300系列托管交换机上基于MAC的访问控制列表(ACL)和访问控制条目(ACE)配置

目标

访问控制列表(ACL)是一种安全技术，用于允许或拒绝网络流量。基于MAC的ACL使用第2层信息来允许或拒绝对流量的访问。访问控制条目(ACE)包含实际访问规则条件。创建ACE后，将其应用于ACL。300系列托管交换机最多支持512个ACL和512个ACE。

本文介绍如何创建基于MAC的ACL以及如何将ACE应用到300系列托管交换机上的ACL。

适用设备

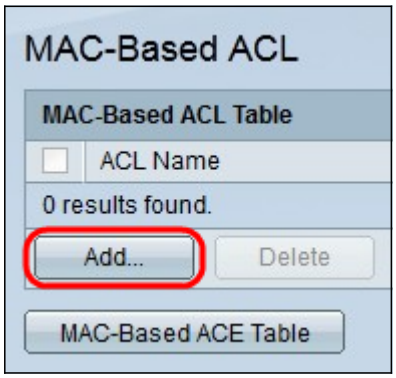
·SG300-10PP
· SG300-10MPP
· SG300-28PP-R
· SG300-28SFP-R
· SF302-08MPP
· SF302-08PP
· SF300-24PP-R
· SF300-48PP-R

软件版本

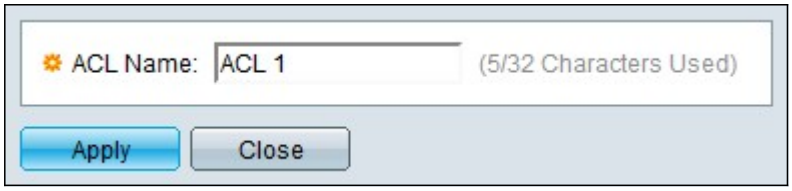
·1.4.0.00p3 [SG300-28SFP-R]
· 6.2.10.18 [所有其他适用设备]

基于 MAC 的ACL

步骤1.登录到Web配置实用程序，然后选择**Access Control > MAC Based ACL**。将打*开"基于MAC*的ACL"页：

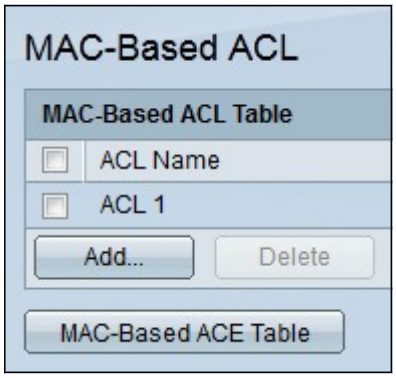


步骤2.单击"**添加**"。系统*将显示Add MAC-Based ACL*窗口。



步骤3.在ACL Name字段中输入ACL的名称。

步骤4.单击“**应用**”。即会创建ACL。



基于MAC的ACE

当端口上收到帧时，交换机通过第一个ACL处理该帧。如果帧与第一个ACL的ACE过滤器匹配，则会执行ACE操作。如果帧不匹配任何ACE过滤器，则处理下一个ACL。如果在所有相关ACL中找不到与任何ACE匹配的ACE，则默认情况下会丢弃该帧。

注意：创建允许所有流量的低优先级ACE可避免此默认操作。

步骤1.登录到Web配置实用程序，然后选择**Access Control > MAC Based ACE**。将打*开“基于MAC*的ACE”页：

步骤2.从ACL Name下拉列表中，选择要应用规则的ACL。

步骤3.单击**Go**。系统将显示已为ACL配置的ACE。

步骤4.单击**Add**将新规则添加到ACL。出现*Add MAC-Based ACE(添加基于MAC的ACE*)窗口。

ACL Name字段显示ACL的名称。

步骤5.在Priority字段中输入ACE的优先级值。优先级值较高的ACE首先处理。值1是最高优先级。

步骤6.点击与帧满足ACE的所需条件时所执行的所需操作对应的单选按钮。

·允许 — 交换机转发符合ACE所需标准的数据包。

·拒绝 — 交换机丢弃不符合ACE所需标准的数据包。

·关闭 — 交换机丢弃不符合ACE所需标准的数据包并禁用接收数据包的端口。

注意：可以在“端口设置”页面重新激*活已禁用*的端口。

步骤7.选中Time Range字**段中**的Enable复选框，以允许将时间范围配置到ACE。时间范围用于限制ACE生效的时间量。

步骤8.从Time Range Name下拉列表中，选择要应用于ACE的时间范围。

注：单击“**编**辑”以导航到“时间范围”页并创*建时间*范围。

步骤9.在Destination MAC Address字段中，点击与ACE所需条件对应的单选按钮。

·任意 — 所有目的MAC地址均应用于ACE。

·用户定义 — 在目标MAC地址值和目标MAC通配符掩码字段中输入要应用于ACE的MAC地址和MAC通配符掩码。通配符掩码用于定义MAC地址范围。

步骤10.在Source MAC Address字段中，点击与ACE的所需条件对应的单选按钮。

·任意 — 所有源MAC地址均应用于ACE。

·用户定义 — 在目标MAC地址值和目标MAC通配符掩码字段中输入要应用于ACE的MAC地址和MAC通配符掩码。通配符掩码用于定义MAC地址范围。

步骤11.输入与帧的VLAN标记匹配的VLAN ID。

第12步。（可选）要在ACE标准中包含802.1p值，请选**中**在802.1p字段中包含。802.1p涉及技术服务类别(CoS)。 CoS是以太网帧中用于区分流量的3位字段。

步骤13.如果包含802.1p值，请输入以下字段。

·802.1p值 — 输入要匹配的802.1p值。802.1p是一项规范，它使第2层交换机能够确定流量的优先级并执行动态组播过滤。

·802.1p掩码 — 输入802.1p值的通配符掩码。此通配符掩码用于定义802.1p值的范围。

步骤14.输入要匹配的帧的Ethertype。Ethertype是以太网帧中的两个二进制八位数字段，用于指示帧的负载使用哪种协议。

步骤15.单击“**应用”**。ACE已创建。在本例中，创建的ACE拒绝从定义的源MAC地址发送到所有目标地址的流量。