在200/300系列被管理的交换机的端口安全配置

客观

在您的网络的安全是重要性。安全网络防止攻击能进入您的网络的入侵者。一种方式增强在您的网络的安全将配置端口安全。端口安全允许您配置在一个特定端口或链路聚合组(滞后)的安全。滞后结合单个接口到单个逻辑链接，提供八条物理链路会聚带宽。您能对特定port/LAG的不同的用户限制或允许。

此条款说明如何配置在200/300系列被管理的交换机的端口安全。

可适用的设备

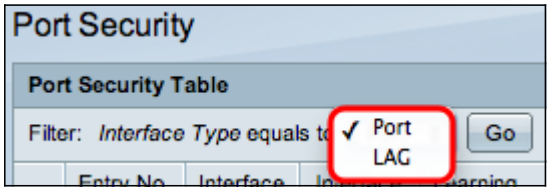
- SF/SG 200和SF/SG 300系列被管理的交换机

软件版本

- 1.3.0.62

端口安全配置

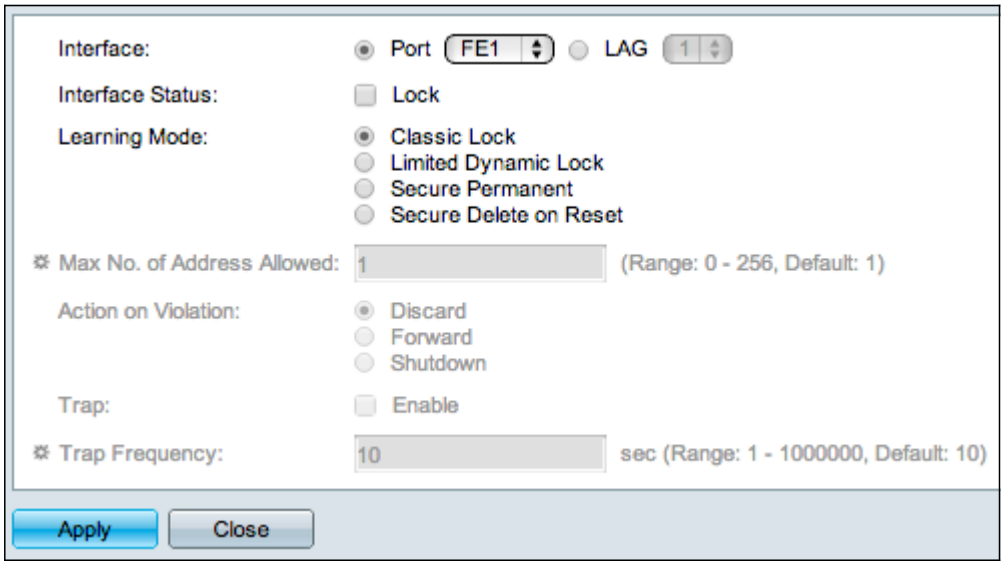
步骤1.登陆到Web配置工具并且选择**安全>端口安全**。*端口安全*页打开：

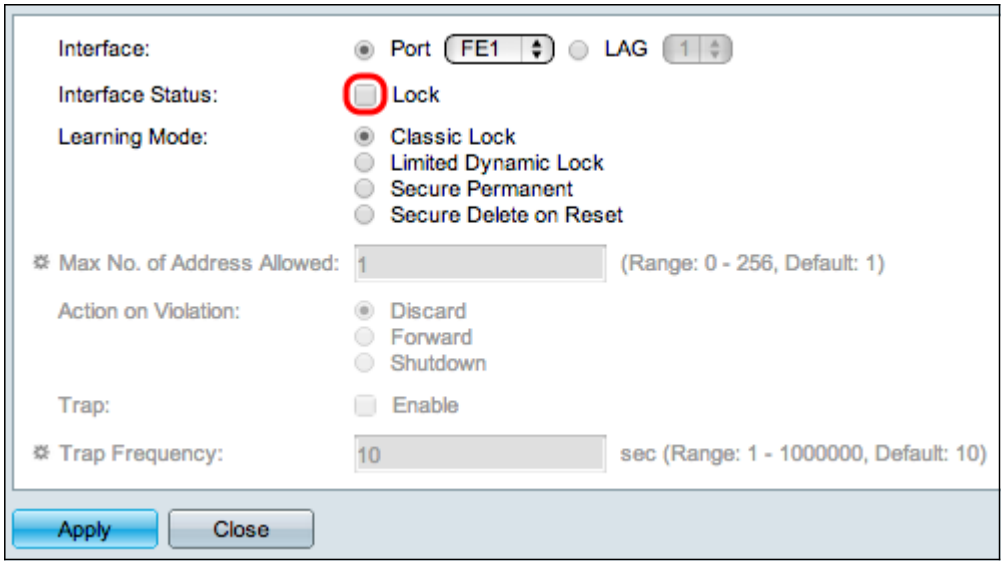


Step 2.从接口类型下来等于丢弃列表，请选择端口或滞后并且点击**去。**

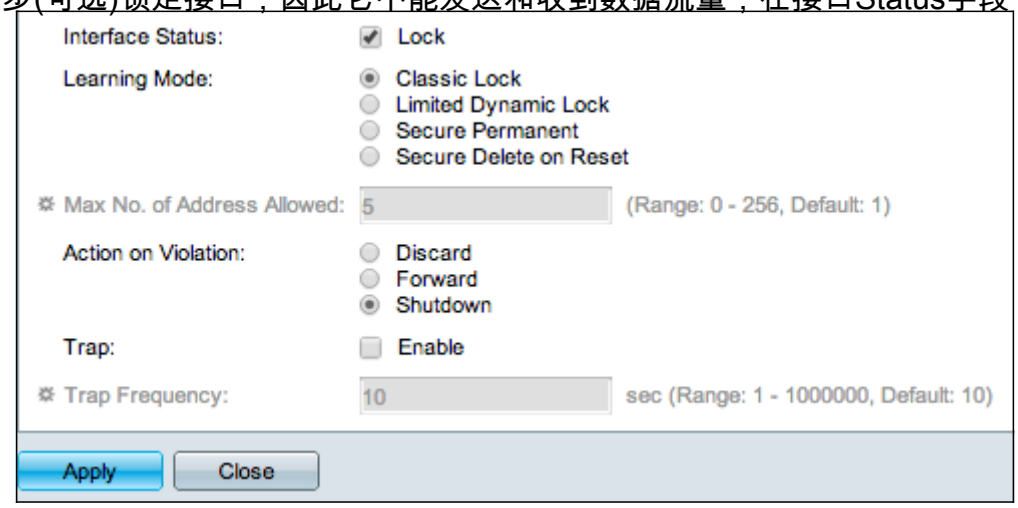
步骤3.点击您要编辑其安全设置接口的单选按钮。

步骤4.点击**编辑**。*Settings窗口编辑端口安全的接口*出现：





第5.步(可选)锁定接口，因此它不能发送和收到数据流量，在接口Status字段，检查**锁定**复选框。



第6.步。在了解Mode字段，请点击期望学习状态的单选按钮。可用的选项是：

- 经典锁定—立即锁定端口，不管已经了解设备的数量。
- 有限的动态锁定—删除当前MAC地址与端口有关锁定它。端口能了解特定量的设备。
- 获取永久性—保持当前MAC地址与端口有关，并且能了解的设备的一个特定编号。
- 获取在重置的删除—删除当前MAC地址与端口有关在重置以后。在重置后交换机，端口能了解特定量的设备。

第 7 步：在最大提供的不地址字段，输入端口允许了解MAC地址的最大数量。如果0输入，则端口只支持静态地址。

第8.步。 如果锁定在第5步的端口，则在对侵害字段的动作，请点击应采取的措施的单选按钮，当侵害发生时。可用的选项是：

- 丢弃—信息包，如果来源未知，丢弃。
- 前言—信息包，如果来源未知，转发。
- 关闭—丢弃信息包，并且端口被关闭。

第9.步(可选的) A陷井被触发，在信息包在一个锁着的端口时候收到，保证信息包不会违犯锁着的端口。对enable (event)陷井，请检查在陷井字段的**Enable复选框**。陷井是一个同步通知从代理程序到包括当前sysUpTime值的管理器，他们生成，当情况在简单网络管理协议(SNMP)代理程序时符合了。这些情况在管理信息库(MIB)被定义

第10.步。如果陷井在第9步允许，请以在每个陷井之间的秒钟送进最短时间在陷井频率区域。

步骤11.点击**适用**。

下面的图片显示在配置端口上的变化。

Note:要运用一个端口的端口安全配置于多个端口，请参见部分*运用端口安全配置于多个端口*。

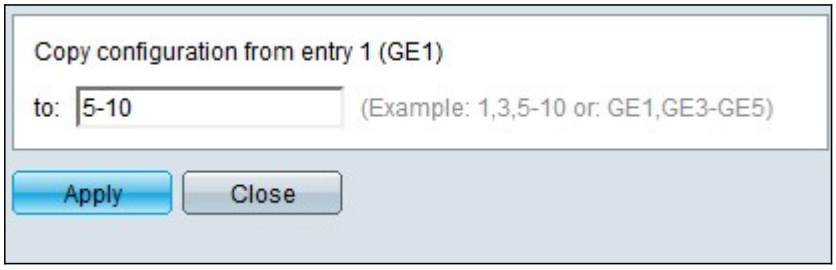
运用端口安全配置于多个端口

此部分说明如何运用单个端口的安全端口配置，于多个端口。

步骤1.登陆到Web配置工具并且选择**安全>端口安全**。*端口安全*页打开：

步骤2.点击您希望运用其配置于多个端口端口的单选按钮。

步骤3.点击**“Copy”设置**。*Settings窗口的复制*出现。



第 4 步：在对字段，请输入将有端口相同端口安全配置您在第2.步选择的端口范围。您能使用端口号或端口的名字作为输入。您能输入一个逗号分离的每个端口，例如1， 3， 5或GE1、GE3， GE5或者您能输入一个端口范围，例如1-5或GE1-GE5。

步骤5.点击**适用**保存您的配置。

下面的镜像显示单个端口安全配置的应用程序，多个端口。