在交换机上配置基于IPv4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IPv4的ACL是使用第3层信息允许或拒绝流量访问的源IPv4地址列表。IPv4 ACL根据已配置的IP过滤器限制与IP相关的流量。过滤器包含匹配IP数据包的规则，如果数据包匹配，规则还规定应允许还是拒绝该数据包。

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受管交换机上配置基于IPv4的ACL和ACE的说明。

适用设备

- Sx350 系列
- SG350X 系列
- Sx500系列
- Sx550X 系列

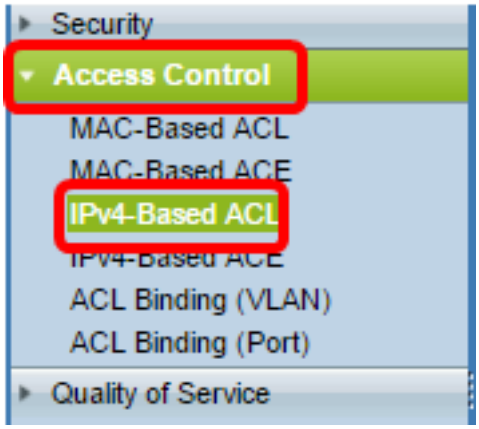
软件版本

- 1.4.5.02 - Sx500系列
- 2.2.5.68 - Sx350系列、SG350X系列、Sx550X系列

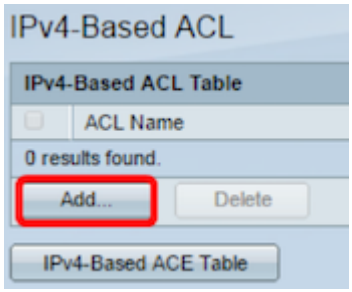
配置基于IPv4的ACL和ACE

配置基于IPv4的ACL

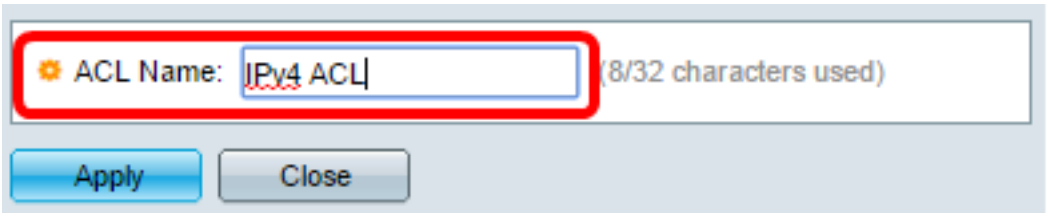
步骤1.登录基于Web的实用程序，然后转**到Access Control > IPv4-Based ACL。**



步骤2.单击“添**加**”按钮。

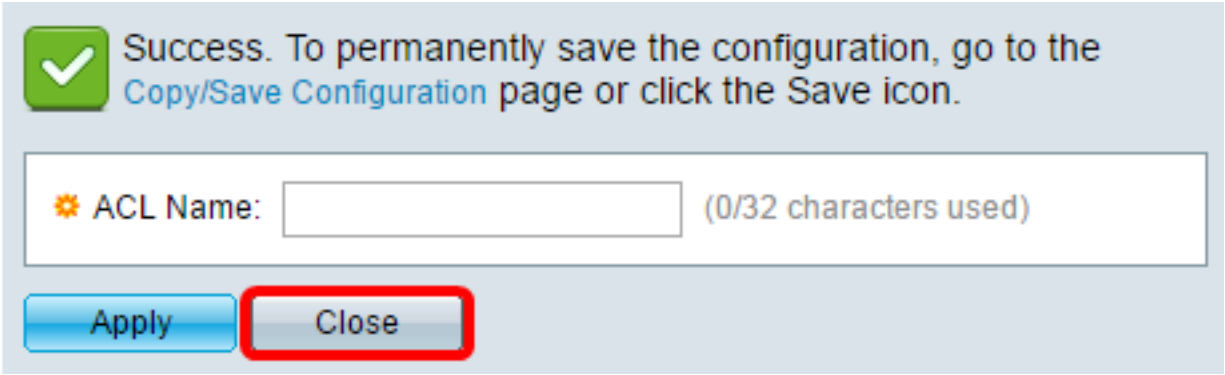


步骤3.在ACL Name字段中输入新ACL*的名*称。



注意：在本例中，使用IPv4 ACL。

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IPv4的ACL。

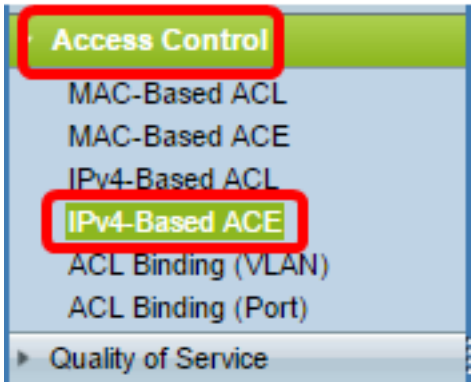
配置基于IPv4的ACE

当端口上收到数据包时，交换机会通过第一个ACL处理该数据包。如果数据包与第一个ACL的ACE过滤器匹配，则会执行ACE操作。如果数据包与任何ACE过滤器都不匹配，则会处理下一个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数据包。

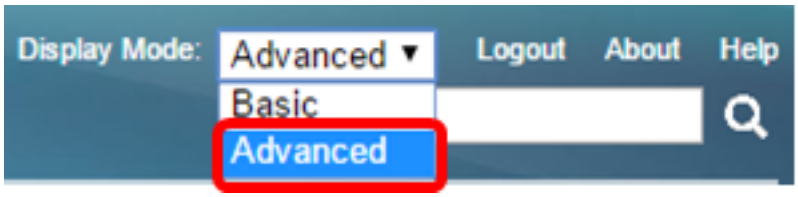
在此场景中，将创建ACE以拒绝从特定用户定义的源IPv4地址发送到任何目标地址的流量。

注意：创建允许所有流量的低优先级ACE可避免此默认操作。

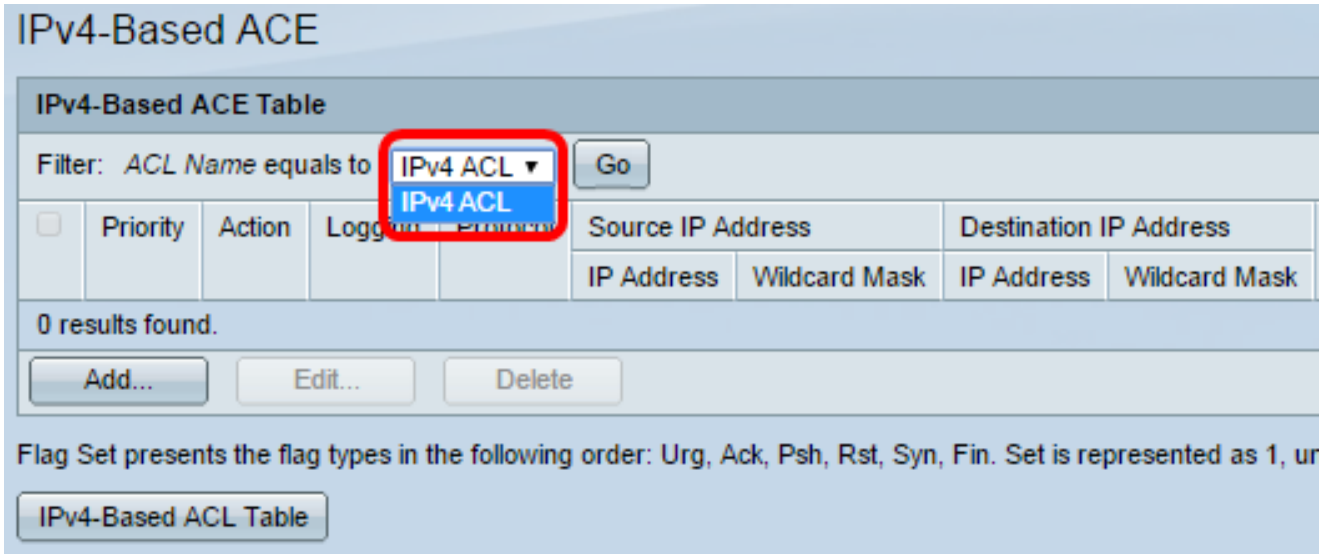
步骤1.在基于Web的实用程序上，转**到Access Control > IPv4-Based ACE**。



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**。

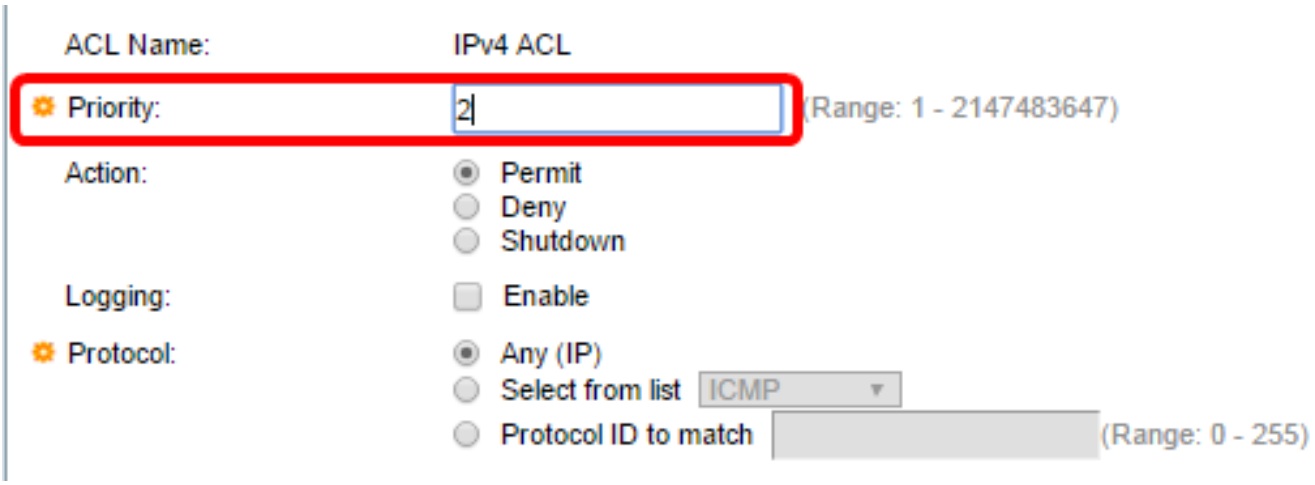


注意：表中将显示已为ACL配置的ACE。

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。范围为1到2147483647。



注意：在本例中，使用2。

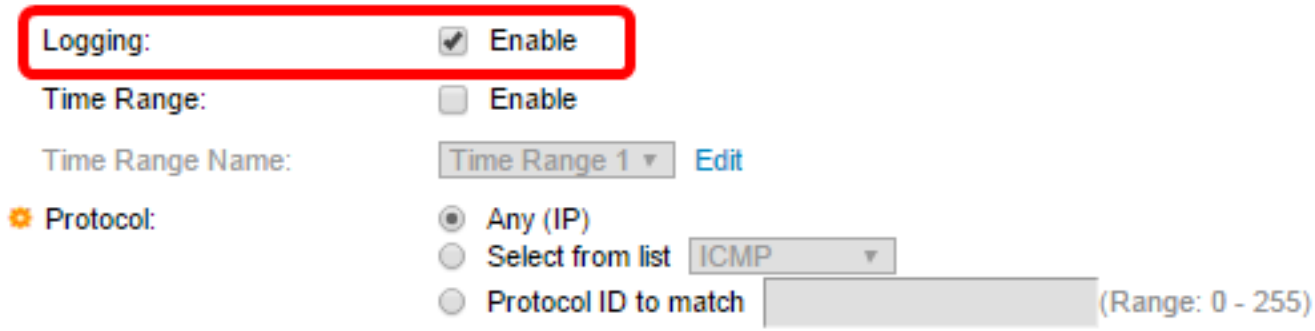
步骤5.点击与帧满足ACE所需标准时所执行的所需操作对应的单选按钮。

注意：在本例中，选择Permit。

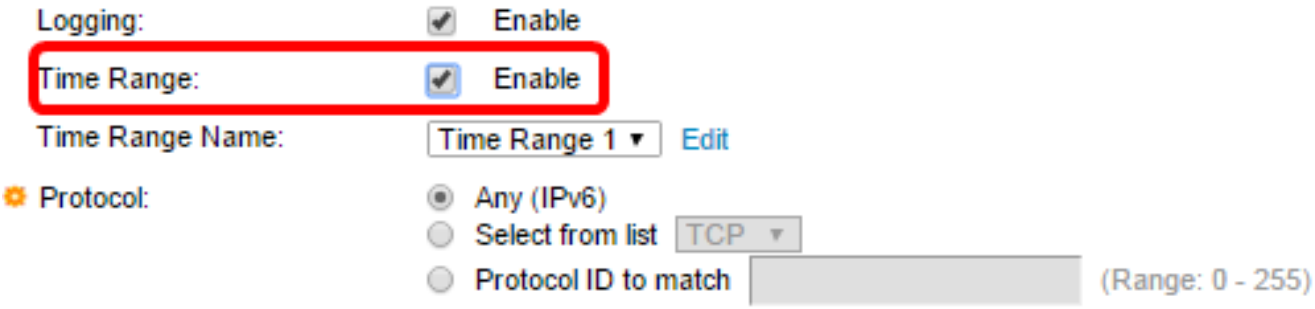
- 允许 — 交换机转发符合ACE所需标准的数据包。
- 拒绝 — 交换机丢弃符合ACE所需标准的数据包。
- 关闭 — 交换机丢弃不符合ACE所需标准的数据包并禁用接收数据包的端口。

注意：禁用的端口可在Port Settings页面上重新激活。

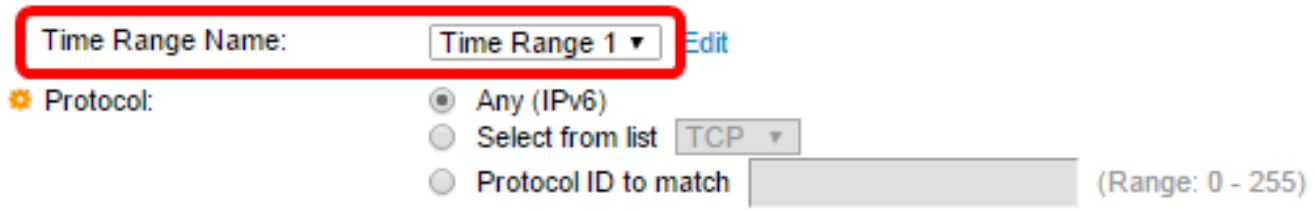
第6步。（可选）选中**Enable** Logging复选框以启用与ACL规则匹配的ACL流的日志记录。



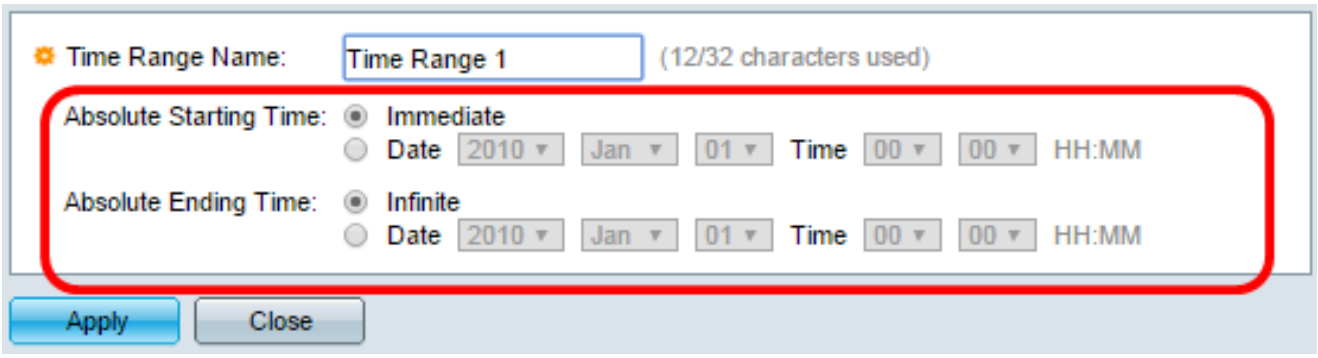
步骤7.（可选）选中**Enable** Time Range复选框，以允许将时间范围配置到ACE。时间范围用于限制ACE生效的时间量。



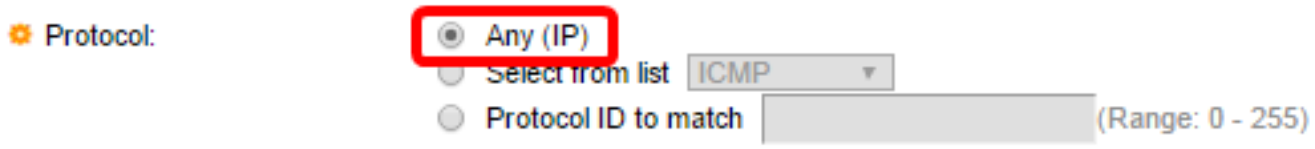
第8步。（可选）从Time Range Name下拉列表中，选择要应用到ACE的时间范围。



注意：可以单击“**编辑**”在“时间范围”页上导航并创建时间范围。



步骤9.在Protocol区域中选择协议类型。ACE将根据特定协议或协议ID创建。

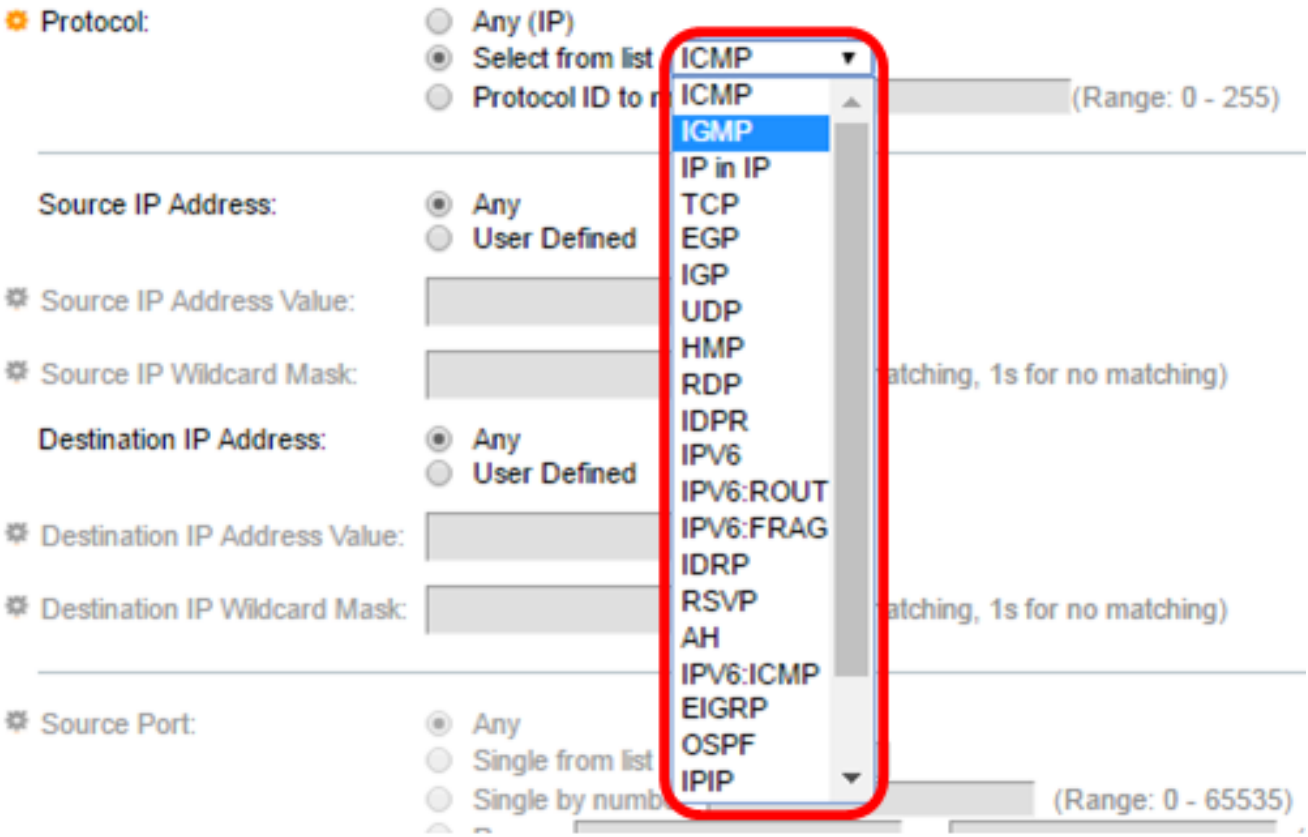


选项有：

- Any(IP) — 此选项将配置ACE以接受所有IP协议。
- 从列表中选择 — 此选项允许您从下拉列表中选择协议。如果您喜欢此选项，请跳至步骤10。
- 要匹配的协议ID — 此选项将允许您输入协议ID。如果您喜欢此选项，请跳至步骤11。

注意：在本例中，选择Any(IP)。

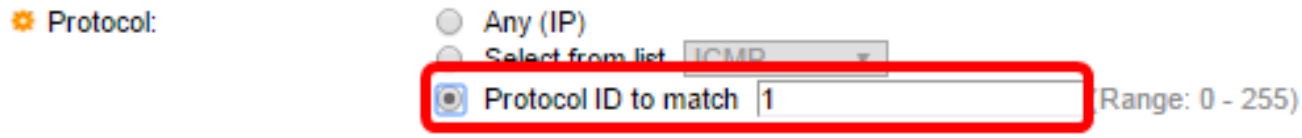
第10步。（可选）如果您在第9步中选择了“从列表中选择”，请从下拉列表中选择协议。



选项有：

- ICMP - Internet控制消息协议
- IP in IP — IP封装中的IP
- TCP — 传输控制协议
- EGP — 外部网关协议
- IGP — 内部网关协议
- UDP — 用户数据报协议
- HMP — 主机映射协议
- RDP — 可靠数据报协议
- IDPR — 域间策略路由
- IPV6 — 通过IPv4隧道的IPv6
- IPV6:ROUT — 匹配属于通过网关的IPv6 over IPv4路由的数据包
- IPV6:FRAG — 匹配属于IPv6 over IPv4分段报头的数据包
- IDRP - IS-IS域间路由协议
- RSVP - ReSerVation协议
- AH — 身份验证报头
- IPV6:ICMP - IPv6的ICMP
- EIGRP — 增强型内部网关路由协议
- OSPF — 开放最短路径优先
- IPIP - IP中的IP
- PIM — 协议无关组播
- L2TP — 第2层隧道协议

第11步。（可选）如果您在第9步中选择要匹配的协议ID，请在“要匹配的协议ID”字*段中输入协议*ID。



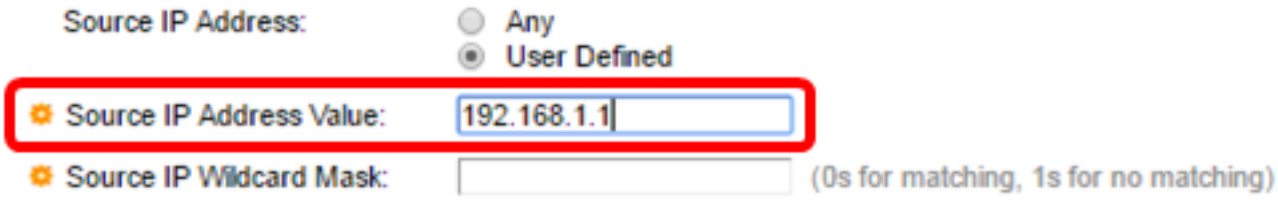
步骤12.在Source IP Address区域中，点击与ACE的所需条件对应的单选按钮。

选项有：

- 任意 — 所有源IPv4地址均应用于ACE。
- 用户定义 — 在源IP地址值和源IP通配符掩码字段中输入要应*用于ACE的*IP*地址和IP通配符*掩码。通配符掩码用于定义IP地址范围。

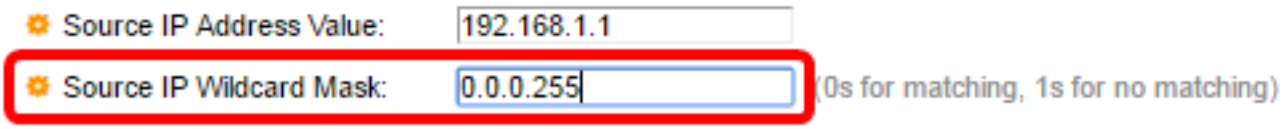
注意：在本例中，选择“用户定义”。如果选择Any，请跳至步骤15。

步骤13.在Source IP Address Value字段中输入*源IP地*址。



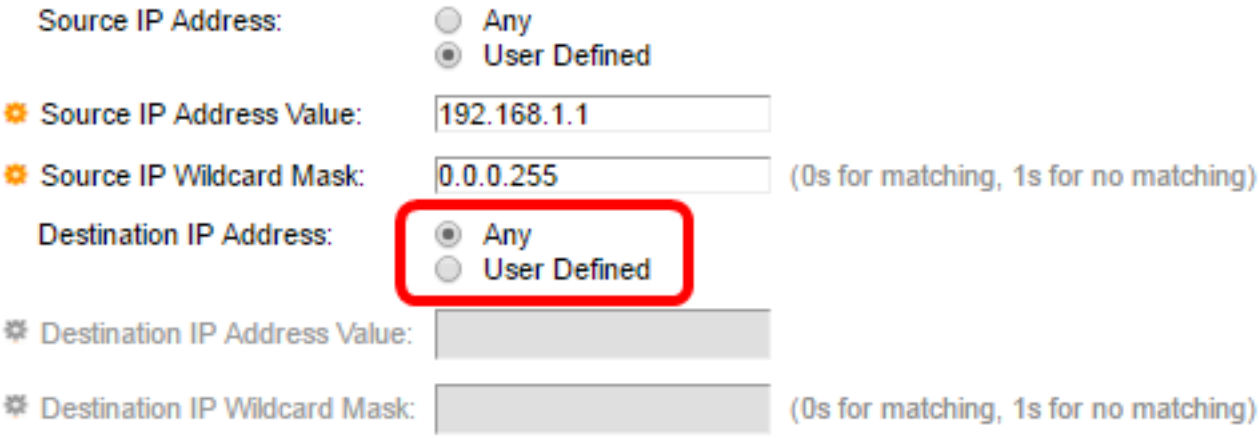
注意：在本例中，使用192.168.1.1。

步骤14.在Source IP Wildcard Mask字段中输入*源通配符*掩码。



注意：在本例中，使用0.0.0.255。

步骤15.在Destination IP Address区域中，单击与ACE的所需条件对应的单选按钮。



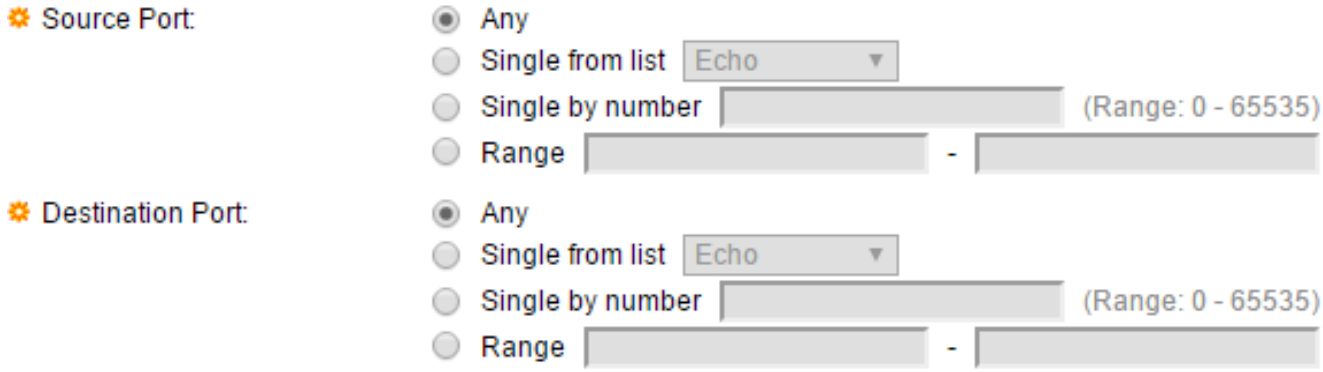
选项有：

- 任意 — 所有目标IPv4地址均应用于ACE。

- 用户定义 — 在目标IP地址值和目标IP通配符掩码字段中输入要*应用于ACE的IP地址和IP通配符*掩码。通配符掩码用于定义IP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将允许从指定IPv4地址到任何目标的ACE流量。

步骤16.（可选）点击Source Port区域中的单选按钮。默认值为Any。



- Any — 匹配所有源端口。
- 单个从列表 — 您可以选择与数据包匹配的单个TCP/UDP源端口。仅当在“从列表选择”下拉菜单中选择800/6-TCP或800/17-UDP时，此字段才处于活动状态。
- 按编号单一(Single by number) — 您可以选择与数据包匹配的单个TCP/UDP源端口。仅当在“从列表选择”下拉菜单中选择800/6-TCP或800/17-UDP时，此字段才处于活动状态。
- 范围 — 您可以选择数据包匹配的TCP/UDP源端口范围。可以配置八个不同的端口范围（源端口和目标端口之间共享）。TCP和UDP协议各有八个端口范围。

步骤17.（可选）点击Destination Port区域中的单选按钮。默认值为Any。

- 任意 — 匹配所有源端口
- 单个从列表 — 您可以选择与数据包匹配的单个TCP/UDP源端口。仅当在“从列表选择”下拉菜单中选择800/6-TCP或800/17-UDP时，此字段才处于活动状态。
- 按编号单一(Single by number) — 您可以选择与数据包匹配的单个TCP/UDP源端口。仅当在“从列表选择”下拉菜单中选择800/6-TCP或800/17-UDP时，此字段才处于活动状态。
- 范围 — 您可以选择数据包匹配的TCP/UDP源端口范围。可以配置八个不同的端口范围（源端口和目标端口之间共享）。TCP和UDP协议各有八个端口范围。

步骤18.（可选）在TCP Flags区域中，选择一个或多个TCP标志，以便过滤数据包。过滤的数据包会被转发或丢弃。通过TCP标志过滤数据包可增强数据包控制，从而提高网络安全性。

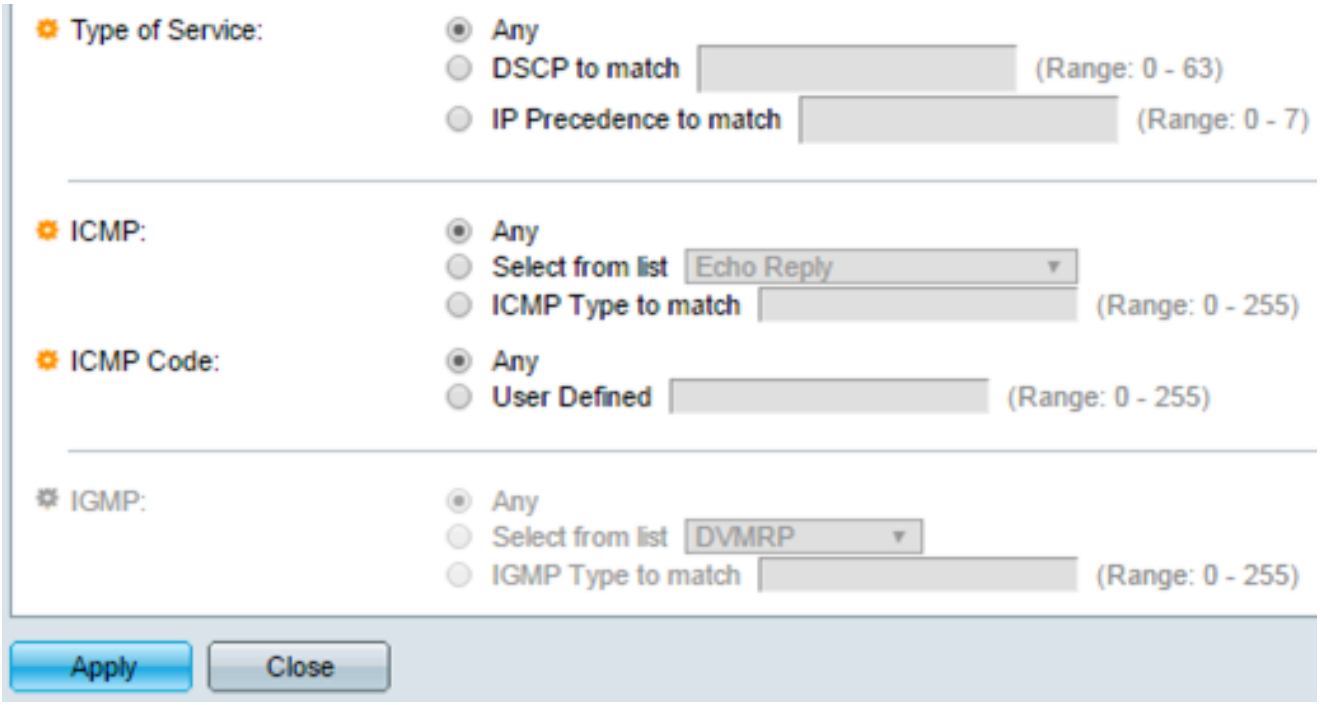
- 设置(Set) — 如果设置了标志，则匹配。
- 取消设置 — 如果未设置标志，则匹配。
- 无所谓 — 忽略TCP标志。

TCP标志包括：

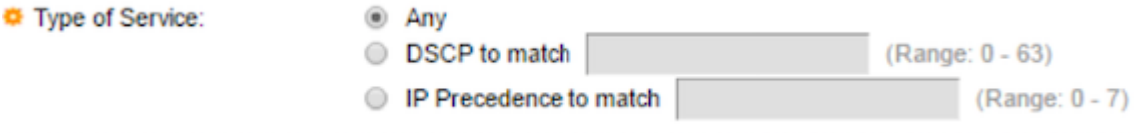
- Urg — 此标志用于将传入数据标识为Urgent。
- 确认 — 此标志用于确认数据包的成功接收。

- Psh — 此标志用于确保数据获得优先级（它应得到的优先级）并在发送或接收端进行处理。
- Rst — 当数据段到达时，不用于当前连接时，使用此标志。
- Syn — 此标志用于TCP通信。
- Fin — 当通信或数据传输完成时使用此标志。

步骤19.（可选）从Type of Service区域点击IP数据包的服务类型。



选项有：



- Any — 它可以是任何类型的流量拥塞服务。
- DSCP to Match - DSCP是用于分类和管理网络流量的机制。6位(0-63)用于选择数据包在每个节点上体验的每跳行为。
- 要匹配的IP优先级 — IP优先级是一种服务类型(TOS)模型，网络使用它来帮助提供适当的服务质量(QoS)承诺。此模型使用IP报头中服务类型字节的三个最重要位，如RFC 791和RFC 1349中所述。具有IP首选项值的关键字如下：

  - 0 — 例程

  - 1 — 优先级

  - 2 — 立即

  - 3 — 用于闪存

  - 4 — 用于flash-override

  - 5 — 关键

  - 6 — 用于互联网

步骤20.（可选）如果ACL的IP协议是ICMP，请点击用于过滤目的的ICMP消息类型。按名称选择消息类型或输入消息类型编号：

- 任意 — 接受所有消息类型。
- 从列表中选择 — 您可以按名称选择消息类型。
- 要匹配的ICMP类型 — 用于过滤目的的消息类型的数量。范围为0到255。

步骤21.（可选）ICMP消息可以有一个代码字段，指示如何处理该消息。单击以下选项之一以配置是否过滤此代码：

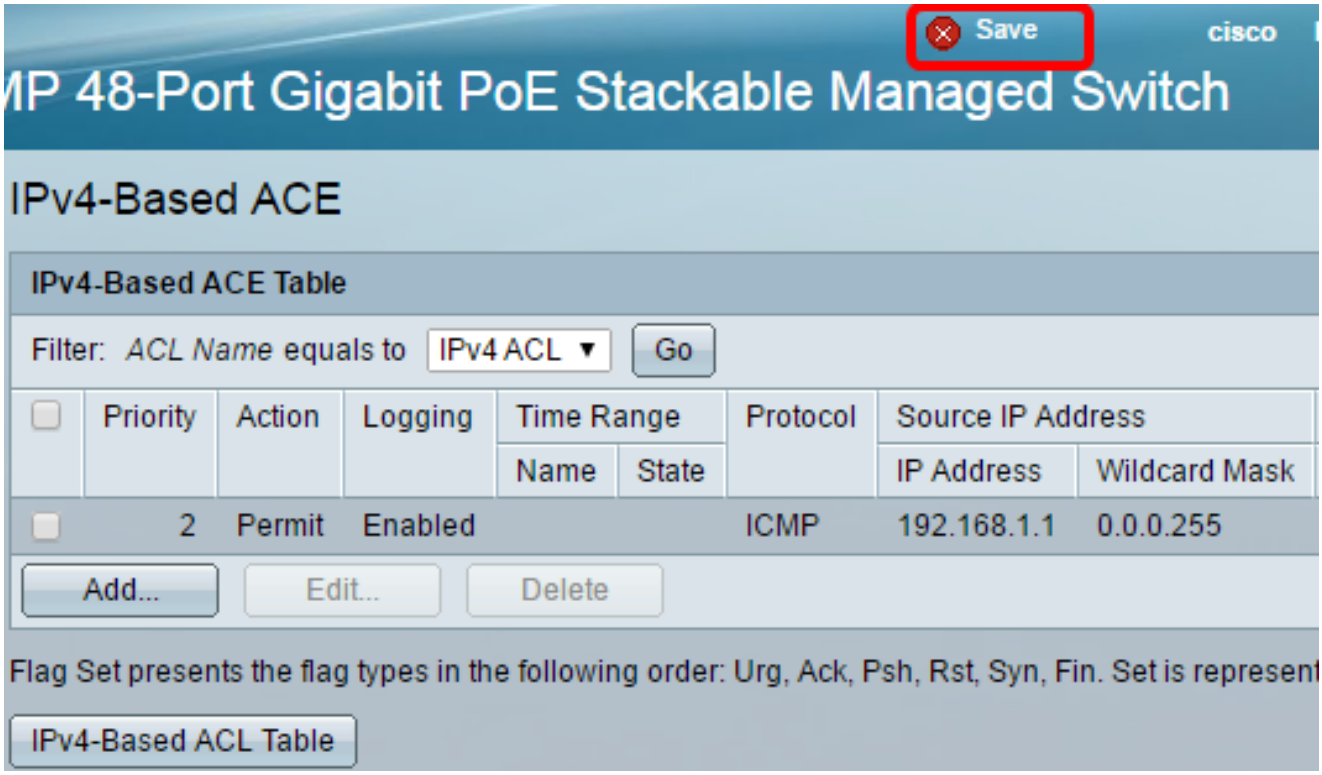
- 任意(Any) — 接受所有代码。
- 用户定义 — 您可以输入用于过滤目的的ICMP代码。范围为0到255。

步骤22.（可选）如果ACL基于IGMP，请点击用于过滤目的的IGMP消息类型。按名称选择消息类型或输入消息类型编号：

- 任意 — 接受所有消息类型。
- 从列表中选择 — 您可以从下拉列表中选择任何选项：
- DVMRP — 使用反向路径泛洪技术，通过每个接口（数据包到达的接口除外）将收到的数据包的副本发送出去。
- Host-Query — 定期在每个连接的网络上发送常规主机查询消息以获取信息。
- Host-Reply — 它对查询作出回复。
- PIM — 本地和远程组播路由器之间使用协议独立组播(PIM)将组播流量从组播服务器定向到多个组播客户端。
- 跟踪 — 提供有关加入和离开IGMP组播组的信息。
- 要匹配的IGMP类型 — 用于过滤目的的消息类型的数量。范围为0到255。

步骤23.单击“应用”，然后单击“**关闭**”。ACE已创建并与ACL名称关联。

步骤24.单击“保**存**”将设置保存到启动配置文件。



现在，您应该已在交换机上配置了基于IPv4的ACE。