

一种面向交换机应用的访问控制模块设计

位荣友,吴龙胜,陈庆宇,赵文琦
(西安微电子技术研究所,陕西 西安 710065)

摘 要: 为了解决交换机中数据风暴、DoS(Denial of Service)攻击等网络安全问题,本文提出了一种基于数据帧差异化控制的访问控制模块,该模块以接收端口数据帧为基本粒度进行解析,生成与接口数据帧一一对应的解析关键字,然后通过解析关键字的匹配分析对数据帧进行差异化管理,同时通过令牌桶和计数器进行数据帧流量控制,从而实现了以太网各种数据帧的过滤、TOS/DSCP 修改以及转发向量更新等。仿真结果表明,该模块实现了预期功能,满足项目应用需求。

关键词: 访问控制;令牌桶;TCAM;DoS 攻击;以太网交换机

中图分类号: TN432

文献标识码: A

文章编号: 1000-7180(2018)10-0136-05

Access Control Module Design for Switcher Applications

WEI Rong-you, WU Long-sheng, CHEN Qing-yu, Zhao Wen-qi

(Xi'an Microelectronics Technology Institute, Xi'an 710065, China)

Abstract: In order to address the network security issues such as data storms and DoS etc, a frame-differentiation-control-based access control module is presented in this paper. Firstly, data frames from the receiving port are analyzed as the basic granularity. And then analytical keywords are generated corresponding to those data frames. Finally, the differentiated management is implemented based on the analysis for analytical keywords of data frames. Simultaneously, frame filtering, TOS/DSCP modification and forwarding vector updates are also implemented by traffic controls of data frame which base on the token bucket and counter. The function of access control module has been verified and analysis, which shows that the expected function are achieved and project application requirements are satisfied.

Key words: access control; token bucket; data storm; DoS attack; ethernet switcher

1 引言

随着计算机网络的发展,数据风暴、DoS 攻击等愈发威胁计算机网络的安全。作为能够实现数据帧的转发、过滤、优先级调度及限速的访问控制模块是一种保护计算机免受网络攻击的有效单元,在交换机系统中具有重要的应用。具体的说,访问控制机制通过检查一个数据帧的 IP 报头是否与预先定义的规则匹配,然后根据匹配的结果进行相应的处理。预先定义的规则被称为访问控制列表(Access Control List, ACL),它由一组有先后次序的规则组成^[1]。

实现访问控制机制有两种方式,一种是通过软件方式实现,另一种是通过硬件方式实现^[2]。软件处理的方式成本低,廉价的路由器或计算机通过编写可执行软件的方式实现访问控制;对于速率要求较高的千兆以太网交换机中,软件实现访问控制的处理速度太慢,不能满足高速以太网交换机的应用需求。

针对上述问题,本文提出了一种基于数据帧差异化控制的硬件访问控制模块,通过对接端口数据帧的细粒度分析,实现了高效率的数据帧过滤、TOS/DSCP 修改等,既满足了千兆及万兆以太网交

换机的数据帧实时处理的性能需求,又提高了网络安全的鲁棒性.

2 访问控制模块的架构

访问控制模块的架构如图 1 所示,各模块之间通过必要的粘合逻辑组成统一的整体. 主要包括以下几个模块,各模块的原理及详细设计将在本文第三部分介绍.

(1)帧解析模块:该模块用于对接收的数据帧进行解析,将解析的结果组成用于对数据帧的 IP 包头进行查询的关键字,然后将关键字送到查询模块.

(2)查询模块:该模块用于存放访问控制列表预

定义的规则,并将接收自帧解析模块的关键字与存放的规则进行查询,得出查询结果,并将查询结果送至动作查找模块.

(3)动作查找模块:该模块用于存放操作数、判断是否存在速率违规以及对操作信息进行统计,查询模块将查询结果送至动作查找模块,动作查找模块根据查询结果来寻找相应的操作数,并将操作数送至动作解析模块.

(4)动作解析模块:该模块用于对操作数进行解析,将解析的结果输出至相应的模块进行操作,操作包括改变发送队列、改变 DSCP 以及改变转发对象等.

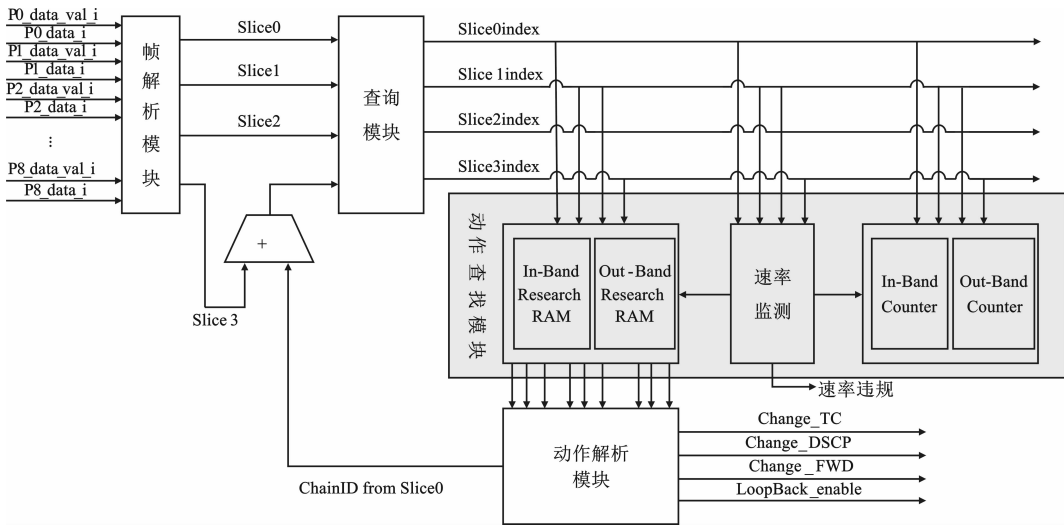


图 1 访问控制模块结构图

3 访问控制模块的设计实现

本模块设计包括支持数据帧解析的帧解析模块、支持智能匹配的查询模块、支持查找操作数的动作查找模块以及支持操作数解析的动作解析模块. 该访问控制模块具有支持对数据帧进行四层解析等特点. 详细设计方案在本部分进行说明.

3.1 帧解析模块

该模块支持以轮询的方式对 9 路数据帧的请求进行操作并将读入的数据帧进行解析,解析的流程如图 2 所示,通过对数据帧进行解析,组成动作查找模块所需的关键字.

从 MAC(Media Access Control)或者其它模块接收的数据帧的格式如图 3 所示. 通过读取数据帧的相应位判定数据帧是 untag, C-tag, S-tag 或者 Double Tag^[3],在判定 Tag 类型之后根据 Ether-Type 位的值判定数据帧是 DIXv2,SNAP 或者 LLC

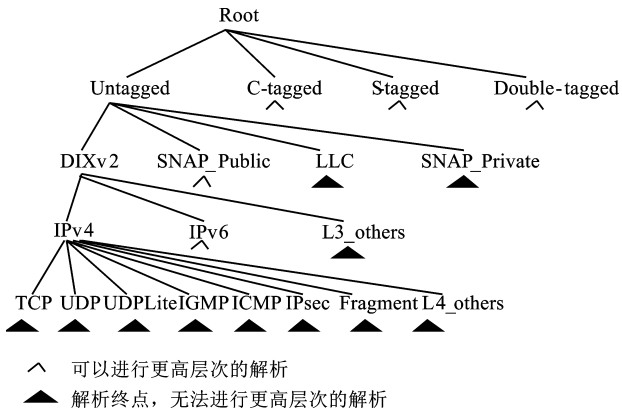


图 2 帧解析流程图

格式(如图 4 所示),DIXv2 格式是主要的用于 IP 通信的数据帧类型,LLC 格式是用于支持 OSI 协议栈的 IEEE 802 标准帧类型,SNAP 格式是 LLC 格式的一种扩展,用以支持 EtherType,其中,SNAP_Public 格式用于标准的基于 EtherType 的协议,

SNAP_Private 格式用于具体 vendor 的协议. 根据不同的格式采取不同的解析策略. 对于 DIXv2 格式的数据帧, 该模块提取 EtherType 位并依据 EtherType 位进行更高层协议的解析, EtherType 位 LLC 格式的数据帧, 该模块提取 DSAP/SSAP 位并根据用户定义位进行解析; 对于 SNAP_Private 格式的数据帧, 该模块提取 VendorID 和 LocalCode,

根据用户自定义位进行解析; 对于 SNAP_Public 格式的数据帧, LocalCode 被当做 EtherType 处理, 更高层次的解析操作和 DIXv2 格式的数据帧相同.

三层解析主要支持 IPv4 和 IPv6 两种类型(如图 5), 此外还有 IPv6 扩展报头类型. 根据 EtherType 位确定协议的类型, EtherType 位的值为 0x0800 为 IPv4 类型, EtherType 位的值为 0x86DD 为 IPv6 类型. 四层解析主要支持 TCP, UDP, UDPLite, IGMP, ICMP 和 IPsec 等类型协议的解析.

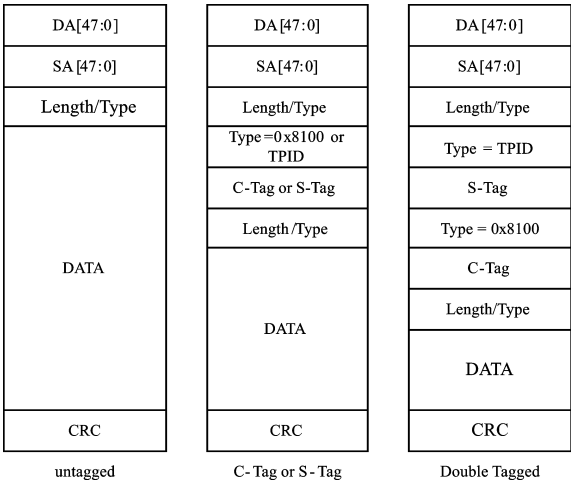


图 3 VLAN Tag 结构图

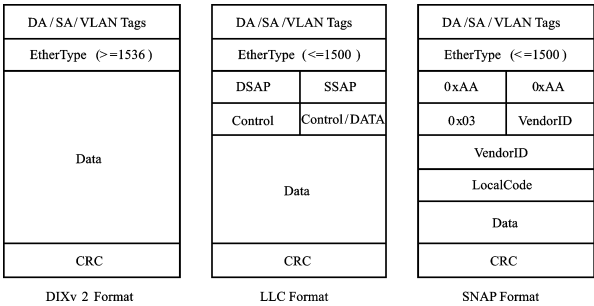


图 4 以太网帧结构图

本关键字最主要的组成部分是用户自定义位 (User Define Field, UDF), 为了方便用户进行配置, 该部分采用寻址操作中常用的基地址+偏移地址的方法进行设计, 在本模块中主要的基地址包括

帧开头、3 层协议起始位和 4 层协议起始位这三个位置, 偏移地址的范围在 0~480 之间, 故采用 3 位基地址和 5 位偏移地址, 偏移地址每个地址代表 16 位二进制数, 基地址的值的变化与接收到的帧的解析路径相关, 用户通过配置寄存器的方式决定提取数据的位置.

3.2 查询模块

该模块对接收到的关键字执行部分字段的模糊查找, 一般的 RAM 执行这种类型的查找需要逐条进行查找, 速度较慢, 查找效率太低. 本模块设计采用 TCAM(Ternary Content Addressable Memory) 作为查询所用的存储器件, TCAM 可以在一个时钟周期内完成关键字与所有预定义规则的匹配查找并返回查找结果, 效率极高.

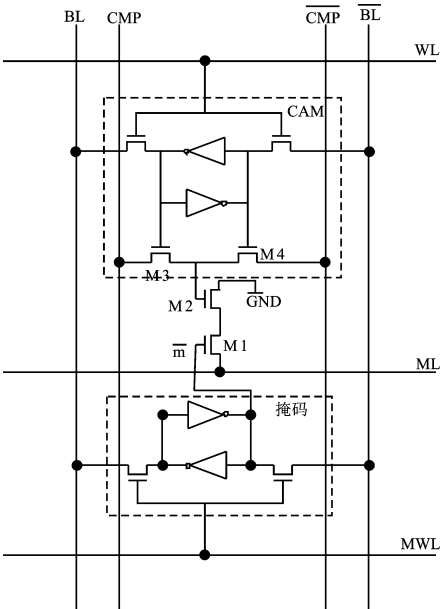


图 5 典型的 TCAM 单元结构

一种典型的 TCAM 单元如图 5 所示, 由一个 CAM 和掩码位组成, 其中 CAM 由一个 SRAM 单元和一个异或门构成, 掩码位是一个 SRAM 单元^[4]. CAM 用于存放数据. 当掩码位的值为 1 时 CAM 中的内容有效, 掩码位的值为 0 时忽略 CAM 中的内容. 宽度为 L 的 TCAM 由 M 个这样的单元连接而成. 在每次查找操作之前, ML(Match Line) 置为高电平, 待比较的位通过 CMP 和 CMP-bar 输入到 TCAM 单元, 与 CAM 中的位进行比较操作. 当掩码位的值为 0 时, M-bar 为低电平, M1 截止, ML 与地之间的断路, ML 保持在高电平; 当掩码位设置为 1 时, M1 导通, 当输入的比较位与存储位的值相同时, M2 截止, ML 维持在高电平, 但是当输入的比较

位与存储位不相同, M2 导通, ML 与地之间产生通路, ML 放电后变为低电平, 表明查询匹配未命中。

3.3 动作查找模块

该模块的作用是对来自于查询模块的索引值进行查找操作数操作、对索引值数据流进行速率监测以及统计操作信息。

典型的查表流水线方案是由 TCAM 搭配 RAM 完成查找和读取作业, 因此本文的查询操作数模块采用 SRAM 设计实现^[5], 操作数的格式如图 6 所示, 本文设计的访问控制模块支持至多 256 条预定义规则的查询, 为了实现查询与操作数的一一对应, 操作数查找 RAM 的大小设计为 256×64 , 使用 DPRAM IP 核。

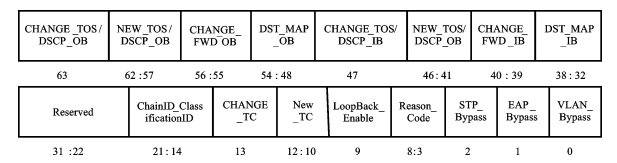


图 6 操作数格式

对索引值数据流进行速率监测采用令牌桶, 令牌桶的设计如 7 图所示, 为了对添加令牌的时间与数量进行精确控制, 根据项目需求对系统时钟进行分频操作, 采用 3 种频率的时钟和相应的令牌数向令牌桶添加令牌, 用户可以根据实际应用需求选择合适的时钟频率, 配置令牌桶的大小、初始令牌值以及每次添加令牌的数量。令牌桶按照用户配置向令牌桶增加令牌, 直到最大值为止。期间有所引致通过时, 通过计算扣除相应令牌值, 将桶内剩余令牌与初始值进行比较, 若大于初始令牌值则说明速率不超过用户配置速率, 反之则为超过用户配置速率^[6]。

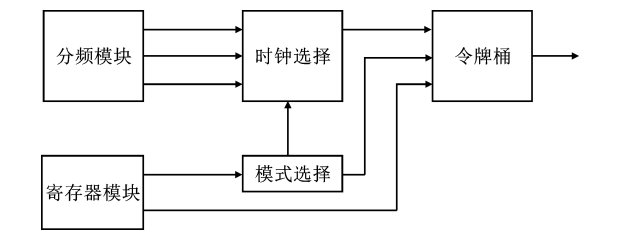


图 7 令牌桶模块设计

3.4 动作解析模块

动作解析模块的设计如图 8 所示, 接收来自于动作查找模块的操作数。本模块会接收到至多 4 个操作数, 分别来自于 4 个不同的查找关键字。读取操作数的相应位进行解析, 解析出有效地动作, 并将动

作送到与操作对应的模块。

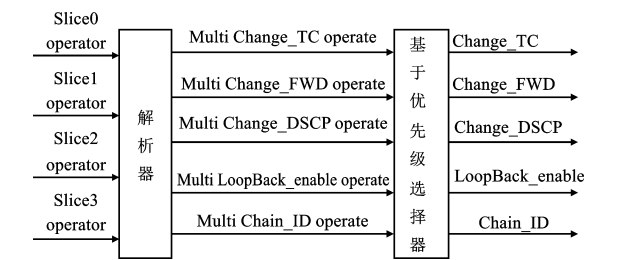


图 8 动作解析模块结构图

解析操作数时, 当多个操作数对同一个动作的执行发生冲突时, 按照如下优先级顺序选择动作行为: 对于配置非联合搜索的 Slice0, Slice1, Slice2 和 Slice3, Slice0 的优先级最低, Slice3 的优先级最高; 对于配置联合搜索的 Slice1, Slice2 和 {Slice0, Slice3}, Slice1 的优先级最低, {Slice0, Slice3} 作为联合搜索拥有最高优先级。

主要动作包括如下几个:

Change_TC: 表示是否对在发送队列中等待发送的数据包增加新的转发端口, 0 表示不增加, 1 表示增加。

Rate_Violation: 表示匹配的数据包的速率是否超过了相应的数据流的速率, 0 表示未超过规定速率, 1 表示超过规定速率。

Change_DSCP: 表示是否修改匹配的数据包的 IP DSCP 位, 0 表示不修改, 1 表示修改。

Change_FWD: 表示是否为匹配的数据包增加新的转发目标, 00 表示不增加, 01 保留, 10 表示用 DST_Map 位替换转发目标, 11 表示将 DST_Map 加入到转发目标。

LoopBack_Enable: 表示匹配的数据包是否可以转发到该数据包被接收的端口^[7]。

4 访问控制模块设计与验证

本设计采用 Verilog HDL 硬件描述语言设计实现, 并搭建 SOC 验证环境, 通过 ModelSim 进行功能仿真, 观察信号波形, 对其功能进行验证。如图 9 所示, 配置 Slice2 对应的寄存器使其依据数据帧源地址不同进行差异化控制, 其它 Slice 对应的寄存器不作配置, 从端口接收一个数据帧, 并对数据帧进行解析, 生成解析关键字并且拉高解析关键字有效位。

如图 10 所示, 通过寄存器配置对应第一个数据帧的行为是改变 DSCP 值、改变转发队列、改变转发端口以及不转发回源端口, 速率监测模块监测到速率不违

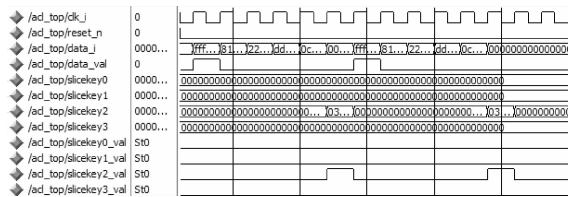


图 9 帧解析验证图

规,计数数值加 1;第二个数据帧的行为是改变 DSCP 值、改变转发队列、不改变转发端口以及不转发回源端口,速率监测模块监测到速率不违规,计数数值加 1,从而实现了以数据帧为基本粒度的差异化控制。

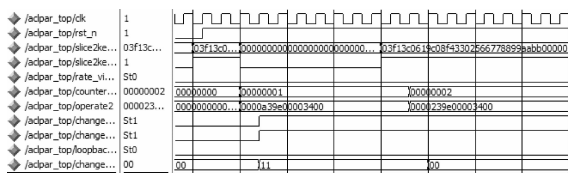


图 10 动作解析验证图

5 结束语

为了抑制数据风暴、DoS 攻击等网络安全问题,同时满足千兆以太网交换机的实时处理需求,本文设计了一款面向交换机应用的访问控制模块,包括帧解析、关键字查询、动作查找和动作解析等子模块,支持用户自定义配置的转发、过滤和改变 TOS/DSCP 等操作.使用 Verilog HDL 语言进行设计,通过 ModelSim 仿真验证,结果表明:本文的设计实现了预期的目标,满足项目应用需求。

参考文献:

[1] 谢声时,陈海鸿,汪浩,等. 交换机 ACL 的研究与应用[J]. 华南金融电脑, 2009 (12): 40-41.

[2] Ishikawa T, Yoshiura N. Decreasing access control list processed in hardware[J]. Management Enabling the Future Internet for Changing Business and New Computing Services, 2009: 453-457.

[3] 薛文莲. 基于双层标签的 VLAN 交换技术的研究[D]. 北京:北京邮电大学, 2013.

[4] 张怀庆. 基于 TCAM 和多核处理器的高速路由查找转发引擎设计[D]. 济南:山东大学, 2008.

[5] 柯向东,黄建华. 基于 TCAM 的 IPSec 快速查找技术[J]. 微计算机信息, 2005, 21(08X): 4-6.

[6] 马徐瀚,吴龙胜,赵坤鹏,等. 一种基于多令牌桶的数据风暴抑制单元[J]. 微电子学与计算机, 2016, 33(9): 84-88.

[7] 周明天,汪文勇. TCP/IP 网络原理与技术[M]. 北京:清华大学出版社有限公司, 1993.

作者简介:

位荣友 男,(1992-),硕士研究生. 研究方向为集成电路设计. E-mail:18792841073@163.com.

吴龙胜 男,(1968-),博士,研究员. 研究方向为集成电路设计.

陈庆宇 男,(1988-),博士,工程师. 研究方向为 VLSI 及抗辐照芯片设计.

赵文琦 女,(1985-),硕士,工程师. 研究方向为集成电路设计.