

在托管交换机上配置基于MAC的访问控制列表(ACL)和访问控制条目(ACE)

目标

访问控制列表(ACL)是用于提高安全性的网络流量过滤器和相关操作的列表。它阻止或允许用户访问特定资源。ACL包含允许或拒绝访问网络设备的主机。基于介质访问控制(MAC)的访问控制列表(ACL)是源MAC地址列表，使用第2层信息允许或拒绝对流量的访问。如果数据包从无线接入点到局域网(LAN)端口，或者从无线接入点到局域网(LAN)端口，则此设备将检查数据包的源MAC地址是否与此列表中的任何条目匹配，并根据帧的内容检查ACL规则。然后，它使用匹配的结果来允许或拒绝此数据包。但是，不会检查从LAN到LAN端口的数据包。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。您应该使用访问列表为访问网络提供基本的安全级别。如果不在网络设备上配置访问列表，则允许通过交换机或路由器的所有数据包进入网络的所有部分。

本文提供有关如何在托管交换机上配置基于MAC的ACL和ACE的说明。

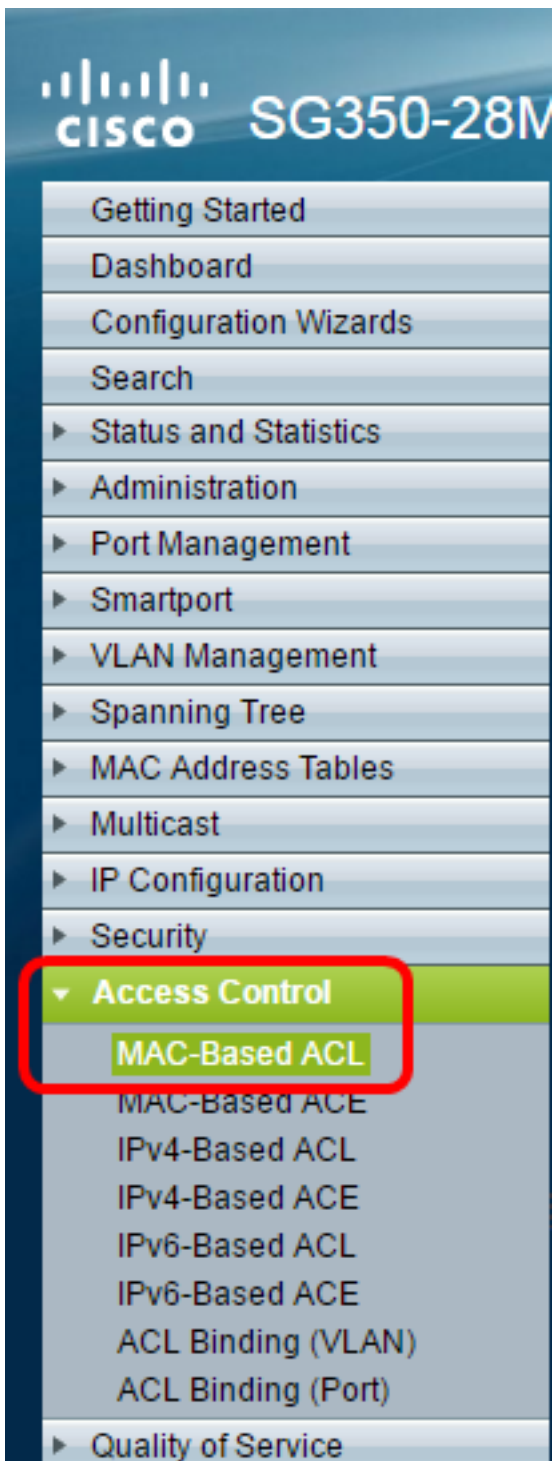
适用设备 | 软件版本

- Sx350 系列 | 2.2.0.66(下载[最新版](#))
- SG350X 系列 | 2.2.0.66(下载[最新版](#))
- Sx500系列 | 1.4.5.02(下载[最新版](#))
- Sx550X 系列 | 2.2.0.66(下载[最新版](#))

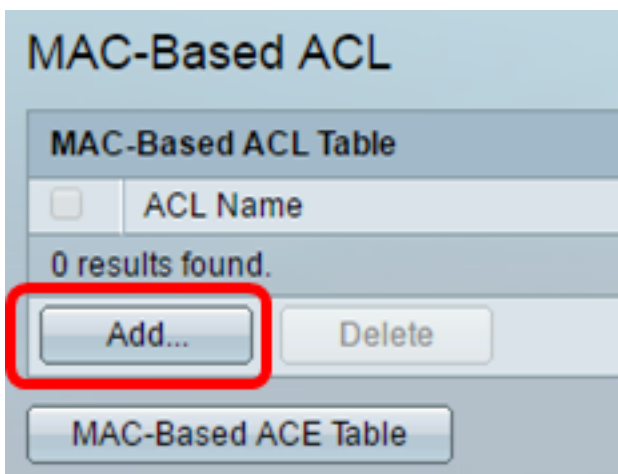
配置基于MAC的ACL和ACE

配置基于MAC的ACL

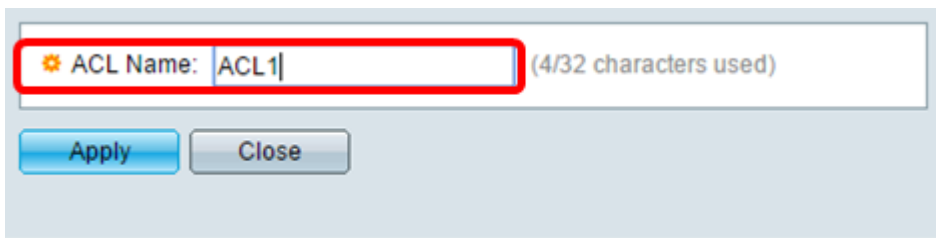
步骤1. 登录基于Web的实用程序，然后转到Access Control > MAC-Based ACL。



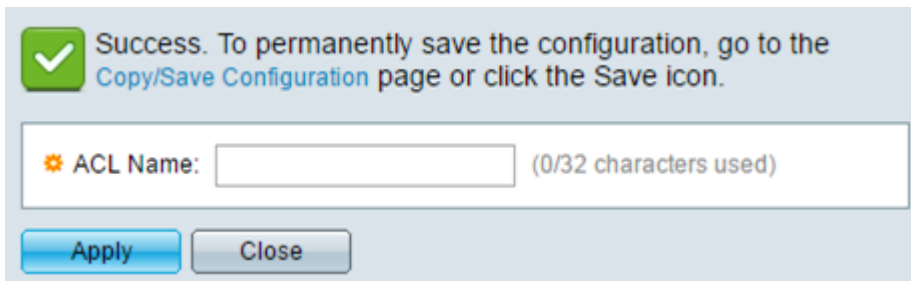
步骤2.单击“添加”按钮。



步骤3.在ACL Name字段中输入新ACL的名称。



步骤4.单击“应用”，然后单击“关闭”。



步骤5. (可选) 单击“保存”以在启动配置文件中保存设置。



现在，您应该已在交换机上配置了基于MAC的ACL。

配置基于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。

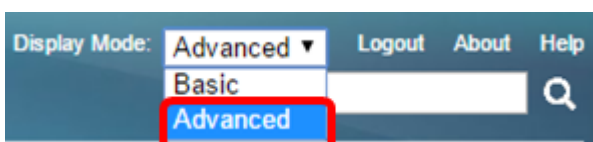
在此场景中，将创建ACE以拒绝从特定用户定义的源MAC地址发送到任何目标地址的流量。

注意：创建允许所有流量的低优先级ACE可避免此默认操作。

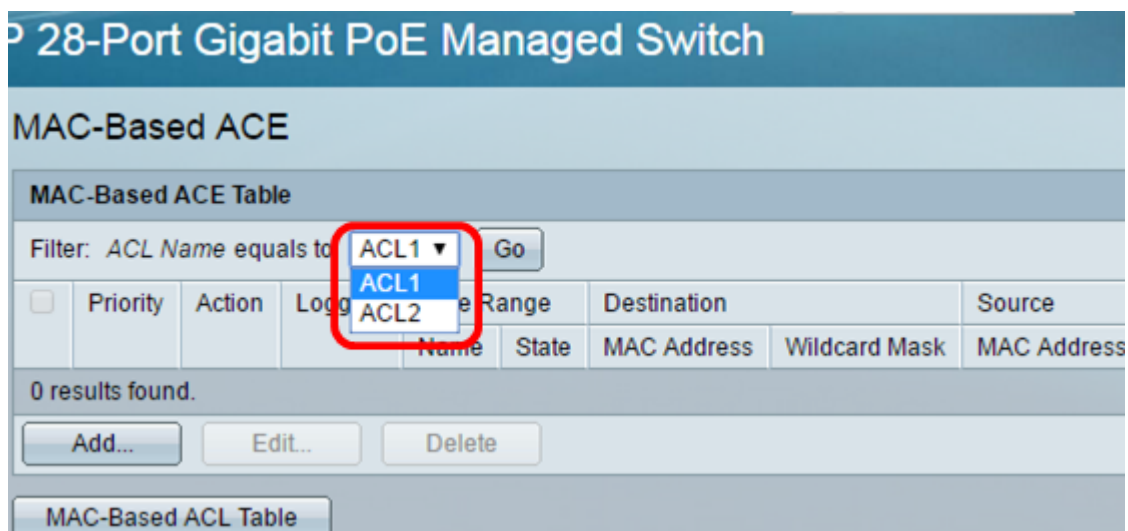
步骤1.在基于Web的实用程序上，转到Access Control > MAC-Based ACE。



重要信息：要充分利用交换机的可用特性和功能，请从页面右上角的“显示模式”下拉列表中选择高级，以更改为高级模式。



步骤2.从ACL Name下拉列表中选择ACL，然后单击Go。

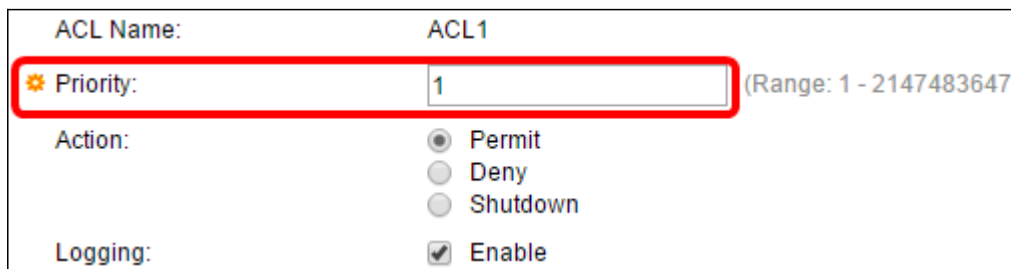


注意：表中将显示已为ACL配置的ACE。

步骤3.单击Add按钮将新规则添加到ACL。

注意： ACL Name 字段显示ACL的名称。

步骤4.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。



ACL Name: ACL1

Priority: 1 (Range: 1 - 2147483647)

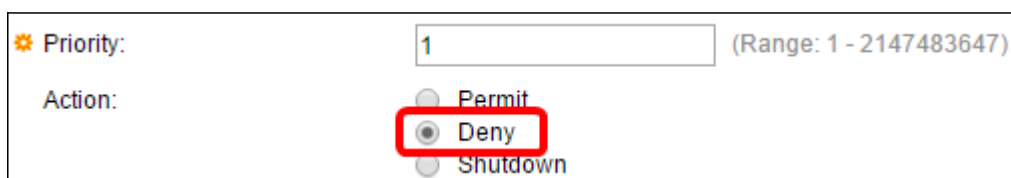
Action: Permit
 Deny
 Shutdown

Logging: Enable

第5步。(可选)选中Enable Logging复选框以启用与ACL规则匹配的日志记录ACL流。

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。

注意：在本例中，选择“拒绝”。



Priority: 1 (Range: 1 - 2147483647)

Action: Permit
 Deny
 Shutdown

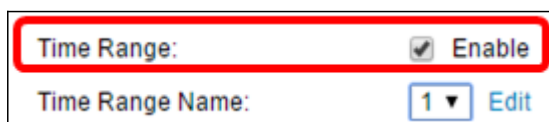
允许 — 交换机转发符合ACE所需标准的数据包。

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：禁用的端口可在Port Settings页面上重新激活。

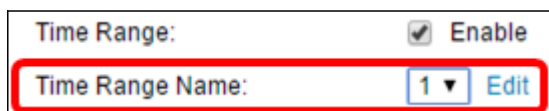
步骤7.(可选)选中Enable Time Range复选框，以允许将时间范围配置到ACE。时间范围用于限制ACE生效的时间量。



Time Range: Enable

Time Range Name: 1 Edit

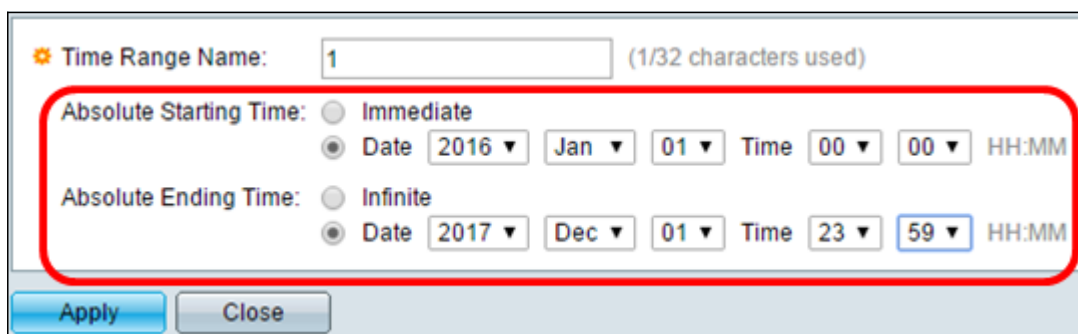
第8步。(可选)从Time Range Name下拉列表中，选择要应用到ACE的时间范围。



Time Range: Enable

Time Range Name: 1 Edit

注意：可以单击“编辑”以导航到“时间范围”页并在其上创建时间范围。



Time Range Name: 1 (1/32 characters used)

Absolute Starting Time: Immediate
 Date 2016 Jan 01 Time 00 00 HH:MM

Absolute Ending Time: Infinite
 Date 2017 Dec 01 Time 23 59 HH:MM

Apply Close

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

Destination MAC Address:	<input checked="" type="radio"/> Any	<input type="radio"/> User Defined
* Destination MAC Address Value:	<input type="text"/>	
* Destination MAC Wildcard Mask:	<input type="text"/>	(0s for matching, 1s for no matching)

选项有：

任意 — 所有目标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。

注意：在本例中，选择Any。选择此选项意味着要创建的ACE将拒绝ACE流量。

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

ACL Name:	ACL1	
* Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input checked="" type="checkbox"/> Enable	
Time Range:	<input checked="" type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="1"/> Edit	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
* Destination MAC Address Value:	<input type="text"/>	
* Destination MAC Wildcard Mask:	<input type="text"/>	(0s for matching, 1s for no matching)
Source MAC Address:	<input type="radio"/> Any <input checked="" type="radio"/> User Defined	
* Source MAC Address Value:	<input type="text" value="a2:b2:c2:d2:e2:f2"/>	
* Source MAC Wildcard Mask:	<input type="text" value="000000001111"/>	(0s for matching, 1s for no matching)
VLAN ID:	<input type="text" value="2"/>	(Range: 1 - 4094)
802.1p:	<input checked="" type="checkbox"/> Include	
* 802.1p Value:	<input type="text" value="1"/>	(Range: 0 - 7)
* 802.1p Mask:	<input type="text" value="0"/>	(Range: 0 - 7)
Ethertype:	<input type="text" value="88AB"/>	(Range: 5DD - FFFF)
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

选项有：

任意 — 所有源MAC地址均应用于ACE。

用户定义 — 在源MAC地址值和源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。

注意：在本例中，选择“用户定义”。

步骤11. (可选) 在VLAN ID字段中，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Include in the 802.1p复选框。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。值如下：

- 0 — 背景。排定优先级最低的数据，如批量传输、游戏等。
- 1 — 尽力而为。需要在普通LAN优先级上尽力传输的数据。网络不提供传输保证，但数据根据流量获取未指定的比特率和传输时间。
- 2 — 尽力而为。需要为重要用户提供尽力交付的数据。
- 3 — 关键应用，如Linux虚拟服务器(LVS)电话会话初始协议(SIP)。
- 4 — 视频。延迟和抖动小于100毫秒。
- 5 — 默认语音Cisco IP电话。延迟和抖动小于10毫秒。
- 6 — 网络间控制LVS电话实时传输协议(RTP)。
- 7 — 网络控制。对通过维护和支持网络基础设施的要求很高。

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. (可选) 输入要匹配的帧的Ethertype。Ethertype是以太网帧中的一个2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14.单击“应用”，然后单击“关闭”。ACE已创建并与ACL名称关联。

步骤15.单击“保存”将设置保存到启动配置文件。

28-Port Gigabit PoE Managed Switch

MAC-Based ACE

MAC-Based ACE Table

Filter: ACL Name equals to

<input type="checkbox"/>	Priority	Action	Logging	Time Range		Destination
				Name	State	MAC Address
<input type="checkbox"/>	1	Deny	Enabled	1	Active	Any
<input type="checkbox"/>	2	Permit	Enabled	1	Active	a1:b1:c1:d1:e1:f1

现在，您应该已在交换机上配置了基于MAC的ACE。

您可能会发现其他有价值的链接：

- [350系列交换机产品页](#)
- [350X系列交换机产品页](#)
- [550系列交换机产品页](#)
- [550X系列交换机产品页](#)

查看与本文相关的视频.....

[单击此处查看思科提供的其他技术讲座](#)