在交换机上配置基于IPv6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。

IPv6中的典型ACL功能与IPv4中的ACL类似。ACL确定要阻止的流量以及要在交换机接口转发的流量。ACL允许根据源地址和目的地址过滤特定接口的入站和出站地址。每个ACL的末尾都有一条隐式deny语句。ACL的规则在访问控制条目(ACE)中配置。

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交换机上配置基于IPv6的ACL和ACE的说明。

适用设备

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

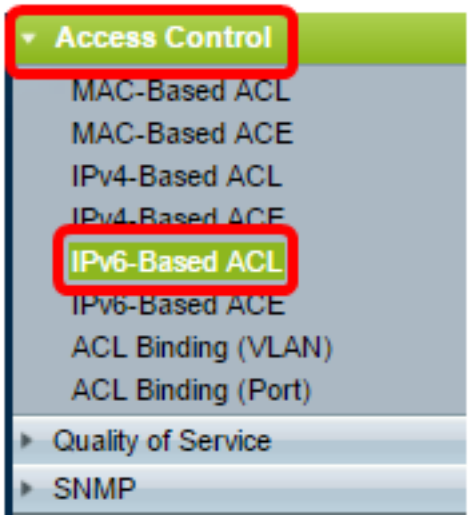
软件版本

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

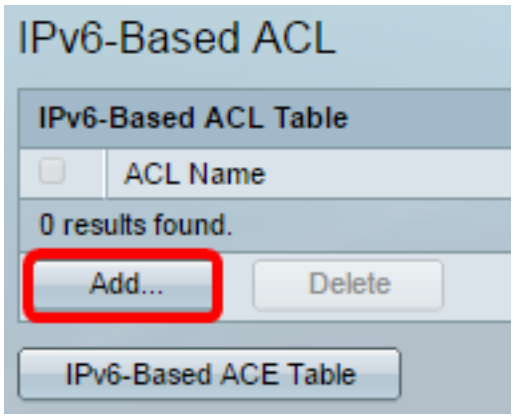
配置基于IPv6的ACL和ACE

配置基于IPv6的ACL

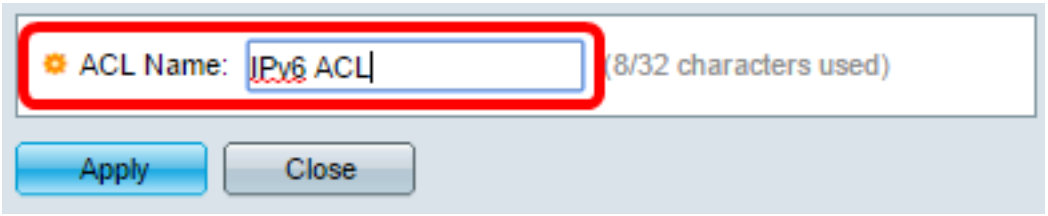
步骤1.登录基于Web的实用程序，然后转到**Access Control > IPv6-Based ACL**。



步骤2.单击“添**加**”按钮。

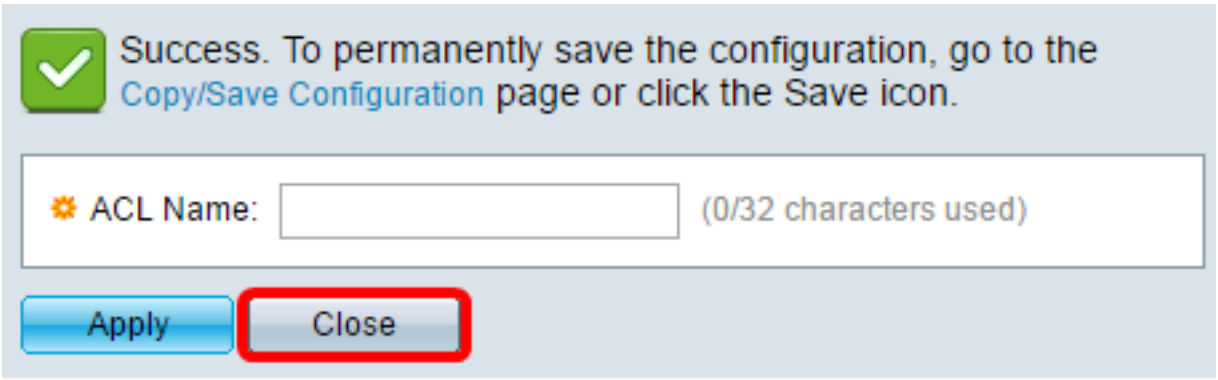


步骤3.在ACL Name字段中输入新ACL*的名*称。



注意：在本例中，使用IPv6 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IPv6的ACL。

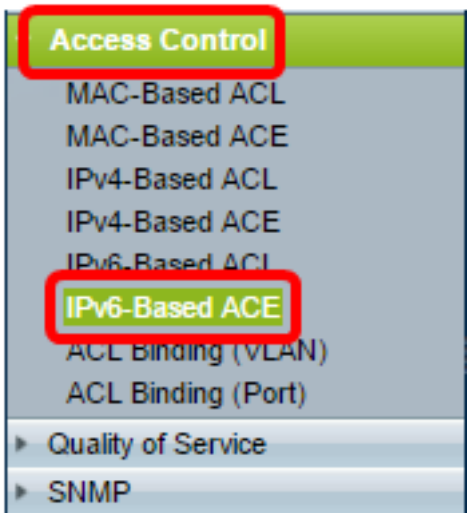
配置基于IPv6的ACE

在端口上收到数据包时，交换机会通过第一个ACL处理该帧。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。

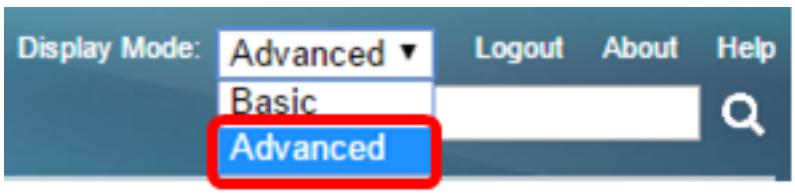
在此场景中，将创建ACE以拒绝从特定用户定义的源IPv6地址发送到任何目标地址的流量。

注意：创建允许所有流量的低优先级ACE可避免此默认操作。

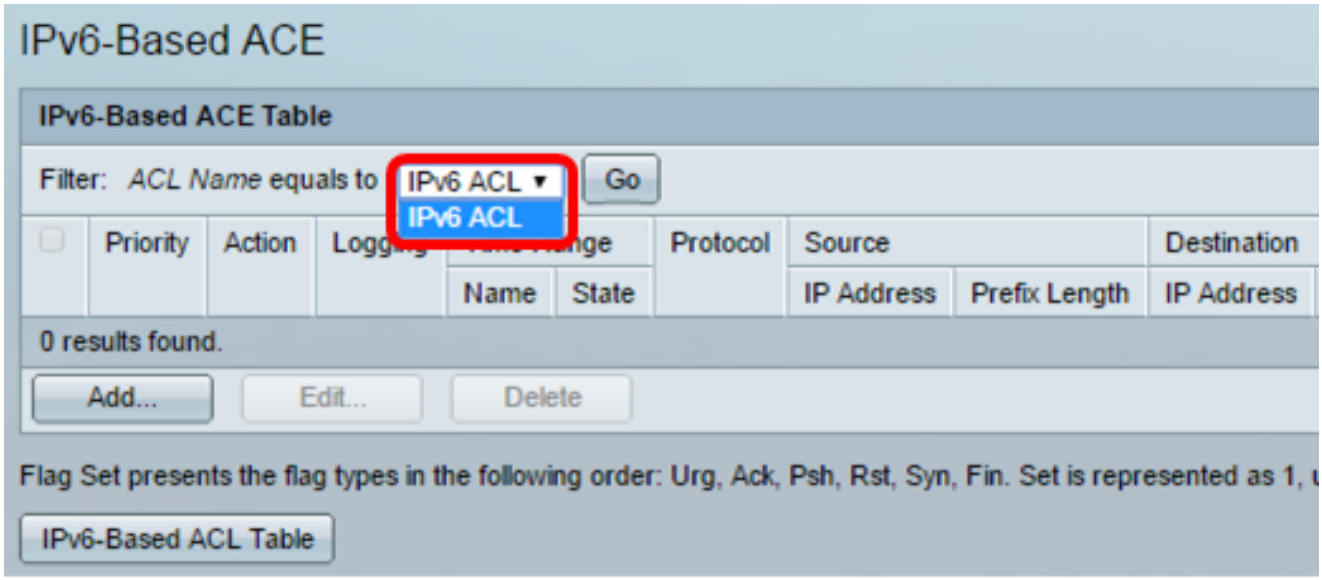
步骤1.在基于Web的实用程序上，转**到Access Control > IPv6-Based ACE**。



重要信息：如果您有Sx350、SG350X、Sx550X交换机，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。

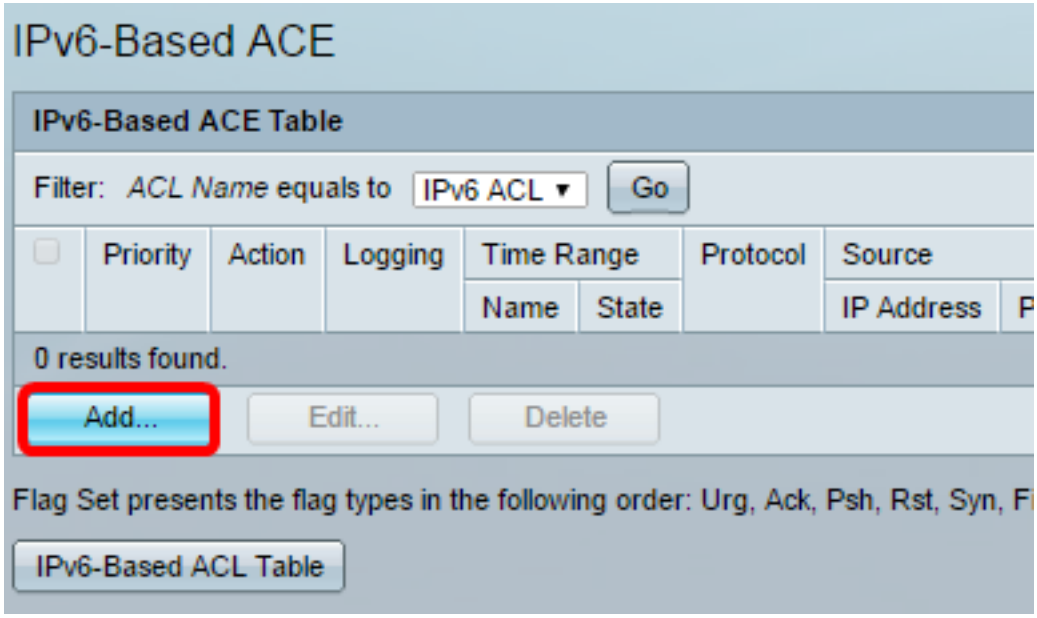


步骤2.从ACL Name下拉列表中选择ACL，然后单击**Go**。



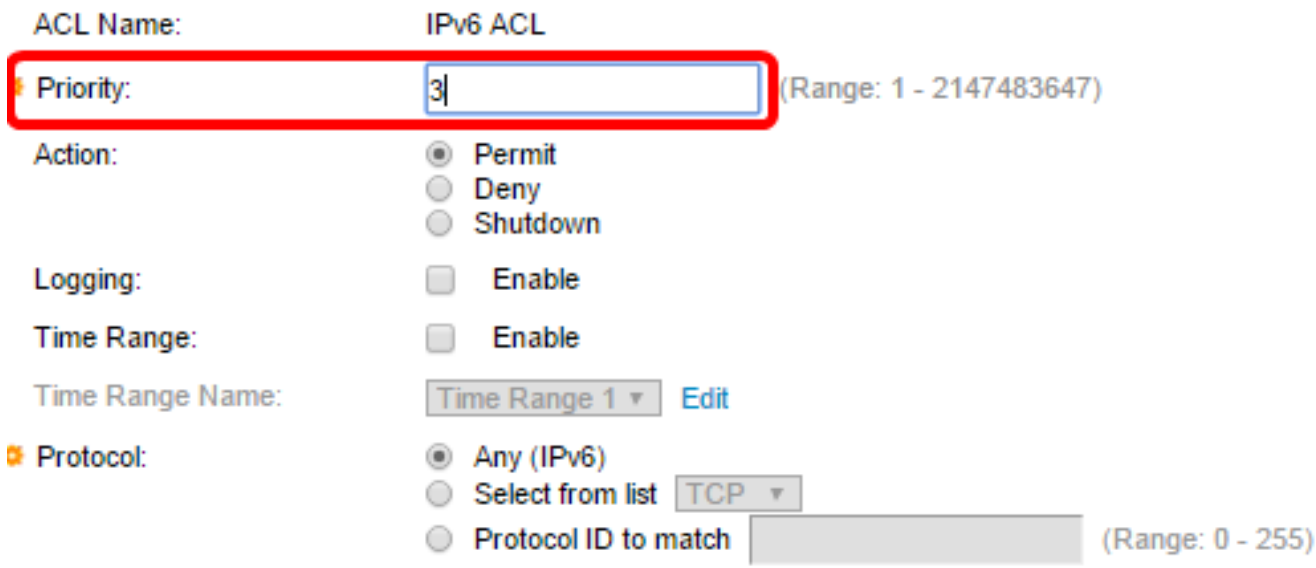
注意：表中将显示已为ACL配置的ACE。

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3。

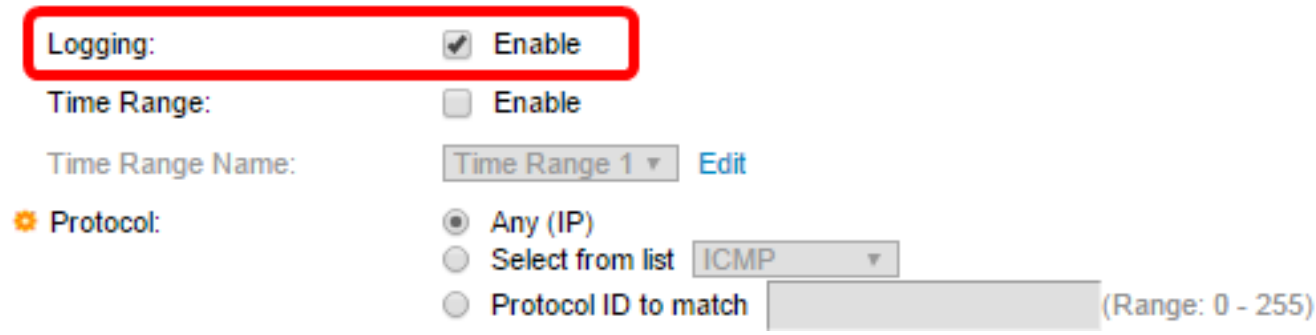
步骤5.点击与帧满足ACE所需标准时所执行的所需操作对应的单选按钮。

注意：在本例中，选择Permit。

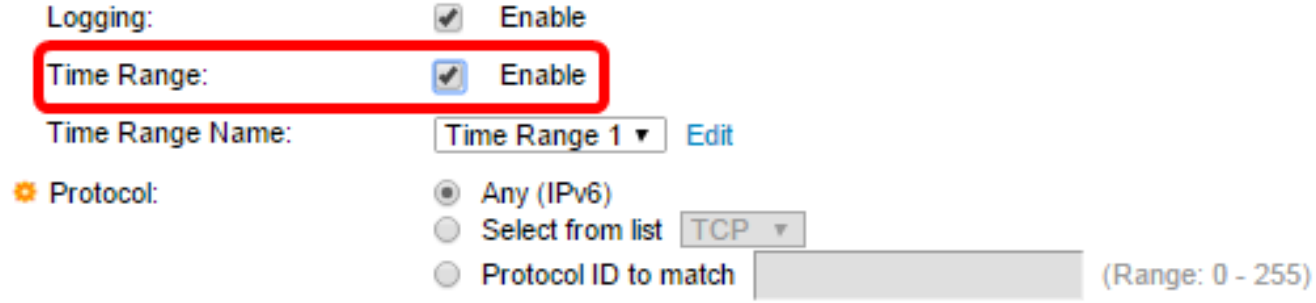
- 允许 — 交换机转发符合ACE所需标准的数据包。
- 拒绝 — 交换机丢弃符合ACE所需标准的数据包。

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。禁用的端口可在Port Settings页面上重新激活。

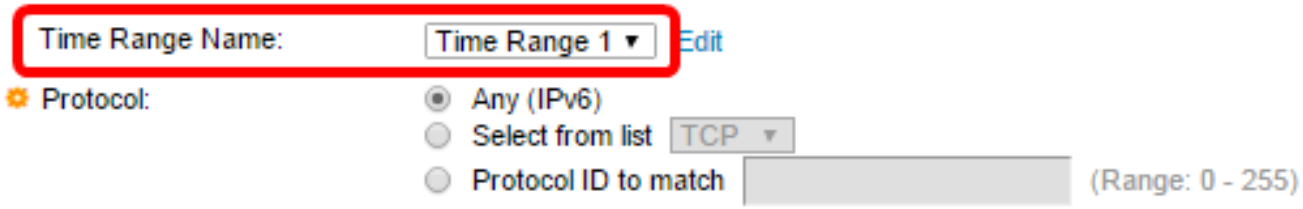
第6步。（可选）选中**Enable** Logging复选框，以启用与ACL规则匹配的日志记录ACL流。



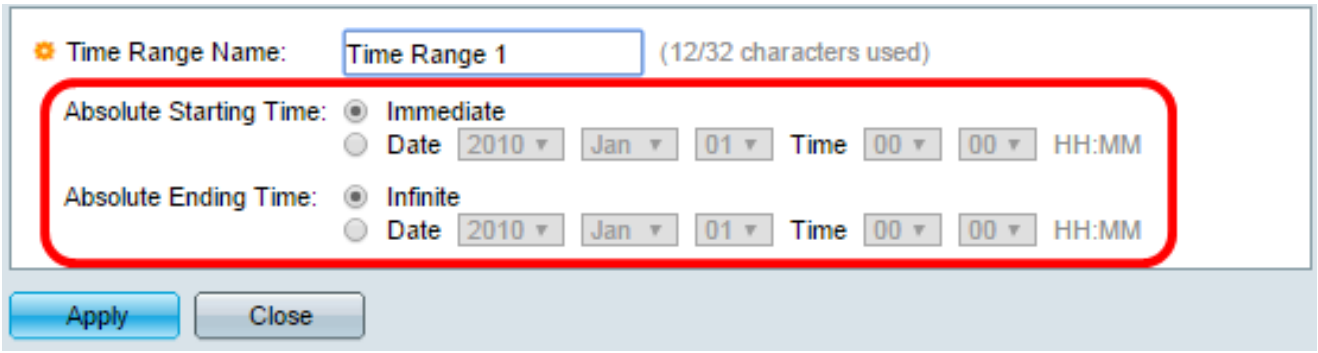
步骤7.（可选）选中**Enable** Time Range复选框，以允许将时间范围配置到ACE。时间范围用于限制ACE生效的时间量。如果禁用此功能，ACE将随时运行。



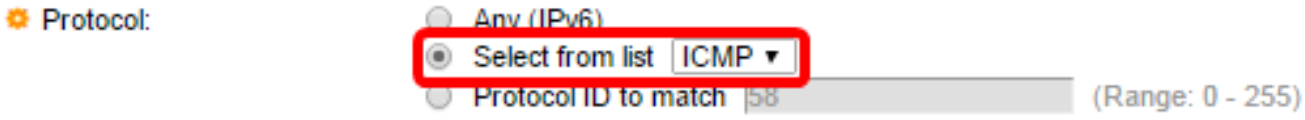
第8步。（可选）从Time Range Name下拉列表中，选择要应用到ACE的时间范围。



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。

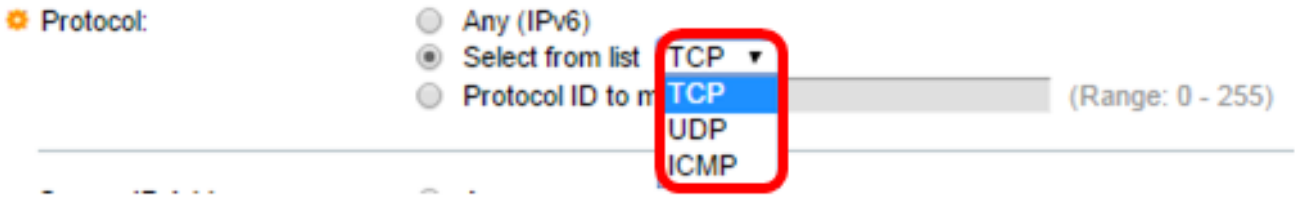


选项有：

- 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：在本示例中，选择“从列表中选择”。

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

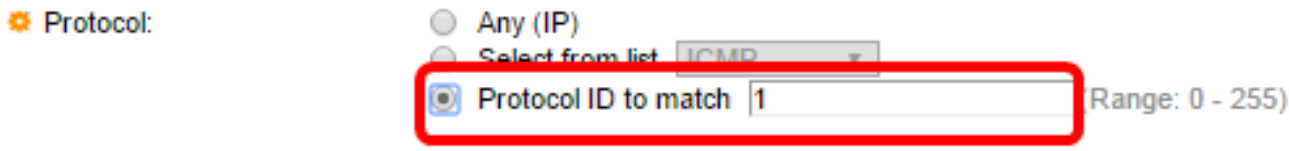


选项有：

- TCP — 传输控制协议(TCP)允许两台主机通信和交换数据流。TCP保证数据包的传输，并保证数据包按发送顺序发送和接收。
- UDP — 用户数据报协议(UDP)传输数据包，但不保证其传输。
- ICMP — 将数据包与Internet控制消息协议(ICMP)匹配。

注意：在本例中，使用TCP。

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。



注意：在本例中，使用1。

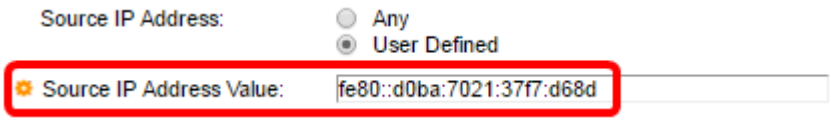
步骤12.在Source IP Address区域中，点击与ACE的所需条件对应的单选按钮。

选项有：

- 任意 — 所有源IPv6地址均应用于ACE。
- 用户定义 — 在源IP地址值和源IP前缀长度字段中输入要应用到*ACE的IP地址和IP通配符掩码*。

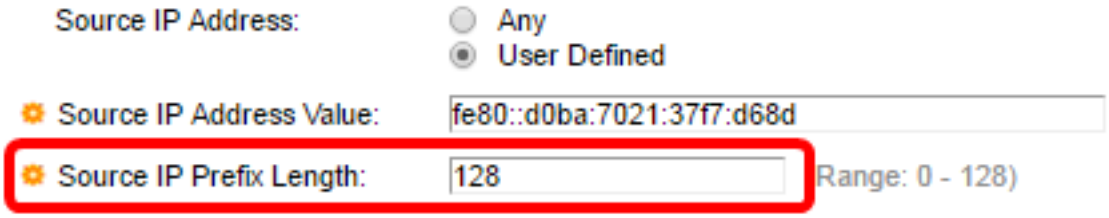
注意：在本例中，选择“用户定义”。如果选择Any，请跳至步骤15。

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



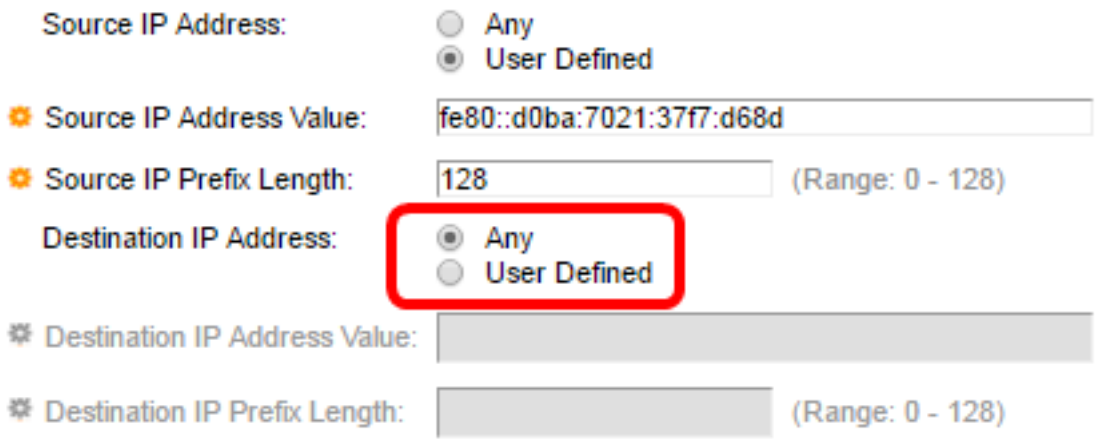
注意：在本示例中，使用fe80::d0ba:7021:37f7:d68d。

步骤14.在Source IP Prefix Length字段中输入*源IP前缀*长度。



注意：在本例中，使用128。

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

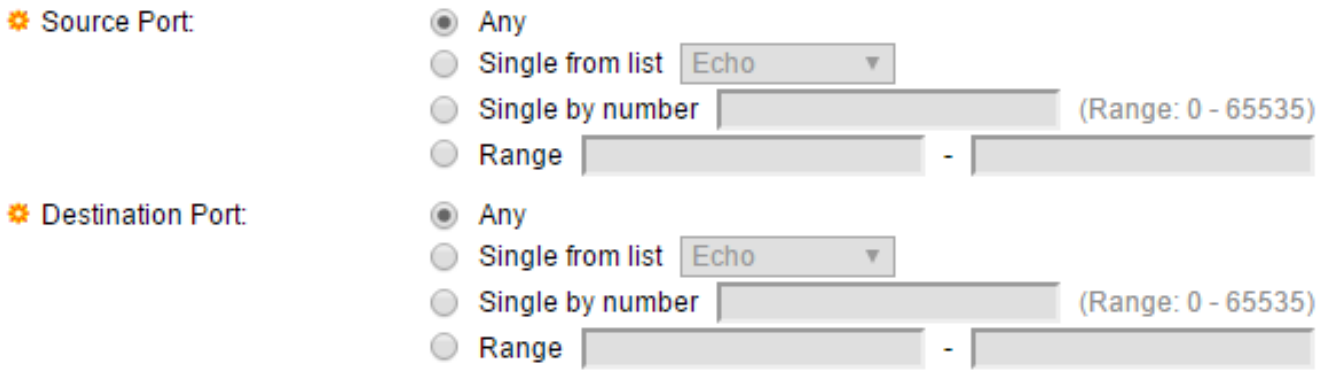


选项有：

- 任意 — 所有目标IPv6地址均应用于ACE。
- 用户定义 — 在目标IP地址值和目标IP修复长度字段中输入要应用于ACE*的IP地址值*和*目标IPP修复长度*的IP地址和IP通配符掩码。

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IPv6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。



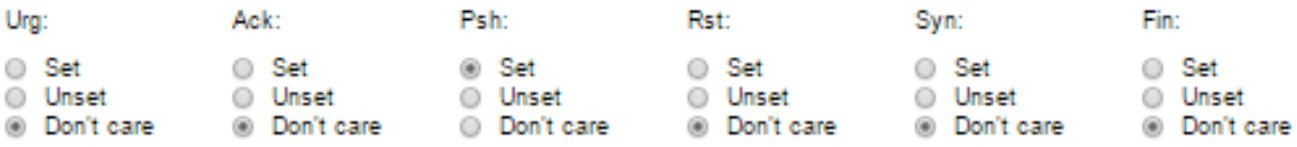
- Any — 匹配所有源端口。
- 单个从列表 — 您可以选择与数据包匹配的单个TCP/UDP源端口。仅当在“从列表选择”下拉菜单中选择800/6-TCP或800/17-UDP时，此字段才处于活动状态。
- 按编号单一(Single by number) — 您可以选择与数据包匹配的单个TCP/UDP源端口。仅当在“从列表选择”下拉菜单中选择800/6-TCP或800/17-UDP时，此字段才处于活动状态。
- 范围 — 您可以选择数据包匹配的TCP/UDP源端口范围。可以配置八个不同的端口范围（源端口和目标端口之间共享）。TCP和UDP协议各有八个端口范围。

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。

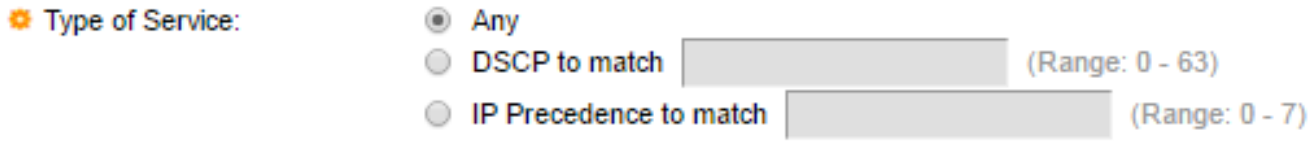


TCP标志包括：

- 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。



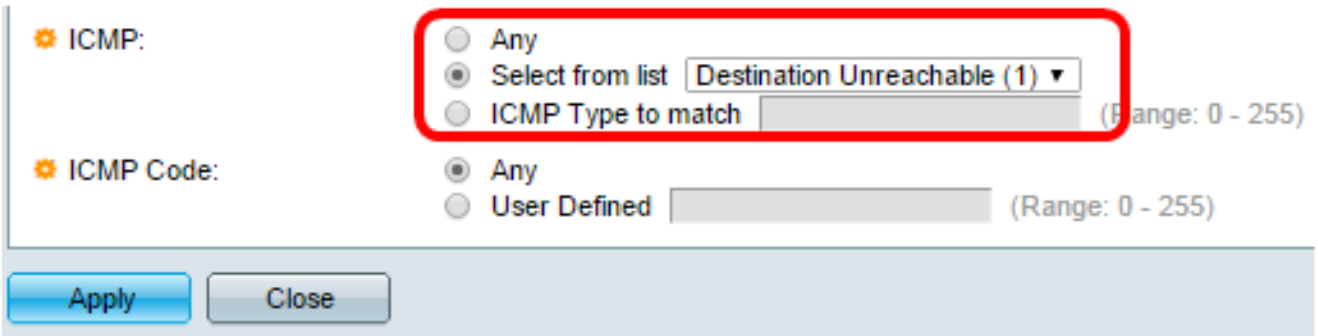
选项有：

- Any — 它可以是任何类型的流量拥塞服务。
- DSCP to Match — 差分服务代码点是一种对网络流量进行分类和管理的机制。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 — 互联网
  - 7 — 网络

注意：在本例中，选择Any。

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：

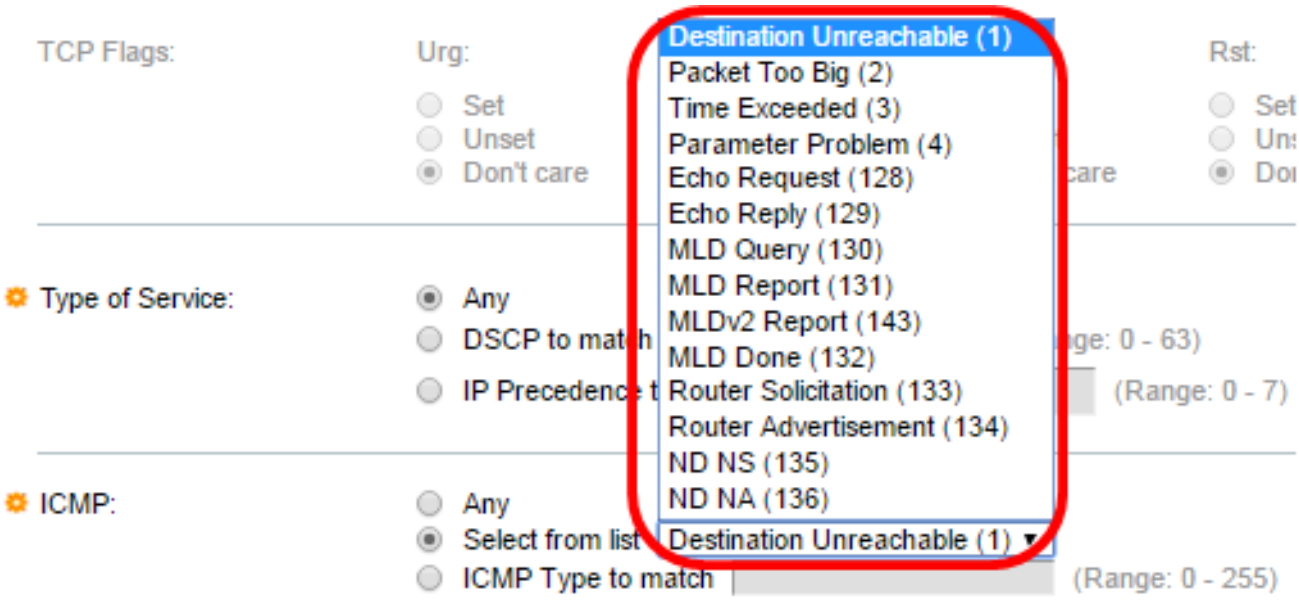


- 任意 — 接受所有消息类型。

- 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。

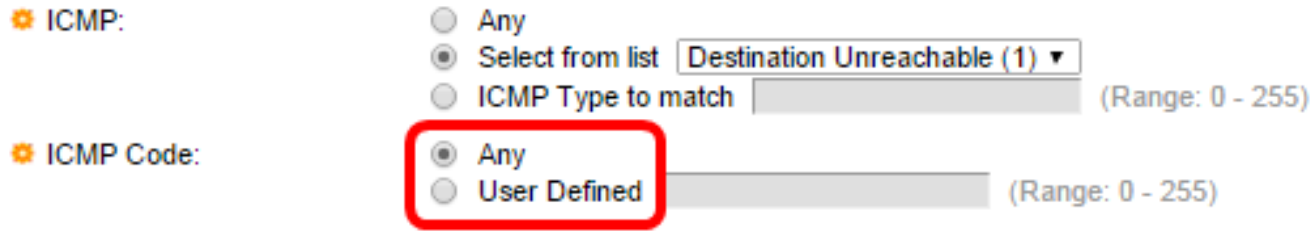
注意：在本示例中，选择“从列表中选择”。

第21步。（可选）如果在第20步中选择“从列表中选择”，请从下拉列表中可能的选项中选择要过滤的控制消息：



- 目标无法到达(1) — 主机或其网关生成该目标，以通知客户端由于某种原因无法到达(例如：网络或主机无法到达错误)。
- 数据包太大(2) — 数据报的大小超过给定MTU。
- 超时(3) — 网关生成该数据报，以通知源由于生存时间字段达到零而丢弃的数据报。
- 参数问题(4) — 它作为对其他ICMP消息未特别涵盖的任何错误的响应生成。
- 回应请求(128) — 它是ping，其数据预期会在回应应答中收到。
- 回应应答(129) — 响应回应请求时生成回应应答。
- MLD查询(130) — 用于了解哪些组播地址在连接的链路上具有侦听程序。十进制键入130。
- MLD报告(131) — 当消息发送方侦听的IPv6组播地址时生成。
- MLD v2报告(143) — 与版本2的MLD报告相同。
- MLD完成(132) — 当主机离开组时，它会向网络上的组播路由器发送组播侦听程序完成消息。
- 路由器请求(133) — 它是路由器发现消息。主机只需侦听通告即可发现相邻路由器的地址。组播的默认值为224.0.0.2，否则为255.255.255.255。
- 路由器通告(134) — 路由器定期从每个组播接口组播路由器通告，并通告该接口的IP地址。
- ND NS(135) — 消息由节点发起，以请求另一个节点的链路层地址，还用于重复地址检测和邻居不可达性检测等功能。
- ND NA(136) — 发送消息以响应NS消息。如果节点更改其链路层地址，它可以发送未经请求的NA来通告新地址。

步骤22.（可选）ICMP消息可以有一个代码字段，指示如何处理该消息。如果在步骤10中选择ICMP协议，则启用此选项。单击以下选项之一以配置是否过滤此代码：

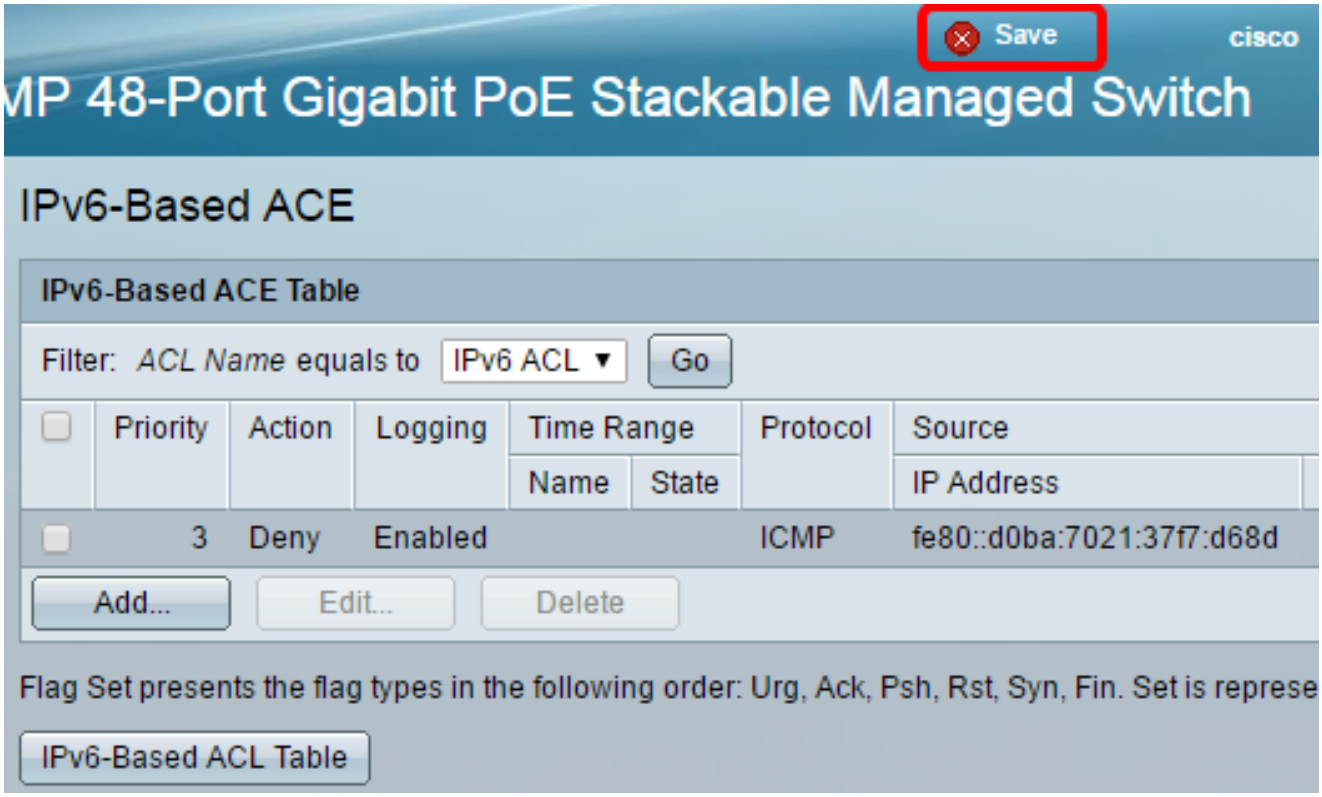


- 任意(Any) — 接受所有代码。
- 用户定义 — 您可以输入用于过滤目的的ICMP代码。

注意：在本例中，选择Any。

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IPv6的ACE。