在200/300系列管理型交换机上配置基于IPv4的访问列表

目标

访问列表是可以应用的规则，用于允许或拒绝网络上的特定流量，这会增加网络的安全性并提高网络的整体性能。

本文档的目标是向您展示如何在200/300系列管理型交换机上配置基于IPv4的访问列表。

适用设备

· SF/SG 200和SF/SG 300系列托管交换机

软件版本

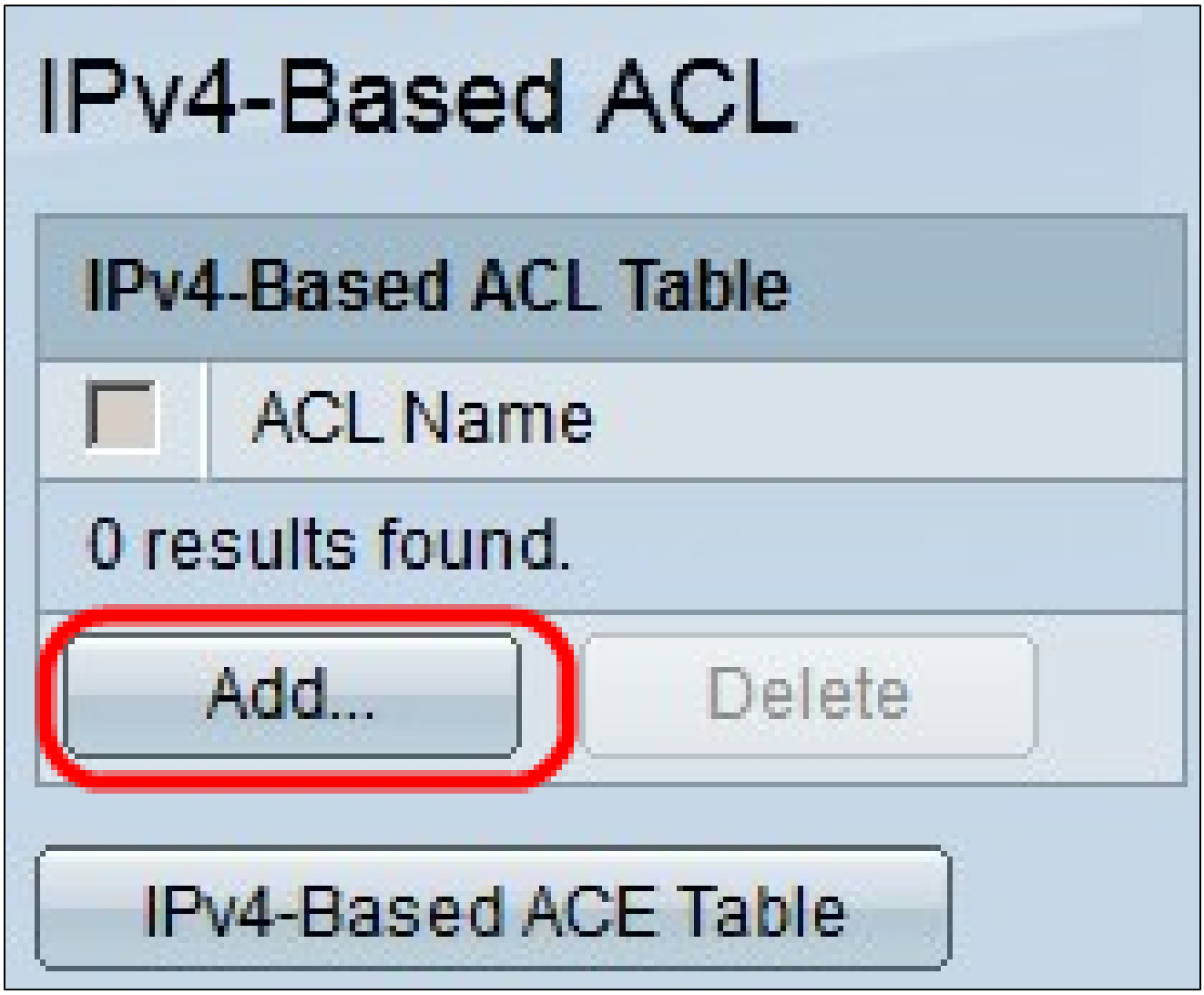
•1.3.0.62

配置基于IPv4的ACL和ACE

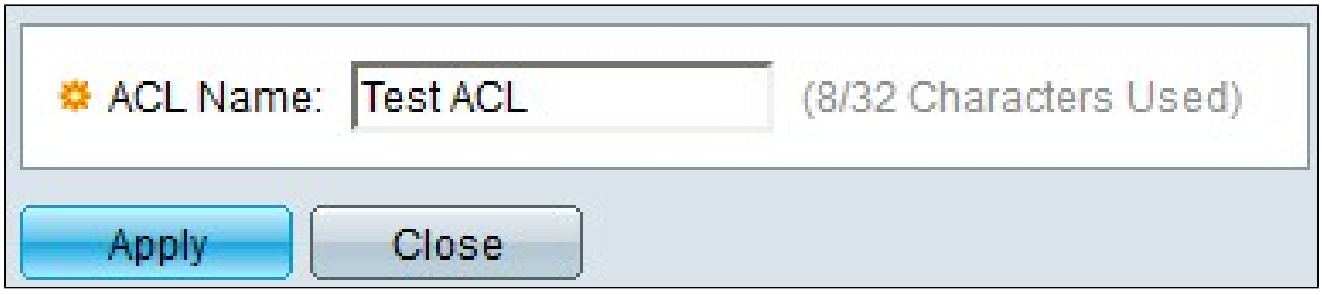
基于IPv4的ACL

步骤1:登录到Web配置实用程序并选择访问控制>基于IPv4的ACL。将打开基于IPv4的ACL页面。

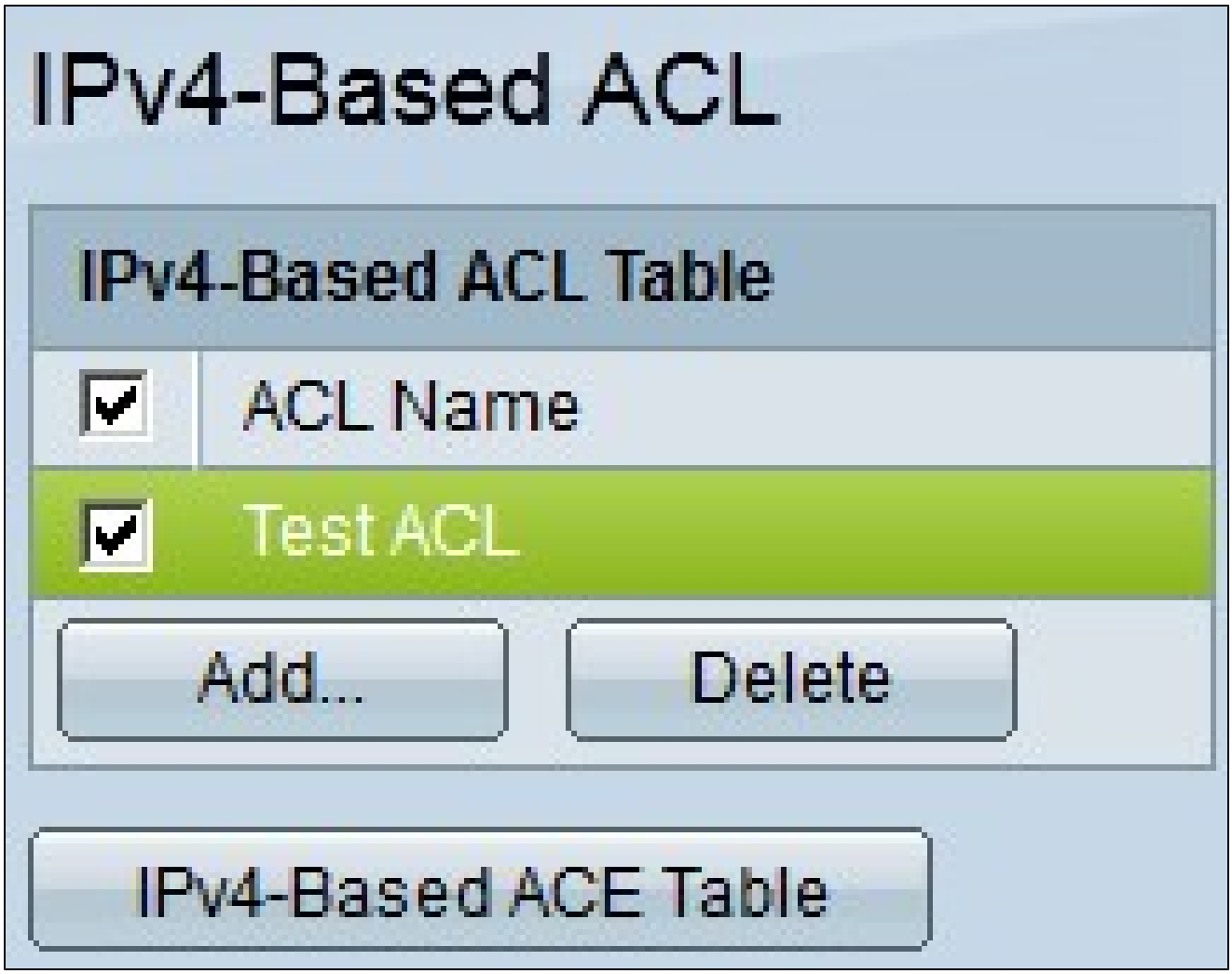
第二步：单击Add以添加新访问列表。



第三步：在ACL名称字段中，输入新访问列表的名称。



第四步：单击Apply保存访问列表。

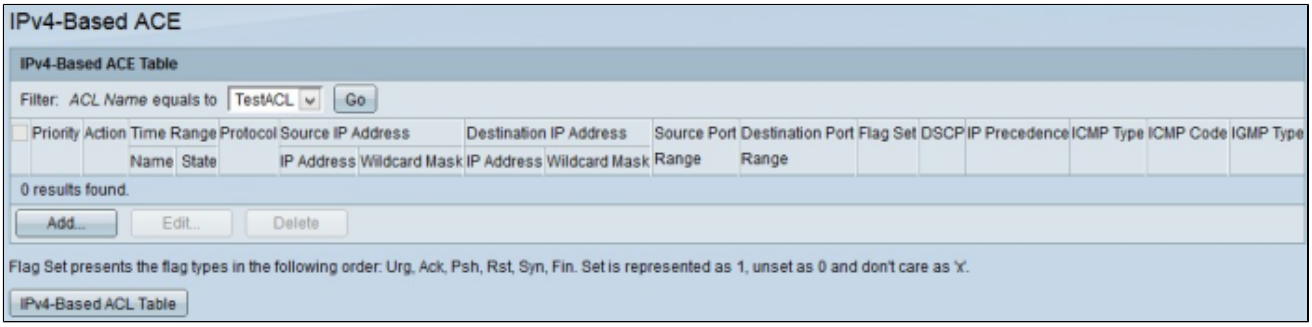


步骤5.（可选）要删除访问列表，请选中要删除的访问列表的复选框，然后点击删除。

基于IPv4的ACE

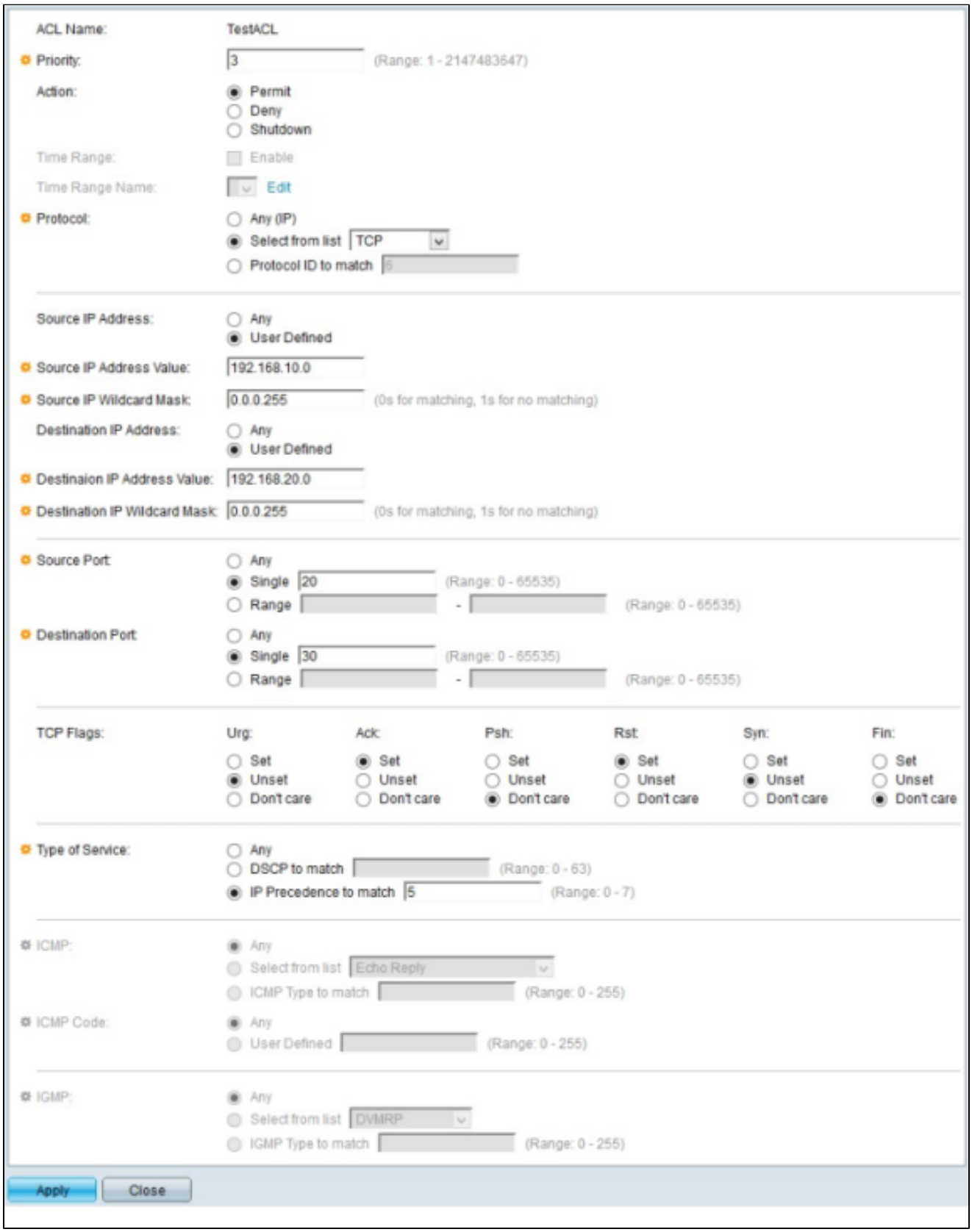
要管理ACL的ACE，需要执行后续步骤。

步骤1:登录到Web配置实用程序并选择访问控制>基于IPv4的ACE。将打开基于IPv4的ACE页面。



第二步：在Filter: ACL Name equals to下拉列表中，选择要分配访问规则的访问列表。

第三步：单击 Add。出现Add IP-Based ACE窗口。



第四步：在优先级字段中输入ACE的优先级。首先处理具有最高优先级的ACE。最高优先级为1。范围为1至2147483647。

第五步：在Action字段中，点击希望此访问规则执行的操作的单选按钮。可用选项包括：

·允许 — 转发由当前ACE过滤的数据包。

·拒绝 — 丢弃由当前ACE过滤的数据包。

·关闭 — 丢弃由当前ACE过滤的数据包，并禁用接收数据包的端口。

第六步：在Protocol字段中，单击要添加到ACE中的协议的单选按钮。为所有路由网络协议配置ACE，以便在数据包通过路由器时过滤数据包。可用选项包括：

· Any — 选择任何基于IPv4的ACE协议。

·从列表中选择 — 从下拉列表中选择所需的协议。

·要匹配的协议ID — 通过此选项，可以输入要使用的协议ID。

步骤 7.在源IP地址字段中，点击其中一个可用选项作为源IP地址：

· Any — 此选项将访问规则应用于特定网段中可用的任何IP地址。

·用户定义 — 此选项允许您输入特定IP地址。

— 源IP地址值 — 在此字段中，输入源IP地址。

— 源IP通配符掩码 — 在此字段中输入源IP地址的通配符掩码。通配符掩码允许您指定将此访问列表应用于源IP地址的主机。

步骤 8在Destination IP Address字段中，点击其中一个可用选项作为目标IP地址：

· Any — 此选项将访问规则应用于特定网段中可用的任何IP地址。

·用户定义 — 通过此选项，可以输入应用访问规则的特定IP地址：

— 目标IP地址值 — 在此字段中，输入目标IP地址。

— 目标IP通配符掩码 — 在此字段中，输入目标IP地址的通配符掩码。通配符掩码可用于指定应用此访问列表的目标IP地址的主机。

步骤 9仅当从步骤5中选择TCP或UDP时，才会启用Source Port字段。点击其中一个可用选项的单选按钮以选择源端口：

· Any — 此选项接受任何源端口。

·单一 — 此选项允许您输入单个源端口值。

·范围 — 此选项可让您输入可用源端口的范围。

步骤 10仅当从步骤5中选择TCP或UDP时，才会启用Destination Port字段。点击其中一个可用选项的单选按钮以选择目标端口：

· Any — 此选项接受任何目标端口。

·单一 — 此选项可让您输入单个目标端口值。

·范围 — 此选项可让您输入可用目标端口的范围。

步骤 11只有从步骤5中选择TCP时，才会启用TCP标志字段。单击每个标志的单选按钮以选择要触发访问规则的状态：

· Urg — 此标志将传入数据标识为紧急。

· Ack — 此标志用于确认数据包成功接收。

· Psh — 此标志用于确保数据具有正确的优先级，并在发送端或接收端进行处理。

· Rst — 当连接收到错误数据段时使用此标志。

· Syn — 此标志用于TCP通信。

· Fin — 通信或数据传输完成时使用此标志。

步骤 12在Type of Service字段中，单击其中一个可用的单选按钮以选择IP数据包的服务类型：

· Any — 此选项可选择任何类型的服务。

· DSCP to match — 选择此选项以实施差分服务代码点(DSCP)作为服务类型。DSCP是对网络流量进行分类和管理的一种机制。输入要应用于访问规则的DSCP值。

· IP优先顺序匹配 — 当前网络使用此类型的服务来提供正确的QoS（服务质量）。输入要应用于访问规则的值。

步骤 13仅当在第5步中选择ICMP时，才会启用ICMP（Internet控制消息协议）字段。ICMP用于在服务不可用时发送错误消息或测试连接。点击可用的单选按钮以过滤ICMP消息类型：

·任何 — 可以是任何错误消息或查询消息。

·从列表中选择 — 从下拉列表中选择任何允许的控制消息。

·要匹配的ICMP类型 — 通过此选项，可以输入要过滤的ICMP类型的数量。

步骤 14仅当从步骤5中选择ICMP时，才会启用ICMP代码字段。ICMP代码用于提供有关控制消息的更具体信息。点击其中一个可用选项：

· Any — 可以是匹配控制消息的任何值。

·用户定义 — 输入要过滤的ICMP代码。

步骤 15仅当您从步骤5中选择IGMP时，才会启用IGMP（互联网组管理协议）字段。IGMP管理网段上IP组播组中的主机成员身份。点击其中一个可用的单选按钮以过滤IGMP消息类型：

· Any — 此选项接受所有IGMP消息类型。

·从列表中选择 — 从下拉列表中选择一个可用选项进行过滤：

- DVMRP — 它使用反向路径泛洪技术，该技术通过除数据包到达的接口以外的每个接口发送收到的数据包的副本。

— 主机查询 — 它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

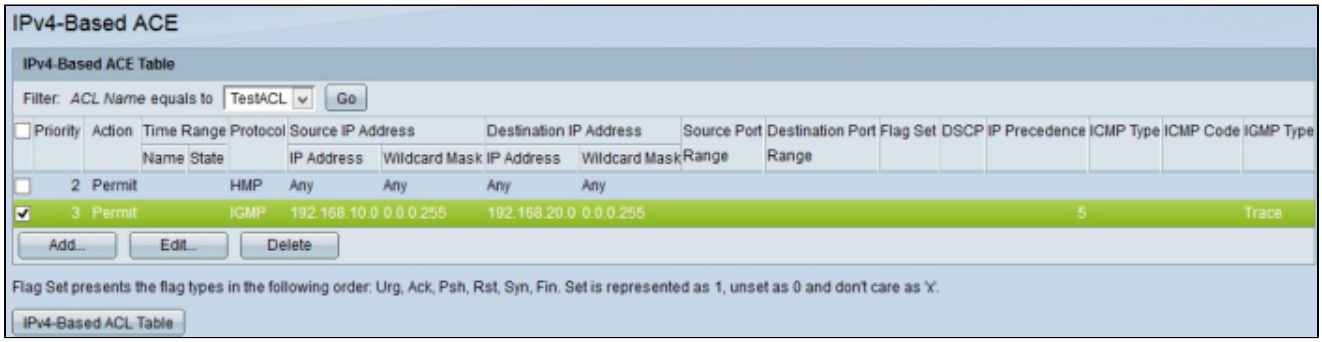
— 主机应答 — 对查询作出应答。

- PIM — 用于在本地和远程组播路由器之间将组播流量从组播服务器转发到许多组播客户端。

- Trace — 它提供加入和退出IGMP组播组的信息。

· IGMP匹配类型 — 通过此选项，可以输入要过滤的IGMP类型的数量。

步骤 16单击确定保存所进行的配置。



步骤17.（可选）要编辑当前访问规则，请选中要编辑的访问规则的复选框，然后点击编辑。

步骤18.（可选）要删除当前访问规则，请选中要删除的访问规则的复选框，然后点击删除。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。