[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/26 (2006.01)
H04L 29/06 (2006.01)
H04L 12/56 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710130726.7

[43] 公开日 2009 年 1 月 21 日

[11] 公开号 CN 101350743A

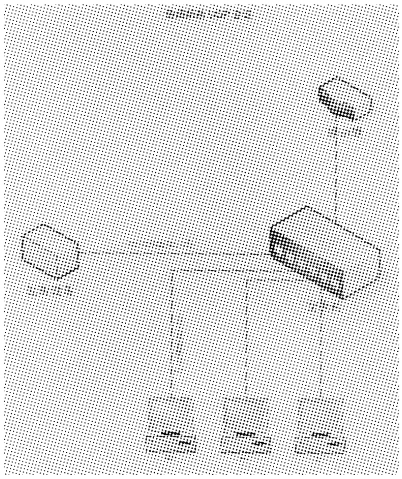
[22] 申请日 2007.7.20
[21] 申请号 200710130726.7
[71] 申请人 莱克斯信息技术（北京）有限公司
地址 100085 北京市海淀区上地三街 9 号嘉华大厦 A1104 室
[72] 发明人 尹志超
权利要求书 1 页 说明书 2 页 附图 1 页

[54] 发明名称

旁路阻断 UDP 会话

[57] 摘要

本发明是一种在旁路方式下对网络上的 UDP 会话进行阻断的方法。 可用于网络安全、网络管理以及网络访问控制等领域。 局域网络中放置一台监听设备，通过集线器或者交换机的镜像端口监听网络。 当需要阻断某个 UDP 会话时，根据监听到的 UDP 数据包信息组装一个伪造的 ICMP 数据包，然后将这个伪造的数据包直接发送到链路层。 持有需要阻断的 UDP 会话的机器就会收到这个伪造的 ICMP 数据包，此时它会认为会话的另一端发送了错误通知信息。 根据标准协议，操作系统会通知应用程序此 UDP 书包发送错误。 这样拥有此会话的应用程序就会断开此次 UDP 会话。 从而达到阻止非法网络访问的目的。



旁路阻断 UDP 应用的方法是以部署以在旁路的方式对通过网络的以 UDP 为基础的应用根据策略进行阻断。

具体特征如下：

1. 在集线器或者交换机的映像端口接入监听设备。

2. 在监听设备上监听到需要阻断的 UDP 数据后，构造一个阻断数据流。

3. 把数据流发送给目标机器。

4. 目标机器收到这个数据包后，断开相应的 UDP 应用。

旁路阻断UDP会话

特定的技术领域

本发明是一种在旁路方式下对网络上的 UDP 会话进行阻断的方法。可用于网络安全、网络管理以及网络访问控制等领域。

背景技术

目前，在中小企业内部办公网络中，对员工的网络访问控制，内容过滤，内容审计，以及网络安全等领域中，需要对网络使用情况进行监控。一般采用旁路监听的方式来减轻网关或路由器的负担。但旁路的控制功能却打了折扣。本发明通过伪造数据包的方式可以实现在旁路阻断特定的 UDP 会话的功能，从而解决了旁路监听方式的功能缺陷。

发明内容

本发明的目的在于解决网络的旁路监听方式下对 UDP 连接无法阻断的问题。

一般情况，如果要断开一个 UDP 的会话，只有服务器端，客户端，以及网关和路由器等网络出口处这三个部位。而对于局域网的网络安全、网络访问控制、网络行为记录、网络审计等领域适用的部位是网络出口。但是这样作的一个缺陷是会影响路由器等设备的性能。因此，网络行为记录，网络审计等功能为了减轻路由器等设备的负担，会用旁路监听的方式来实现（运行环境如图 1）。但是同时这样旁路监听的方式对数据包却缺乏控制能力。如果在旁路监听的方式下可以阻断 UDP 的会话，就可以既分担路由器的负担，又具有网络控制能力。本发明就解决了这个问题。

详细介绍：

这种旁路阻断方式的实现需要三个前提：

首先，必须能够监听到网络上的数据包。

其次，能将自己伪造的数据包写入到链路层。

第三，根据 UDP 协议的要求：如果发送一个 UDP 包后，对方没有相应的接收进程，对方会返回一个 ICMP 报文来通知发送方。

由此可知，如果我们根据监听到的 UDP 信息，伪造一个符合要求的恰当的 ICMP 数据包发送出去，并且能被连接的---端收到的话，就可以实现在旁路阻断的目的。

具体过程是，通过监听设备监听到一个 A-->B 的 UDP 数据包 P1 中的 IP 地址端口号等信息。

P1 数据包的信息如下：

源 ip: ipA

目的 ip ipB

源端口 portA

目的端口 portB

如果需要阻断，根据 P1 中的信息构造一个反向 B-->A 的 ICMP 回复数据包 P2 如下：

P2 数据包的信息如下：

ICMP 类型： 端口不可达

ICMP 载荷：

源 ip: ipA

目的 ip ipB

源端口 portA

目的端口 portB

通过原始套接字（raw socket)把数据包 P2 写入到链路层。此时，这个伪造的数据包 P2 会被网络设备当作正确的数据包进行转发，最后会被 A 收到。A 会认为 B 没有开启相应的服务。所以 A 把个 UDP 会话关闭。至此，达到了在旁路阻断 UDP 会话的目的。

附图说明

图 1:系统结构图

具体实施方式

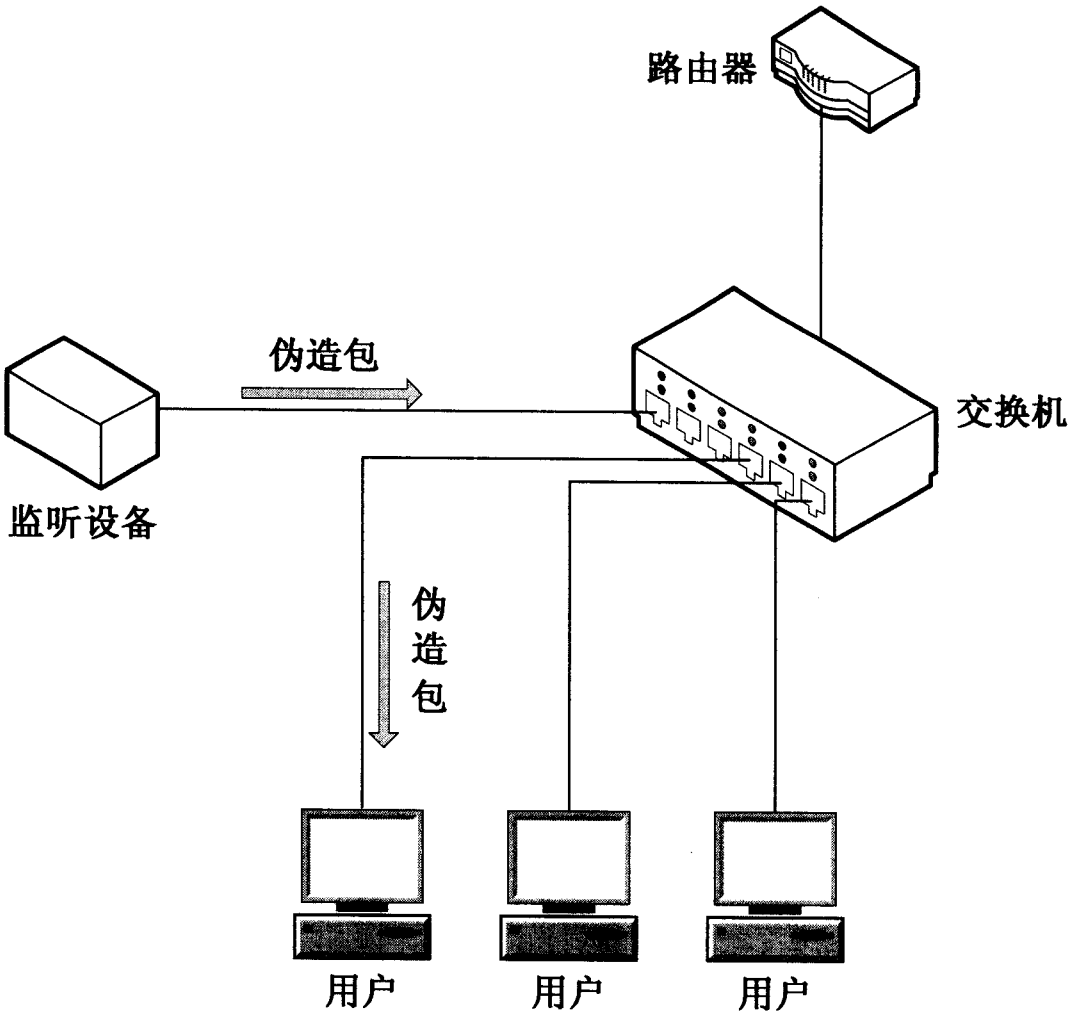
系统实施方式图 1。

1.将监听设备接入集线器或者交换机的镜像端口进行监听。

2.在监听到的数据包中分辨出需要阻断的 UDP 数据包。

3.根据需要阻断的 UDP 会话信息，构造伪造的 ICMP 数据包。

4.将伪造的数据包用 raw socket 发送到链路层。从而阻断 UDP 会话。


路由器
伪造包
交换机
监听设备
伪造包
用户
用户
用户