(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103780630 A
(43)申请公布日 2014.05.07

(21)申请号 201410056954.4

(22)申请日 2014.02.18

(71)申请人 迈普通信技术股份有限公司
地址 610041 四川省成都市高新区九兴大道16号迈普大厦

(72)发明人 严林

(74)专利代理机构 成都宏顺专利代理事务所（普通合伙） 51227
代理人 李顺德

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/46(2006.01)

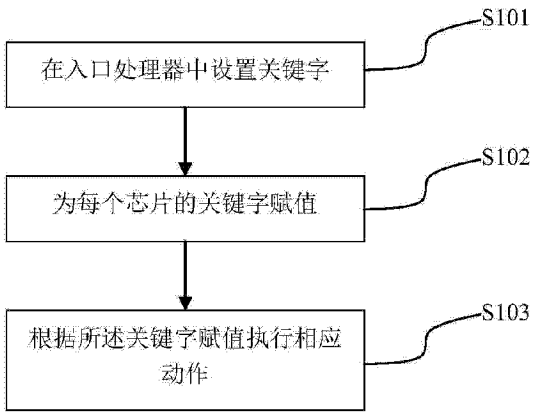
权利要求书1页 说明书3页 附图1页

(54)发明名称

虚拟局域网端口隔离方法及系统

(57)摘要

本发明涉及数据通信领域的端口隔离技术。本发明公开了一种虚拟局域网端口隔离方法，包括步骤：a、在每个交换芯片的入口处理器中设置关键字，所述关键字包括虚拟局域网编号、芯片编号、端口地址和是否经过路由字段；b、为每个交换芯片的所述关键字赋值，设置是否经过路由字段的值为未经过路由；c、报文进入交换机后，进行关键字匹配，根据所述关键字赋值执行相应动作。本发明同时公开了虚拟局域网端口隔离系统，包括关键字设置模块、关键字赋值模块、关键字匹配模块。本发明可以灵活配置隔离端口和被隔离端口在哪个虚拟局域网被隔离，解决了在一个虚拟局域网中被隔离的用户在其他虚拟局域网也被隔离的问题。



CN 103780630 A

1. 虚拟局域网端口隔离方法，包括步骤：

a、在每个交换芯片的入口内容处理器中设置关键字，所述关键字包括虚拟局域网编号、芯片编号、端口地址和是否经过路由字段；

b、为每个交换芯片的所述关键字赋值，设置是否经过路由字段的值为未经过路由；

c、报文进入交换机后，进行关键字匹配，根据所述关键字赋值执行相应动作。

2. 根据权利要求 1 所述的虚拟局域网端口隔离方法，其特征在于，步骤 a 中，所述关键字存储在入口内容处理器的三态内容寻址存储器中。

3. 根据权利要求 2 所述的虚拟局域网端口隔离方法，其特征在于，所述端口地址通过出口掩码中的位图进行标识。

4. 根据权利要求 1 所述的虚拟局域网端口隔离方法，其特征在于，步骤 b 中，每个交换芯片的所述关键字赋值相同或不相同。

5. 根据权利要求 1 所述的虚拟局域网端口隔离方法，其特征在于，步骤 c 中，所述相应动作是指入口内容处理器策略引擎中的数据流重定向动作。

6. 虚拟局域网端口隔离系统，包括关键字设置模块、关键字赋值模块、关键字匹配模块；

所述键字设置模块，用于在每个交换芯片的入口处理器中设置关键字，所述关键字包括虚拟局域网编号、芯片编号、端口地址和是否经过路由字段；

所述关键字赋值模块，用于为每个交换芯片的所述关键字赋值；

所述关键字匹配模块，用于报文进入交换机后，进行关键字匹配，根据所述关键字赋值执行相应动作。

7. 根据权利要求 6 所述的虚拟局域网端口隔离系统，其特征在于，所述关键字存储在入口内容处理器的三态内容寻址存储器中。

8. 根据权利要求 6 所述的虚拟局域网端口隔离系统，其特征在于，所述端口地址通过出口掩膜中的位图标识。

9. 根据权利要求 6 所述的虚拟局域网端口隔离系统，其特征在于，所述关键字赋值模块为每个交换芯片的所述关键字赋值相同或不相同。

10. 根据权利要求 6 所述的虚拟局域网端口隔离系统，其特征在于，所述相应动作是指入口内容处理器策略引擎中的数据流重定向动作。

虚拟局域网端口隔离方法及系统

技术领域

[0001] 本发明涉及数据通信领域的端口隔离技术，尤其涉及采用IFP（Ingress ContentAware Processor，入口内容处理器）实现的基于VLAN（Virtual Local Area Network，虚拟局域网）的端口隔离技术。

背景技术

[0002] 随着内部网络用户数量的增加和对业务多样性要求的提高，交换机接入安全的问题日益突出。出于安全的考虑，必须保证只有合法的用户才能接入数据中心的网络系统。

[0003] 早期虚拟局域网的出现就是把一个局域网（LAN）划分成多个逻辑的局域网——虚拟局域网。每个虚拟局域网是一个广播域，虚拟局域网内的主机间通信就和在一个局域网内一样，而虚拟局域网间则不能直接互通，这样就可以把一个公司内部的不同部门划分不同虚拟局域网，相互隔离各个部门，提高安全性。

[0004] 网络安全的问题日益突出，网络安全的要求越来越高，在各种虚拟局域网内部又要求更为严格的安全措施——对整个虚拟局域网内部的用户进行严格的隔离。

[0005] 出于安全的考虑，在多种应用场景中都需要隔离指定虚拟局域网中的每个用户。现有交换芯片提供了基于端口的出口表项，设置该表项中的位图用于指定从该端口进来的报文不能从位图中指定的端口出去。该功能只是简单的实现了从隔离端口进来的报文不能从被隔离端口出去。在很多应用场景中，这种简单的隔离存在天然的缺陷——不管隔离端口和被隔离端口属于哪个虚拟局域网，在这些虚拟局域网中，隔离端口和被隔离端口都是被隔离的。这种粗犷的隔离方式不能满足用户的灵活需求，还会导致本来不需要被隔离的用户实际上被隔离起来了。egress 表项不能实现基于虚拟局域网的端口隔离。

发明内容

[0006] 针对上述现有技术的问题，本发明的目的是提供一种虚拟局域网端口隔离方法，这种基于虚拟局域网的端口隔离，保证了在一个虚拟局域网被隔离的用户在其他虚拟局域网不会被隔离，用户可以灵活配置隔离端口和被隔离端口在哪个虚拟局域网被隔离。

[0007] 本发明解决所述技术问题，采用的技术方案是，虚拟局域网端口隔离方法，包括步骤：

[0008] a、在每个交换芯片的入口处理器中设置关键字，所述关键字包括虚拟局域网编号、芯片编号、端口地址和是否经过路由字段；

[0009] b、为每个交换芯片的所述关键字赋值，设置是否经过路由字段的值为未经过路由；

[0010] c、报文进入交换机后，进行关键字匹配，根据所述关键字赋值执行相应动作。

[0011] 具体的，步骤 a 中，所述关键字存储在入口内容处理器的三态内容寻址存储器中。

[0012] 进一步的，所述端口地址通过出口掩码中的位图进行标识。

[0013] 进一步的，步骤 b 中，每个交换芯片的所述关键字赋值相同或不相同。

[0014] 具体的，步骤 c 中所述相应动作，是指入口内容处理器策略引擎中的数据流重定向动作。

[0015] 本发明的另一个目的是，提供一种虚拟局域网端口隔离系统包括关键字设置模块、关键字赋值模块、关键字匹配模块；

[0016] 所述键字设置模块，用于在每个交换芯片的入口内容处理器中设置关键字，所述关键字包括虚拟局域网编号、芯片编号、端口地址和是否经过路由字段；

[0017] 所述关键字赋值模块，用于为每个交换芯片的所述关键字赋值；

[0018] 所述关键字匹配模块，用于报文进入交换机后，进行关键字匹配，根据所述关键字赋值执行相应动作。

[0019] 具体的，所述关键字存储在入口内容处理器的三态内容寻址存储器中。

[0020] 具体的，所述端口地址通过出口掩码中的位图进行标识。

[0021] 进一步的，所述关键字赋值模块为每个交换芯片的所述关键字赋值相同或不相同。

[0022] 具体的，所述相应动作是指 IFP 策略引擎中的数据流重定向动作。

[0023] 本发明的有益效果是，用户可以灵活配置隔离端口和被隔离端口在哪个虚拟局域网被隔离，解决了在一个虚拟局域网中被隔离的用户在其他虚拟局域网也被隔离的问题。本发明采用入口内容处理器来实现该方案，该部件在现有的任何交换芯片都支持，通用性好、应用广泛。

附图说明

[0024] 图 1 为实施例的方法流程图；

[0025] 图 2 为实施例的系统结构示意图。

具体实施方式

[0026] 下面结合附图及及具体实施方式，详细描述本发明的技术方案。

[0027] 在交换芯片中都有 IFP、EFP（Egress ContentAware Processor，出口内容处理器）、VFP（Vlan ContentAware Processor，虚拟局域网内容处理器）三个 CAP（ContentAware Processor，内容处理器）部件，其中 IFP 部件对入方向的报文做匹配和过滤处理，EFP 部件对出方向的报文做匹配和过滤处理，VFP 部件对 QINQ 报文（一种 VLAN 报文）做添、删、改处理。VFP 部件不能达到本发明的需求，不能选择。在 IFP 和 EFP 部件的选择上，结合该功能的特性——隔离端口和被隔离端口可能会处于不同的芯片中，这样如果选择 EFP 部件，由于 EFP 部件中不能支持隔离和被隔离端口不在同一芯片的情况，这样导致隔离端口和被隔离端口是跨芯片端口时不能达到隔离的目的，存在缺陷。而恰好在 IFP 中对隔离端口可以识别标识该端口属于哪个芯片的 modId（芯片 ID），这样在 IFP 中设置匹配隔离端口的 srcPortId（源端口 ID）加上该端口的 modId 就可以解决隔离端口和被隔离端口跨芯片的问题。

[0028] 实施例

[0029] 如图 1 所示，本发明实施例虚拟局域网端口隔离方法，主要步骤如下：

[0030] S101，在每个交换芯片的入口内容处理器中设置关键字，所述关键字包括虚拟局

域网编号、芯片编号、端口地址。并将上述关键字存储在入口内容处理器的三态内容寻址存储器中。

[0031] 选择了CAP中的IFP部件后，然后要决定匹配的字段，匹配的字段就是根据用户需求设定的能够满足场景需求的关键字。在本发明实施例中，由于要隔离虚拟局域网中的用户，匹配的字段首先必须要包括虚拟局域网的编号(VLAN ID)，其次要包括隔离端口的端口地址(srcPort ID)和芯片编号(mod ID)，通常还要将三层路由(L3route)字段设置为0，表示没有经过路由。

[0032] S102，为每个交换芯片的所述关键字赋值，设置是否经过路由字段的值为未经过路由。

[0033] 为了达到隔离报文源端口和目的端口的目的，同时解决源端口和目的端口在不同芯片的问题，除了在交换机中每个交换芯片的IFP中的TCAM（ternary content addressable memory）设置如上所述的匹配字段外，还需要根据用户的需求差异为关键字设置相同或不同的值。如果需要在每个芯片中隔离相同的端口，即执行相同的动作，就可以为上述关键字设置相同的值，如果在不同芯片上匹配相同的字段，而需要执行不同的动作，即在不同芯片隔离不同的端口，就需要为上述关键字设置不同的值。

[0034] S103，进入交换机后，进行关键字匹配，根据所述关键字赋值执行相应动作。

[0035] 本发明实施例执行的动作采用了入口内容处理器策略引擎(IFP policy engine)中的redirect（数据流重定向）的动作，该动作本来用于对匹配的流做重定向动作，改变该条流的出端口。但是该动作中有一个egressMask（出口掩码）行为，通过该动作中的egressMask行为可以指定被隔离端口的位图，这样从一个端口进入的报文可以与多个端口隔离。如果从芯片0端口进来的报文需要与芯片1端口的报文进行隔离而不需要隔离芯片0上的端口，这时芯片0和芯片1上的关键字设置一样，芯片0上的egressMask动作是不隔离入端口的报文，而芯片1上的egressMask动作是隔离本芯片指定端口或者所有端口的报文，通过分别设置egressMask为0或者设置egressMask为指定端口来实现这个功能。

[0036] 因为IFP中的匹配规则包括了VLAN ID，所以当一个报文从入口进入交换机，走到IFP处理流程时，只有完成匹配了如上规则包括VLAN ID才执行redirect动作来实现隔离，所以在不同的VLAN中由于VLAN ID不能匹配，不能实现隔离，这样本发明就真正实现了的基于虚拟局域网的隔离。

[0037] 本发明实施例系统结构如图2所示，包括关键字设置模块201、关键字赋值模块202、关键字匹配模块203。

[0038] 所述键字设置模块，用于在每个交换芯片的入口处理器中设置关键字，所述关键字包括虚拟局域网编号、芯片编号、端口地址，并将所述关键字存储在入口内容处理器的三态内容寻址存储器中。所述端口地址通过出口掩码中的位图标识。

[0039] 所述关键字赋值模块，用于为每个交换芯片的所述关键字赋值，根据用户的不同需要，关键字赋值模块为每个交换芯片的所述关键字赋值可以相同或不相同。

[0040] 所述关键字匹配模块，用于报文进入交换机后，进行关键字匹配，根据所述关键字赋值执行相应动作，该相应动作是指入口内容处理器策略引擎中的数据流重定向动作。

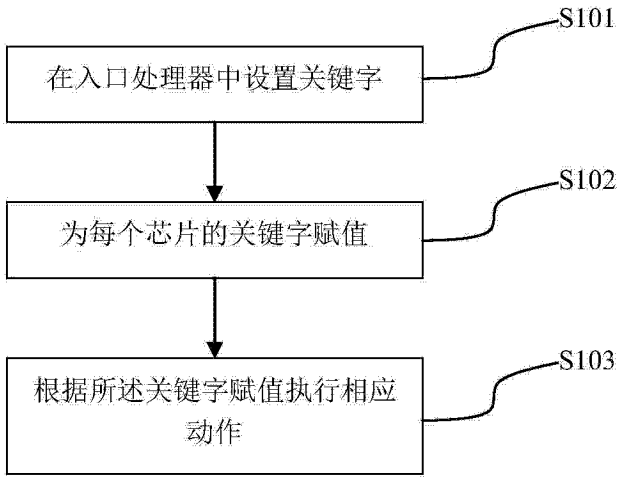

S101
在入口处理器中设置关键字
S102
为每个芯片的关键字赋值
S103
根据所述关键字赋值执行相应动作

图 1

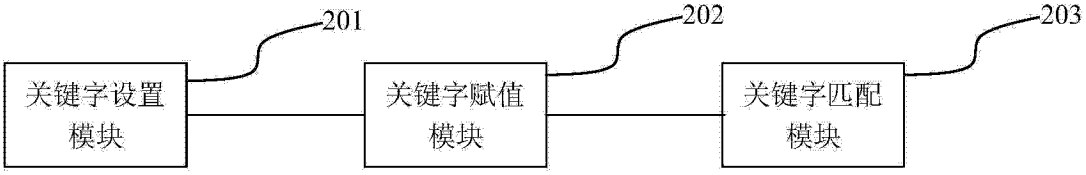

201
关键字设置模块
202
关键字赋值模块
203
关键字匹配模块

图 2