22, 全文.
CN 101951367 A,2011.01.19, 全文.
WO 2011020254 A1,2011.02.24, 全文.
CN 101039176 A,2007.09.19, 全文.
审查员 尤一名

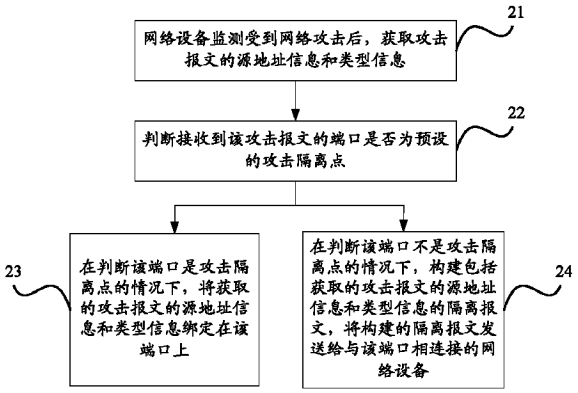
权利要求书5页 说明书15页 附图8页

(54)发明名称

网络攻击的防御方法及装置、网络设备

(57)摘要

本发明公开了一种网络攻击的防御方法及装置、网络设备，其中，该方法包括：网络设备监测受到网络攻击后，获取攻击报文的源地址信息和类型信息；判断接收到该攻击报文的端口是否为预设的攻击隔离点；在判断该端口是攻击隔离点的情况下，将获取的攻击报文的源地址信息和类型信息绑定在该端口上；否则，构建包括获取的攻击报文的源地址信息和类型信息的隔离报文，将构建的隔离报文发送给与该端口相连接的网络设备。该方法能够通过预设为攻击隔离点的端口过滤掉攻击报文，减少网络中多余的攻击报文，从而能够解决现有技术中网络中转发大量的攻击报文浪费网络带宽资源、占用网络设备系统处理资源的问题。



CN 102594834 B

1. 一种网络攻击的防御方法，其特征在于，包括：

网络设备监测受到网络攻击后，获取攻击报文的源地址信息和类型信息；

判断接收到该攻击报文的端口是否为预设的攻击隔离点，所述攻击隔离点为网络设备上接收到攻击报文的端口；

在判断该端口是攻击隔离点的情况下，将获取的攻击报文的源地址信息和类型信息绑定在该端口上；

在判断该端口不是攻击隔离点的情况下，构建包括获取的攻击报文的源地址信息和类型信息的隔离报文，将构建的隔离报文发送给与该端口相连接的网络设备。

2. 根据权利要求 1 所述的方法，其特征在于，所述攻击报文的源地址信息包括：所述攻击报文的源互联网协议 IP 地址信息；

将构建的隔离报文发送给与该端口相连接的网络设备，具体包括：

根据所述攻击报文的源 IP 地址信息、判断网络设备与源攻击设备是否处于直连网段，在判断处于直连网段的情况下，将该隔离报文组播发送给与所述端口相连接的网络设备，在判断处于非直连网段的情况下，将该隔离报文单播发送给与所述端口相连接的、转发所述攻击报文的网络设备。

3. 根据权利要求 2 所述的方法，其特征在于，所述攻击报文的源地址信息还包括：攻击报文的源媒体接入控制 MAC 地址信息；

在判断处于非直连网段的情况下，将该隔离报文单播发送给与所述端口相连接的、转发所述攻击报文的网络设备，具体包括：

将该隔离报文中的攻击报文源 MAC 地址信息设置为零，将设置后的隔离报文单播发送给与所述端口相连接的、转发所述攻击报文的网络设备。

4. 根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

在预定时间内未接收到隔离成功消息的情况下，在构建的隔离报文中添加用于指示找不到攻击隔离点的信息，将添加信息后的隔离报文组播发送给与接收到攻击报文的端口相连接的网络设备。

5. 根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

在接收到携带有隔离失败信息的隔离报文后，将隔离报文中的攻击报文源地址信息和类型信息绑定在接收到携带有隔离失败信息的隔离报文的端口上。

6. 根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

在所述接收到攻击报文的端口是攻击隔离点，并且存在多个源地址信息相同、类型不同的攻击报文的情况下，将攻击报文的源地址信息绑定在该端口上。

7. 一种网络攻击的防御装置，其特征在于，包括：

获取模块，用于在网络设备监测受到攻击后，获取攻击报文的源地址信息和类型信息；

第一判断模块，用于判断接收到该攻击报文的端口是否预设为攻击隔离点，所述攻击隔离点为网络设备上接收到攻击报文的端口；

绑定模块，用于在所述第一判断模块判断该端口是攻击隔离点的情况下，将所述获取模块获取的攻击报文的源地址信息和类型信息绑定在该端口上；

构建模块，用于在所述第一判断模块判断该端口不是攻击隔离点的情况下，构建包括

所述获取模块获取的攻击报文的源地址信息和类型信息的隔离报文；

发送模块，用于将所述构建模块构建的隔离报文发送给与该端口相连接的网络设备。

8. 根据权利要求 7 所述的装置，其特征在于，所述装置还包括：

第二判断模块，用于根据所述获取模块获取的攻击报文的源地址信息中的源互联网协议 IP 地址信息，判断网络设备与源攻击设备是否处于直连网段；

所述发送模块，具体用于在所述第二判断模块判断处于直连网段的情况下，将该隔离报文组播发送给与所述端口相连接的网络设备，在判断处于非直连网段的情况下，将该隔离报文单播发送给与所述端口相连接的、转发所述攻击报文的网络设备。

9. 根据权利要求 8 所述的装置，其特征在于，所述装置还包括：

设置模块，用于在所述第二判断模块判断处于非直连网段的情况下，将所述构建模块构建的隔离报文中的攻击报文源地址信息的源媒体接入控制 MAC 地址信息设置为零；

所述发送模块，具体用于将所述设置模块设置后的隔离报文单播发送给与所述端口相连接的、转发所述攻击报文的网络设备。

10. 根据权利要求 7 所述的装置，其特征在于，所述装置还包括：

接收模块，用于接收隔离成功报文；

定时器，用于对所述接收模块接收到隔离成功报文的预定时长进行定时；

设置模块，用于在所述定时器超时、所述接收模块未接收到隔离成功报文的情况下，在所述构建模块构建的隔离报文中添加用于指示找不到攻击隔离点的信息；

所述发送模块，还用于将所述设置模块添加信息后的隔离报文、组播发送给与接收到攻击报文的端口相连接的网络设备。

11. 根据权利要求 7 所述的装置，其特征在于，所述装置还包括：

接收模块，用于接收携带有隔离失败信息的隔离报文；

所述绑定模块，还用于在所述接收模块接收到携带有隔离失败信息的隔离报文后，将该隔离报文中的攻击报文源地址信息和类型信息绑定在接收到携带有隔离失败信息的隔离报文的端口上。

12. 根据权利要求 7 所述的装置，其特征在于，所述绑定模块，还用于在所述第一判断模块判断接收到所述攻击报文的端口是攻击隔离点，并且存在多个源地址信息相同、类型不同的攻击报文的情况下，将攻击报文的源地址信息绑定在该端口上。

13. 一种网络攻击的防御方法，其特征在于，包括：

网络设备接收到隔离报文后，根据该隔离报文中的攻击报文源地址信息，判断网络设备接收到该隔离报文中所指示的攻击报文的端口是否为预设的攻击隔离点，所述攻击隔离点为网络设备上接收到攻击报文的端口；

在判断该端口是攻击隔离点的情况下，将该隔离报文中的攻击报文源地址信息和类型信息绑定在该端口上；

在判断该端口不是攻击隔离点的情况下，将接收到的隔离报文发送给与该端口相连接的网络设备。

14. 根据权利要求 13 所述的方法，其特征在于，所述攻击报文的源地址信息包括：所述攻击报文的源互联网协议 IP 地址信息；

在判断该端口不是攻击隔离点的情况下，将接收到的隔离报文发送给与接收到所述攻

击报文的端口相连接的网络设备，具体包括：

根据隔离报文中的攻击报文源 IP 地址信息、判断网络设备与该攻击报文源 IP 地址信息所指的网络设备是否处于直连网段，在判断处于直连网段的情况下，将该隔离报文组播发送给与接收到所述攻击报文的端口相连接的网络设备，在判断处于非直连网段的情况下，将该隔离报文单播发送给与接收到所述攻击报文的端口相连接的、转发所述攻击报文的网络设备。

15. 根据权利要求 14 所述的方法，其特征在于，在判断处于直连网段的情况下，将该隔离报文组播发送给与接收到所述攻击报文的端口相连接的网络设备，具体包括：

根据所述攻击报文的源 IP 地址信息、查找到与该源 IP 地址信息相对应的攻击报文的源媒体接入控制 MAC 地址信息，将该源 MAC 地址信息添加到所述隔离报文中，将携带有所述攻击报文源 MAC 地址信息的隔离报文组播发送给与接收到所述攻击报文的端口相连接的网络设备。

16. 根据权利要求 13 所述的方法，其特征在于，所述方法还包括：

在接收到所述攻击报文的端口是攻击隔离点的情况下，在监测该端口对所述攻击报文过滤失败后，在所述隔离报文中添加隔离失败信息，将添加了隔离失败信息的隔离报文发送给与接收到隔离报文的端口相连接的网络设备；

网络设备在接收到携带有隔离失败信息的隔离报文后，将隔离报文中的攻击报文源地址信息和类型信息绑定在接收到携带有隔离失败信息的隔离报文的端口上。

17. 根据权利要求 13 所述的方法，其特征在于，所述方法还包括：

在接收到所述攻击报文的端口是攻击隔离点的情况下，将源地址信息相同、类型不同的多个攻击报文合并为一条记录绑定在该端口上。

18. 根据权利要求 13 所述的方法，其特征在于，所述方法还包括：

接收到携带有找不到攻击隔离点信息的隔离报文后，将该隔离报文中的攻击报文源地址信息和类型信息绑定在接收到该隔离报文中所指示的攻击报文的端口上，并将接收到的该隔离报文组播发送给与接收到该隔离报文中所指示的攻击报文的端口相连接的网络设备。

19. 根据权利要求 13 所述的方法，其特征在于，所述隔离报文中还包括攻击报文的目的地址信息；

所述方法还包括：

在监测到所述端口对所述攻击报文过滤成功后，向攻击报文的目的地址信息所指的网络设备发送隔离成功消息。

20. 一种网络攻击的防御装置，其特征在于，包括：

接收模块，用于接收隔离报文；

第一判断模块，用于根据所述接收模块接收到的隔离报文中的攻击报文源地址信息、判断网络设备接收到该隔离报文所指示的攻击报文的端口是否为预设的攻击隔离点，所述攻击隔离点为网络设备上接收到攻击报文的端口；

绑定模块，用于在所述第一判断模块判断该端口是攻击隔离点的情况下，将所述接收模块接收到的隔离报文中的攻击报文源地址信息和类型信息绑定在该端口上；

发送模块，用于在所述第一判断模块判断该端口不是攻击隔离点的情况下，将所述接

收模块接收到的隔离报文发送给与接收到所述攻击报文的端口相连接的网络设备。

21. 根据权利要求 20 所述的装置，其特征在于，所述装置还包括：

第二判断模块，用于根据所述接收模块接收到的隔离报文中的攻击报文源互联网协议 IP 地址信息、判断网络设备与该攻击报文源 IP 地址信息所指的网络设备是否处于直连网段；

所述发送模块，具体用于在所述第二判断模块判断处于直连网段的情况下，将所述接收模块接收到的隔离报文组播发送给与接收到所述攻击报文的端口相连接的网络设备，在所述第二判断模块判断处于非直连网段的情况下，将所述接收模块接收到的隔离报文单播发送给与接收到所述攻击报文的端口相连接的、转发所述攻击报文的网络设备。

22. 根据权利要求 21 所述的装置，其特征在于，所述装置还包括：

查找模块，用于根据所述接收模块接收到的隔离报文中的攻击报文的源 IP 地址信息、查找到与该源 IP 地址信息相对应的攻击报文的源媒体接入控制 MAC 地址信息；

设置模块，用于将所述查找模块查找到的攻击报文的源 MAC 地址信息添加到所述接收模块接收到的隔离报文中；

所述发送模块，具体用于将所述设置模块添加了攻击报文源 MAC 地址信息后的隔离报文组播发送给与接收到所述攻击报文的端口相连接的网络设备。

23. 根据权利要求 20 所述的装置，其特征在于，所述装置还包括：

监测模块，用于对端口过滤攻击报文的情况进行监测；

设置模块，用于在第一判断模块判断接收到所述攻击报文的端口是攻击隔离点的情况下，所述监测模块监测该接收到所述攻击报文的端口对所述攻击报文过滤失败后，在所述接收模块接收到的隔离报文中添加隔离失败信息；

所述发送模块，还用于将所述设置模块添加了隔离失败信息后的隔离报文发送给与接收到隔离报文的端口相连接的网络设备；

所述接收模块，还用于接收携带有隔离失败信息的隔离报文；

所述绑定模块，还用于在所述接收模块接收到携带有隔离失败信息的隔离报文后，将该隔离报文中的攻击报文源地址信息和类型信息、绑定在接收到携带有隔离失败信息的隔离报文的端口上。

24. 根据权利要求 20 所述的装置，其特征在于，所述绑定模块，还用于在所述第一判断模块判断所述接收到攻击报文的端口是攻击隔离点，并且存在多个源地址信息相同、类型不同的攻击报文的情况下，将攻击报文的源地址信息绑定在该端口上。

25. 根据权利要求 20 所述的装置，其特征在于，所述接收模块，还用于接收携带有找不到攻击隔离点信息的隔离报文；

所述绑定模块，还用于将所述接收模块接收到的该隔离报文中的攻击报文源地址信息和类型信息绑定在接收到该隔离报文中所指示的攻击报文的端口上；

所述发送模块，还用于将所述接收模块接收到的该隔离报文组播发送给与接收到该隔离报文中所指示的攻击报文的端口相连接的网络设备。

26. 根据权利要求 20 所述的装置，其特征在于，所述装置还包括：

监测模块，用于对端口过滤攻击报文的情况进行监测；

所述发送模块，还用于在所述监测模块监测所述端口对所述攻击报文过滤成功后，向

攻击报文的目的地址信息所指的网络设备发送隔离成功消息。

27. 一种网络设备，其特征在于，包括如权利要求 7 至 12 中任一项所述的网络攻击的防御装置、和 / 或如权利要求 20 至 26 中任一项所述的网络攻击的防御装置。

网络攻击的防御方法及装置、网络设备

技术领域

[0001] 本发明涉及数据通信系统，具体地，涉及一种网络攻击的防御方法及装置、网络设备。

背景技术

[0002] 目前，在大型网络中，通常在接入交换机上部署接入控制安全功能，以防御网络攻击。例如，在如图 1 中所示的网络中，接入交换机 SW1 通过 Port1-Port4 连接个人电脑 (PC，Personal Computer)PC1-PC4，接入交换机 SW2 通过 Port1-Port3 连接 PC5-PC7，SW1 分别通过 Port5、Port6 连接至汇聚交换机 SW3 的 Port1、SW4 的 Port1，SW2 通过 Port4 连接至汇聚交换机 SW5 的 Port1，SW3 与 SW4 之间均通过 Port2 连接，SW3 通过 port3 连接至核心交换机 SW8 的 port2，SW4 通过 port3 连接至 SW8 的 port1，SW5 通过 port2 连接至核心交换机 SW6 的 port1，SW6 与核心交换机 SW7 分别通过 port2 连接，SW6 与 SW8 分别通过 port3 连接，SW8 通过 port4 与 SW7 的 port1 连接，在接入交换机 SW1、SW2 上部署接入控制安全功能，例如 802.1x、WEB 认证等，能够有效地控制接入 PC 的身份合法性，接入交换机只转发来自合法的互联网协议 (IP，Internet Protocol) 和媒体接入控制 (MAC，Media Access Control) 地址的 PC 发出的报文。

[0003] 目前虽然通过控制用户的身份能够防御非法用户发起的网络攻击，但是，上述方法无法防御具备合法身份的用户发起的攻击，即具备合法的 IP+MAC 地址的 PC，也发起非法的网络攻击，这种可能是用户有意的攻击、也可能是因为感染病毒后由病毒自动发起的攻击。例如图 1 所示，PC1 使用合法的 IP+MAC 正在对核心交换机 SW7 攻击，攻击报文由 PC1 发至 SW1 的 port1，SW1 将攻击报文经由 port5 发至 SW3 的 port1，SW3 将攻击报文经由 port3 发至 SW8 的 port2，SW8 将攻击报文经由 port4 发至 SW7 的 port1。目前，现有技术中有两种方法来应对由合法用户发起的网络攻击，具体如下所述。

[0004] 第一种方法是在交换机 SW7 上配置基础网络保护策略 (NFPP，Network Foundation Protection Policy) 来防御合法用户发起的网络攻击，该策略能够对攻击报文进行限速、对攻击用户进行隔离。但是这种方法只是对攻击报文进行限速，攻击报文依然在网络中存在，极大的浪费了网络的带宽，例如，在图 1 中，SW7 所处的位置是核心交换机，下联的用户比较多，若存在大量攻击的话，需要浪费很多的硬件资源去隔离这些攻击用户，若被攻击者为路由器，每个攻击报文都会送给 SW7 的 CPU，需要使用 SW7 软件资源对攻击源进行判断是否过滤，极大地占用了软件资源，降低了 CPU 处理正常业务的性能，并且即使隔离了该报文对 SW7 造成的攻击，该攻击报文流依然在网络中存在，极大地浪费了网络的带宽。

[0005] 第二种方法是被攻击的设备通过发送告警信息给网络管理员，由网络管理员去查找攻击者具体在哪台交换机上，然后在该交换机上通过手动绑定一条过滤表项、来过滤掉该攻击源，或者通过对称多处理器结构 (SMP，Symmetric Multi-Processor) 服务器来对交换机下发阻断策略，过滤掉该攻击报文。但是，这种方法需要人工来查找定位攻击源，处理过程费时费力效率低下。

[0006] 综上所述，可见在现有技术中，对于合法用户发起的攻击、网络中存在大量转发的攻击报文、浪费网络带宽资源、占用网络设备系统处理资源的问题。

发明内容

[0007] 有鉴于此，本发明实施例提供了一种网络攻击的防御方法，用以解决现有技术中对于合法用户发起的攻击、网络中存在大量转发的攻击报文、浪费网络带宽资源、占用网络设备系统处理资源的问题。

[0008] 相应地，本发明实施例还提供了一种网络攻击的防御装置及网络设备。

[0009] 本发明实施例的技术方案如下：

[0010] 一种网络攻击的防御方法，包括：网络设备监测受到网络攻击后，获取攻击报文的源地址信息和类型信息；判断接收到该攻击报文的端口是否为预设的攻击隔离点；在判断该端口是攻击隔离点的情况下，将获取的攻击报文的源地址信息和类型信息绑定在该端口上；在判断该端口不是攻击隔离点的情况下，构建包括获取的攻击报文的源地址信息和类型信息的隔离报文，将构建的隔离报文发送给与该端口相连接的网络设备。

[0011] 一种网络攻击的防御装置，包括：获取模块，用于在网络设备监测受到攻击后，获取攻击报文的源地址信息和类型信息；第一判断模块，用于判断接收到该攻击报文的端口是否预设为攻击隔离点；绑定模块，用于在所述第一判断模块判断该端口是攻击隔离点的情况下，将所述获取模块获取的攻击报文的源地址信息和类型信息绑定在该端口上；构建模块，用于在所述第一判断模块判断该端口不是攻击隔离点的情况下，构建包括所述获取模块获取的攻击报文的源地址信息和类型信息的隔离报文；发送模块，用于将所述构建模块构建的隔离报文发送给与该端口相连接的网络设备。

[0012] 一种网络攻击的防御方法，包括：网络设备接收到隔离报文后，根据该隔离报文中的攻击报文源地址信息，判断网络设备接收到该隔离报文中所指示的攻击报文的端口是否为预设的攻击隔离点；在判断该端口是攻击隔离点的情况下，将该隔离报文中的攻击报文源地址信息和类型信息绑定在该端口上；在判断该端口不是攻击隔离点的情况下，将接收到的隔离报文发送给与该端口相连接的网络设备。

[0013] 一种网络攻击的防御装置，包括：接收模块，用于接收隔离报文；第一判断模块，用于根据所述接收模块接收到的隔离报文中的攻击报文源地址信息、判断网络设备接收到该隔离报文所指示的攻击报文的端口是否为预设的攻击隔离点；绑定模块，用于在所述第一判断模块判断该端口是攻击隔离点的情况下，将所述接收模块接收到的隔离报文中的攻击报文源地址信息和类型信息绑定在该端口上；发送模块，用于在所述第一判断模块判断该端口不是攻击隔离点的情况下，将所述接收模块接收到的隔离报文发送给与接收到所述攻击报文的端口相连接的网络设备。

[0014] 一种网络设备，包括如上所述的第一种网络攻击的防御装置和／或第二种网络攻击的防御装置。

[0015] 在本发明实施例中，受到网络攻击的网络设备判断接收到攻击报文的端口为预设的攻击隔离点时，将攻击报文的源地址信息和类型信息绑定在该端口上，判断该端口不是预设的攻击隔离点时，构建包括获取攻击报文的源地址信息和类型信息的隔离报文，将构建的隔离报文发送给与该端口相连接的网络设备；接收到隔离报文的网络设备，判断接收

到攻击报文的端口为预设的攻击隔离点时，将攻击报文的源地址信息和类型信息绑定在该端口上，判断该端口不是预设的攻击隔离点时，将接收到的隔离报文发送给与接收到攻击报文的端口相连接的网络设备，能够通过预设为攻击隔离点的端口过滤掉攻击报文，能够减少网络中多余转发的攻击报文，释放网络带宽资源、提高网络带宽的利用率，减少占用的网络设备系统处理资源、提高网络设备系统处理资源的利用率，从而能够解决现有技术中、对于合法用户发起的攻击、网络中存在大量转发的攻击报文、浪费网络带宽资源、占用网络设备系统处理资源的问题。

[0016] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0017] 图 1 为现有技术中网络拓扑结构示意图；

[0018] 图 2 为根据本发明实施例的网络攻击的防御方法的工作流程图；

[0019] 图 3 为图 2 所示方法的优选实施处理方式的工作流程图；

[0020] 图 4 为根据本发明实施例的网络攻击的防御装装置的结构框图；

[0021] 图 5 为图 4 所示装置的优选实施方式的结构框图；

[0022] 图 6 为根据发明实施例的网络攻击的防御方法的另一种工作流程图；

[0023] 图 7 为图 6 所示方法的优选实施处理方式的工作流程图；

[0024] 图 8 为根据本发明实施例的网络攻击的防御装置的结构框图；

[0025] 图 9 为图 8 所示装置的优选实施方式的结构框图；

[0026] 图 10 为根据本发明实施例具体应用的网络攻击的防御系统的结构示意图。

具体实施方式

[0027] 以下结合附图对本发明的实施例进行说明，应当理解，此处所描述的实施例仅用于说明和解释本发明，并不用于限定本发明。

[0028] 针对现有技术中、对于合法用户发起的攻击、网络中存在大量转发的攻击报文、浪费网络带宽资源、占用系统处理资源的问题，本发明实施例提出了一种网络攻击的防御方案，以解决该问题。

[0029] 本发明实施例提供的网络攻击的防御方案中，首先提供了一种对攻击报文的隔离机制。

[0030] 该隔离机制包括：预先将选定的网络设备的端口设置为攻击隔离点；网络设备受到网络攻击后，判断接收到攻击报文的端口为预先设置的攻击隔离点时，将攻击报文的源地址信息和类型信息绑定在该端口上，以使该端口对后续接收到的攻击报文进行过滤隔离，判断接收到攻击报文的端口不是预设的攻击隔离点时，构建包括攻击报文的源地址信息和类型信息的隔离报文，将该隔离报文发送给与该端口相连接的网络设备；接收到隔离报文的网络设备，判断接收到隔离报文中所指示的攻击报文的端口是预设的攻击隔离点时，将隔离报文中携带的攻击报文的源地址信息和类型信息绑定在接收到攻击报文的端口上，以使该端口对后续接收到的攻击报文进行过滤隔离，判断该端口不是预设的攻击隔离

点时，将接收到的隔离报文发送给与该端口相连接的网络设备。通过上述方案，能够通过预设的攻击隔离点（即网络设备上接收到攻击报文的端口）将攻击报文隔离在该攻击隔离点之外，减少网络中多余转发的攻击报文、提高网络带宽利用率，减少攻击报文占用的网络系统资源、提高网络系统处理资源的利用率。

[0031] 本发明实施例提供的网络攻击的防御方案中，还提供了一种隔离确认机制和一种隔离无效后的补救机制。

[0032] 下面对本发明实施例进行详细说明。

[0033] 图 2 示出了根据本发明实施例的网络攻击的防御方法的工作流程图，如图 1 所示，该方法包括如下处理过程。

[0034] 步骤 21、网络设备监测受到网络攻击后，获取攻击报文的源地址信息和类型信息；

[0035] 步骤 22、判断接收到该攻击报文的端口是否为预设的攻击隔离点；

[0036] 步骤 23、在判断该端口是攻击隔离点的情况下，将获取的攻击报文的源地址信息和类型信息绑定在该端口上；

[0037] 步骤 24、在判断该端口不是攻击隔离点的情况下，构建包括获取的攻击报文的源地址信息和类型信息的隔离报文，将构建的隔离报文发送给与该端口相连接的网络设备。

[0038] 网络设备受到网络攻击后，在判断接收到攻击报文的端口是预设的攻击隔离点的情况下，将攻击报文的源地址信息和类型信息绑定在该端口上，以使该端口对后续接收到的攻击报文进行过滤隔离，能够对合法用户发送的网络攻击报文进行隔离，并将攻击报文隔离在网络设备上预设为攻击隔离点的端口之外，减少网络上多余转发的攻击报文、减少攻击报文占用的网络带宽、提高网络带宽的利用率，减少网络设备对攻击报文的处理、释放网络设备的系统处理资源、提高网络设备的系统处理效率，从而能够解决现有技术中存在的对于合法用户发起的攻击、网络中存在大量转发的攻击报文、浪费网络带宽资源、占用系统处理资源的问题。

[0039] 图 3 示出了图 2 所示方法的优选实施处理方式，如图 3 所示，该优选处理方式包括如下过程。

[0040] 步骤 31、预先对选定的网络设备的端口设置攻击隔离点标识，具体地，可以根据网络实际运行的需要、将网络设备上连接下层网络设备的一个或多个物理端口设置为攻击隔离点，或者根据需要选定网络上特定位置上的网络设备的物理端口作为攻击隔离点，例如，根据实际需要，可以选择汇聚层网络设备的端口作为攻击隔离点，或者选择接入层网络设备的端口作为攻击隔离点；

[0041] 步骤 32、监测网络设备受到网络攻击后，获取攻击报文的源地址信息和类型信息；

[0042] 步骤 33、判断接收到该攻击报文的端口是否预设为攻击隔离点，具体包括：判断接收到攻击报文的端口已经设置有攻击隔离点标识的情况下，确定该端口是攻击隔离点，处理进行到步骤 34；判断接收到攻击报文的端口没有设置攻击隔离点标识的情况下，确定该端口不是攻击隔离点，处理进行到步骤 35；

[0043] 步骤 34、将获取的攻击报文的源地址信息和类型信息绑定在接收到攻击报文的端口上，以使该端口对后续接收到的攻击报文进行过滤；一种优选的方式，将源地址信息相

同、类型不同的多个攻击报文合并为一条记录绑定在该端口上，该记录用于指示对来自该相同源地址的报文均进行过滤；一种优选的方式，在接收到携带有隔离失败信息的隔离报文后，将隔离报文中的攻击报文源地址信息和类型信息绑定在接收到携带有隔离失败信息的隔离报文的端口上，以使该端口对后续接收到的攻击报文进行过滤；处理结束。

[0044] 步骤 35、构建包括获取的攻击报文的源地址信息和类型信息的隔离报文；一种优选的方式，在隔离报文中设置对攻击报文进行过滤隔离的时长信息；

[0045] 步骤 36、根据攻击报文的源地址信息中包括的源互联网协议 IP 地址信息，判断网络设备自身与源攻击设备是否处于直连网段，在判断处于直连网段的情况下，处理进行到步骤 37；在判断处于非直连网段的情况下，处理进行到步骤 38；

[0046] 步骤 37、将构建的隔离报文组播发送给与接收到攻击报文的端口相连接的网络设备，处理进行到步骤 39；

[0047] 步骤 38、将构建隔离报文单播发送给与接收到攻击报文的端口相连接的、转发该攻击报文的网络设备；一种优选的方式，在攻击报文的源地址信息中还包括攻击报文的源媒体接入控制 MAC 地址信息的情况下，将构建的隔离报文中的攻击报文源 MAC 地址信息设置为零，在现有技术中，在网络设备接收到的转发的报文中，MAC 地址并不是发送该报文的源设备的MAC地址，而是上一次转发该报文的网络设备的MAC地址，因此，攻击报文中的MAC地址并不是发起网络攻击的设备的 MAC 地址，而且上一次转发攻击报文的网络设备的 MAC 地址，根据攻击报文中的 MAC 地址去寻址将会导致定位到错误的网络设备上，所以，此处将构建的隔离报文中的攻击报文源 MAC 地址信息设置为零，并将设置后的隔离报文单播发送给与接收到攻击报文的端口相连接的、转发该攻击报文网络设备；

[0048] 步骤 39、在预定时间内未接收到隔离成功消息的情况下，在构建的隔离报文中添加找不到攻击隔离点的信息，将添加后的隔离报文组播发送给与接收到攻击报文的端口相连接的网络设备。

[0049] 通过图 3 所示的处理过程，网络设备受到网络攻击后，在接收到攻击报文的端口是预设的攻击隔离点的情况下，能够将攻击报文的源地址信息和类型信息绑定在作为攻击隔离点的端口上、以使该攻击隔离点对后续接收到的攻击报文进行过滤隔离，能够减少网络上转发的攻击报文，当具有攻击隔离点的网络设备位于较低的网络架构层次上时，就能够过滤隔离更多的攻击报文、更显著地减少网络上多余转发的攻击报文，相应地能够减少网络设备对攻击报文的处理，减少攻击报文占用的网络设备的系统处理资源，提高网络设备的系统处理效率。

[0050] 在图 3 所示的处理过程中，判断攻击源设备与网络设备自身是否处于直连网段、以对隔离报文进行组播或单播发送，能够对网络设备和攻击源设备之间的网络关系进行区别、以节约网络设备及网络系统的处理资源。

[0051] 在图 3 所示的处理过程中，还提供了一种确认机制，该机制针对具备攻击隔离点的网络设备为非目的攻击设备、攻击隔离点对攻击报文进行隔离成功与否的情况进行处理，该机制包括两种策略，第一种策略为对过滤成功后的确认处理，第二种策略为对过滤失败后的补救处理。根据第一种策略，网络设备对攻击报文进行过滤隔离成功后，向攻击报文的目的设备发送隔离成功报文、以确认攻击报文已被成功隔离。根据第二种策略，在受到网络攻击的网络设备超时未接收到隔离成功报文的情况下，受到攻击的网络设备在隔离报文

中添加找不到攻击隔离点的信息，并将该隔离报文组播发送给与接收到攻击报文的端口相连接的网络设备，以使接收到该隔离报文的网络设备均对该攻击报文进行隔离，该策略能够使位于网络架构中有效工作的、层次较低的网络设备对攻击报文进行过滤，防止具备攻击隔离点的网络设备出现故障、或攻击隔离点无效，从而使整个网络无法对攻击报文进行过滤的问题，提高对攻击报文的过滤隔离的有效率。

[0052] 在图 3 所示的处理过程中，还提供了一种隔离无效后的补救机制。根据该机制，当网络设备接收到携带有隔离失败信息的隔离报文时，说明具备攻击隔离点的网络设备无法有效地将攻击报文过滤掉，接收到携带有隔离失败信息的隔离报文后，网络设备将接收到的该隔离报文中的攻击报文的源地址信息和类型信息、绑定在接收到该隔离报文的端口上，以使该端口对后续接收到的攻击报文进行过滤。该机制在具备攻击隔离点的网络设备无法对攻击报文进行有效过滤时，能够使该网络设备的上层网络设备对攻击报文进行过滤，防止攻击隔离点无法有效过滤攻击报文的问题，提高对攻击报文的过滤隔离的有效率。

[0053] 为实现上述功能，本发明实施例这里的网络攻击的防御方法可以通过硬件实现，也可以通过下述软件程序实现，即网络设备中包括以下的网络攻击的防御装置。

[0054] 图 4 示出了根据本发明实施例的网络攻击的防御装装置的结构框图，如图 4 所示，该装置包括获取模块 41、第一判断模块 42、绑定模块 43、构建模块 44、发送模块 45 ；其中，

[0055] 获取模块 41，用于在网络设备监测受到攻击后，获取攻击报文的源地址信息和类型信息 ；

[0056] 第一判断模块 42，用于判断接收到该攻击报文的端口是否预设为攻击隔离点 ；

[0057] 绑定模块 43，连接至获取模块 41、第一判断模块 42，用于在第一判断模块 42 判断该端口是攻击隔离点的情况下，将获取模块 41 获取的攻击报文的源地址信息和类型信息绑定在该端口上，以使该端口对后续接收到的攻击报文进行过滤 ；

[0058] 构建模块 44，连接至获取模块 41、第一判断模块 42，用于在第一判断模块 42 判断该端口不是攻击隔离点的情况下，构建包括获取模块 41 获取的攻击报文的源地址信息和类型信息的隔离报文 ；

[0059] 发送模块 45，连接至构建模块 44，用于将构建模块 44 构建的隔离报文发送给与该端口相连接的网络设备。

[0060] 通过图 4 所示的装置，在网络设备受到网络攻击后，在接收到攻击报文的端口是预设的攻击隔离点的情况下，能够将攻击报文的源地址信息和类型信息绑定在作为攻击隔离点的端口上、以使该攻击隔离点对后续接收到的攻击报文进行过滤隔离，能够减少网络上转发的攻击报文，当具有攻击隔离点的网络设备位于较低的网络架构层次上时，就能够更早地过滤隔离攻击报文、显著地减少网络上多余转发的攻击报文，相应地能够减少网络设备对攻击报文的处理，减少攻击报文占用的网络设备的系统处理资源，提高网络设备的系统处理效率。

[0061] 图 4 所示装置的工作原理如图 2 所示，这里不再赘述。

[0062] 一种优选的方式，图 5 示出了图 4 所示装置的优选实施结构，如图 5 所示，该结构包括 ：预设模块 46、获取模块 41、第一判断模块 42、绑定模块 43、构建模块 44、发送模块 45、第二判断模块 47、设置模块 48、接收模块 49、定时器 50 ；其中，上述模块如图 4 中的已述结构和功能不再赘述 ；

[0063] 预设模块 46，用于对预先选定的网络设备的端口设置攻击隔离点标识；

[0064] 第一判断模块 42，具体用于判断接收到攻击报文的端口已经设置有所述攻击隔离点标识的情况下，确定该端口是攻击隔离点；判断接收到攻击报文的端口没有设置所述攻击隔离点标识的情况下，确定该端口不是攻击隔离点；

[0065] 绑定模块 43，还用于在第一判断模块 42 判断接收到攻击报文的端口是攻击隔离点的情况下，将源地址信息相同、类型不同的多个攻击报文合并为一条记录、将攻击报文的源地址信息绑定在该端口上；

[0066] 构建模块 44，还用于在隔离报文中设置对攻击报文进行过滤隔离的时长信息；

[0067] 接收模块 49，用于接收隔离成功报文；

[0068] 定时器 50，用于对接收模块 49 接收到隔离成功报文的预定时长进行定时；

[0069] 第二判断模块 47，连接至获取模块 41，用于根据获取模块 41 获取的攻击报文的源地址信息中的源互联网协议 IP 地址信息，判断网络设备自身与源攻击设备是否处于直连网段；

[0070] 设置模块 48，连接至构建模块 44、第二判断模块 47、接收模块 49、定时器 50，用于在第二判断模块判断处于非直连网段的情况下，将构建模块 44 构建的隔离报文中的源地址信息的攻击报文源媒体接入控制 MAC 地址信息设置为零；还用于在定时器 50 超时、接收模块 49 未接收到隔离成功报文的情况下，在构建模块 44 构建的隔离报文中添加找不到攻击隔离点的信息；

[0071] 发送模块 45，具体用于在第二判断模块 47 判断处于直连网段的情况下，将构建模块 44 构建的隔离报文组播发送给与接收到攻击报文的端口相连接的网络设备；在判断处于非直连网段的情况下，将构建模块 44 构建的隔离报文单播发送给与接收到攻击报文的端口相连接的、转发该攻击报文的网络设备，或者，将设置模块 48 将攻击报文源 MAC 地址信息设置为零后的隔离报文单播发送给与接收到攻击报文的端口相连接的、转发该攻击报文的网络设备；还用于将设置模块 48 添加了找不到攻击隔离点的信息后的隔离报文、组播发送给与接收到攻击报文的端口相连接的网络设备。

[0072] 图 5 所示装置的工作原理如图 3 所示，这里不再赘述。

[0073] 通过图 5 所示的装置，能够减少网络中多余转发的攻击报文、提高网络带宽的利用率，提高网络设备的处理效率；还能够实现对攻击隔离点过滤攻击报文成功与否的确认机制，提高对攻击报文隔离的有效率。

[0074] 图 6 示出了根据发明实施例的网络攻击的防御方法的另一种工作流程图，如图 6 所示，该流程包括如下处理过程。

[0075] 步骤 61、网络设备接收到隔离报文后，根据该隔离报文中的攻击报文源地址信息，判断网络设备接收到该隔离报文中所指示的攻击报文的端口是否为预设的攻击隔离点；

[0076] 步骤 62、在判断该端口是攻击隔离点的情况下，将该隔离报文中的攻击报文源地址信息和类型信息绑定在该端口上

[0077] 步骤 63、在判断该端口不是攻击隔离点的情况下，将接收到的隔离报文发送给与该端口相连接的网络设备。

[0078] 根据如图 6 所示的处理过程，接收到隔离报文的网络设备，在判断网络设备自身接收到隔离报文中指示的攻击报文的端口为攻击隔离点时，将隔离报文中的攻击报文的

源地址信息和类型信息绑定在该端口上，以使该端口对后续接收到的攻击报文进行过滤隔离，能够对合法用户发送的网络攻击报文隔离，将攻击报文隔离在网络设备上预设为攻击隔离点的端口之外，减少网络上多余转发的攻击报文、减少攻击报文占用的网络带宽、提高网络带宽的利用率，减少网络设备对攻击报文的处理、释放网络设备的系统处理资源、提高网络设备的系统处理效率，从而能够解决现有技术中存在的对于合法用户发起的攻击、网络中存在大量转发的攻击报文、浪费网络带宽资源、占用系统处理资源的问题。

[0079] 图 7 示出了图 6 所示方法的优选实施方式，如图 7 所示，该优选实施方式包括如下处理过程：

[0080] 步骤 71、预先对选定的网络设备上连接下层网络设备的端口设置攻击隔离点标识；

[0081] 步骤 72、网络设备接收到隔离报文后，根据隔离报文中的攻击报文的源 IP 地址信息，判断网络设备自身接收到该隔离报文中所指示的攻击报文的端口是否为预设的攻击隔离点，具体包括：判断网络设备自身接收到该隔离报文所指示的攻击报文的端口已经设置有所述攻击隔离点标识的情况下，确定该端口是攻击隔离点，处理进行到步骤 73；判断网络设备自身接收到该隔离报文所指示的攻击报文的端口没有设置所述攻击隔离点标识的情况下，确定该端口不是攻击隔离点，处理进行到步骤 75；

[0082] 步骤 73、将该隔离报文中的攻击报文源地址信息和类型信息绑定在该端口上，以使该端口对后续接收到的攻击报文进行过滤；一种优选的方式，将源地址信息相同、类型不同的多个攻击报文合并为一条记录，将攻击报文的源地址信息绑定在该端口上；

[0083] 一种优选的方式，在接收到携带有隔离失败信息的隔离报文后，将隔离报文中的攻击报文源地址信息和类型信息绑定在接收到携带有隔离失败信息的隔离报文的端口上，以使该端口对后续接收到的攻击报文进行过滤；

[0084] 一种优选的方式，在接收到携带有找不到攻击隔离点信息的隔离报文后，将隔离报文中的攻击报文源地址信息和类型信息绑定在接收到攻击报文的端口上，以使该端口对后续接收到的隔离报文中指示的攻击报文进行过滤，并将携带有找不到攻击隔离点信息的隔离报文广播发送给与接收到该隔离报文中指示的攻击报文的端口相连接的网络设备；

[0085] 步骤 74、监测到端口对所述攻击报文过滤失败后，在所述隔离报文中携带隔离失败信息，将携带有隔离失败信息的隔离报文发送给与接收到隔离报文的端口相连接的网络设备；监测到端口对攻击报文过滤成功后，向隔离报文中的攻击报文的目的地址信息所指的网络设备发送隔离成功消息，处理结束。

[0086] 步骤 75、将接收到的隔离报文发送给与接收到攻击报文的端口相连接的网络设备，具体包括：根据隔离报文中的攻击报文源 IP 地址信息、判断网络设备自身与该攻击报文源 IP 地址信息所指的网络设备是否处于直连网段，在判断处于直连网段的情况下，处理进行到步骤 76；在判断处于非直连网段的情况下，处理进行到步骤 77；

[0087] 步骤 76、将该隔离报文组播发送给与接收到所述攻击报文的端口相连接的网络设备；一种优选方式，由于网络设备与攻击报文源 IP 地址信息所指的网络设备处于直连网段，就可以根据隔离报文中的攻击报文的源 IP 地址信息、在网络设备自身上查找到与该源 IP 地址信息相对应的攻击报文的源 MAC 地址信息，即发送攻击报文的源设备的 MAC 地址信息，将该源 MAC 地址信息添加到所述隔离报文中，将携带有所述攻击报文源 MAC 地址信息的

隔离报文组播发送给与接收到所述攻击报文的端口相连接的网络设备，这样使接收到该携带有攻击报文源 MAC 地址信息的隔离报文的网络设备、能够更准确地对接收到攻击报文的端口以及发送攻击报文的源设备进行定位，处理结束。

[0088] 步骤 77、将该隔离报文单播发送给与接收到所述攻击报文的端口相连接的、转发所述攻击报文的网络设备，处理结束。

[0089] 根据如图 7 所示的处理流程，网络设备在接收到隔离报文后，判断网络设备自身接收到攻击报文的端口为预设的网络节点的情况下，将隔离报文中的攻击报文的源地址信息和类型信息绑定在作为攻击隔离点的端口上、以使该攻击隔离点对后续接收到的攻击报文进行过滤隔离，能够减少网络上转发的攻击报文，当具有攻击隔离点的网络设备位于较低的网络架构层次上时，就能够过滤隔离更多的攻击报文、减少更多网络上多余转发的攻击报文，相应地能够减少网络设备对攻击报文的处理，减少攻击报文占用的网络设备的系统处理资源，提高网络设备的系统处理效率。

[0090] 在图 7 所示的处理过程中，判断攻击源设备与网络设备自身是否处于直连网段、以对隔离报文进行组播或单播发送，能够对网络设备和攻击源设备之间的网络关系进行区别、以节约网络设备及网络系统的处理资源。

[0091] 在图 7 所示的处理过程中，还应用了如上所述的确认机制和隔离无效后的补救机制，这里不再赘述。

[0092] 为实现上述功能，本发明实施例这里的网络攻击的防御方法可以通过硬件实现，也可以通过下述软件程序实现，即网络设备中包括以下的网络攻击的防御装置。

[0093] 图 8 示出了本发明实施例提供的网络攻击的防御装置的结构框图，如图 8 所示，该装置包括 :接收模块 81、第一判断模块 82、绑定模块 83、发送模块 84 ;其中，

[0094] 接收模块 81，用于接收隔离报文 ;

[0095] 第一判断模块 82，连接至接收模块 81，用于根据接收模块 81 接收到的隔离报文中的攻击报文源地址信息、判断网络设备接收到该隔离报文所指示的攻击报文的端口是否为预设的攻击隔离点 ;

[0096] 绑定模块 83，连接至接收模块 81、第一判断模块 82，用于在第一判断模块 82 判断该端口是攻击隔离点的情况下，将接收模块 81 接收到的隔离报文中的攻击报文源地址信息和类型信息绑定在该端口上，以使该端口对后续接收到的攻击报文进行过滤 ;

[0097] 发送模块 84，连接至接收模块 81、第一判断模块 82，用于在第一判断模块 82 判断该端口不是攻击隔离点的情况下，将接收模块 81 接收到的隔离报文发送给与接收到所述攻击报文的端口相连接的网络设备。

[0098] 图 8 所示装置的工作原理如图 7 所示，这里不再赘述。

[0099] 根据如图 8 所示的装置，接收到隔离报文的网络设备，在判断网络设备自身接收到隔离报文中指示的攻击报文的端口为攻击隔离点时，将隔离报文中的攻击报文的源地址信息和类型信息绑定在该端口上，以使该端口对后续接收到的攻击报文进行过滤隔离，能够对合法用户发送的网络攻击报文隔离，将攻击报文隔离在网络设备上预设为攻击隔离点的端口之外，减少网络上多余转发的攻击报文、减少攻击报文占用的网络带宽、提高网络带宽的利用率，减少网络设备对攻击报文的处理、释放网络设备的系统处理资源、提高网络设备的系统处理效率，从而能够解决现有技术中存在的对于合法用户发起的攻击、网络中存

在大量转发的攻击报文、浪费网络带宽资源、占用系统处理资源的问题。

[0100] 图 9 示出了图 8 所示装置的优选实施结构，如图 9 所示，该结构包括接收模块 81、第一判断模块 82、绑定模块 83、发送模块 84、第二判断模块 85、查找模块 86、设置模块 87、监测模块 88、预设模块 89；其中，上述模块在图 8 中的已述结构和功能不再赘述；

[0101] 预设模块 89，用于预先对选定的网络设备上连接下层网络设备的端口设置攻击隔离点标识；

[0102] 第一判断模块 82，具体用于判断网络设备接收到该隔离报文所指示的攻击报文的端口已经设置有所述攻击隔离点标识的情况下，确定该端口是攻击隔离点；判断网络设备自身接收到该隔离报文所指示的攻击报文的端口没有设置所述攻击隔离点标识的情况下，确定该端口不是攻击隔离点；

[0103] 第二判断模块 85，连接至接收模块 81，用于根据接收模块 81 接收到的隔离报文中的攻击报文源互联网协议 IP 地址信息、判断网络设备自身与该攻击报文源 IP 地址信息所指的网络设备是否处于直连网段；

[0104] 查找模块 86，连接至接收模块 81，用于根据接收模块 81 接收到的隔离报文中的攻击报文的源 IP 地址信息、查找到与该源 IP 地址信息相对应的攻击报文的源 MAC 地址信息；

[0105] 监测模块 88，用于对端口过滤攻击报文的情况进行监测；

[0106] 设置模块 87，连接至接收模块 81、第一判断模块 82、查找模块 86、监测模块 88，用于将查找模块 86 查找到的攻击报文的源 MAC 地址信息添加到接收模块 81 接收到的隔离报文中；还用于在第一判断模块 82 判断接收到攻击报文的端口是攻击隔离点的情况下，监测模块 88 监测该端口对攻击报文过滤失败后，在接收模块 81 接收到的隔离报文中添加隔离失败信息；

[0107] 接收模块 81，还用于接收携带有隔离失败信息的隔离报文；用于接收携带有找不到攻击隔离点信息的隔离报文；

[0108] 绑定模块 83，还连接至接收模块 81，还用于在接收模块 81 接收到携带有隔离失败信息的隔离报文后，将该隔离报文中的攻击报文源地址信息和类型信息、绑定在接收到携带有隔离失败信息的隔离报文的端口上，以使该端口对后续接收到的攻击报文进行过滤；还用于在第一判断模块 82 判断接收到攻击报文的端口是攻击隔离点的情况下，将源地址信息相同、类型不同的多个攻击报文合并为一条记录、将攻击报文的源地址信息绑定在该端口上；还用于将接收模块 81 接收到携带有找不到攻击隔离点信息的隔离报文的情况下，将该隔离报文中的攻击报文源地址信息和类型信息绑定在接收到该隔离报文中所指示的攻击报文的端口上，以使该端口对后续接收到的攻击报文进行过滤；

[0109] 发送模块 84，还连接至接收模块 81、第二判断模块 85、监测模块 88，具体用于在第二判断模块 85 判断处于直连网段的情况下，将接收模块 81 接收到的隔离报文组播发送给与接收到攻击报文的端口相连接的网络设备，一种优选的方式，具体用于将设置模块 87 添加了攻击报文源 MAC 地址信息后的隔离报文组播发送给与接收到攻击报文的端口相连接的网络设备；在第二判断模块 85 判断处于非直连网段的情况下，将接收模块 81 接收到的隔离报文单播发送给与接收到攻击报文的端口相连接的、转发攻击报文的网络设备；在监测模块 88 监测端口对攻击报文过滤成功后，向攻击报文的目的地址信息所指的网络设备发送隔离成功消息；将接收模块 81 接收到的携带有找不到攻击隔离点信息的隔离报文广播

发送给与接收到该隔离报文中指示的攻击报文的端口相连接的网络设备。

[0110] 图 9 所示装置的工作原理如图 7 所示，这里不再赘述。

[0111] 如图 9 所示的装置，能够减少网络中多余转发的攻击报文、提高网络带宽的利用率，提高网络设备的处理效率；还能够实现对攻击隔离点过滤攻击报文成功与否的确认机制，提高对攻击报文隔离的有效率。

[0112] 本发明实施例还提供了一种网络设备，该网络设备包括如图 4 和图 8 所示的网络攻击的防御装置，该网络设备的工作原理分别如图 2 和图 6 所示，这里不再赘述。一种优选的方式，包括如图 4 和图 8 所示装置的网络设备的优选实施结构，可包括如图 5 和图 9 所示的结构，其工作原理分别如图 3 和图 7 所示，这里不再赘述。

[0113] 本发明实施例还提供了一种网络攻击的防御系统，该系统具有多个包括如图 4 和 / 或图 8 所示装置的网络设备，该系统的优选实施结构为具有多个包括如图 5 和 / 或图 9 所述装置的网络设备，该系统的工作原理如上所述，这里不再赘述。

[0114] 下面对本发明实施例具体应用的情况进行说明。

[0115] 图 10 示出了本发明实施例具体应用的网络攻击的防御系统的结构示意图，如图 10 所示，接入交换机 SW1 通过 Port1-Port4 连接 PC1-PC4，接入交换机 SW2 通过 Port1-Port3 连接 PC5-PC7，SW1 分别通过 Port5、Port6 连接至汇聚交换机 SW3 的 Port1、SW4 的 Port1，SW2 通过 Port4 连接至汇聚交换机 SW5 的 Port1，SW3 与 SW4 之间均通过 Port2 连接，SW3 通过 port3 连接至核心交换机 SW8 的 port2，SW4 通过 port3 连接至 SW8 的 port1，SW5 通过 port2 连接至核心交换机 SW6 的 port1，SW6 与核心交换机 SW7 分别通过 port2 连接，SW6 与 SW8 分别通过 port3 连接，SW8 通过 port4 与 SW7 的 port1 连接，在接入交换机 SW1、SW2 上部署接入控制安全功能，例如 802.1x、WEB 认证等，能够有效地控制接入 PC 的身份合法性，接入交换机只转发来自合法的 IP 地址和 MAC 地址的 PC 发出的报文。在图 10 所示的系统中，PC1 的 IP 地址为 192.168.3.2/24、MAC 地址为 00d0.f800.0001，SW1 的管理 IP 地址为 192.168.1.1/24，SW3 的 port1 的 IP 地址为 192.168.3.1/24、port3 的 IP 地址为 192.168.8.2/24，SW8 的 port2 的 IP 地址为 192.168.8.1/24、port1 的 IP 地址为 192.168.7.2/24，SW7 的 port1 的 IP 地址为 192.168.7.1/24，PC5 的 IP 地址为 192.168.5.2/24，SW2 的管理 IP 地址为 192.168.2.1/24，SW5 的 port1 的 IP 地址为 192.168.5.1/24。

[0116] 场景一

[0117] 在如图 10 所示的系统中，预先将 SW1 的 port1 至 port4 均设置为攻击隔离点，对这四个端口分别设置攻击隔离点标识。

[0118] PC1 通过认证后以合法的身份通过端口 1234 对 SW7 的端口 7 进行用户数据包协议 (UDP，User Datagram Protocol) 的环回攻击，SW7 上检测到攻击信息，检测到攻击的方法可以为 NFPP、或者其他应用层协议。SW7 检测到攻击后，根据以下处理步骤对攻击报文进行防御。

[0119] 步骤一、SW7 监测到受到网络攻击、即端口 1 接收到攻击协议数据单元 (PDU，Protocol Data Unit) 后，获取攻击 PDU 的相关信息、主要包括攻击报文的源地址信息和类型信息，如表 1 所示，攻击 PDU 的相关信息包括：攻击报文的源 MAC 地址、攻击报文类型、攻击报文源 IP、目的 IP，攻击报文协议号、源端口、目的端口号，其中，只有传输控制协议

(TCP, Transmission Control Protocol) 或者 UDP 报文的攻击,才携带源端口和目的端口号,只有当攻击报文是 IPv4 或者 IPv6 报文时,该攻击 PDU 的相关信息才携带协议号 ;

[0120] 在表 1 中,源 MAC 是 192.168.7.2 对应的源 MAC,这是因为经过跨网段转发后,源 MAC 信息会被修改为上一跳转发报文的 IP 地址对应的 MAC 地址 ;

[0121] 表 1

[0122]

攻击者报文源 MAC	攻击报文类型	攻击报文源 IP	攻击报文目的 IP	协议号	源端口	目的端口
192.168.7.2 对应的 MAC 地址	0x0800	192.168.3.2	192.168.7.1	17(UDP)	1234	7

[0123] 步骤二、SW7 判断接收到该攻击 PDU 的端口 1 没有设置攻击隔离点标识,确定端口 1 不是攻击隔离点 ;

[0124] 步骤三、SW7 构建包括获取的攻击 PDU 的相关信息 (如表 1 所示) 的隔离 PDU,如表 2 所示,该隔离 PDU 包括以太网报头、IP 报头、TCP 报头、以及攻击报文的相关信息, SW7 根据攻击报文的源地址信息中包括的源 IP 地址以及 SW7 自身的 IP 地址,判断网络设备自身与源攻击设备处于非直连网段,将构建的隔离 PDU 中的攻击报文源 MAC 地址信息设置为零,如表 2 所示,将如表 2 所示的隔离 PDU 单播发送给与接收到攻击 PDU 的端口 1 相连接的、转发该攻击 PDU 网络设备,即 SW8。

[0125] 表 2

[0126]

以太网报头 (单播)	IP 报头 (单播)	TCP 报头	攻击报文信息

攻击者报文源 MAC	攻击报文类型	攻击报文源 IP	攻击报文目的 IP	协议号	源端口	目的端口
0000.0000.0000	0x0800	192.168.3.2	192.168.7.1	17(UDP)	1234	7

[0127] SW8 接收到如表 2 所示的隔离 PDU 后,判断 SW8 自身接收到攻击 PDU 的端口 2 不是预设的攻击隔离点,并且根据隔离 PDU 中的攻击报文源 IP 地址以及 SW8 自身的 IP 地址、判断 SW8 与源攻击设备 PC1 不处于直连网段,将接收到的如表 2 所示的隔离 PDU 单播发送给与接收到攻击 PDU 的端口 2 相连接的网络设备,即 SW3。

[0128] SW3 接收到隔离 PDU 后,判断 SW3 自身接收到攻击 PDU 的端口 1 不是攻击隔离点,根据隔离 PDU 中的攻击报文源 IP 地址以及 SW3 自身的 IP 地址、判断 SW3 与源攻击设备 PC1 处于直连网段,根据攻击报文源 IP 查找 MAC 地址表、查找到攻击源设备 PC1 的 MAC 地址为

00d0.f800.0001，将 PC1 的该 MAC 地址填入到接收到的隔离 PDU 中，如表 3 所示，并将如表 3 所示的隔离 PDU 组播发送给与端口 1 相连接的网络设备，即 SW1。

[0129] SW1 接收到如表 3 所示的隔离报文后，判断 SW1 自身接收到攻击 PDU 的端口 1 为攻击隔离点，就将表 3 中携带的攻击报文信息绑定在端口 1 上，端口 1 对后续接收到的相应的攻击报文进行过滤隔离。

[0130] SW1 对攻击报文过滤隔离成功后，根据隔离报文中的攻击报文目的 IP，向该目的 IP 所指的网络设备、即 SW7 发送隔离成功消息，SW7 在预定时间内接收到该隔离成功消息后，确认攻击报文已被隔离。

[0131] 表 3

[0132]

以太网报头（组播）	IP 报头（组播）	TCP 报头	找不到攻击隔离点（标志位=1）	攻击报文信息

攻击者报文源 MAC	攻击报文类型	攻击报文源 IP	攻击报文目的 IP	协议号	源端口	目的端口
00d0.f800.0001	0x0800	192.168.3.2	192.168.7.1	17(UDP)	1234	7

[0133] SW7 在预定时间内未接收到隔离成功消息的情况下，在构建的如表 3 所示的隔离报文中添加找不到攻击隔离点的信息，例如，设置找不到攻击隔离点的标志位，该标志位为 1 时表示在网络中找不到攻击隔离点，如表 4 所示，将添加后的隔离报文组播发送给与接收到攻击报文的端口相连接的网络设备，即 SW8。SW8 接收到携带有找不到攻击隔离点信息的隔离报文后，将该隔离报文中的攻击报文信息绑定在接收到该隔离报文中指示的攻击报文的端口 2 上，并将该隔离报文组播发送给与端口 2 相连接的网络设备 SW3，接收到该隔离报文的 SW3 进行与 SW8 所做的相同的处理。

[0134] 此外，当 SW1 对攻击 PDU 无法过滤隔离、或者过滤失败时，在如表 3 所示的隔离报文中添加隔离失败信息，例如，设置隔离失败的标志位，该标志位为 1 时表示对攻击 PDU 隔离失败，如表 5 所示，并设置后的如表 5 所示的隔离报文、发送给与接收到隔离报文的端口 5 相连接的网络设备，即 SW3。SW3 的端口 1 接收到如表 5 所示的隔离 PDU 后，发现该隔离 PDU 中隔离失败标志位为 1，则将该隔离 PDU 中的攻击 PDU 相关信息绑定在端口 1 上，SW3 的端口 1 对后续接收到的相应攻击 PDU 进行过滤隔离。同理，当 SW3 对攻击 PDU 过滤失败后，将如表 5 所示的隔离 PDU 通过端口 3 发送给 SW8，SW8 通过端口 2 对攻击报文进行过滤。

[0135] 表 4

[0136]

以太网报头（组播）	IP 报头（组播）	TCP 报头	找不到攻击隔离点标志位=1	攻击报文信息

攻击者报文源 MAC	攻击报文类型	攻击报文源 IP	攻击报文目的 IP	协议号	源端口	目的端口
0000.0000.0000	0x0800	192.168.3.2	192.168.7.1	17(UDP)	1234	7

[0137] 表 5

[0138]

以太网报头（组播）	IP 报头（组播）	TCP 报头	隔离失败标志位=1	攻击报文信息

攻击者报文源 MAC	攻击报文类型	攻击报文源 IP	攻击报文目的 IP	协议号	源端口	目的端口
0000.0000.0000	0x0800	192.168.3.2	192.168.7.1	17(UDP)	1234	7

[0139] 上述各网络设备，当需要对相同攻击报文源 IP 地址、不同报文类型的多个攻击报文进行过滤隔离时，可将这多个攻击报文合并为一条记录，对来自该 IP 地址的报文均进行过滤隔离，例如 SW1 对来自 192.168.3.2 即 PC1 的多个类型不同的攻击报文进行隔离时，可将这多个攻击报文合并为一条记录，对来自 PC1 的报文均进行隔离，以避免来自 PC1 的报文过多地占用网络带宽资源、避免过滤攻击报文过多地占用 SW1 的系统处理资源。

[0140] 通过上述处理过程，SW1 的端口 1 作为攻击隔离点能够将来自 PC1 的攻击报文隔离在网络架构的边缘，由于 SW1 作为接入层设备、所处的网络层次较低，能够尽可能地减少在网络中传输的攻击报文，能够提高网络带宽的利用率，提高网络设备的处理效率。

[0141] 场景二

[0142] 在如图 10 所示的系统中，预先将 SW2 的 port1 至 port3 均设置为攻击隔离点，对这三个端口分别设置攻击隔离点标识。

[0143] PC5 以合法身份对 SW5 进行互联网控制报文协议（ICMP，Internet Control Message Protocol）的大流量长 ping 攻击，SW5 的端口 1 接收到该攻击后，获取攻击报文的相关信息，该相关信息如表 6 所示，其中包括攻击者报文源 MAC、攻击报文类型、攻击报文源 IP、攻击报文目的 IP、协议号。

[0144] 表 6

[0145]

攻击者报文源 MAC	攻击报文类型	攻击报文源 IP	攻击报文目的 IP	协议号
00d0.f800.0005	0x0800	192.168.5.2	192.168.5.1	1(icmp)

[0146] SW5 判断端口 1 不是预设的攻击隔离点，进一步通过 SW5 自身的 IP 地址和攻击报文源 IP 地址判断 SW5 与 PC5 处于直连网段，构建将如表 7 所示的隔离报文，该隔离报文中携带如表 6 所示的攻击报文信息，并将如表 7 所示的隔离报文组播发送给与端口 1 相连接的网络设备，即 SW2。

[0147] 表 7

[0148]

以太网报头（组播）	IP 报头（组播）	TCP 报头	攻击报文信息

攻击者报文源 MAC	攻击报文类型	攻击报文源 IP	攻击报文目的 IP	协议号
00d0.f800.0005	0x0800	192.168.5.2	192.168.5.1	1(ICMP)

[0149] SW2 接收到如表 7 所示的隔离报文后，判断接收到该隔离报文中的攻击报文的端口 1 为攻击隔离点，就将该隔离报文中的攻击报文信息绑定在端口 1 上，端口 1 对后续接收到的相应攻击报文进行过滤隔离。

[0150] SW2 对过滤隔离成功后进行确认的处理、对隔离失败的处理、以及对来自同一 IP 地址的多个类型的攻击报文的处理，与上述场景一中的描述类似，这里不再赘述。

[0151] 通过上述处理过程，SW2 的端口 1 作为攻击隔离点能够将来自 PC5 的攻击报文隔离在网络架构的边缘，由于 SW1 作为接入层设备、所处的网络层次较低，能够尽可能地减少在网络中传输的攻击报文，能够提高网络带宽的利用率，提高网络设备的处理效率。

[0152] 综上所述，根据本发明实施例提供的网络攻击的防御方案，应用隔离机制，通过全网设备相互联动和识别，能够将攻击报文隔离在攻击隔离点之外，当攻击隔离点位于较低的网络层次上时，能够大量地减少网络中存在的无用的攻击报文，能够提供网络带宽利用率、提高网络设备系统处理资源利用率，能够提供整网的稳定性和业务流的传输效率；应用确认机制和隔离失败后的补救机制，能够提高对攻击报文隔离的有效率。

[0153] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

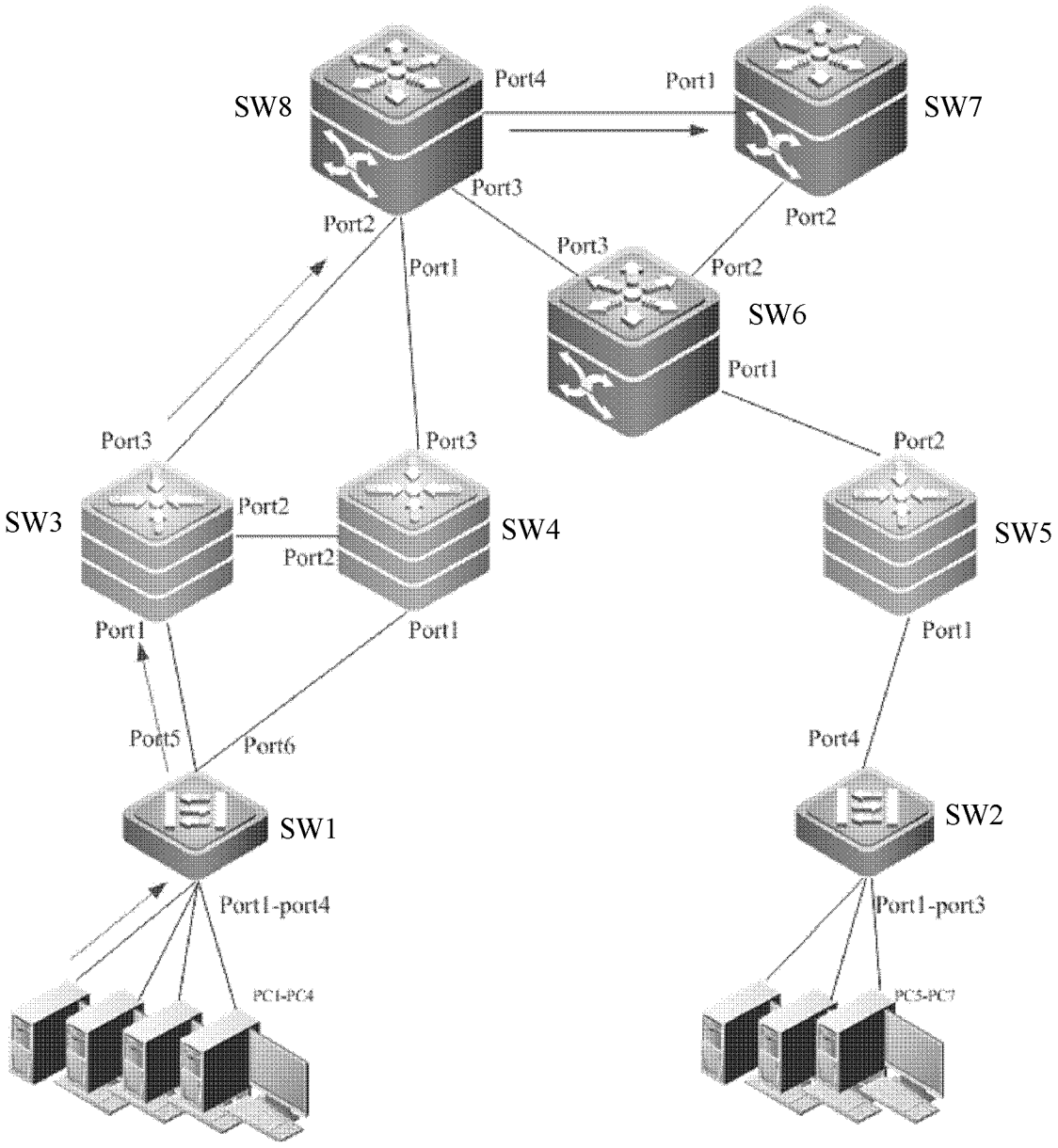

SW8
Port4
Port1
SW7
Port3
Port2
Port2
Port3
Port1
Port3
Port2
SW6
Port1
Port3
Port3
Port2
SW3
Port2
SW4
SW5
Port2
Port1
Port1
Port5
Port6
Port4
SW1
SW2
Port1-port4
Port1-port3
PC1-PC4
PC5-PC7

图 1

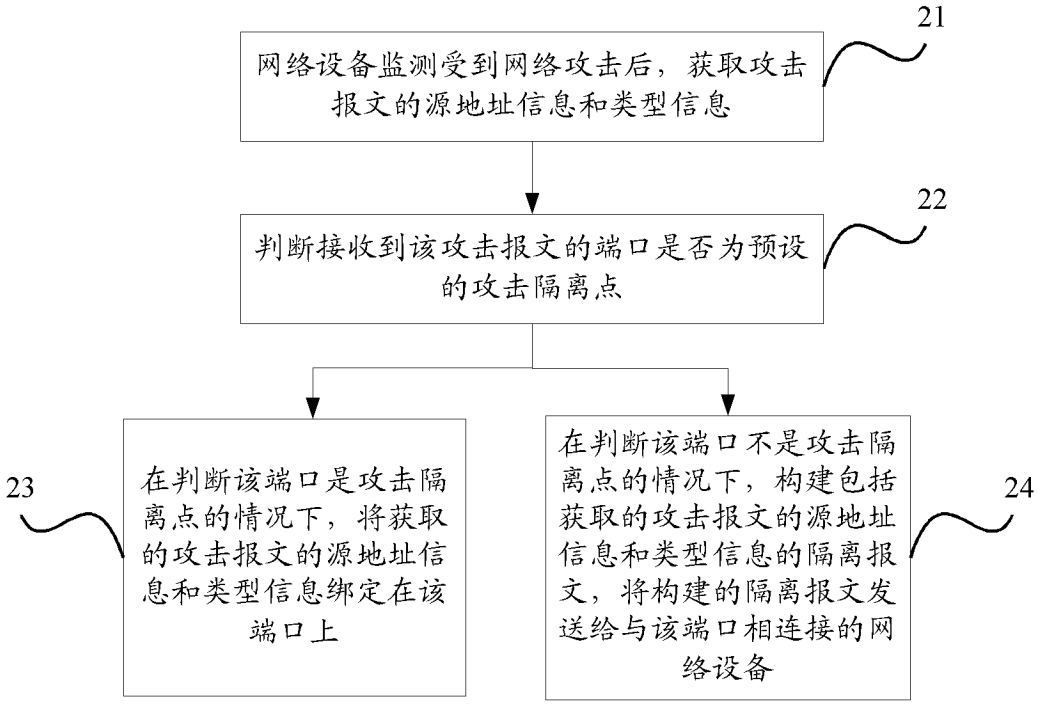

21
网络设备监测受到网络攻击后，获取攻击报文的源地址信息和类型信息
22
判断接收到该攻击报文的端口是否为预设的攻击隔离点
23
在判断该端口是攻击隔离点的情况下，将获取的攻击报文的源地址信息和类型信息绑定在该端口上
24
在判断该端口不是攻击隔离点的情况下，构建包括获取的攻击报文的源地址信息和类型信息的隔离报文，将构建的隔离报文发送给与该端口相连接的网络设备

图 2

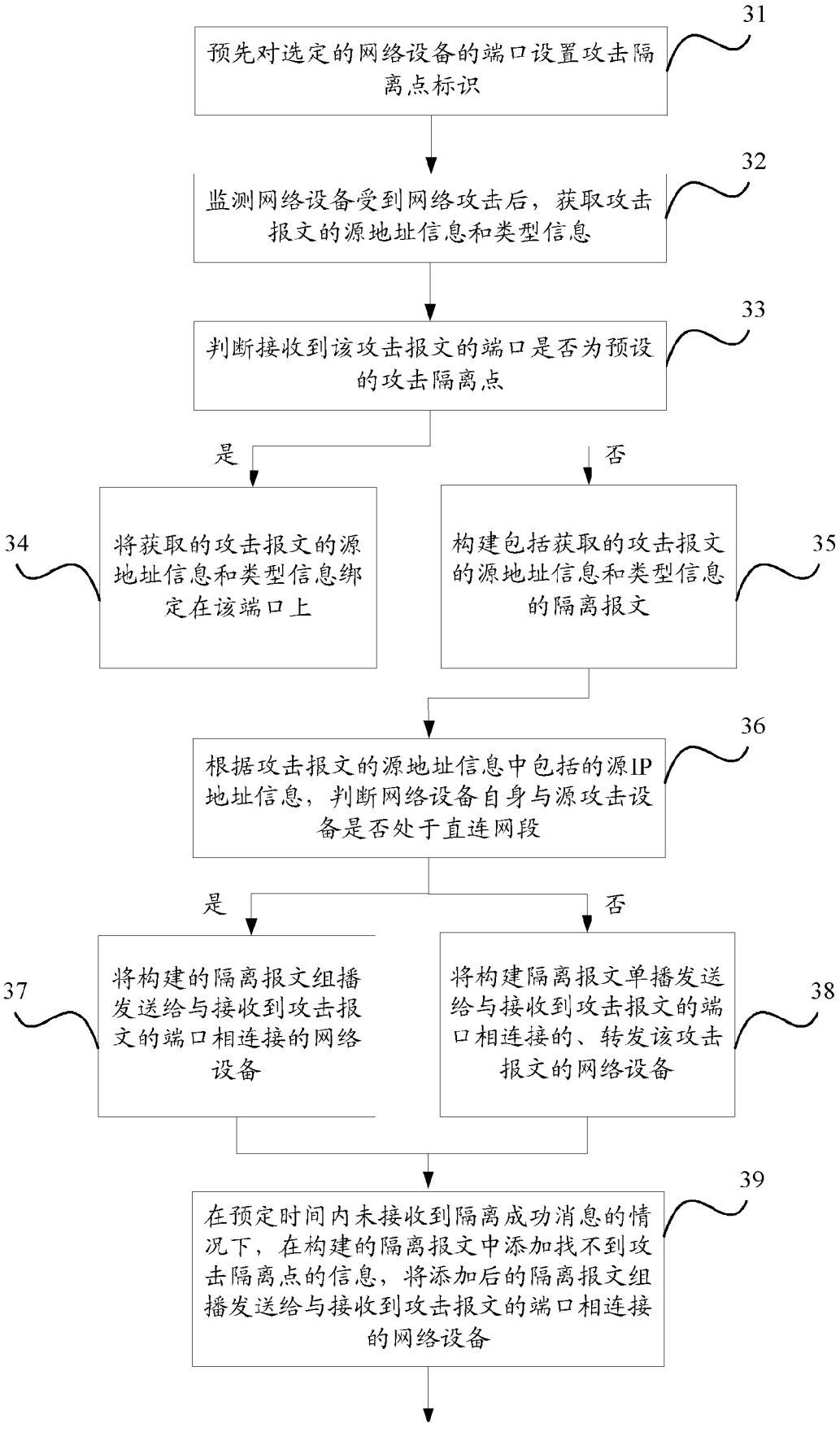

31
预先对选定的网络设备的端口设置攻击隔离点标识
32
监测网络设备受到网络攻击后，获取攻击报文的源地址信息和类型信息
33
判断接收到该攻击报文的端口是否为预设的攻击隔离点
是
否
34
将获取的攻击报文的源地址信息和类型信息绑定在该端口上
35
构建包括获取的攻击报文的源地址信息和类型信息的隔离报文
36
根据攻击报文的源地址信息中包括的源IP地址信息，判断网络设备自身与源攻击设备是否处于直连网段
是
否
37
将构建的隔离报文组播发送给与接收到攻击报文的端口相连接的网络设备
38
将构建隔离报文单播发送给与接收到攻击报文的端口相连接的、转发该攻击报文的网络设备
39
在预定时间内未接收到隔离成功消息的情况下，在构建的隔离报文中添加找不到攻击隔离点的信息，将添加后的隔离报文组播发送给与接收到攻击报文的端口相连接的网络设备

图 3

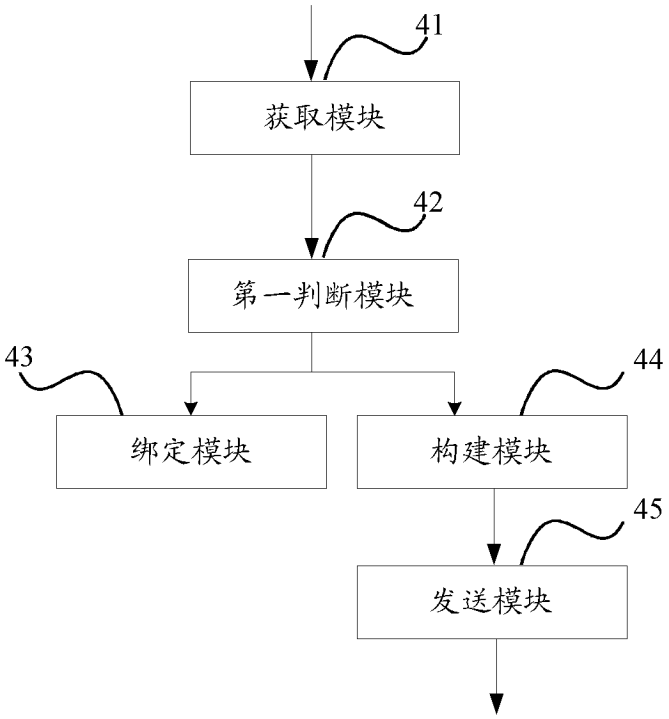

41
获取模块
42
第一判断模块
43
44
绑定模块
构建模块
45
发送模块

图 4

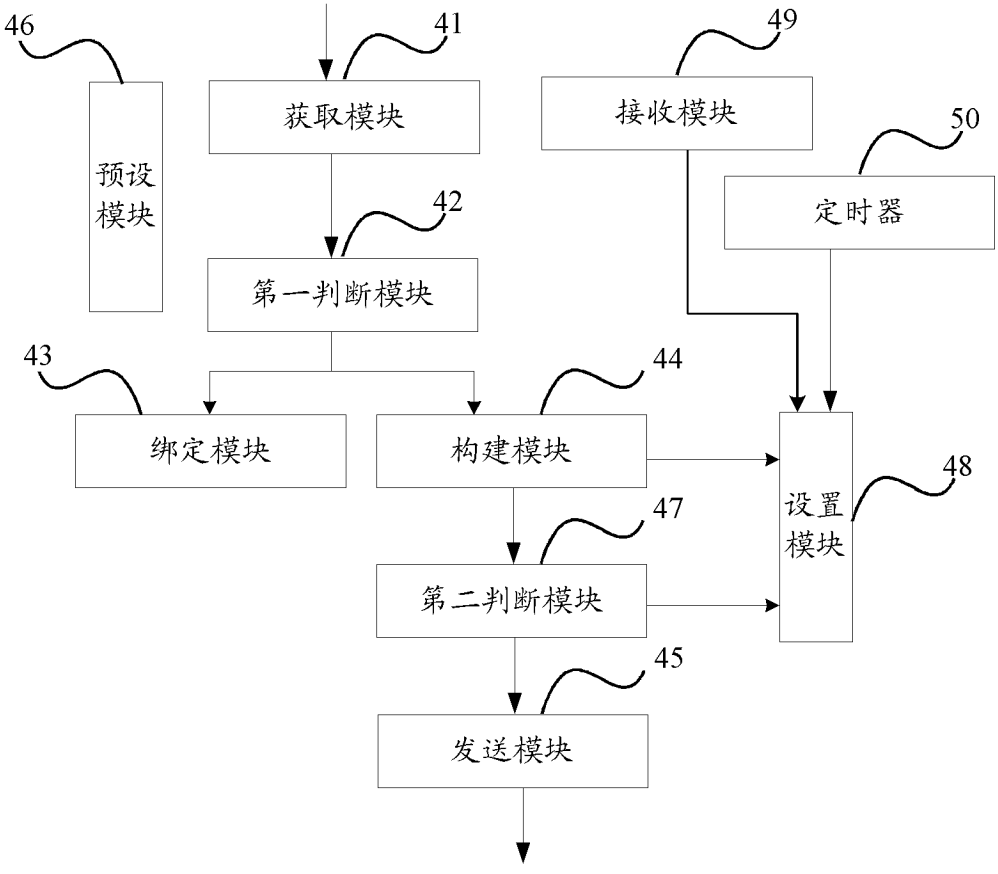

46
预设模块
41
获取模块
49
接收模块
50
定时器
42
第一判断模块
43
44
绑定模块
构建模块
47
48
设置模块
第二判断模块
45
发送模块

图 5

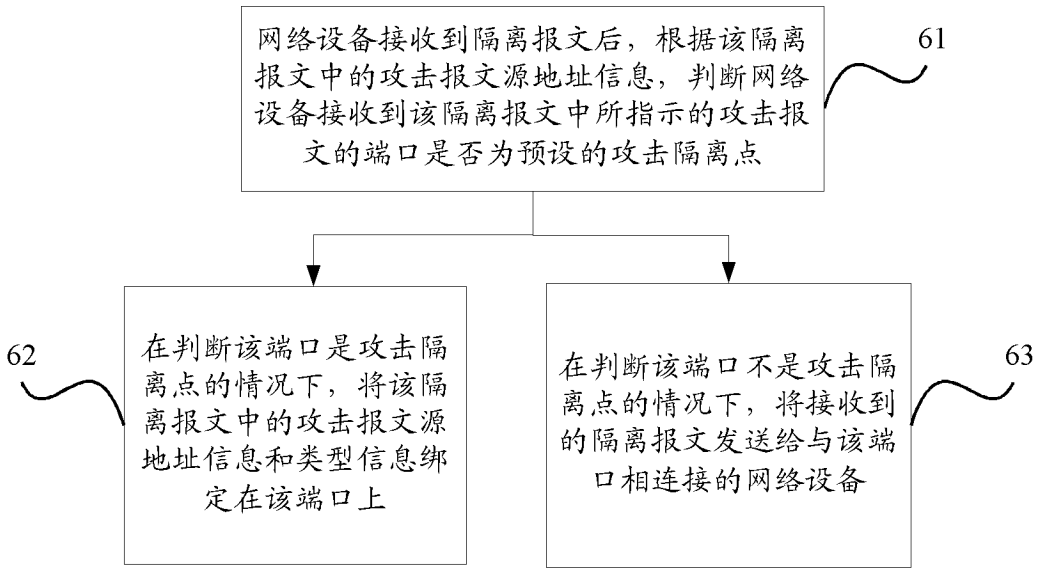

网络设备接收到隔离报文后，根据该隔离报文中的攻击报文源地址信息，判断网络设备接收到该隔离报文中所指示的攻击报文的端口是否为预设的攻击隔离点
61
在判断该端口是攻击隔离点的情况下，将该隔离报文中的攻击报文源地址信息和类型信息绑定在该端口上
62
在判断该端口不是攻击隔离点的情况下，将接收到的隔离报文发送给与该端口相连接的网络设备
63

图 6

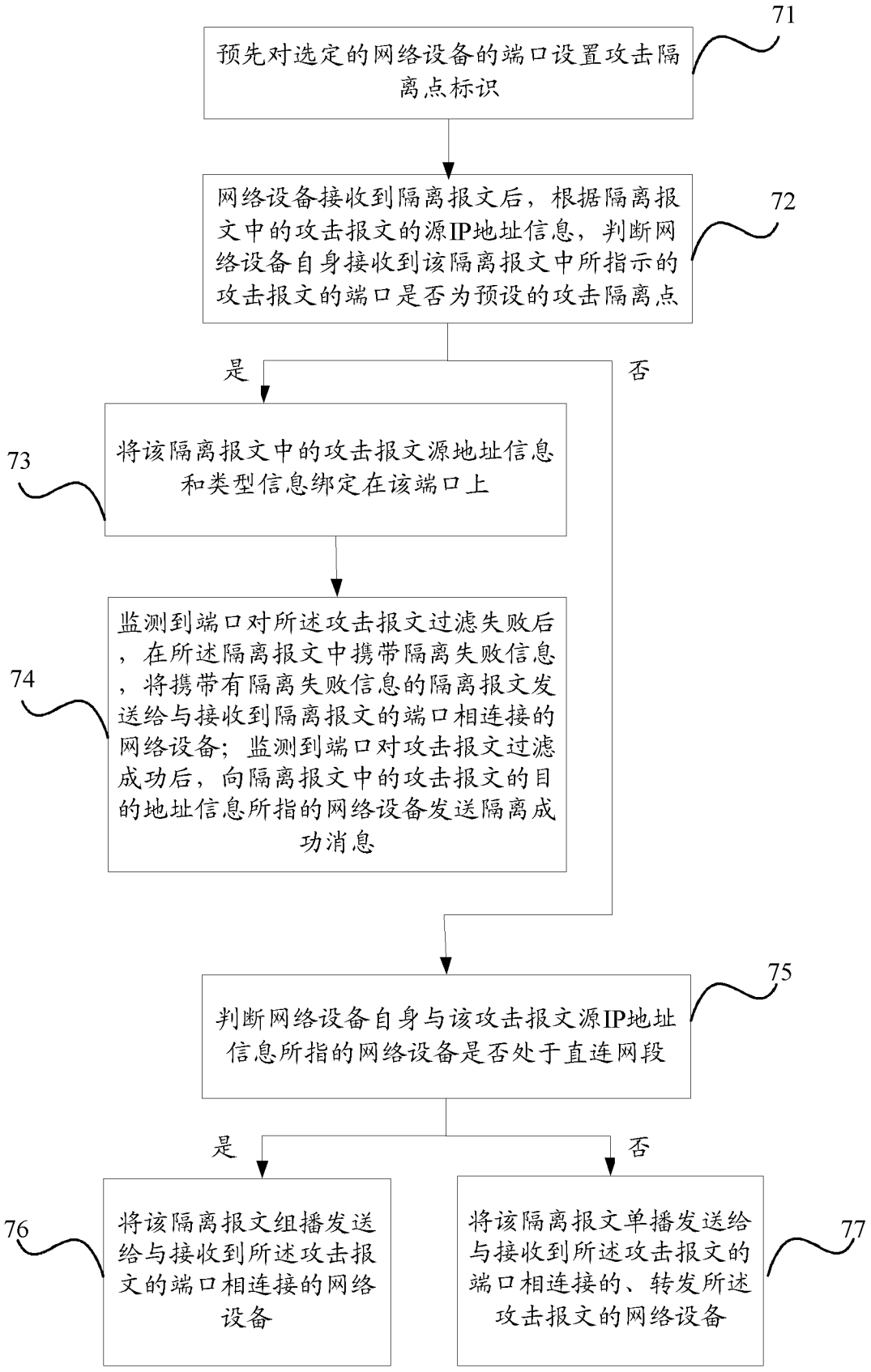

71
预先对选定的网络设备的端口设置攻击隔离点标识
网络设备接收到隔离报文后，根据隔离报文中的攻击报文的源IP地址信息，判断网络设备自身接收到该隔离报文中所指示的攻击报文的端口是否为预设的攻击隔离点
72
是
否
将该隔离报文中的攻击报文源地址信息和类型信息绑定在该端口上
73
监测到端口对所述攻击报文过滤失败后，在所述隔离报文中携带隔离失败信息，将携带有隔离失败信息的隔离报文发送给与接收到隔离报文的端口相连接的网络设备；监测到端口对攻击报文过滤成功后，向隔离报文中的攻击报文的目的地址信息所指的网络设备发送隔离成功消息
74
判断网络设备自身与该攻击报文源IP地址信息所指的网络设备是否处于直连网段
75
是
否
将该隔离报文组播发送给与接收到所述攻击报文的端口相连接的网络设备
76
将该隔离报文单播发送给与接收到所述攻击报文的端口相连接的、转发所述攻击报文的网络设备
77

图 7

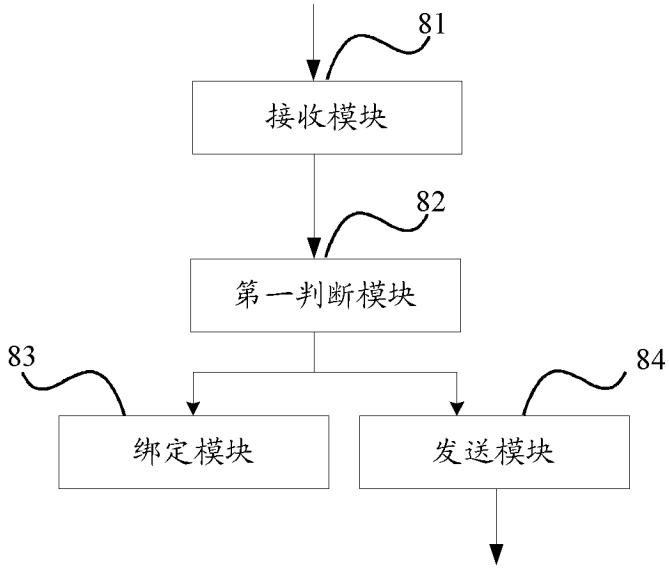

81
接收模块
82
第一判断模块
83
84
绑定模块
发送模块

图 8

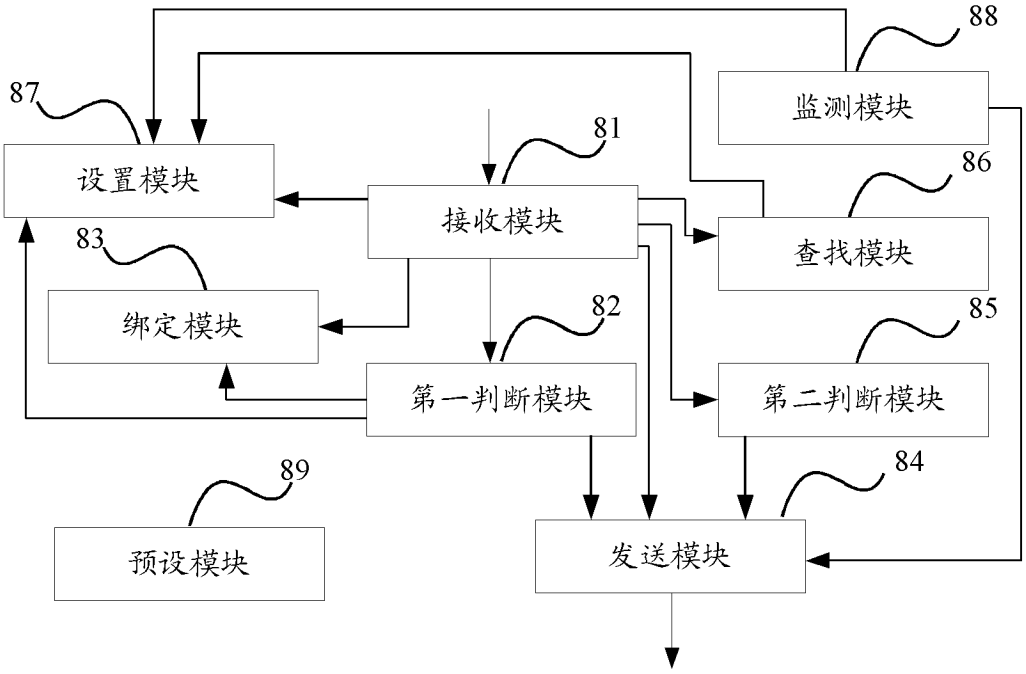

88
87
监测模块
81
设置模块
86
接收模块
查找模块
83
绑定模块
82
85
第一判断模块
第二判断模块
89
84
预设模块
发送模块

图 9

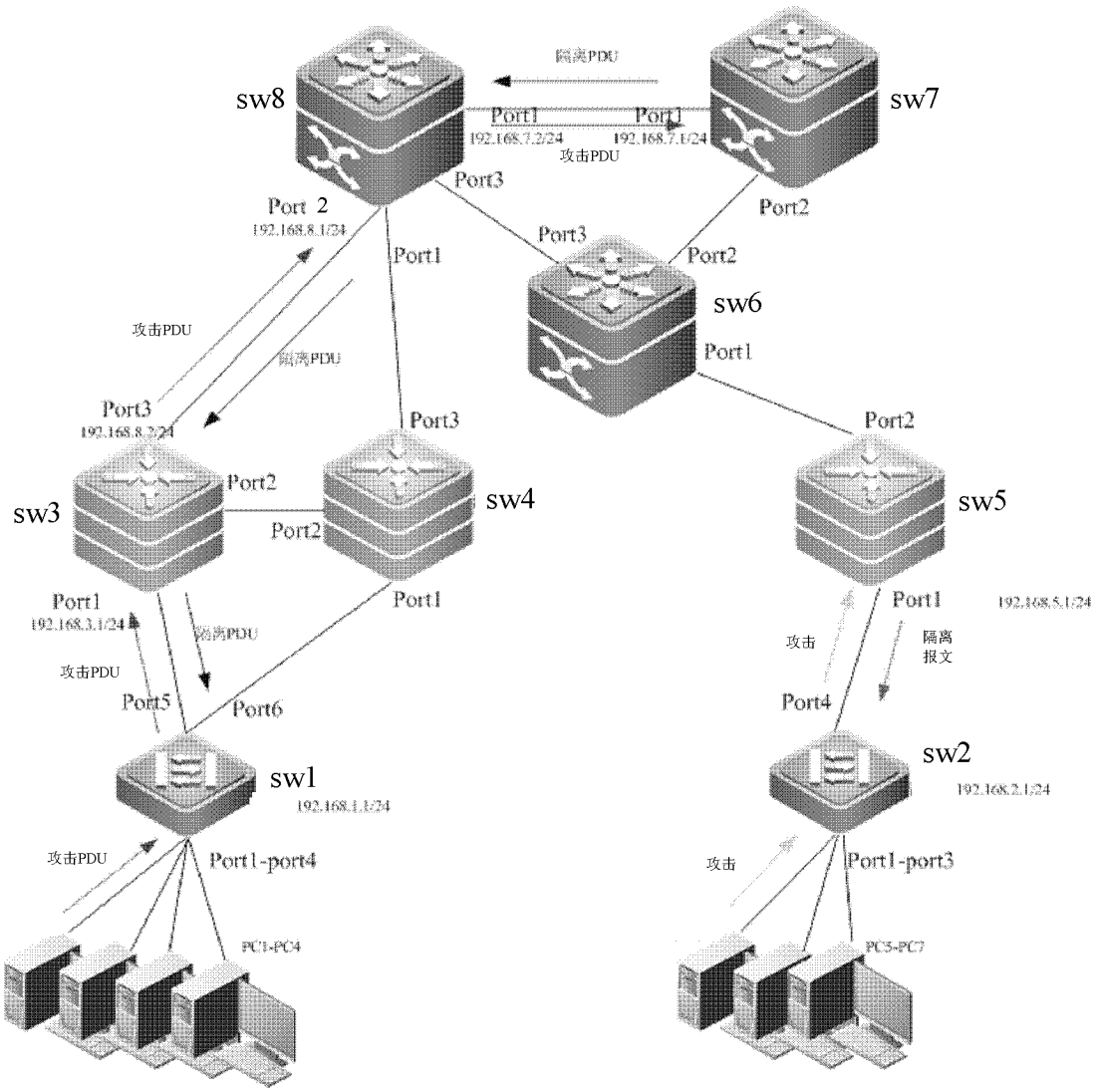

隔离PDU
sw8
sw7
Port1
Port1
192.168.7.2/24
192.168.7.1/24
攻击PDU
Port3
Port2
Port 2
192.168.8.1/24
Port1
Port3
Port2
sw6
攻击PDU
隔离PDU
Port1
Port3
192.168.8.2/24
Port3
Port2
sw3
Port2
sw4
sw5
Port1
192.168.3.1/24
Port1
Port1
192.168.5.1/24
隔离PDU
攻击
隔离
报文
攻击PDU
Port5
Port6
Port4
sw2
sw1
192.168.1.1/24
192.168.2.1/24
攻击PDU
Port1-port4
攻击
Port1-port3
PC1-PC4
PC5-PC7

图 10