MAC根据访问控制表(ACL)和访问控制项(ACE)配置300系列被管理的交换机

客观

访问控制表(ACL)是使用允许或拒绝网络通信流的安全技术。允许或拒绝对数据流的访问的基于MAC的ACL使用第2层信息。访问控制项(ACE)包含实际访问规则标准。一旦ACE被创建，适用于ACL。300系列被管理的交换机支持最多512个ACL和512 ACE。

此条款说明如何创建MAC基于ACL和如何适用ACE于在300系列被管理的交换机的ACL。

可适用的设备

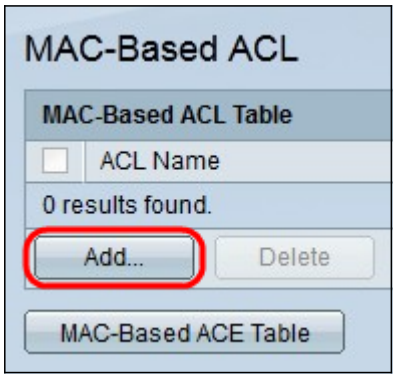
- SG300-10PP
- SG300-10MPP
- SG300-28PP-R
- SG300-28SFP-R
- SF302-08MPP
- SF302-08PP
- SF300-24PP-R
- SF300-48PP-R

软件版本

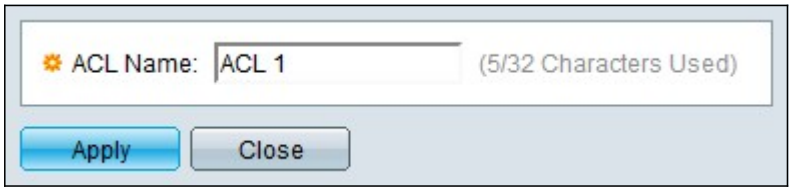
- 1.4.0.00p3 [SG300-28SFP-R]
- 6.2.10.18 [All other Applicable Devices]

基于MAC的ACL

步骤1.登陆到Web配置工具并且选择**访问控制> MAC基于ACL**。*MAC基于ACL*页打开：

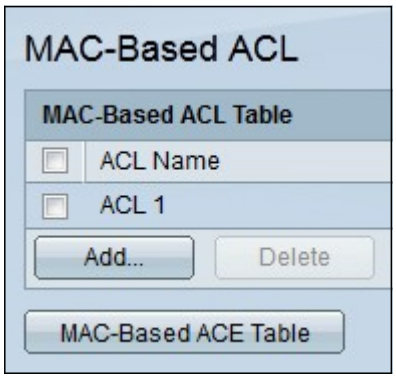


步骤2.点击**添加**。*添加基于MAC的ACL*窗口出现。



步骤3.输入一个名字对于ACL在ACL名称字段。

步骤4.点击**适用**。ACL被创建。



基于MAC的ACE

当帧在端口时接收，交换机通过第一个ACL处理帧。如果帧匹配第一个ACL的一台ACE过滤器，ACE动作发生。如果帧不匹配ACE过滤器，下个ACL被处理。如果匹配没有被找到对在所有相关ACL的任何ACE，默认情况下帧被丢弃。

Note: 此默认动作可以由允许所有数据流低优先级的ACE的创建避免。

步骤1.登陆到Web配置工具并且选择**访问控制> MAC基于ACE**。*MAC基于ACE*页打开：

Step 2.从ACL名称下拉列表，请选择ACL运用规则。

步骤3.点击**去**。为ACL已经被配置的ACE显示。

步骤4.点击**添加**添加新规则到ACL。*添加基于MAC的ACE*窗口出现。

ACL名称字段显示ACL的名字。

步骤5.输入ACE的优先级值在优先级字段。与更加高优先级的值的ACE首先被处理。值1是最高优先级的。

步骤6.点击对应于所需的动作采取的单选按钮，当帧满足ACE的必需的标准时。

- 许可证—交换机转发满足ACE的必需的标准的信息包。
- 拒绝—交换机丢弃不满足ACE的必需的标准的信息包。
- 关闭—交换机丢弃不满足ACE的必需的标准的信息包并且使信息包收到的端口无效。

Note: 失效端口在*Settings页的端口*可以恢复活动。

第 7 步：检查在时间范围字段的**Enable复选框**允许时间范围被配置到ACE。时间范围用于限制ACE有效的时间。

第8.步。从时间范围名字下拉列表，请选择时间范围适用于ACE。

Note: 点击**编辑**连接对和创建在*时间范围*页的时间范围。

步骤9.点击对应于ACE期望标准在目的地MAC Address字段的单选按钮。

- 其中任一—所有目的地MAC地址适用于ACE。

•用户定义—输入将适用于在目的地MAC地址值和目的地MAC通配符屏蔽字段的ACE的MAC地址和MAC通配符屏蔽。通配符屏蔽用于定义MAC地址的范围。

步骤10.点击对应于ACE期望标准在源MAC地址地址字段的单选按钮。

•其中任一—所有源MAC地址适用于ACE。

•用户定义—输入将适用于在目的地MAC地址值和目的地MAC通配符屏蔽字段的ACE的MAC地址和MAC通配符屏蔽。通配符屏蔽用于定义MAC地址的范围。

步骤11.输入与帧的VLAN标记将匹配的VLAN ID。

步骤12。(可选)包括802.1p值在ACE标准，检查在802.1p字段**包括**。802.1p介入技术业务类别(CoS)。Cos是使用区分数据流的以太网帧的一个3位域。

第13步。如果802.1p值是包括的，请输入以下字段。

•802.1p值—输入将被匹配的802.1p值。 802.1p是产生层2交换机能力指定优先级数据流和执行动态组播过滤的规格。

•802.1p掩码—输入802.1p值的通配符屏蔽。此通配符屏蔽用于定义802.1p值的范围。

步骤14。进入将被匹配帧的以太网类型。以太网类型是在使用指示的以太网帧的一个两个八位位组字段哪个协议为帧的有效载荷使用。

第15步。单击 Apply。ACE被创建。在本例中，被创建的ACE否决从被定义的源MAC地址被发送到所有目的地地址的数据流。