# 配置IPv6-based访问控制表(ACL)和访问控制项(ACE)在交换机

## 客观

访问控制表(ACL)是网络列表用于的数据流过滤器和关联的动作改进安全。它阻拦或允许用户访问特定资源。ACL包含允许或对网络设备的拒绝访问的主机。

在IPv6的典型的ACL功能类似于在IPv4的ACL。ACL确定阻拦的转发的哪数据流，并且哪数据流在交换机接口。ACL允许过滤根据源地址和目的地址，入站和outbound对特定接口。每个ACL有一个含蓄Deny语句在末端。ACL的规则在访问控制条目(ACE)被配置。

您应该使用访问列表提供一个基本的安全级别进入入口您的网络。如果不配置在您的网络设备的访问列表，穿过交换机或路由器的所有信息包可能允许在您的网络上的所有部分。

此条款提供指令关于怎样配置IPv6-based ACL和ACE在交换机。

## 可适用的设备

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

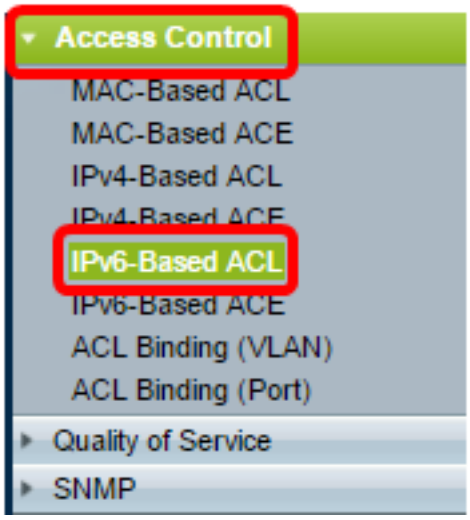
## 软件版本

- 1.4.5.02 – Sx500系列
- 2.2.5.68 – Sx350系列， SG350X系列， Sx550X系列

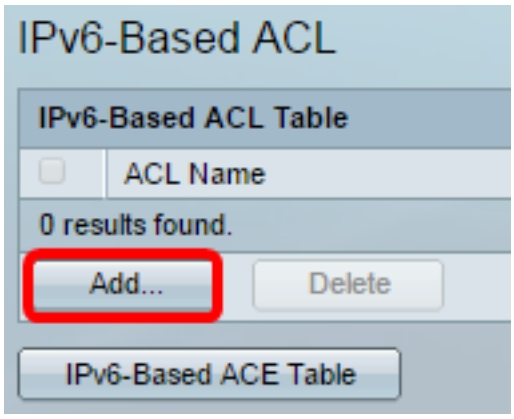
## 配置IPv6-Based ACL和ACE

### 配置IPv6-Based ACL

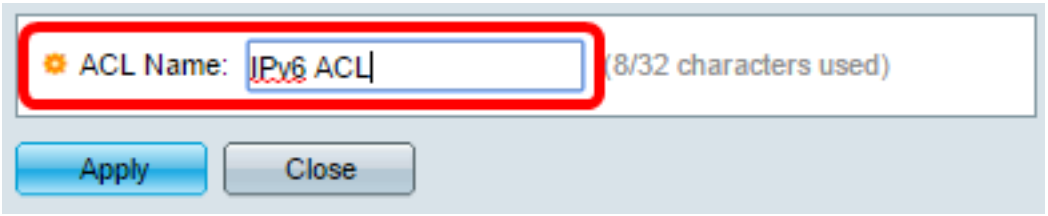
步骤1.基于Web的工具的洛金然后去**访问控制> IPv6-基于ACL**。




步骤2.点击**Add按钮**。

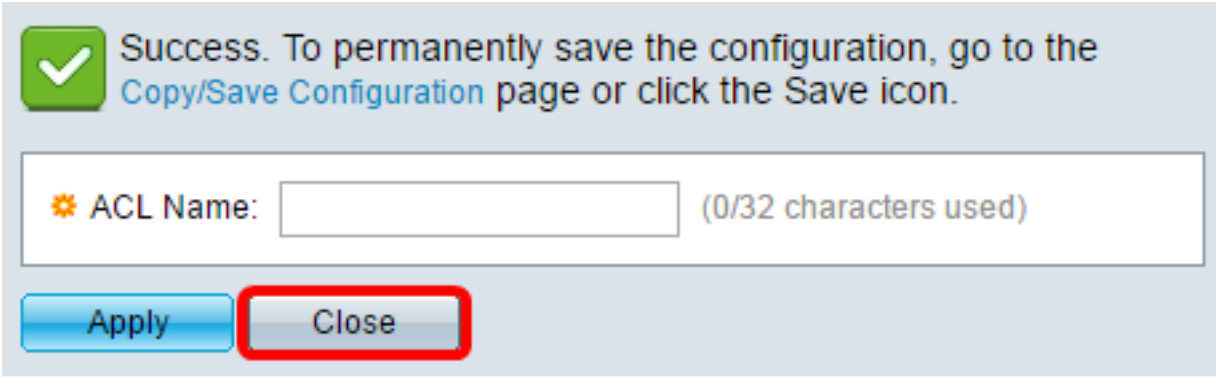



步骤3.输入新的ACL的名字在*ACL名称*字段。




**Note:**在本例中，使用IPv6 ACL。

步骤4.点击**适用**然后点击**Close**。




第5.步(可选)点击**"Save"**保存在启动配置文件的设置。


您应该当前配置了在您的交换机的IPv6-based ACL。

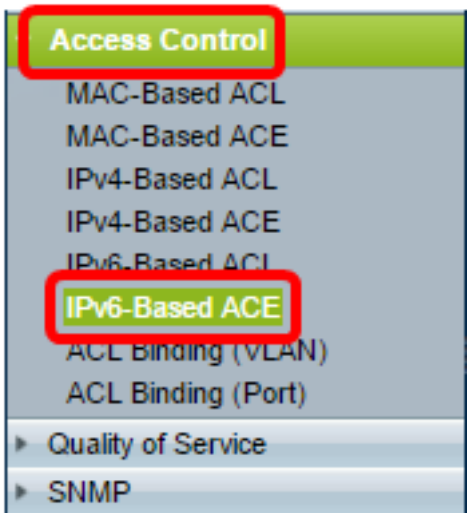
## 配置IPv6-Based ACE

当信息包在端口时收到，交换机通过第一个ACL处理帧。如果信息包匹配第一个ACL的一台ACE过滤器， ACE动作发生。如果信息包不匹配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，默认情况下信息包被丢弃。

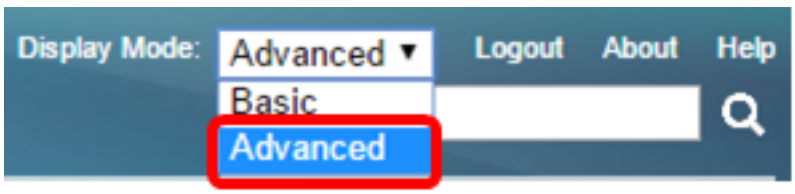
在此方案中， ACE将被创建否决从一个特定用户定义的来源IPv6地址被发送到所有目的地地址的数据流。

**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。

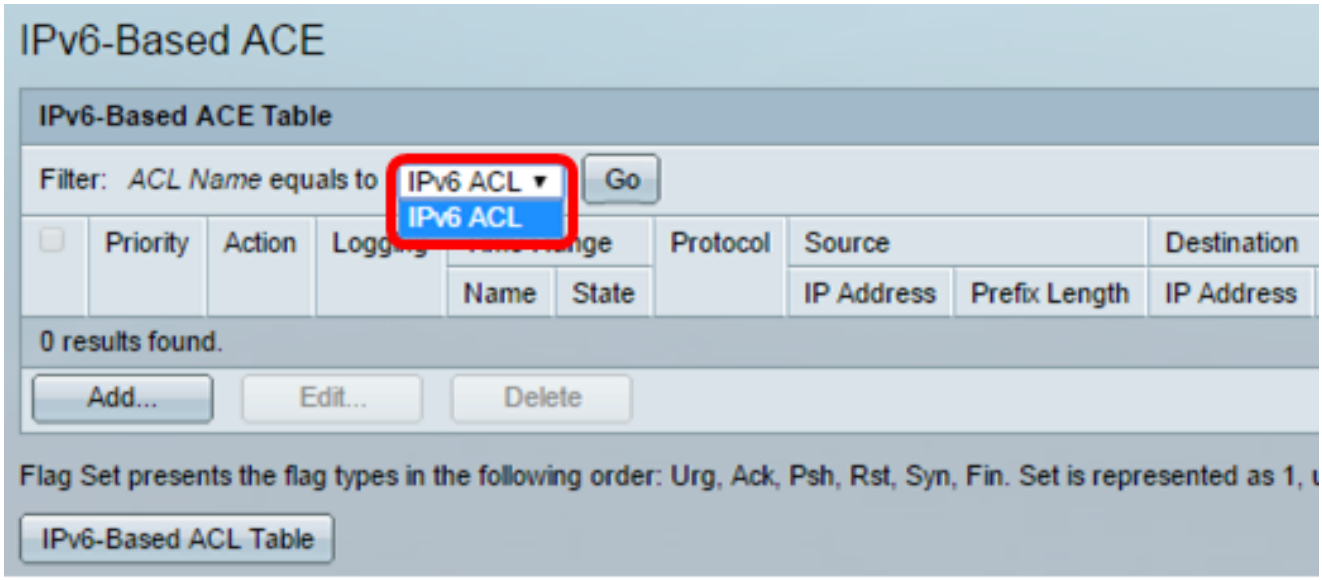
第 1 步：在基于Web的工具上，请去**访问控制> IPv6-基于ACE**。




**重要信息：**如果有Sx350， SG350X， Sx550X交换机，对Advanced模式的更改通过选择**提前**从显示模式下拉列表在页的右上角。

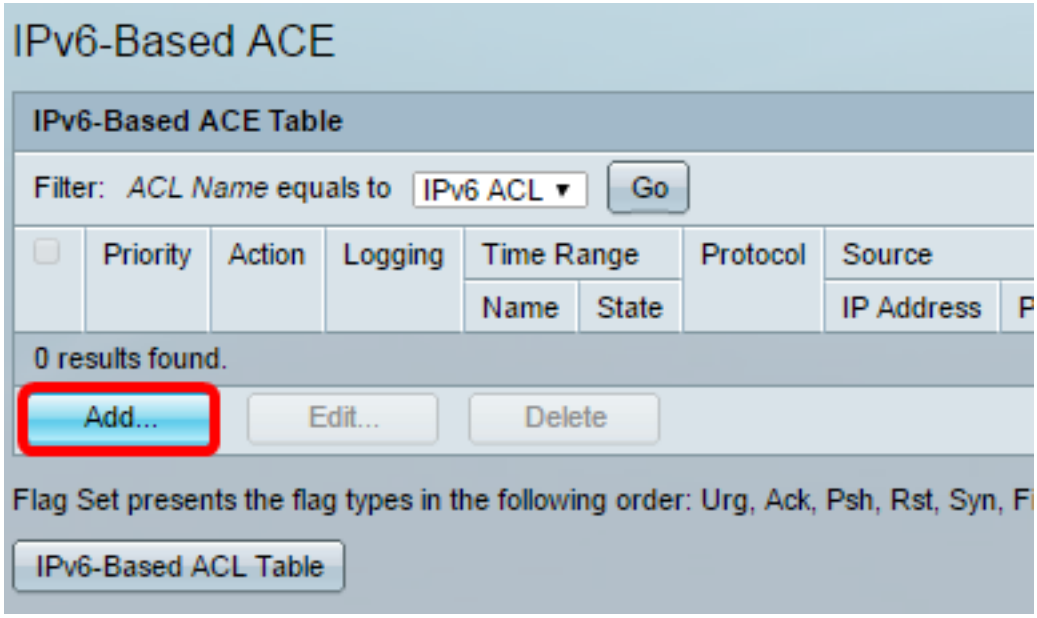


步骤2.从ACL名称下拉列表选择ACL然后点击**去**。



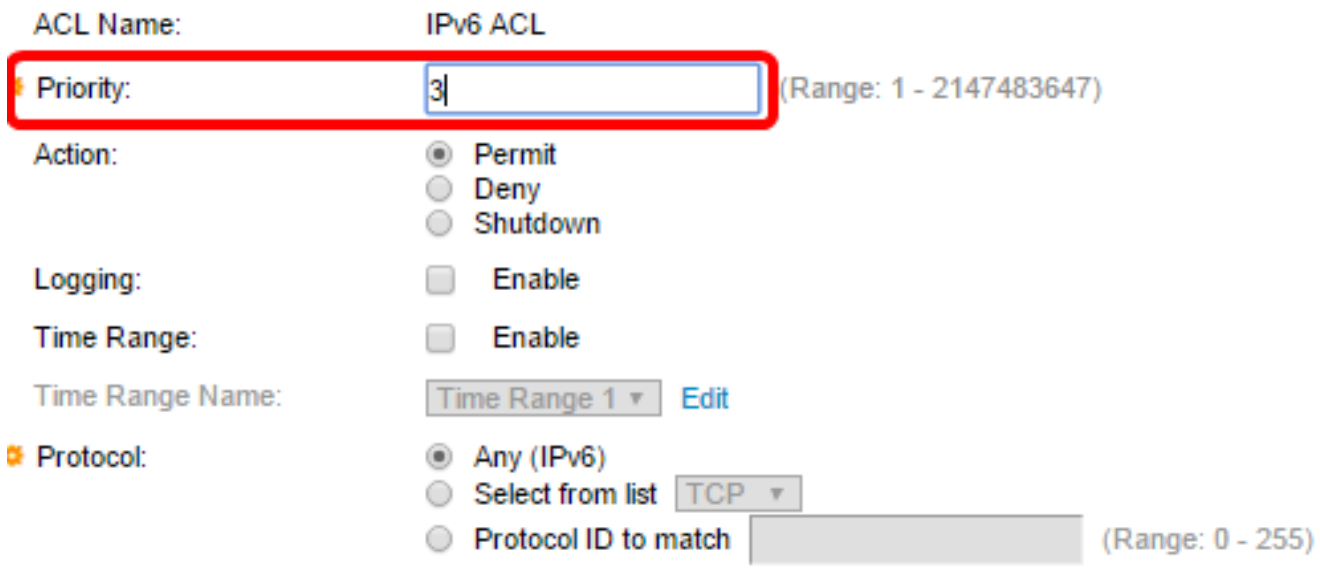

**Note:**为ACL已经被配置的ACE在表里将显示。

步骤3.点击**Add按钮**添加新规则到ACL。




**Note:***ACL名称*字段显示ACL的名字。

步骤4.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。它有范围的1到2147483647。




**Note:**在本例中，使用3。

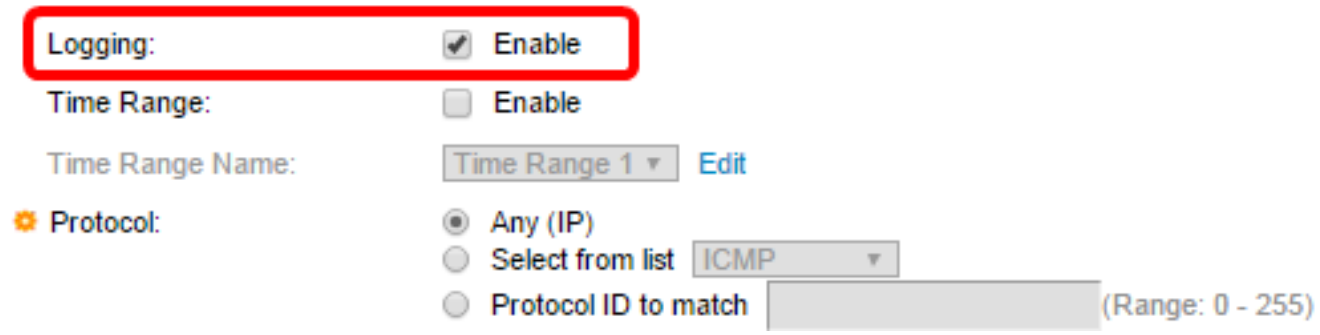
步骤5.点击对应于所需的动作采取的单选按钮，当帧满足ACE的必需的标准时。

**Note:**在本例中，许可证被选择。

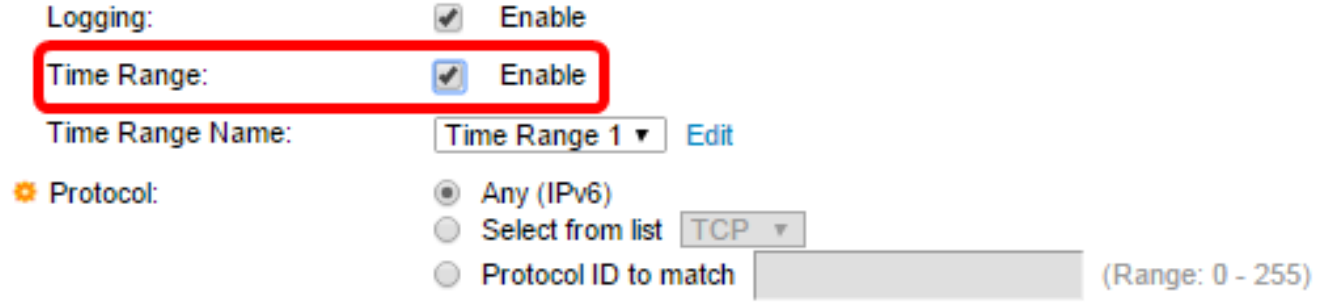
- 许可证—交换机转发满足ACE的必需的标准的信息包。
- 拒绝—交换机丢弃满足ACE的必需的标准的信息包。

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。失效端口在Settings页的端口可以恢复活动。

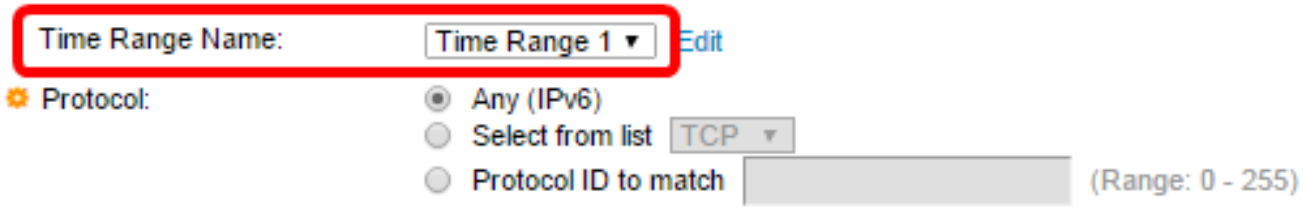
第6.步(可选的)检查对启用日志ACL的**启用日志**复选框流该匹配ACL规则。



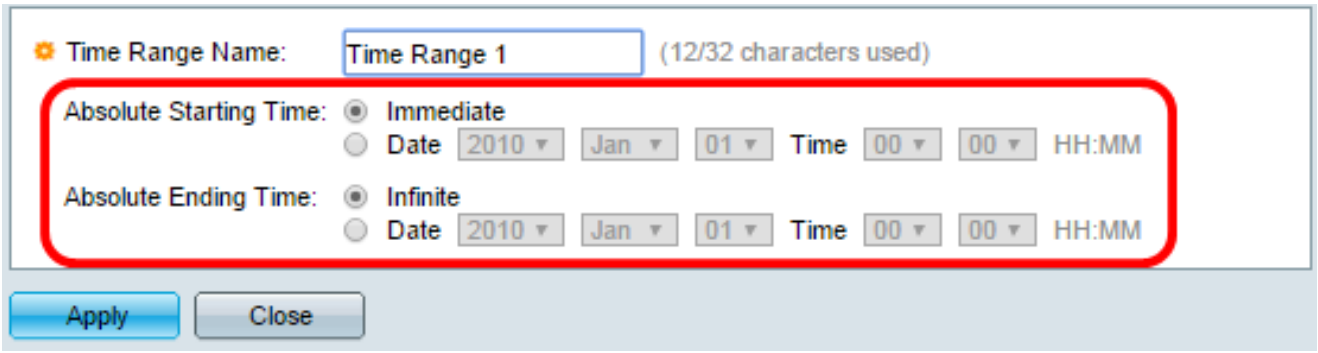

第7.步(可选的)检查允许时间范围的**Enable (event)**时间范围复选框被配置到ACE。时间范围用于限制ACE有效的时间。如果这留给失效， ACE在任何时间运作。



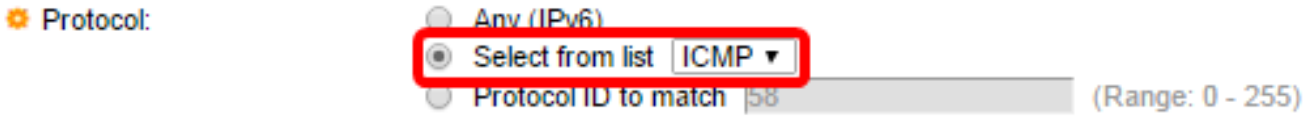

从时间范围名字下拉列表的第8.步(可选)，选择时间范围适用于ACE。




**Note:**您能点击**编辑**连接和创建在时间范围页的时间范围。




步骤9.选择协议类型协议地区。ACE根据特定协议或协议ID将被创建。

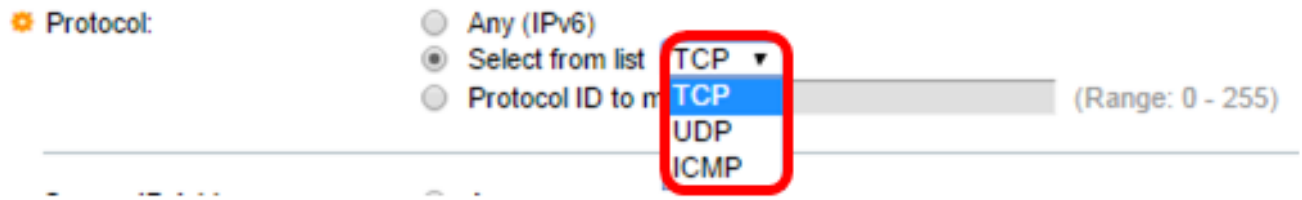



选项是：

- 其中任一(IP) —此选项将配置ACE接受所有IP协议。
- 从列表挑选—此选项将允许您从一张下拉列表选择协议。如果更喜欢此选项，请跳到第10.步。
- 匹配的协议ID —此选项将允许您输入协议ID。如果更喜欢此选项，请跳到第11.步。

**Note:**在本例中，请从列表挑选被选择。

第10.步(可选)，如果选择了从在第9步的列表挑选，从下拉列表选择协议。

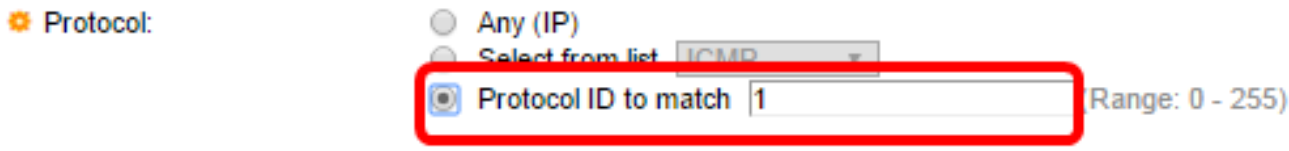



选项是：

- TCP —传输控制协议(TCP) enable (event)两台主机沟通的和交换数据流。TCP保证信息包发送，并且保证发送他们的信息包按顺序传输并且收到。
- UDP —用户数据报协议(UDP)传输信息包，但是不保证他们的发运。
- ICMP —匹配信息包对互联网控制消息协议(ICMP)。

**Note:**在本例中，使用TCP。

第11.步(可选)，如果在第9步选择协议ID配比，在*协议ID*输入协议ID*匹配*字段。




**Note:**在本例中，使用1。

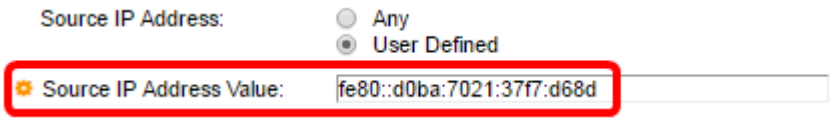
步骤12。点击在IP原地址地区对应于ACE期望标准的单选按钮。


选项是：

- 其中任一—所有来源IPv6地址适用于ACE。
- 用户定义—输入将适用于在*来源的*ACE *IP Address值*和*来源IP前缀*长度域的IP地址和IP通配符屏蔽。

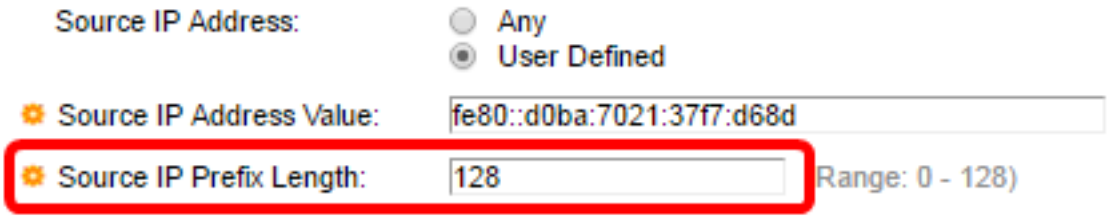
**Note:**在本例中，用户定义被选择。如果选择了其中任一，请跳到第15步。

第13步。输入IP原地址在*来源IP Address值*字段。



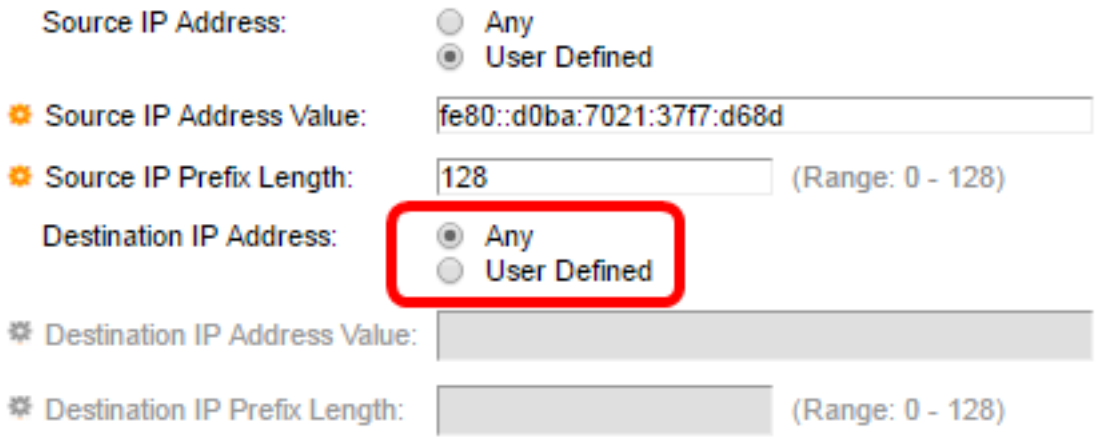

**Note:**在本例中，使用fe80::d0ba:7021:37f7:d68d。

步骤14。输入来源IP前缀长度在*来源IP前缀*长度域。




**Note:**在本例中，使用128。

第15步。点击在DestinationIP地址地区对应于ACE期望标准的单选按钮。

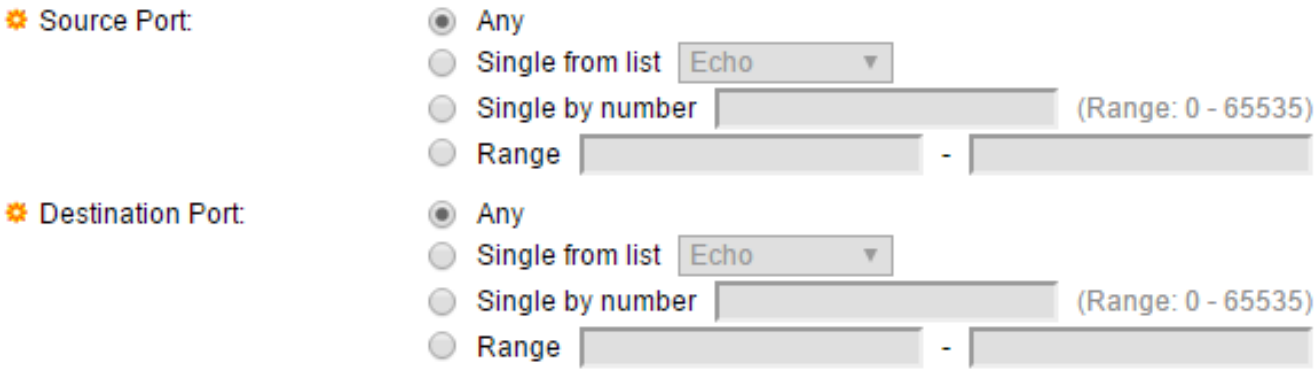



选项是：

- 其中任一—所有目的地IPv6地址适用于ACE。
- 用户定义—输入将适用于在*IP Address值的目的地*和*目的地IPPrefix*长度域的ACE的IP地址和IP通配符屏蔽。

**Note:**在本例中，其中任一被选择。选择此选项意味着将被创建的ACE将允许来自指定的IPv6地址的ACE数据流到所有目的地。

第16步。(可选)请点击一个单选按钮在theSource港区。DEFAULT值是其中任一个。




- 其中任一—对所有源端口的匹配。
- 单个从列表—您能选择信息包被匹配的单个TCP/UDP源端口。只有当800/6-TCP或800/17-UDP在挑选被选择从列表下拉菜单，此字段是活跃的。
- 单个由编号—您能选择信息包被匹配的单个TCP/UDP源端口。只有当800/6-TCP或800/17-UDP在挑选被选择从列表下拉菜单，此字段是活跃的。
- 范围—您能选择的TCP/UDP源端口的范围信息包被匹配。有可以配置的八个不同的端口范围(共享在来源和目的地端口之间)。TCP和UDP协议其中每一个有八个端口范围。

第17步。(可选)请点击一个单选按钮在theDestination港区。DEFAULT值是其中任一个。

- 其中任一—对所有源端口的匹配
- 单个从列表—您能选择信息包被匹配的单个TCP/UDP源端口。只有当800/6-TCP或800/17-UDP在挑选被选择从列表下拉菜单，此字段是活跃的。
- 单个由编号—您能选择信息包被匹配的单个TCP/UDP源端口。只有当800/6-TCP或800/17-UDP在挑选被选择从列表下拉菜单，此字段是活跃的。
- 范围—您能选择的TCP/UDP源端口的范围信息包被匹配。有可以配置的八个不同的端口范围(共享在来源和目的地端口之间)。TCP和UDP协议其中每一个有八个端口范围。

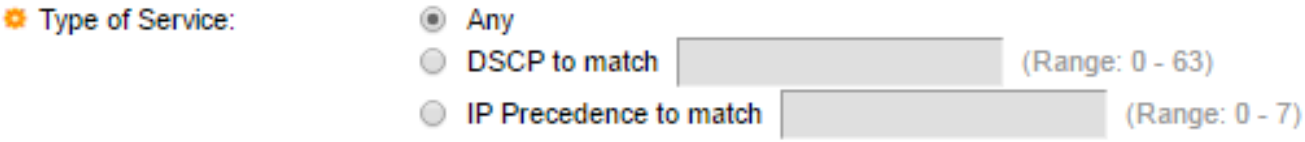
第18步。(可选)在TCP标记区域，选择过滤信息包的一个或更多TCP标志位。转发被过滤的信息包或被丢弃。由TCP标志位的过滤信息包增加信息包控制，强化网络安全。

- 集—，如果设置，请匹配标志位。
- 移置—，如果没有设置，请匹配标志位。
- 请勿关心—忽略TCP标志位。


TCP标志位是：

- Urg —此标志位用于识别流入的数据如紧急。
- Ack —此标志位用于承认信息包成功的接收。
- Psh —此标志位用于保证制定数据优先级(该该当)和被处理在发送或接收端。
- Rst —使用此标志位，当没有供当前连接使用的分段到达时。
- 同步符—此标志位使用TCP通信。
- 飞翅—此标志位，当通信或数据传输完成时，使用。

第19步。(可选)请点击IP信息包的服务类型自服务类型标准地区的。

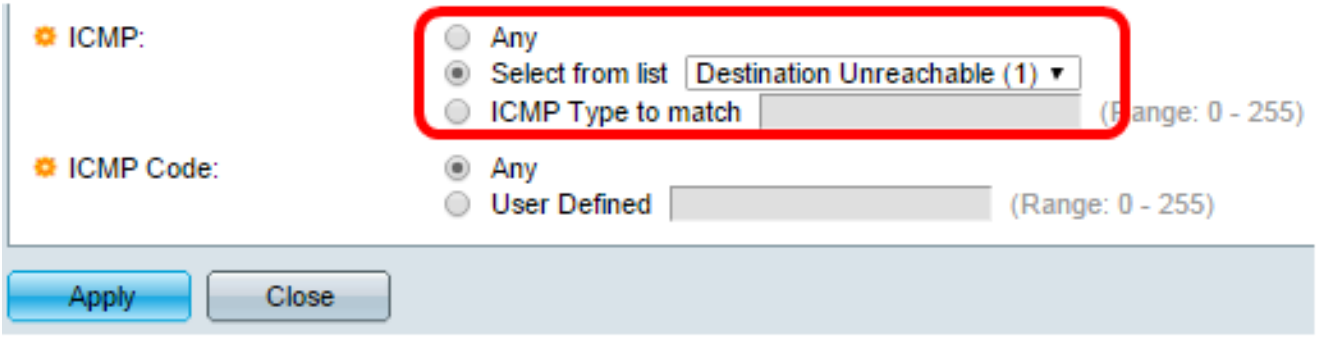



选项是：

- 其中任一—它可以是流量拥塞的任一种服务。
- 匹配的DSCP —差分服务代码点是分类的一个机制和管理网络流量。六位(0-63)用于选择每跳行为信息包经验在每个节点。
- 匹配的IP优先级— IP优先级是网络使用帮助提供适当的服务质量(QoS)承诺服务类型(ToS)的型号。此型号在IP头使用服务类型字节的三个多数有效位，正如RFC 791和RFC 1349所描述。与IP首选值的关键字下列：
  - 0 —惯例的
  - 1 —优先级的
  - 2 —立即的
  - 3 —闪存的
  - 4 — FLASH覆盖的
  - 5 —重要的
  - 6 —互联网的
  - 7 —网络的

**Note:**在本例中，其中任一被选择。

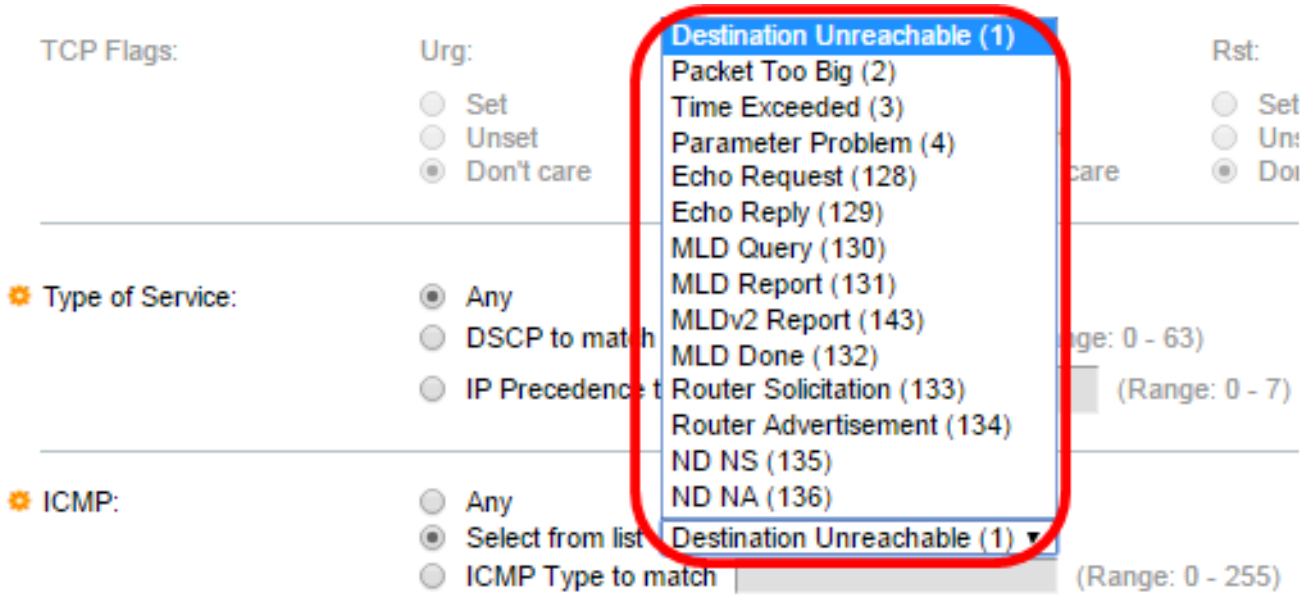
第20步。(可选)，如果ACL的IP协议是ICMP，请点击过滤目的使用的ICMP信息类型。名义上请选择消息类型或进入消息类型编号：




- 其中任一—所有消息类型被接受。
- 从列表挑选—您能名义上选择消息类型。
- ICMP键入配比—通讯数量将用于过滤类型目的。

**Note:**在本例中，请从列表挑选被选择。

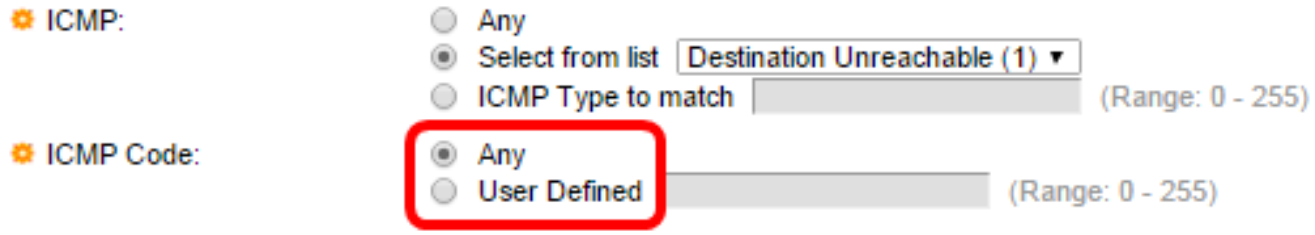
第21步。(可选)，如果请从列表挑选被选择在第20步，选择控制消息从在下拉列表的可能的选项过滤：




- 目的地不可得到(1) —它是由主机或其网关生成的通知客户端目的地是不可得到的由于某种原因(示例：网络或主机不可及错误)。
- 信息包太大(2) —数据包的大小超出被测量的MTU。
- Time exceeded (3) —它是由网关生成的通知来源一个被丢弃的数据包由于存活时间字段到达的零。
- 参数第(4)个问题—它生成作为别的不特别地包括的所有错误的一种回应ICMP信息。
- ECHO请求(128) —它是ping，数据在ECHO回复预计被接受。
- ECHO回复(129) —它生成以回应ECHO请求。
- MLD查询(130) —用于了解哪些组播地址有一条附上链路的监听程序。在十进制的类型130。
- MLD报告(131) —它生成，当消息发送方监听的IPv6组播地址。
- MLD v2报告(143) —它同与版本2的MLD报告一样。
- 执行的MLD (132) —当主机离开组时，传送组播监听程序完成的信息到网络的组播路由器。
- 路由器垦请(133) —它是路由器发现消息。当他们细听广告时，主机发现他们的相邻路由器的地址。默认值是组播的224.0.0.2，否则它是255.255.255.255。

- 路由器通告(134) —路由器周期地组播从其组播接口中的每一个的一个路由器通告，并且宣布该接口的IP地址。
- ND NS (135) —消息产生由节点请求另一个节点的链路层地址并且为功能例如相同的地址检测和相邻unreachability检测。
- ND NA (136) —信息传送以回应NS消息。如果节点更改其链路层地址，能发送未经请求的NA通告新的地址。

第22步。(可选) ICMP消息能有指示如何处理消息的代码字段。如果是否在此代码，选择在第10.步的ICMP协议点击以下选项之一配置过滤这是启用的：

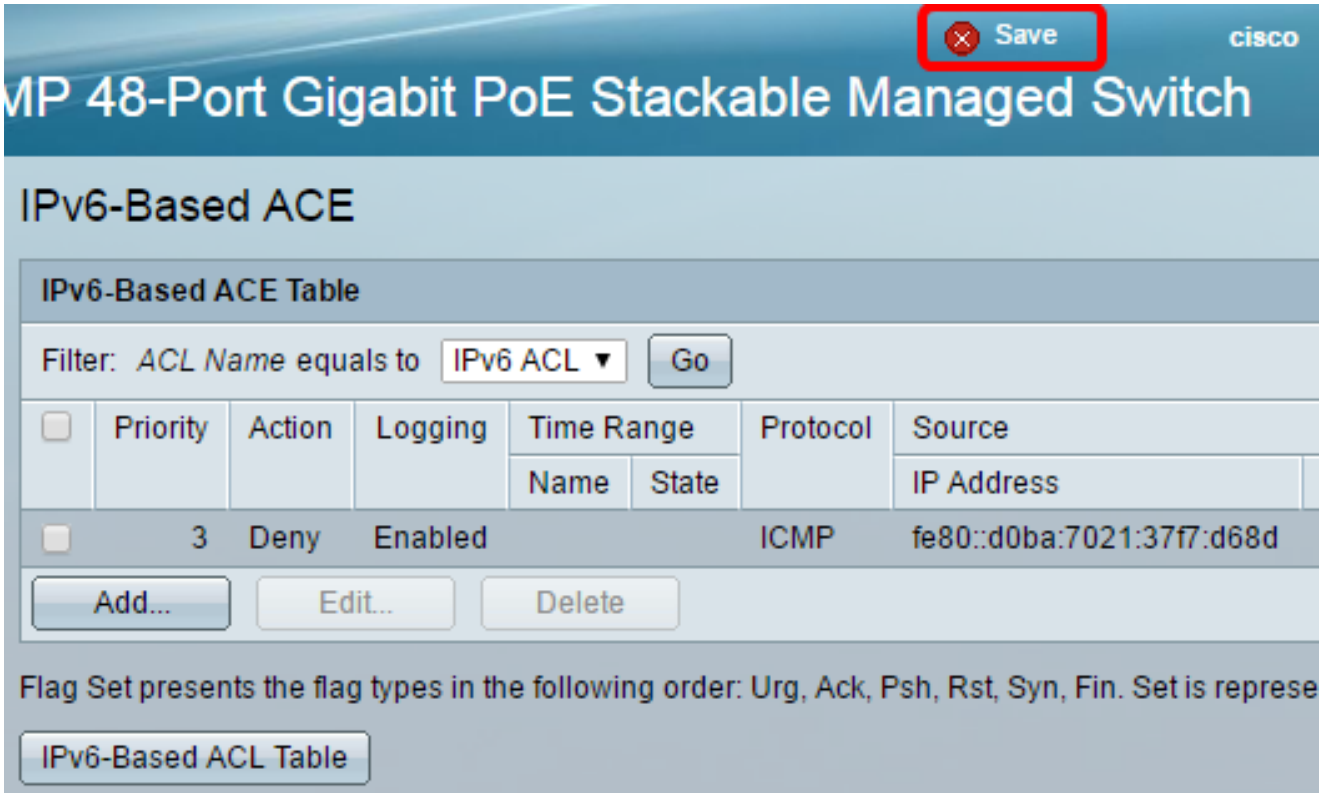



- 其中任一—接受所有代码。
- 用户定义—您能输入过滤的目的一个ICMP代码。

**Note:**在本例中，其中任一被选择。

第23步。点击**适用**然后点击**Close**。ACE被创建并且被关联对ACL名称。

第24步。点击**"Save"**保存设置到启动配置文件。




您应该当前配置了在您的交换机的IPv6-based ACE。