WAP371上的ACL规则配置

目标

网络访问控制列表(ACL)是可选的安全层，用作控制进出子网的流量的防火墙。访问列表是允许和拒绝条件（或规则）的集合，这些条件出于多种原因提供安全性。例如，这些规则可以阻止未授权用户、允许授权用户访问特定资源以及阻止任何不必要的尝试访问网络资源。

本文档旨在向您展示如何在WAP 371上配置ACL规则。

适用设备

·WAP371

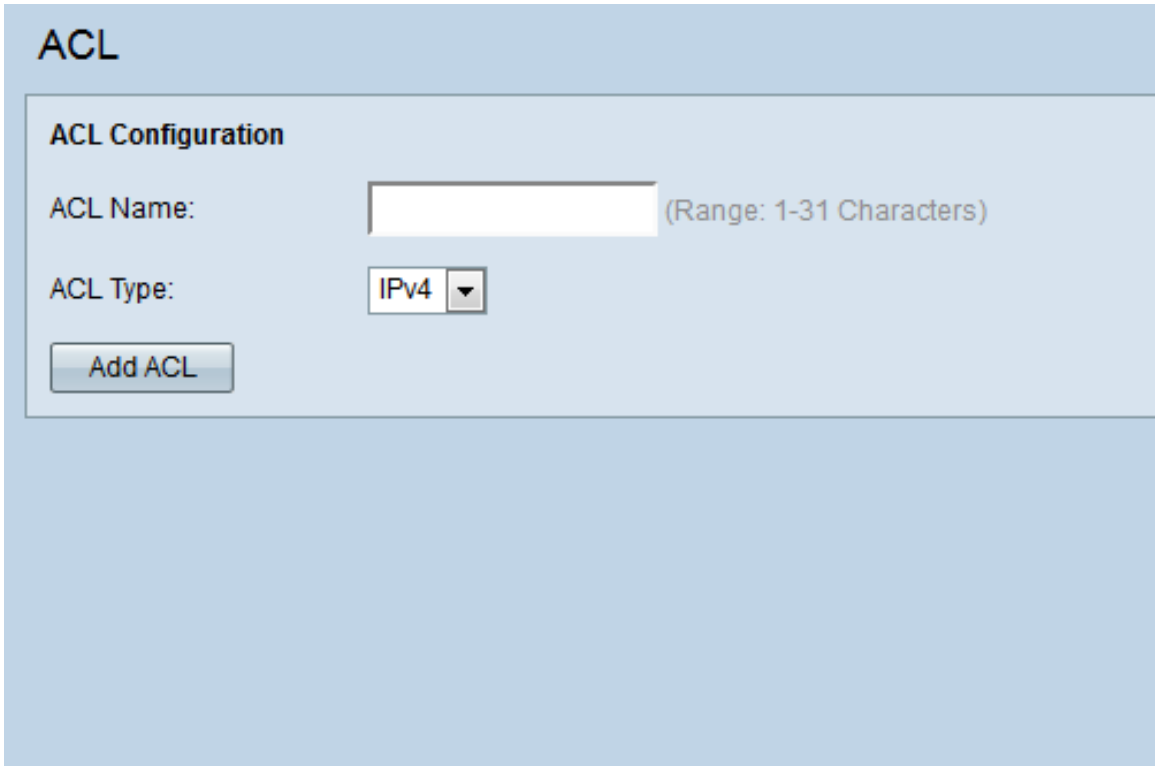
软件版本

•v1.2.0.2

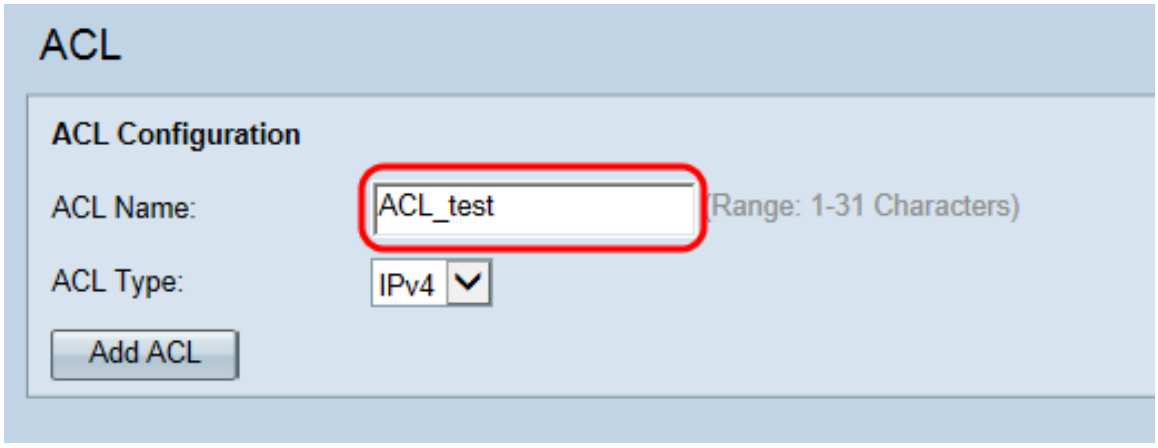
ACL规则配置

ACL 配置

步骤1.登录Web配置实用程序并选择**Client QoS > ACL**。ACL*页面*打开：

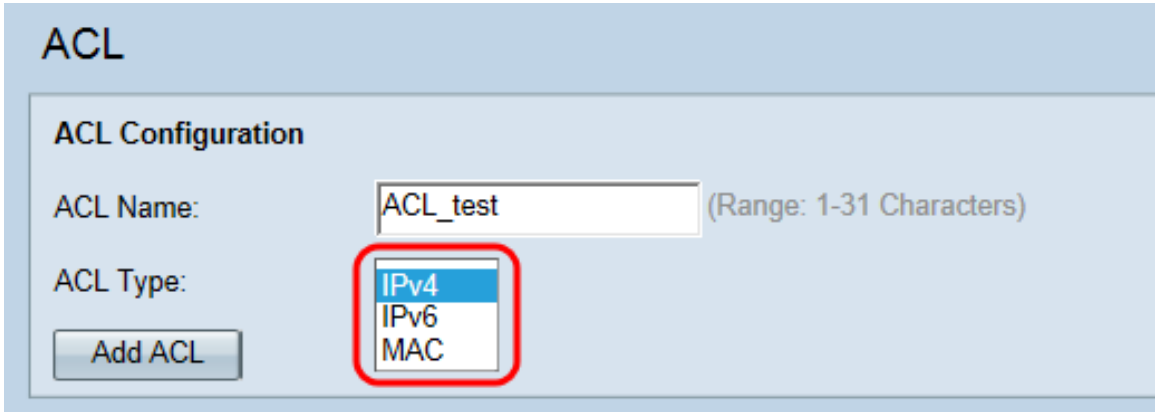


步骤2.在ACL Name字段中输入所需*的ACL*名称。范围为1到31个字符。



注意：ACL名称是特定ACL的标识符；对设备的运行没有影响。

步骤3.从ACL Type下拉列表*中选择*ACL类型。



选项如下：

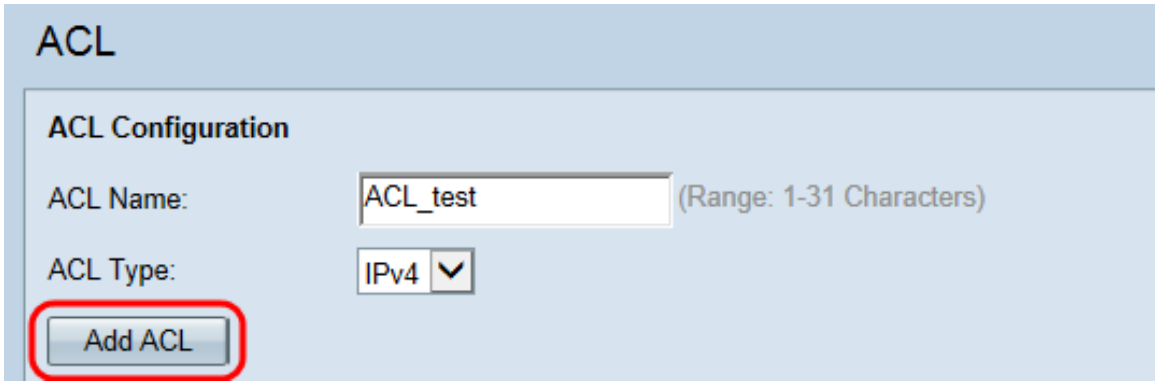
·IPv4 — 一个32位（四字节）地址。

·IPv6 - IPv4的后继路由器，包含128位（8字节）地址。

·MAC - MAC地址是分配给网络接口的唯一地址。

注意：IPv4和IPv6 ACL根据第3层和第4层标准控制对网络资源的访问。MAC ACL根据第2层标准控制访问。

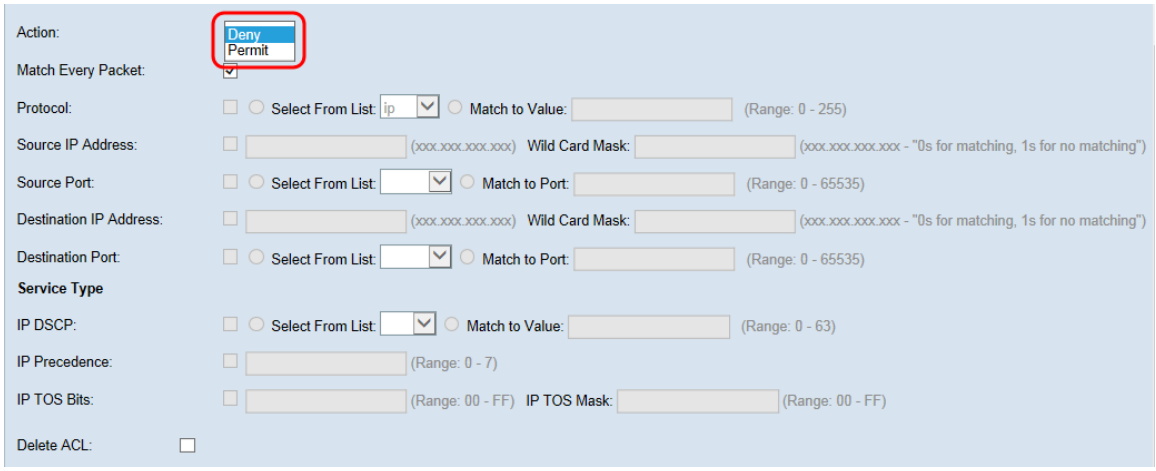
步骤4.单击**Add ACL**以添加新ACL。



IPv4和IPv6的ACL规则配置

注意：以下屏幕截图适用于IPv4 ACL规则，但可与IPv6 ACL规则互换。

步骤1.从“操作”下拉列表中为规*则选*择操作。

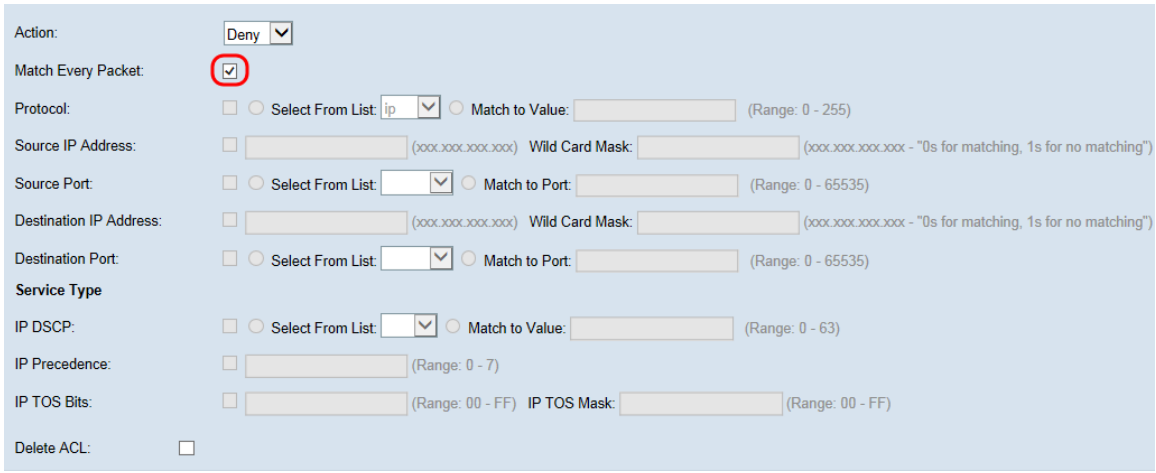


选项描述如下：

·允许 — 规则允许符合规则条件的所有流量进入或退出WAP设备。不符合条件的流量将被丢弃。

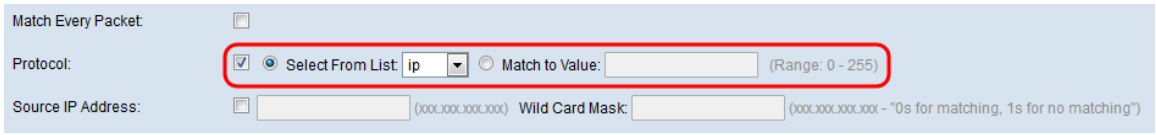
·拒绝 — 规则阻止符合规则条件的所有流量进入或退出WAP设备。不符合条件的流量将转发到下一条规则。如果这是最终规则，则不明确允许的流量将被丢弃。

步骤2.选中或取消选中Match Every Packet**复选框。**如果选中，规则（具有允许或拒绝操作）将匹配该帧或数据包，而不管其内容如何。



注意：如果选择此字段，则无法配置任何其他匹配条件。默认**情况下，为新规**则选择“匹配每个数据包”选项。您必须清除选项以配置其他匹配字段。

步骤3.选中**Protocol**复选框以根据IPv4数据包中的IP Protocol字段或IPv6数据包中的Next Header字段的值使用L3或L4协议匹配条件。如果选中Protocol复选框，请选择以下单选按钮之一。



选项描述如下：

·从列表中选择 — 从从列表中选择 *下拉列表*中选择协议。选项如下：

- IP - Internet协议(IP)是Internet协议簇中用于在网络间中继数据的主要通信协议。

- ICMP - Internet控制消息协议(ICMP)是Internet协议簇中的一种协议，供路由器等设备用于发送错误消息。

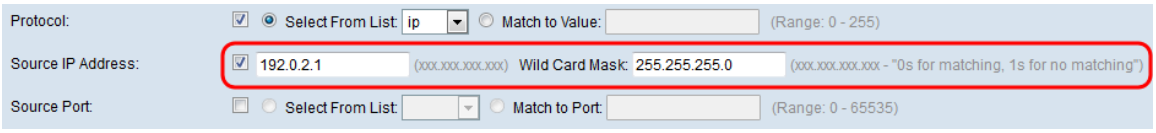
- IGMP — 互联网组管理协议(IGMP)是主机用于在IPv4网络上建立组播组成员身份的通信协议。

- TCP — 传输控制协议(TCP)使两台主机能够建立连接并交换数据流。

- UDP — 用户数据报协议是Internet协议簇中使用无连接传输模型的协议。

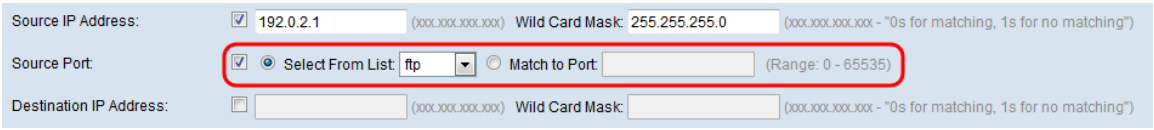
·与值匹配 — 输入标准IANA分配的协议ID，范围为0到255，用于所有未列出的协议。有关IANA分*配的协议ID的详细信*息，请参阅分配的Internet协议编号。

步骤4.选中**Source IP Address复**选框，在匹配条件中包含源的IP地址。在各自的字段中输入源的IP地址和通配符掩码。通配符掩码确定使用源地址的哪些位和忽略哪些位。它可以视为反向子网掩码。这对于指示某些路由协议的网络或子网大小或允许或拒绝IP地址范围非常有用。



注意：如果选中Source IP Address复选框，则需**要Wild Card Mask**字段。

步骤5.选中Source **Port复选**框，将源端口包括在匹配条件中。如果选中**源端口**复选框，请选择以下单选按钮之一。



选项描述如下：

·从列表中选择 — 从从列表中选择下*拉列表中*选择源端口。选项如下：

- FTP — 文件传输协议(FTP)是一种标准网络协议，用于通过基于TCP的网络（如互联网）将文件从一台主机传输到另一台主机。

- FTP数据 — 由连接到客户端的服务器发起的数据通道，通常通过端口20。

- HTTP — 超文本传输协议(HTTP)是万维网数据通信的基础应用协议。

- SMTP — 简单邮件传输协议(SMTP)是电子邮件（邮件）传输的Internet标准。

- SNMP — 简单网络管理协议(SNMP)是用于管理IP网络上设备的Internet标准协议。

- Telnet — 一种会话层协议，用于Internet或局域网，用于提供双向的面向文本的交互通信。

- TFTP — 简单文件传输协议(TFTP)是用于传输比FTP更简单但功能更差的文件的Internet软件实用程序。

- WWW — 万维网是支持HTTP格式文档的Internet服务器系统。

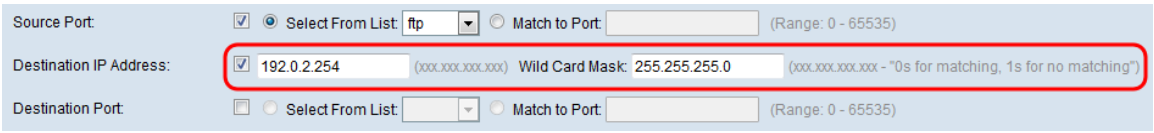
·匹配到端口 — 在未列出源端口的匹配到端口(Match to Port)字*段中输入*范围为0到65535的端口号。范围包括三种不同类型的端口。范围描述如下：

- 0到1023 — 公认端口。

- 1024至49151 — 注册端口。

- 49152到65535 — 动态和/或专用端口。

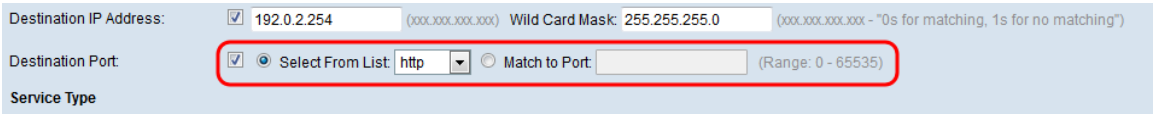
步骤6.选中**Destination IP Address复**选框，将目标的IP地址包括在匹配条件中。在各自的字段中输入目的地的IP地址和通配符掩码。通配符掩码确定使用源地址的哪些位和忽略哪些位。它可以视为反向子网掩码。这对于指示某些路由协议的网络或子网大小或允许或拒绝IP地址范围非常有用。



注意：如果选*中"目标IP*地址"复选框，则**需要"通配符**掩码"字段。

注意：如果只想匹配一个IP地址，请使用通配符掩码0.0.0.0。

步骤7.选中Destination Port复**选框**，将目标端口包括在匹配条件中。如果选中**Destination Port**复选框，请选择以下单选按钮之一。



选项描述如下：

·从列表中选择 — 从从列表中选择下*拉列表中*选择目标端口。下拉列表选项如下：

- FTP — 文件传输协议(FTP)是一种标准网络协议，用于通过基于TCP的网络（如互联网）将文件从一台主机传输到另一台主机。

- FTP数据 — 由连接到客户端的服务器发起的数据通道，通常通过端口20。

- HTTP — 超文本传输协议(HTTP)是万维网数据通信的基础应用协议。

- SMTP — 简单邮件传输协议(SMTP)是电子邮件（邮件）传输的Internet标准。

- SNMP — 简单网络管理协议(SNMP)是用于管理IP网络上设备的Internet标准协议。

- Telnet — 一种会话层协议，用于Internet或局域网，用于提供双向的面向文本的交互通信。

- TFTP — 简单文件传输协议(TFTP)是用于传输比FTP更简单但功能更差的文件的Internet软件实用程序。

- WWW — 万维网是支持HTTP格式文档的Internet服务器系统。

·与端口匹配 — 在未列出目标端口的与端口匹配字段中，输*入范围*为0到65535的端口号。范围包括三种不同类型的端口。范围描述如下：

- 0到1023 — 公认端口。

- 1024至49151 — 注册端口。

- 49152到65535 — 动态和/或专用端口。

注意：只能从“服务类型”区域选择其中一项服务，并且可以为匹配条件添加。

IPv4的ACL规则服务类型配置

步骤1.选中**IP DSCP**复选框以根据IP DSCP值匹配数据包。DSCP用于指定帧的IP报头上的流量优先级。这会将关联流量流的所有数据包与您从列表中选择的IP DSCP值进行分类。如果选中IP DSCP复选框，请选择以下单选按钮之一。

选项描述如下：

·从列表中选择 — 从从列表中选择下拉列*表中选择*IP DSCP值。选项如下：

- DSCP保证转发(AS) — 允许运营商提供交付保证，只要流量不超过某些订用速率。

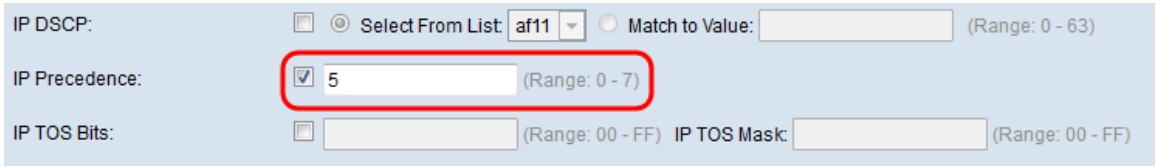
— 服务类别(CS) — 允许向后兼容仍使用Precedence字段的网络设备。

— 加速转发(EF) — 用于通过DS(DiffServ)域构建低损耗、低延迟、低抖动、有保证的带宽和端到端服务。

·Match to Value — 在Match to Value字段中输入范围为0到63的DSCP值，*以自*定义DSCP值。

注意：有关DSCP的*更多详细信息，*请参阅DSCP和优先级值。

步骤2.选中IP Precedence复**选框**，以在匹配条件中包含IP Precedence值。这是一种为每个IP数据包分配优先级的机制，其中0是最低优先级，7是最高优先级。如果选**中IP Precedence**复选框，请输入一个介于0到7之间的IP优先级值。

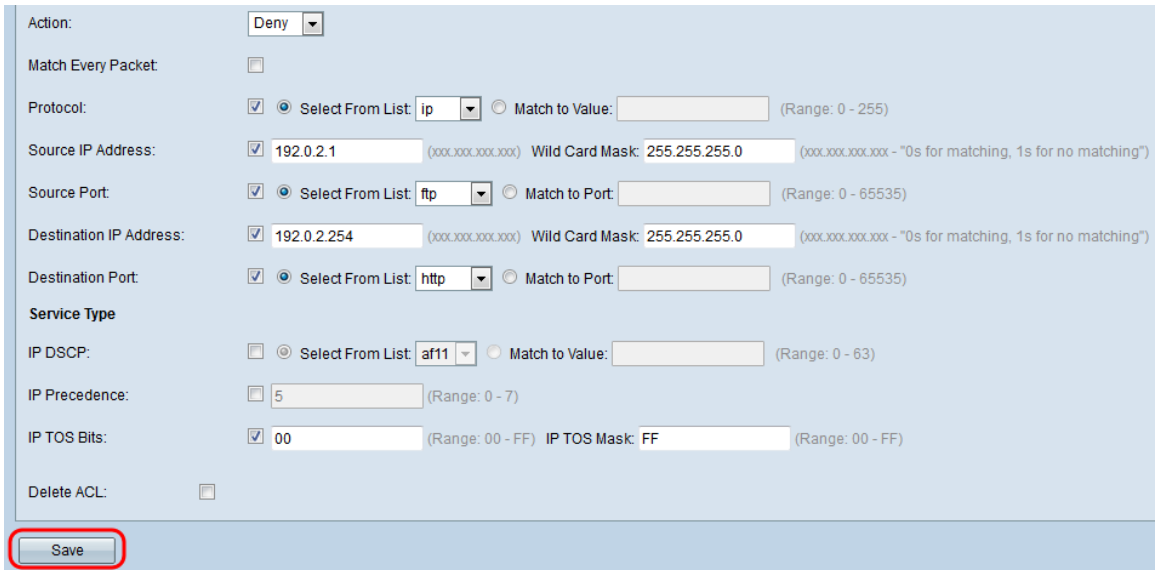


注意：有关IP优先*级的更多详细信*息，请参阅DSCP和优先级值。

步骤3.选中**IP TOS Bits复**选框，将IP报头中数据包的服务类型(TOS)位用作匹配条件。TOS字段用于指定数据报的优先级并相应地路由该优先级。如果选中IP TOS Bits复选框，请在其各自的字段中输入IP TOS位，范围为00-FF，IP TOS掩码范围为00-FF。

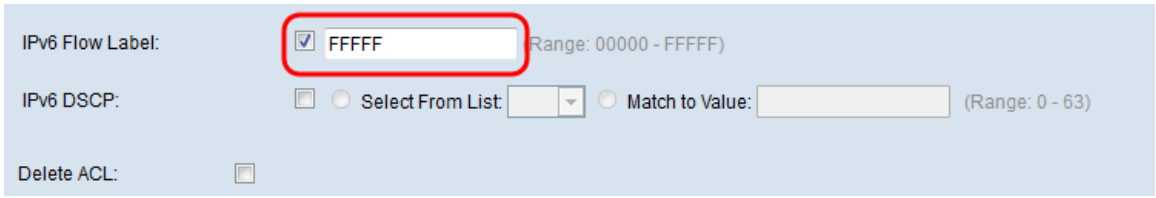
步骤4.（可选）如果要删除已配置的ACL，请选中Delete ACL**复选**框。

第 5 步： 点击 Save（保存），以保存设置。

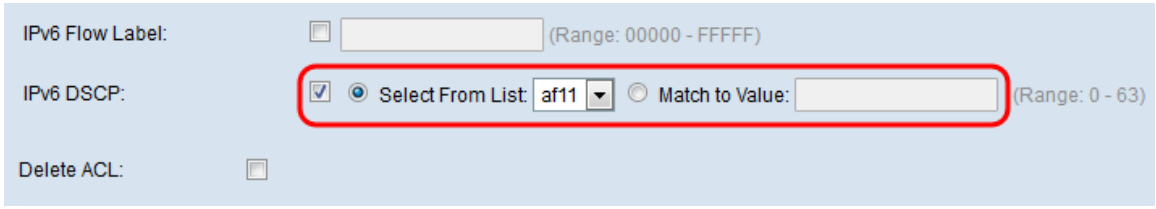


IPv6的ACL规则配置

步骤1.选中**IPv6流标签**复选框以设置IPv6数据包唯一的20位编号。终端站使用它表示路由器(范围0到1048575)中的QoS处理。



步骤2.选中**IPv6 DSCP复**选框以根据IP DSCP值匹配数据包。DSCP用于指定帧的IP报头上的流量优先级。这会将关联流量流的所有数据包与您从列表中选择的IP DSCP值进行分类。如果选**中IPv6 DSCP**复选框，请选择以下单选按钮之一。



选项描述如下：

·从列表中选择 — 从从列表中选择下拉列*表中选择*IP DSCP值。选项如下：

- DSCP保证转发(AS) — 允许运营商提供交付保证，只要流量不超过某些订用速率。

— 服务类别(CS) — 允许向后兼容仍使用Precedence字段的网络设备。

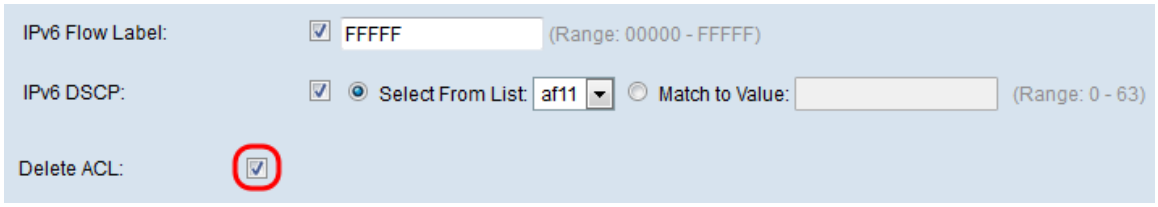
— 加速转发(EF) — 用于通过DS(DiffServ)域构建低损耗、低延迟、低抖动、有保证的带宽

和端到端服务。

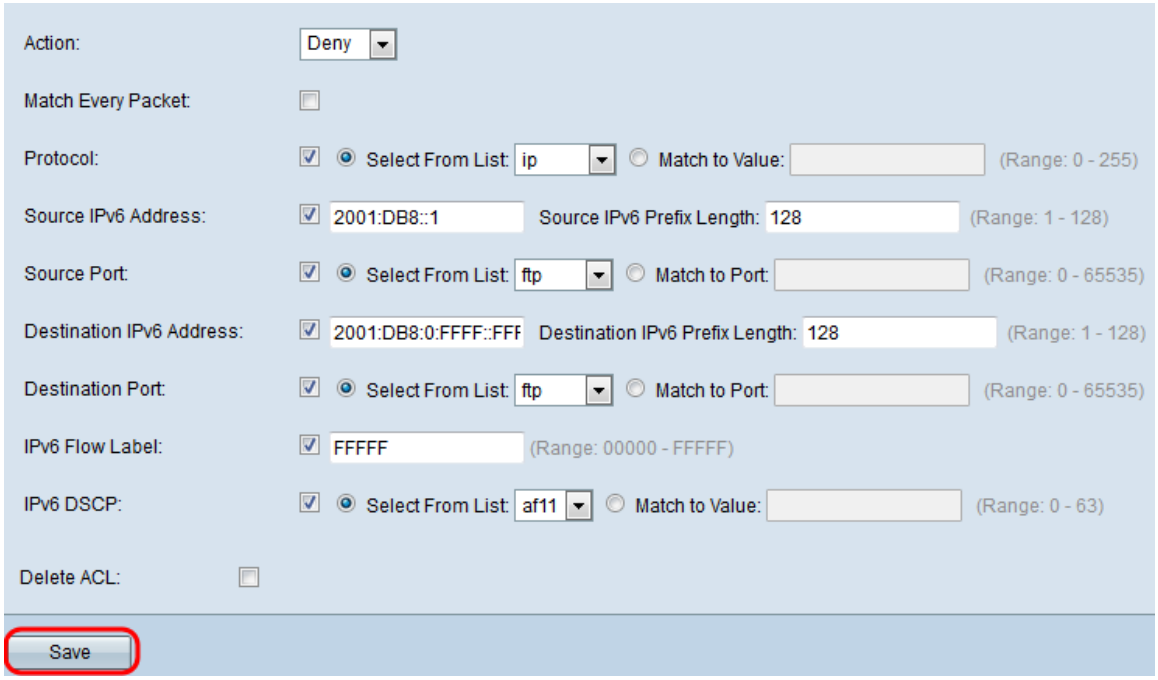
·Match to Value — 在Match to Value字段中输入范围为0到63的DSCP值，*以自*定义DSCP值。

注意：有关DSCP的更*多详细信息，请参*阅DSCP和优先级值。

步骤3.（可选）如果要删除已配置的ACL，请选中Delete ACL**复选**框。

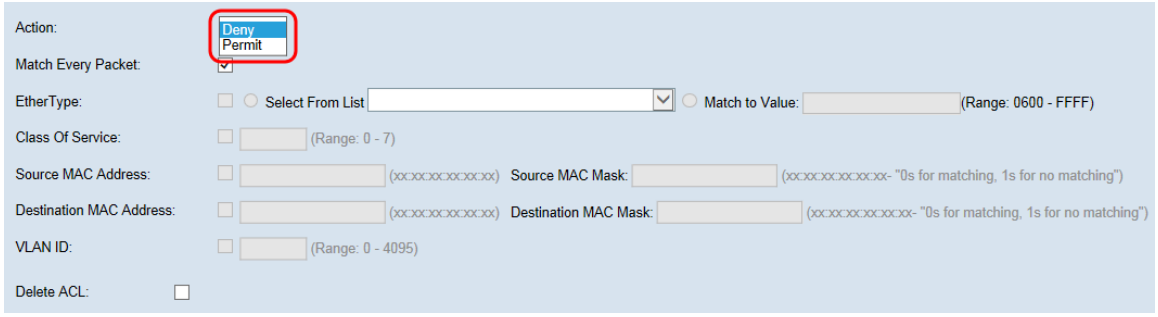


步骤4.单击“**保存**”以保存设置。



MAC的ACL规则配置

步骤1.从“操作”下拉列表中为*规则*选择操作。

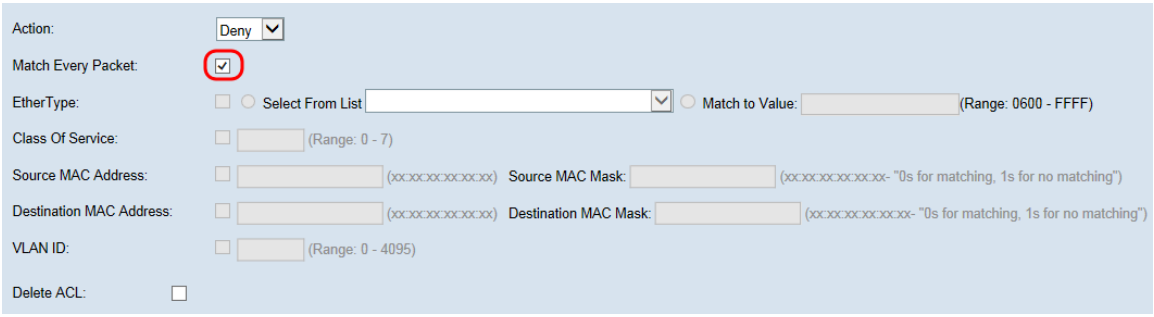


选项描述如下：

·允许 — 规则允许符合规则条件的所有流量进入或退出WAP设备。不符合条件的流量将被丢弃。

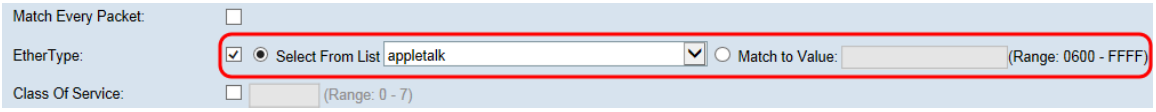
·拒绝 — 规则阻止符合规则条件的所有流量进入或退出WAP设备。不符合条件的流量将转发到下一条规则。如果这是最终规则，则不明确允许的流量将被丢弃。

步骤2.选中或取消选中Match Every Packet**复选框。**如果选中，规则（具有允许或拒绝操作）将匹配该帧或数据包，而不管其内容如何。



注意：如果选择此字段，则无法配置任何其他匹配条件。默认**情况下，为新规**则选择"匹配每个数据包"选项。您必须清除选项以配置其他匹配字段。

步骤3.选中**Ether Type**复选框，将匹配条件与以太网帧报头中的值进行比较。如果选**中Ether Type复**选框，请选择以下单选按钮之一。



选项描述如下：

·从列表中选择 — 从从列表中选择 *下拉列*表中选择协议。选项如下：

- AppleTalk - AppleTalk是Apple Inc.为其Macintosh计算机开发的一组专有网络协议。AppleTalk包含许多功能，允许在无需预先设置或需要任何类型的集中式路由器或服务器的情况下连接局域网。

- ARP — 地址解析协议(ARP)是一种电信协议，用于将网络层地址解析为链路层地址，这是多路访问网络中的一项关键功能。

- IPv4 - Internet协议第4版(IPv4)是Internet协议(IP)开发的第四版。 它是Internet中基于标准的网际互联方法的核心协议之一。

- IPv6 - Internet协议第6版(IPv6)是Internet协议(IP)的最新版本。IP是一种通信协议，可为网络上的计算机提供识别和定位系统，并通过Internet路由流量。

- IPX — 网际数据包交换(IPX)是IPX/SPX协议簇中的网络层协议。IPX源自Xerox网络系统的IDP。它也可以用作传输层协议。

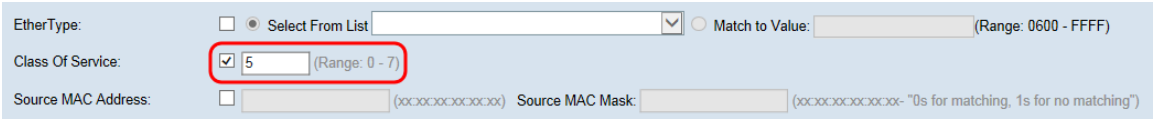
- NetBIOS - NetBIOS是网络基本输入/输出系统的首字母缩略词。它提供与OSI模型会话层相关的服务，允许独立计算机上的应用通过局域网进行通信。作为严格的API，NetBIOS不是网络协议。

- PPPOE — 以太网点对点协议(PPPoE)是用于将PPP帧封装在以太网帧中的网络协议。

·Match to Value — 输入数据包匹配的自定义协议标识符。该值是0600到FFFF范围内的四位十六进制数。

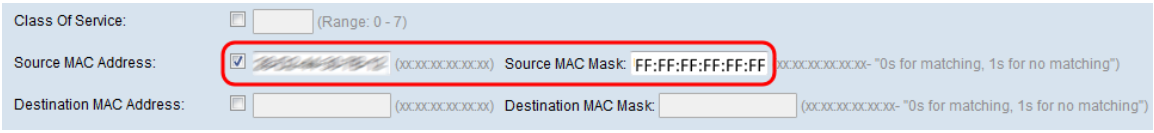
步骤4.选中**Class of Service复选**框，输入802.1p用户优先级，以与以太网帧进行比较。与IP优

先级一样，0是最低优先级，7是最高优先级。有效范围为0到7。

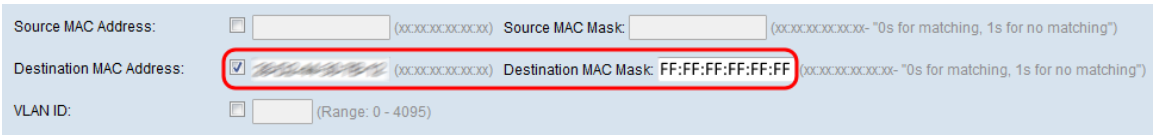


步骤5.选中Source MAC Address**复选框**，输入源MAC地址以与以太网帧进行比较。如果选中Source MAC Address复选框，请在Source MAC Address字段中输入*源MAC地*址。然后在源MAC掩码字段中输入*源MAC地址*掩码。这将指定源MAC地址中的哪些位将与以太网帧进行比较。

注意：如果只想匹配一个MAC地址，请使用通配符掩码00:00:00:00:00:00。

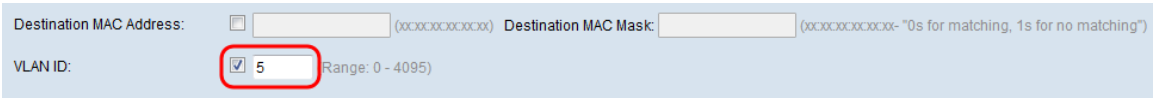


步骤6.选中Destination MAC Address**复选框**，输入要与以太网帧进行比较的目标MAC地址。如果选中Destination MAC Address复选框，请在Destination MAC Address字段中输入*目标MAC*地址。然后在Destination MAC Mask字段中输入*MAC地址*掩码。这将指定将与以太网帧比较目的MAC地址中的哪些位。

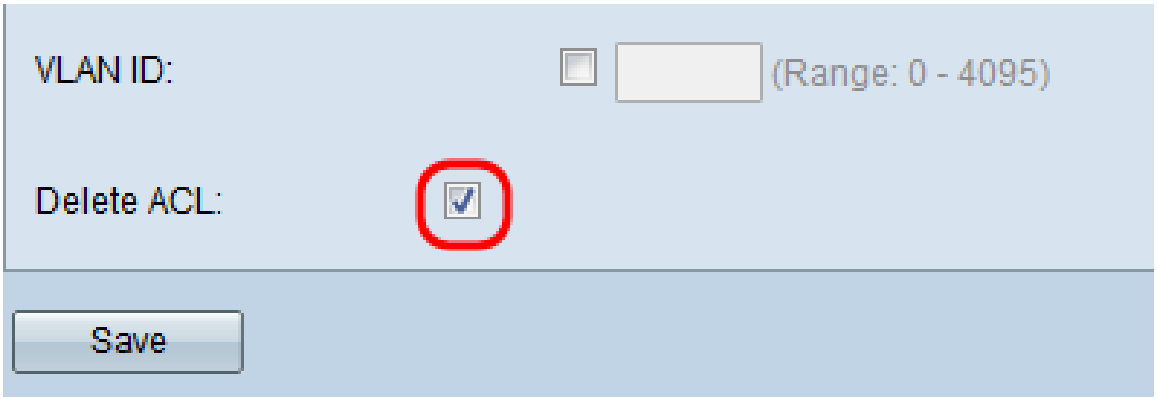


注意：如果只想匹配一个MAC地址，请使用通配符掩码00:00:00:00:00:00。

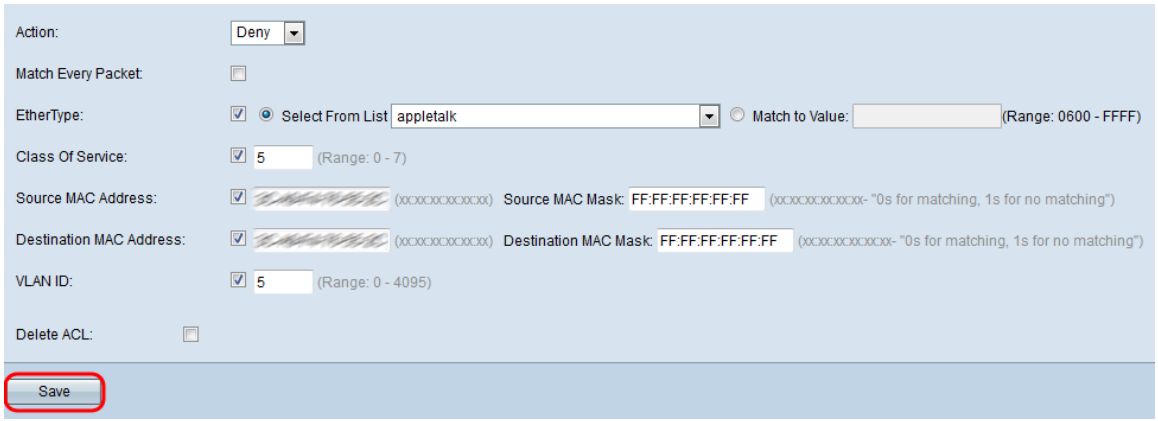
步骤7.选中**VLAN ID**复选框，输入VLAN ID以与以太网帧进行比较。如果选**中VLAN ID**复选框，请在VLAN ID字段中*输入VLAN* ID。VLAN ID范围为0-4095。



步骤8.（可选）如果要删除已配置的ACL，请选中Delete ACL**复选**框。



第 9 步： 点击 **Save（保存），以保存设置。**


Action:
Deny
Match Every Packet:
EtherType:
Select From List
appletalk
Match to Value:
(Range: 0600 - FFFF)
Class Of Service:
5
(Range: 0 - 7)
Source MAC Address:
(xx:xx:xx:xx:xx:xx)
Source MAC Mask:
FF:FF:FF:FF:FF:FF
(xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
Destination MAC Address:
(xx:xx:xx:xx:xx:xx)
Destination MAC Mask:
FF:FF:FF:FF:FF:FF
(xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
VLAN ID:
5
(Range: 0 - 4095)
Delete ACL:
Save