300系列托管交换机上的端口安全配置

目标

您的网络中的安全至关重要。安全网络可防止入侵者侵入您的网络。增强网络安全性的一种方法是配置端口安全。端口安全允许您在特定端口或链路聚合组(LAG)上配置安全。LAG将各个接口合并到单个逻辑链路中，这可提供最多八个物理链路的聚合带宽。您可以限制或允许对给定端口/LAG上不同用户的访问。

本文介绍如何在300系列托管交换机上配置端口安全。

适用设备

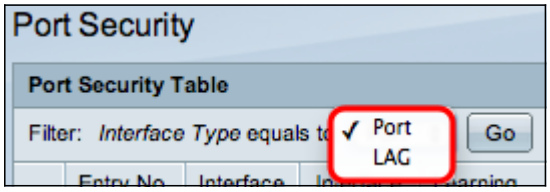
·SG300-10PP
· SG300-10MPP
· SG300-28PP-R
· SG300-28SFP-R
· SF302-08MPP
· SF302-08PP
· SF300-24PP-R
· SF300-48PP-R

软件版本

·1.4.0.00p3 [SG300-28SFP-R]
· 6.2.10.18 [所有其他适用设备]

端口安全配置

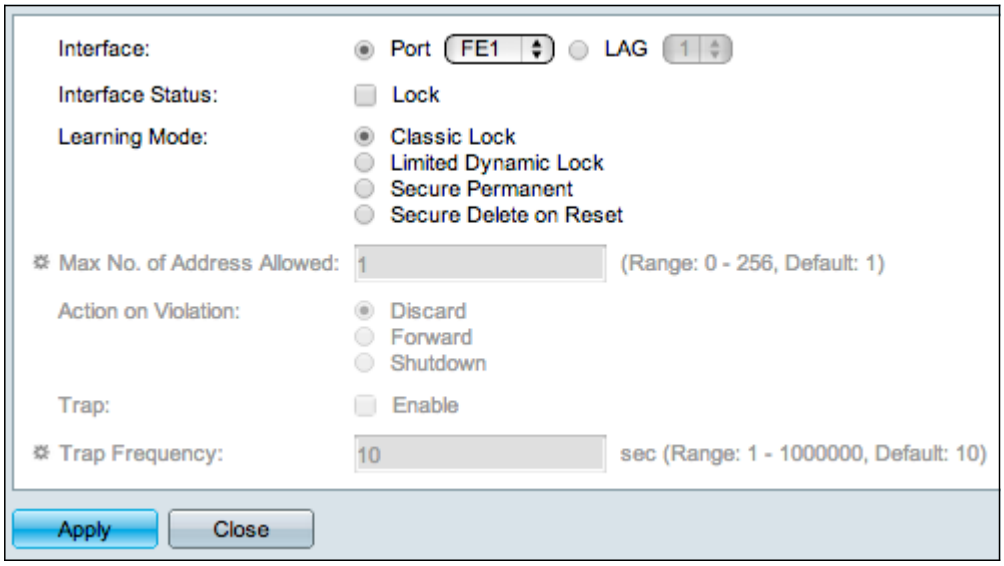
步骤1.登录Web配置实用程序，然后选择Security **> Port Security**。“端*口安全*”页打开：

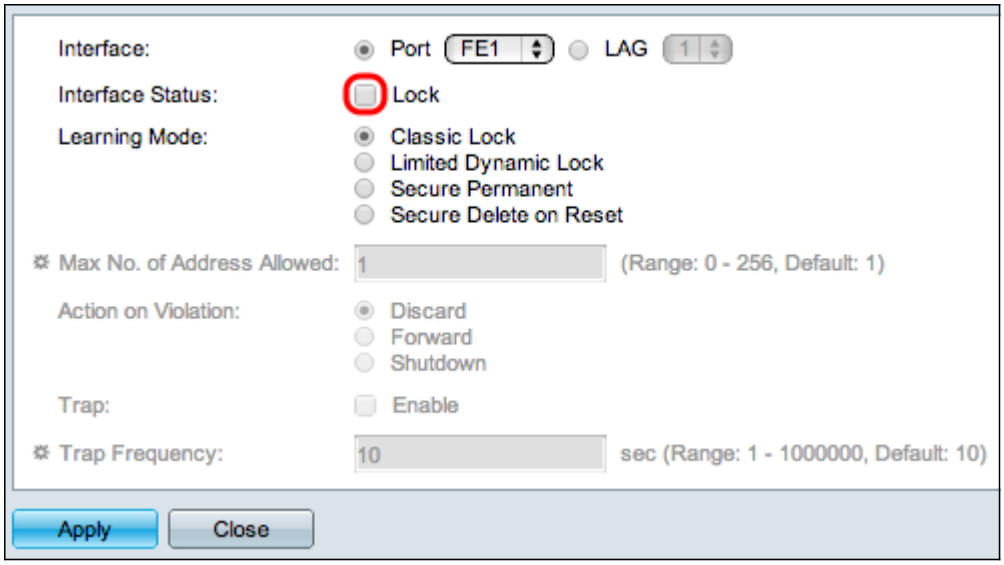


步骤2.从Interface Type Equals下拉列表中，选择Port或LAG，然后单击**Go**。

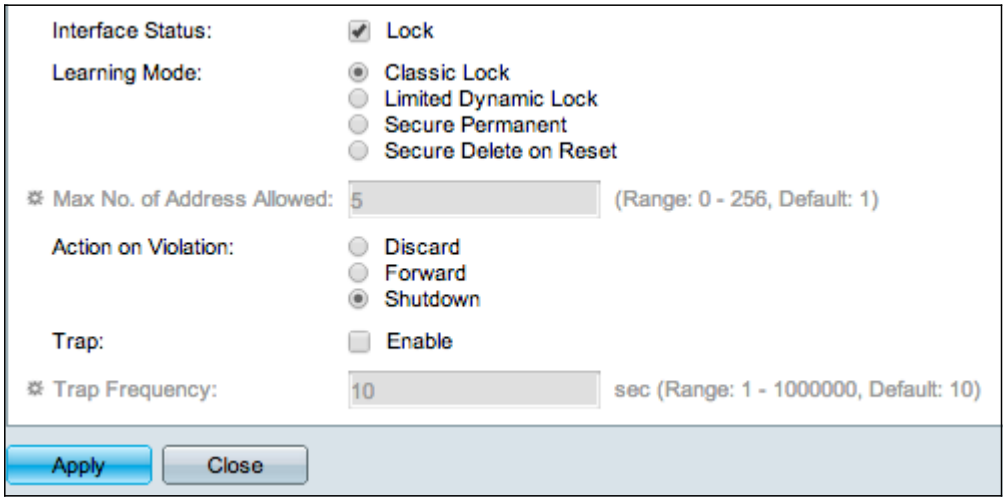
步骤3.单击要编辑其安全设置的接口的单选按钮。

步骤4.单击“**编辑**”。系统将*显示“编辑端口安全接口*设置”窗口：





步骤5.（可选）要锁定接口，使其无法发送和接收数据流量，请在“接口状态”字段中选中“锁定”**复选框**。



步骤6.在Learning Mode字段中，点击所需学习模式的单选按钮。可用选项包括：

·经典锁 — 立即锁定端口，无论已获知的设备数量如何。

·受限动态锁 — 删除与端口相关的当前MAC地址以将其锁定。端口可以获知特定数量的设备。

·安全永久 — 保留与端口相关的当前MAC地址，并可以获取特定数量的设备。

·重置时安全删除 — 重置后删除与端口相关的当前MAC地址。重置交换机后，端口可以获知特定数量的设备。

步骤7.在Max No. of Addresses Allowed字段中，输入允许端口学习的最大MAC地址数。如果输入0，则端口仅支持静态地址。

步骤8.如果在步骤5中锁定端口，则在Action on Violation字段中，点击发生违规时要采取的操作的单选按钮。可用选项包括：

·丢弃 — 如果源未知，则丢弃数据包。

·转发 — 如果源未知，则转发数据包。

·关闭 — 数据包被丢弃，端口关闭。

步骤9.（可选）每次在锁定端口上收到数据包时都会触发陷阱，这可确保数据包不会违反锁定端口。要启用陷阱，请选中Trap字段中的**Enable**复选框。陷阱是从代理到管理器的同步通知，包括当前sysUpTime值，它们在简单网络管理协议(SNMP)代理上满足条件时生成。这些条件在管理信息库(MIB)中定义

步骤10.如果在步骤9中启用陷阱，请在Trap Frequency字段中输入每个陷阱之间的最短时间（以秒为单位）。

步骤11.单击“**应用”**。

下图显示所配置端口的更改。

注意：要将一个端口的端口安全配置应用到多个端口，请参阅将端口安*全配置应用到多个端口一节*。

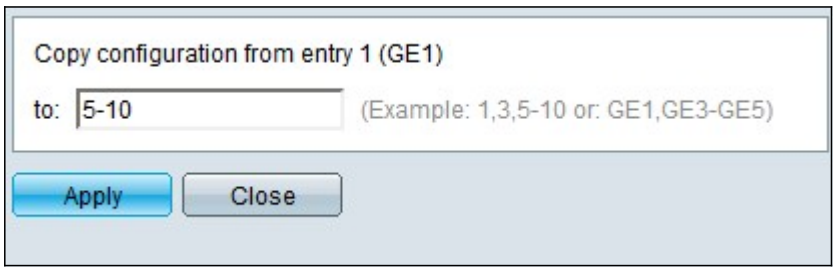
将端口安全配置应用于多个端口

本节介绍如何将单个端口的安全端口配置应用到多个端口。

步骤1.登录Web配置实用程序，然后选择Security **> Port Security**。“端*口安全*”页打开：

步骤2.点击要将其配置应用于多个端口的端口的单选按钮。

步骤3.单击“**复制设置**”。系统将显示“*复制*设置”窗口。



步骤4.在至字段中，输入具有与步骤2中选择的端口相同的端口安全配置的端口范围。可以使用端口号或端口名称作为输入。可以输入以逗号分隔的每个端口，如1、3、5或GE1、GE3、GE5，也可以输入端口范围，如1-5或GE1-GE5。

步骤5.单击“**应用**”保存配置。

下图显示单个端口安全配置对多个端口的应用。