在SFE/SGE可堆叠的被管理的交换机的端口安全配置

客观

*端口安全*页用于强化在交换机的安全。可以配置端口锁定以端口安全。对锁着的端口的访问对有特定MAC地址的用户被限制。这些MAC地址在端口在端口统计性地定义或了解至允许的MAC地址最大数量。当自未知MAC地址的一个信息包在一个锁着的端口时到达，端口安全能转发信息包，丢弃信息包没有陷井，丢弃与陷井的信息包或者关闭了端口。

此条款说明如何配置在SFE/SGE可堆叠的被管理的交换机的端口安全。

可适用的设备

•SFE/SGE可堆叠的被管理的交换机

软件版本

•v3.0.2.0

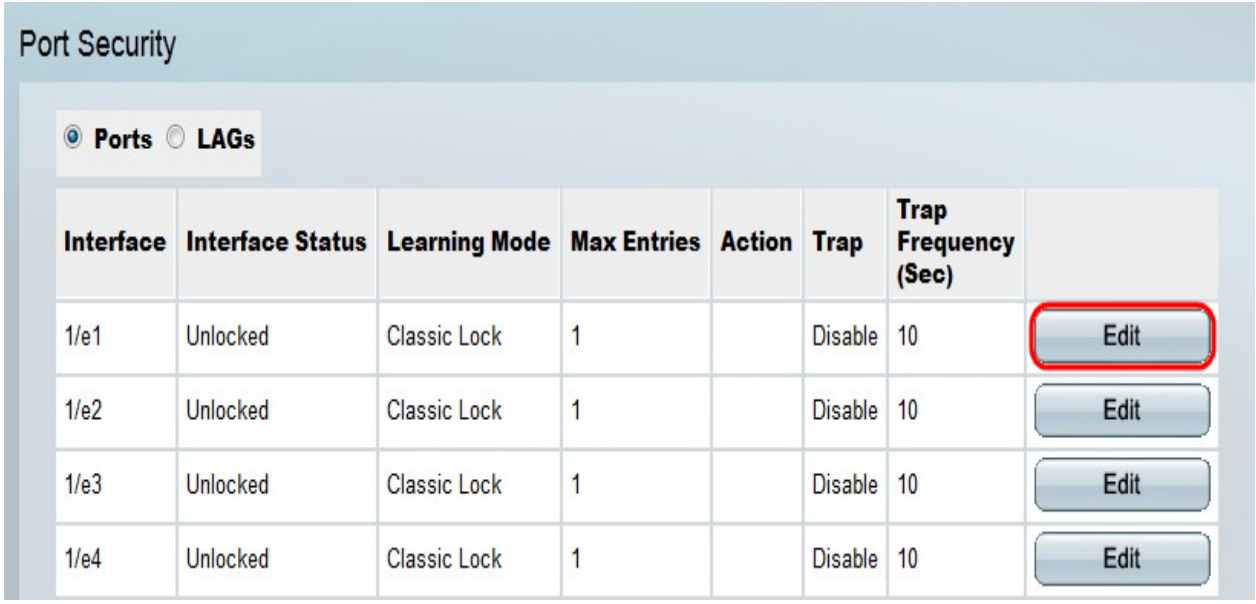
端口安全性

步骤1.登陆到Web配置工具并且选择**安全套件>数据流控制>端口安全**。*端口安全*页打开：

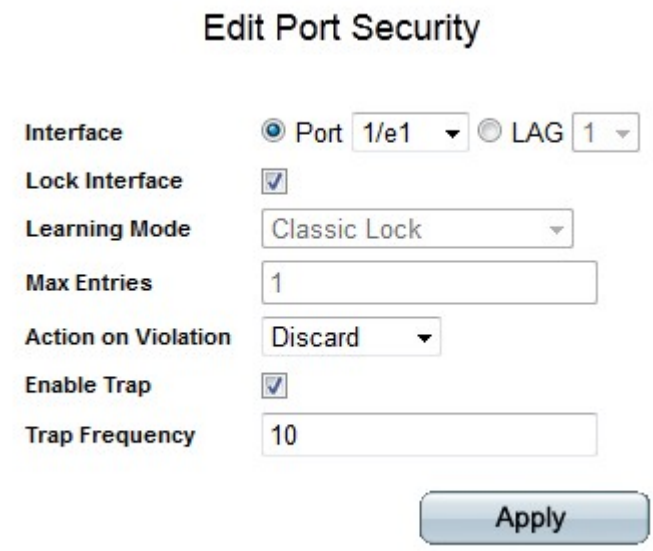
步骤2.点击对应于所需的接口您要编辑的单选按钮。

•端口—显示端口的端口安全配置。

•滞后—显示滞后的端口安全配置。



步骤3.点击**编辑**编辑接口。*编辑端口安全*窗口出现。



第4.步(可选)点击对应于所需的接口您在接口字段要编辑的单选按钮。

- •端口—从端口下拉列表请选择端口配置。这只将影响选择的单个端口。
- •滞后—从滞后下拉列表请选择滞后配置。这将影响在滞后配置定义的端口组。

第 5 步：检查**锁定接口**锁定接口。

第6.步。从学习状态下拉列表请选择一个学习状态。学习状态定义了锁着的端口类型。

- •经典锁定—端口是锁着的不管已经了解地址的数量。
- •有限的动态锁定—删除与端口产生关联的当前动态MAC地址锁定端口。端口了解至在端口允许的最大地址。

Note:必须开锁接口更改学习状态。

步骤7.输入在最大条目字段的接口可以了解MAC地址的最大数量。

第8.步。从对侵害下拉列表的动作，当信息包在一个锁着的端口时，到达请选择应采取的措施。

- •丢弃—丢弃自所有无学问的来源的信息包。
- •前言—转发自了解MAC地址的未知源withouth的信息包。
- •关闭—丢弃自所有无学问的来源的信息包并且关闭端口。端口将保持关闭，直到恢复活动或重置交换机。

第9.步。当信息包在一个锁着的端口时，收到请检查**Enable (event)陷井**发送陷井。陷井是用于的生成的SNMP消息报告系统事件。陷井将强制连接的设备发送SNMP信息到单个主机侵害发生了

步骤10.进入期望时间允许在被发送的陷井之间在陷井频率区域。

步骤11.点击**适用**。

警告：这只保存您的配置对运行配置文件。这意味着做的所有变动将丢失，如果重新启动设备。如果希望在系统重新启动以后保存这些更改，您需要复制运行配置文件到启动配置文件。请

参阅*复制在SFE/SGE系列被管理的交换机的配置文件*关于如何执行此的更多信息。