在WAP371的ACL规则配置

客观

网络访问控制表(ACL)是作为控制流量的一防火墙进出子网安全的一个可选的层。访问列表是许可证的集并且拒绝情况或者规则，为一定数量的原因提供安全。例如，这些规则能阻拦未授权的用户，允许授权用户访问特定资源和阻拦所有无保证的尝试到达网络资源。

本文目标将显示您如何配置在WAP 371的ACL规则。

可适用的设备

•WAP371

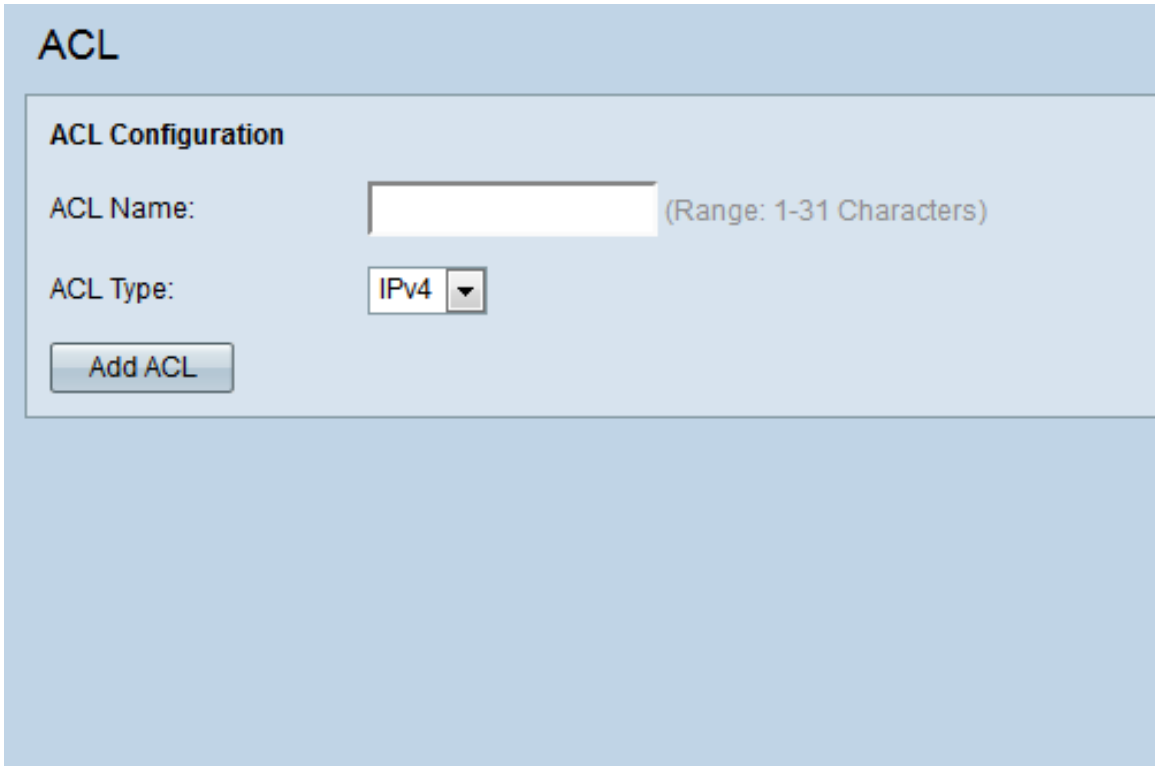
软件版本

•v1.2.0.2

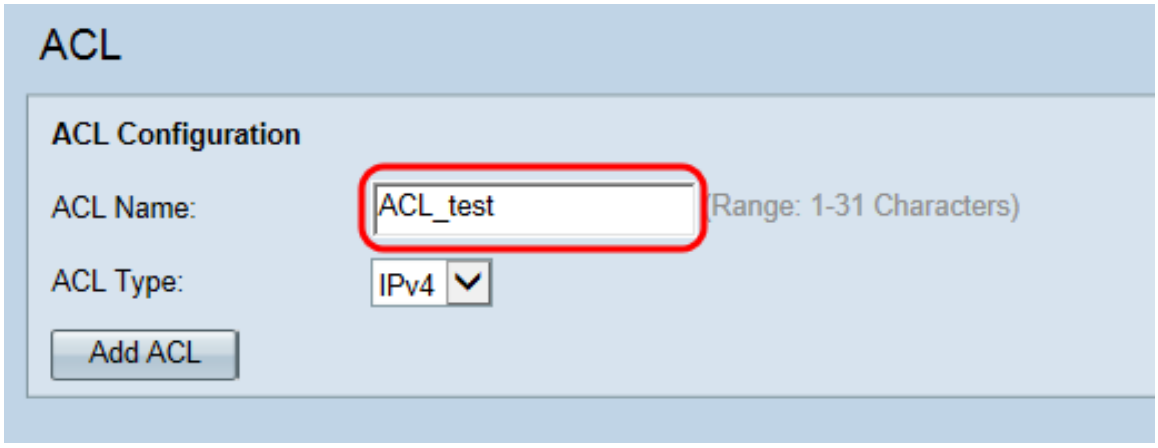
ACL规则配置

ACL配置

步骤1.登陆到Web配置工具并且选择**客户端QoS > ACL**。*ACL*页打开：

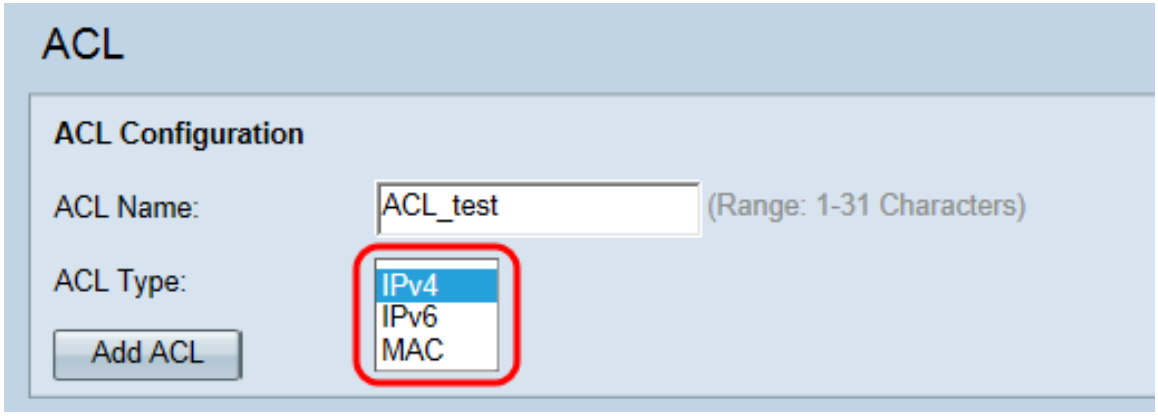


步骤2.送进期望ACL名称在*ACL名称*字段。范围是从1-31个字符。



Note:ACL名称是特定ACL的一个标识;它对设备的操作没有影响。

步骤3.选择ACL类型从*ACL类型*下拉列表。

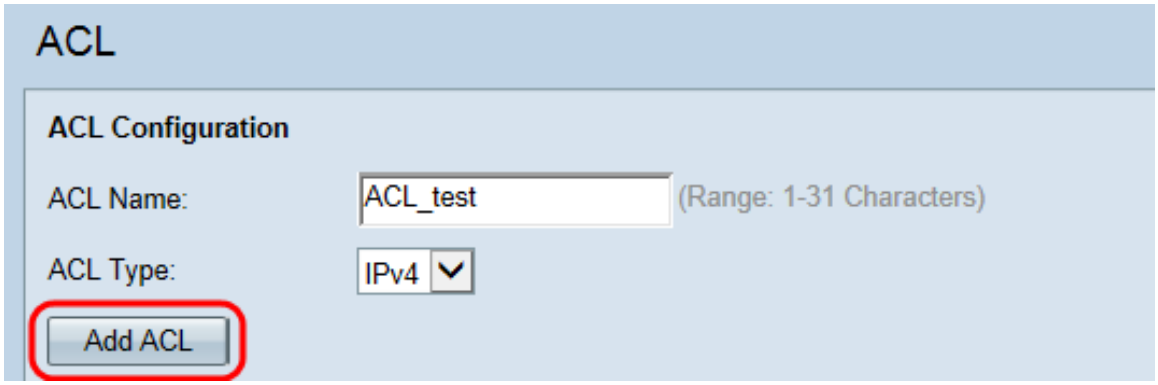


选项如下：

- IPv4 – 32位(四字节的)地址。
- IPv6 –一个后继到IPv4，包括128-bit (8字节)地址。
- MAC – MAC地址是唯一地址分配到网络接口。

Note:IPv4和IPv6 ACL控制对根据第3层和Layer4标准的网络资源的访问。MAC ACL控制根据第2层标准的访问。

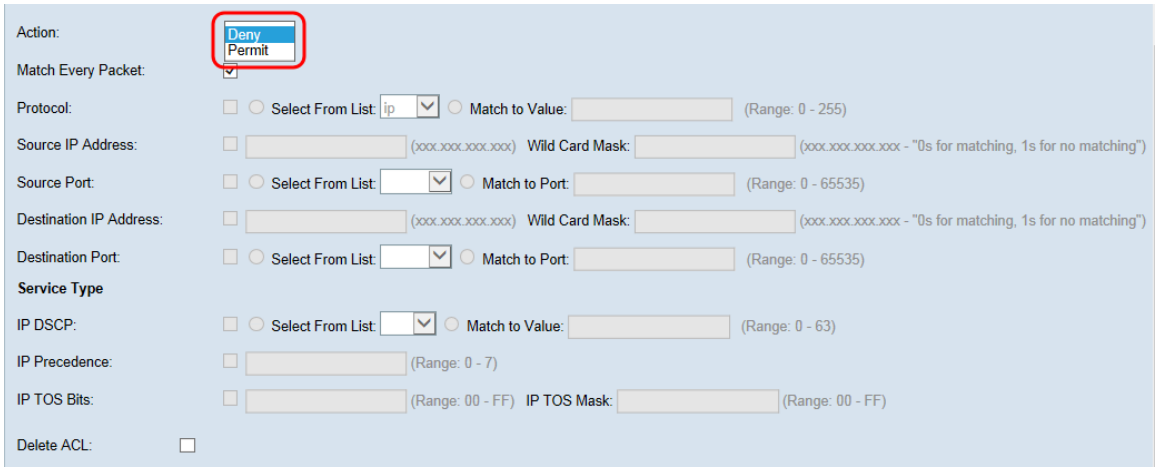
步骤4.点击**添加ACL**添加新的ACL。



IPv4和IPv6的ACL规则配置

Note:以下屏幕画面与IPv6 ACL规则是为IPv4ACL规则，但是可互换的。

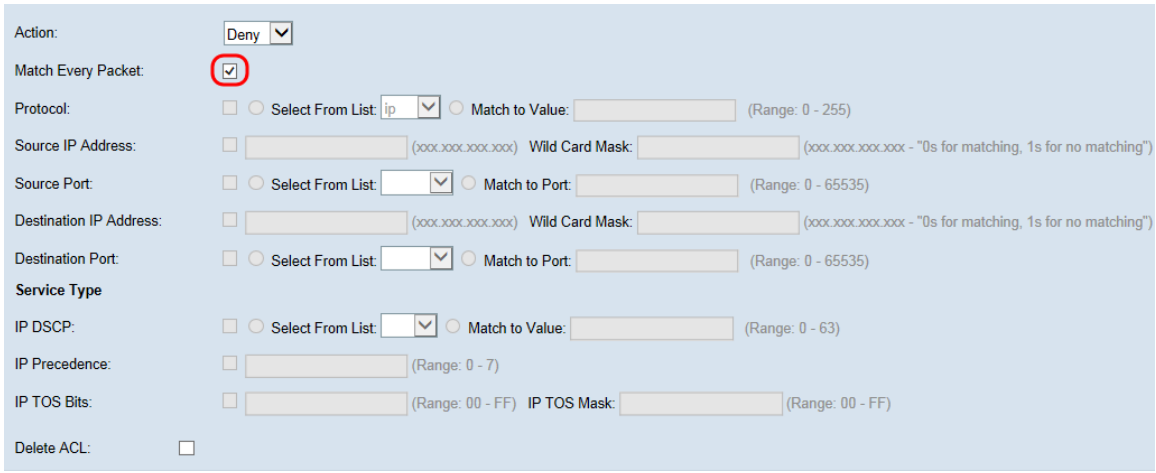
步骤1.为从*动作*下拉列表的规则选择一个动作。



选项被描述如下：

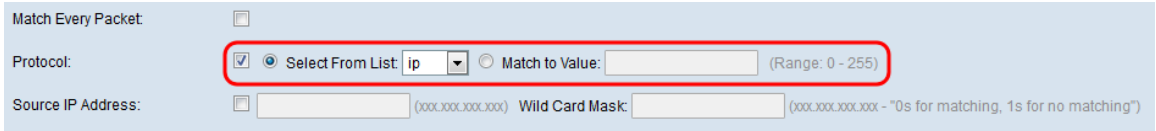
- •许可证–规则允许满足规则标准进入或退出WAP设备的所有数据流。不满足标准的数据流降低。
- •拒绝–规则阻塞满足从进入或退出WAP设备的规则标准的所有数据流。不满足标准的数据流转发到下个规则。如果它是最终规则，没有明确地允许的数据流降低。

Step 2.检查或不选定**匹配每个信息包**复选框。如果选择，规则，不管其内容，把一个许可证或拒绝动作，匹配帧或信息包。



Note:如果选择此字段，您不能配置任何另外的匹配标准。默认情况下**匹配每个信息包**选项为新规则选择。您必须清除选项配置其他匹配字段。

第3.步。检查**协议**复选框使用L3或L4协议根据IP Protocol字段的值的匹配情况在IPv4信息包或下报头字段在IPv6信息包。如果协议复选框被检查，请选择以下单选按钮之一。



选项被描述如下：

- •从列表挑选—从*挑选*选择协议*从列表*下拉列表。选项如下：

– IP –网络协议(IP)是原理通信协议在传递的数据互联网协议套件在间网络。

– ICMP –互联网控制消息协议(ICMP)是一个协议在设备使用类似路由器发错误信息的互联网协议套件。

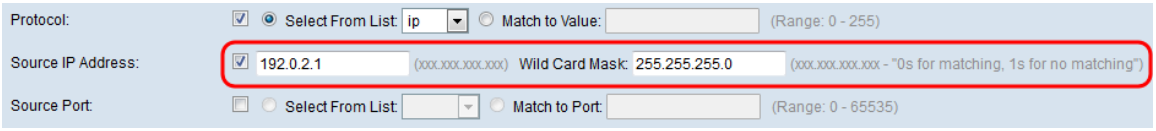
– IGMP –互联网组管理协议(IGMP)是主机用于的通信协议设立在IPv4网络的组播组成员。

– TCP –传输控制协议(TCP) enable (event)设立连接和交换数据流的两台主机。

– UDP –用户数据协议是一个协议在使用一个无连接发射型号的互联网协议套件。

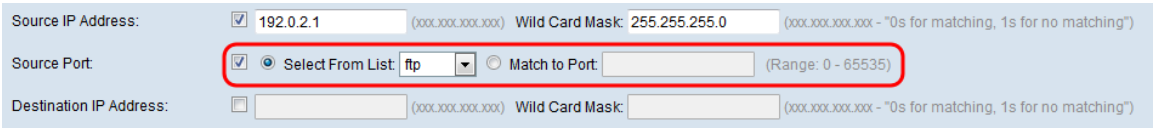
•重视的匹配—输入范围自0到255所有未入册的协议的标准IANA分配的协议ID。请参见*分配的互联网协议编号*关于IANA分配的协议ID的更多信息。

第4.步。检查**IP Address复选框的来源**包括来源的IP地址在匹配情况。输入来源的IP地址和通配符掩码在他们的各自字段。通配符掩码确定使用源地址的哪些位，并且哪些被忽略。可以设想作为一个被倒置的子网掩码。这为指示网络的一些路由协议的大小或子网是有用的或允许或拒绝IP地址的范围。



Note:需要通配符掩码字段**IP Address复选框的来源**是否被检查。

第5.步。检查**源端口**复选框包括源端口在匹配情况。如果**源端口**复选框被检查，请选择以下单选按钮之一。



选项被描述如下：

•从列表挑选—从*挑选*选择源端口*从列表*下拉列表。选项如下：

– FTP –文件传输协议(FTP)是用于的标准网络协议从一台主机调用文件到另一个过渡基于TCP的网络例如互联网。

– FTP数据–服务器起动的数据信道被连接了到客户端，典型地通过端口20。

– HTTP –超文本传输协议(HTTP)是基础数据通信万维网的应用协议。

– SMTP –简单邮件传输协议(SMTP)是电子邮件(电子邮件)发射互联网标准。

– SNMP –简单网络管理协议(SNMP)是管理设备的一个互联网标准协议在IP网络。

– Telnet –在互联网或区域网用于的会话层协议提供双向交互文本导向通信。

– TFTP –简单文件传输协议(TFTP)是更加简单使用比FTP调用的文件的互联网软件实用工具，但是较不能够的。

– WWW –万维网是的互联网服务器系统支持HTTP被格式化的文件。

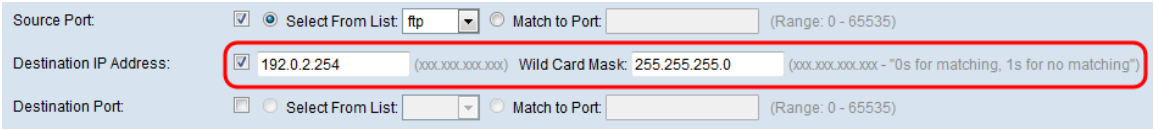
•对端口的匹配—输入范围自0到65535在*匹配到Port字段*未入册的源端口的端口号。范围包括三不同种类的端口。范围被描述如下：

– 0到1023 —众所周知的端口。

– 1024到49151 —注册的端口。

– 49152到65535 —动态并且/或者专用的端口。

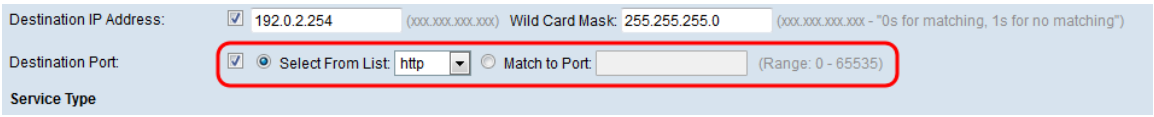
第6.步。检查**IP Address复选框的目的地**包括目的地的IP地址在匹配情况。输入目的地的IP地址和通配符掩码在他们的各自字段。通配符掩码确定使用源地址的哪些位，并且哪些被忽略。可以设想作为一个被倒置的子网掩码。这为指示网络的一些路由协议的大小或子网是有用的或允许或拒绝IP地址的范围。



Note:需要*通配符掩码*字段**IP Address复选框的目的地**是否被检查。

Note:如果希望匹配仅单个IP地址，请使用0.0.0.0通配符掩码。

第7.步。检查**Port复选框的目的地**包括目的地端口在匹配情况。如果**目的地Port复选框**被检查，请选择以下单选按钮之一。



选项被描述如下：

•从列表挑选—从*挑选*选择目的地端口*从列表*下拉列表。下拉列表选项如下：

– FTP –文件传输协议(FTP)是用于的标准网络协议从一台主机调用文件到另一个过渡基于TCP的网络例如互联网。

– FTP数据–服务器起动的数据信道被连接了到客户端，典型地通过端口20。

– HTTP –超文本传输协议(HTTP)是基础数据通信万维网的应用协议。

– SMTP –简单邮件传输协议(SMTP)是电子邮件(电子邮件)发射互联网标准。

– SNMP –简单网络管理协议(SNMP)是管理设备的一个互联网标准协议在IP网络。

– Telnet –在互联网或区域网用于的会话层协议提供双向交互文本导向通信。

– TFTP –简单文件传输协议(TFTP)是更加简单使用比FTP调用的文件的互联网软件实用工具，但是较不能够的。

– WWW –万维网是的互联网服务器系统支持HTTP被格式化的文件。

•对端口的匹配—输入范围自0到65535在*匹配到Port字段*未入册的目的地端口的端口号。范围包括三不同种类的端口。范围被描述如下：

– 0到1023 —众所周知的端口。

– 1024到49151 —注册的端口。

– 49152到65535 —动态并且/或者专用的端口。

Note:仅一服务从服务类型标准地区被挑选，并且可以为匹配情况被添加。

ACL规则IPv4的服务类型配置

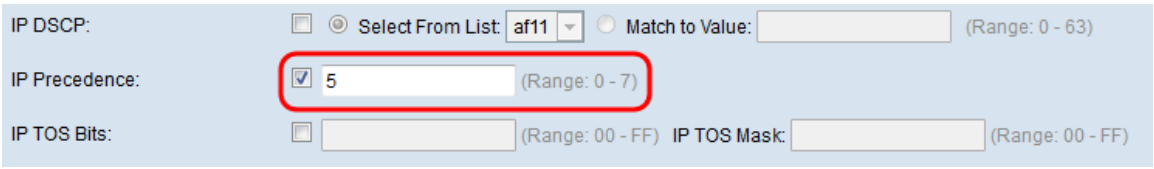
Step 1.检查**IP DSCP**复选框匹配根据IP DSCP值的信息包。DSCP用于指定在帧的IP头的数据流优先级。这分类相关的数据流的所有信息包与您从列表挑选的IP DSCP值。如果IP DSCP复选框被检查，请选择以下单选按钮之一。

选项被描述如下：

- 从列表挑选—从*挑选*选择IP DSCP值*从列表*下拉列表。选项如下：
  - DSCP保证的转发(AS) -允许运算符提供发运保证，只要数据流不超出一些被预订的费率。
  - 业务类别(CS) –允许向后兼容性用仍然使用优先级字段的网络设备。
  - 紧急转发(EF) -用于通过DS (DiffServ)域建立低损耗，低延时，低抖动，确定带宽，端到端服务。
- 重视的匹配—输入范围自0到63在*匹配到*值字段定制DSCP值的DSCP值。

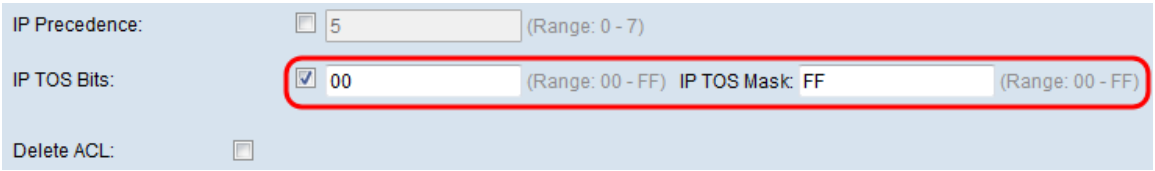
Note:参考*DSCP和优先值*关于更详细的资料在DSCP。

Step 2.检查**IP优先级**复选框包括IP优先级值在匹配情况。这是指定的优先级一个机制到0是最低优先级的每个IP信息包，并且7最高。如果**IP优先级**复选框被检查，请输入范围自0到7.的IP优先级值。



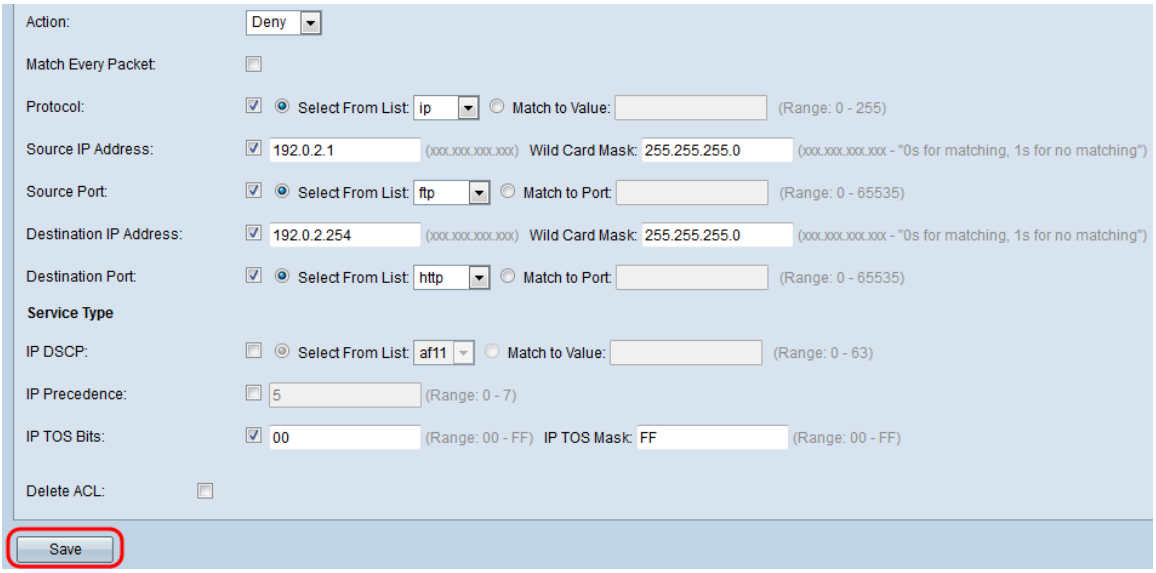
Note:参考*DSCP和优先值*关于更详细的资料在IP优先级。

第3.步。检查**IP TOS位**复选框使用信息包的服务类型(ToS)位在IP头作为匹配标准。ToS字段用于指定数据包的优先级和相应地路由它。如果范围自00-FF和IP TOS掩码范围自在他们的各自字段的00-FF的IP TOS位复选框被检查，请输入IP TOS位。



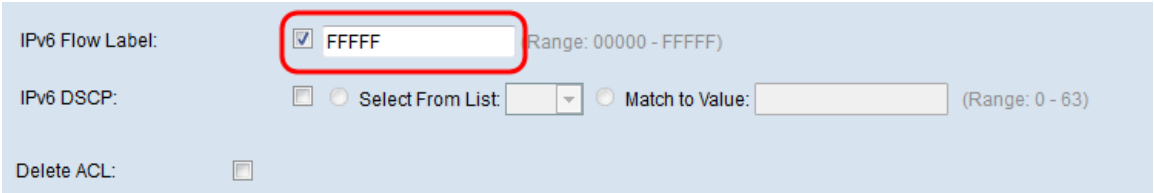
第4.步(可选)，如果要然后删除被配置的ACL，检查**删除ACL**复选框。

步骤5.点击**"Save"**保存设置。

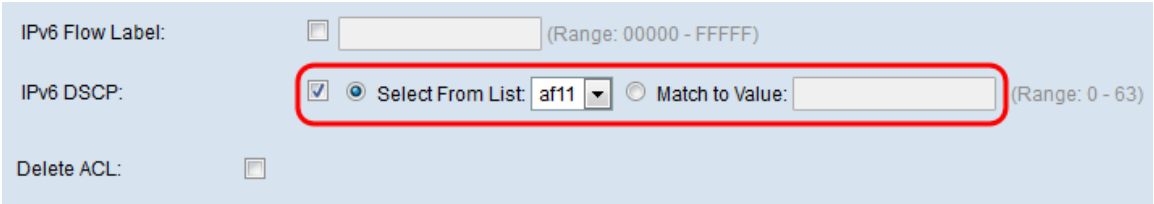


IPv6的ACL规则配置

Step 1.检查**IPv6流标签**复选框设置对IPv6数据包是唯一的20位编号。终端站用于它表示在路由器(范围0到1048575)的QoS处理。



Step 2.检查**IPv6 DSCP**复选框匹配根据IP DSCP值的信息包。DSCP用于指定在帧的IP头的数据流优先级。这分类相关的数据流的所有信息包与您从列表挑选的IP DSCP值。如果**IPv6 DSCP**复选框被检查，请选择以下单选按钮之一。



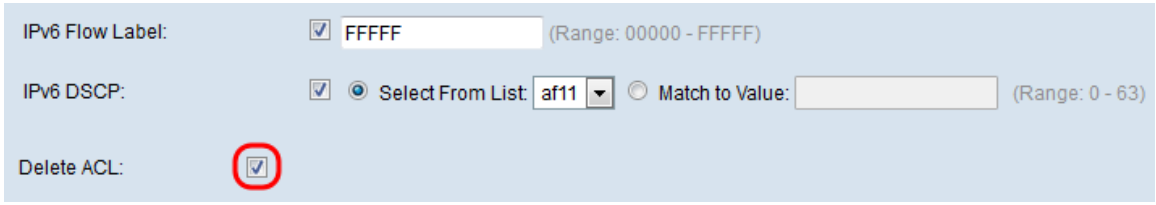
选项被描述如下：

- 从列表挑选—从*挑选*选择IP DSCP值*从列表*下拉列表。选项如下：
  - DSCP保证的转发(AS) -允许运算符提供发运保证，只要数据流不超出一些被预订的费率。
  - 业务类别(CS) –允许向后兼容性用仍然使用优先级字段的网络设备。
  - 紧急转发(EF) -使用通过DS (DiffServ)域建立低损耗，低延时，低抖动，确定带宽，端到端服务。

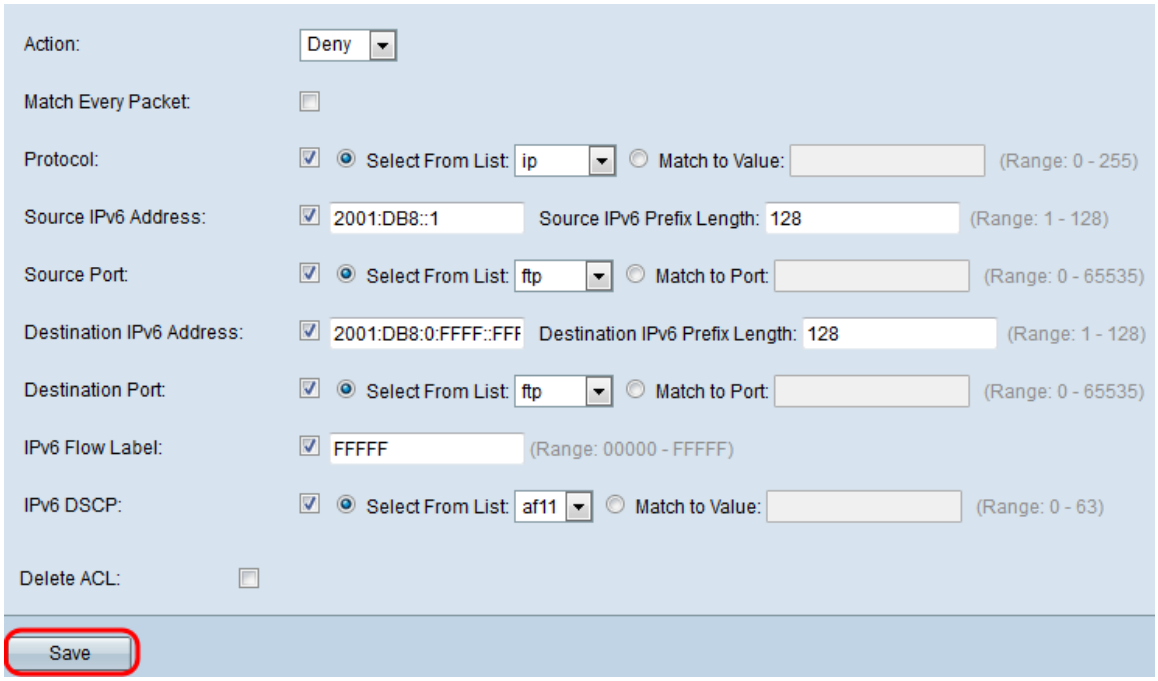
•重视的匹配—输入范围自0到63在*匹配到*值字段定制DSCP值的DSCP值。

Note:参考*DSCP和优先值*关于更详细的资料在DSCP。

第3.步(可选)，如果要然后删除被配置的ACL，检查**删除ACL**复选框。

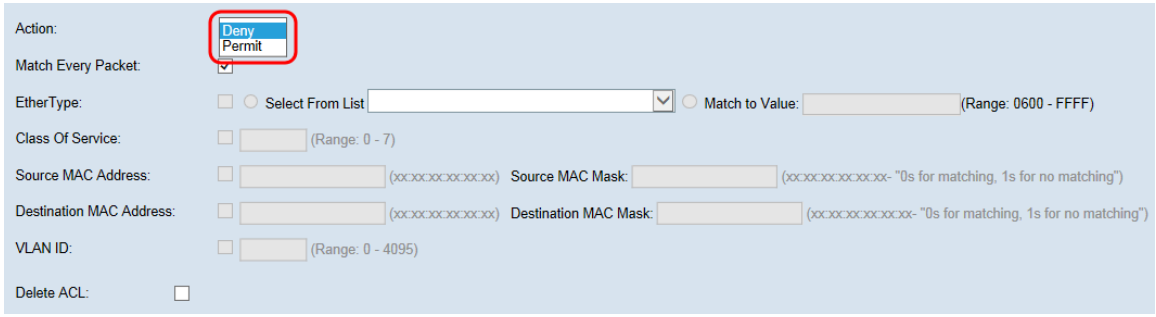


步骤4.点击**"Save"**保存设置。



MAC的ACL规则配置

步骤1.为从*动作*下拉列表的规则选择一个动作。

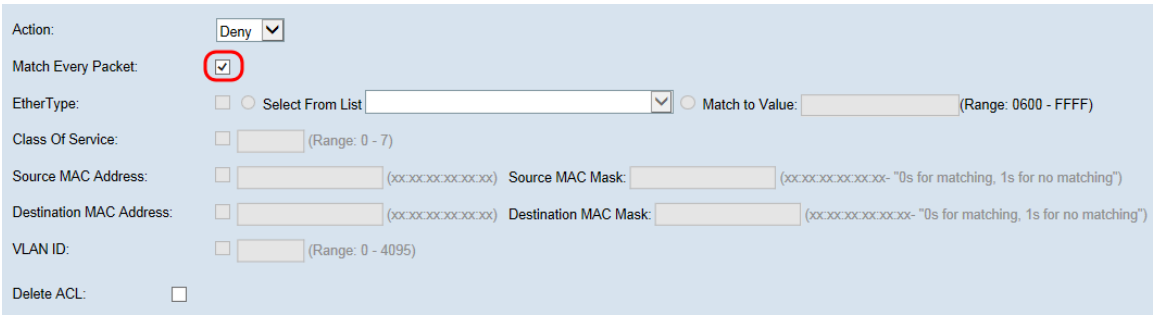


选项被描述如下：

•许可证–规则允许满足规则标准进入或退出WAP设备的所有数据流。不满足标准的数据流降低。

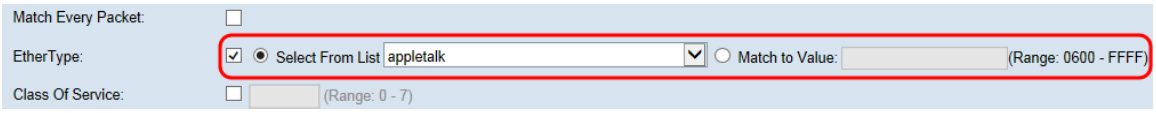
•拒绝–规则阻塞满足从进入或退出WAP设备的规则标准的所有数据流。不满足标准的数据流转发到下个规则。如果它是最终规则，没有明确地允许的数据流降低。

Step 2.检查或不选定**匹配每个信息包**复选框。如果选择，规则，不管其内容，把一个许可证或拒绝动作，匹配帧或信息包。



Note:如果选择此字段，您不能配置任何另外的匹配标准。默认情况下**匹配每个信息包**选项为新规则选择。您必须清除选项配置其他匹配字段。

第3.步。检查**以太类型**复选框对在以太网帧的报头的值比较匹配标准。如果**以太类型**复选框被检查，请选择以下单选按钮之一。



选项被描述如下：

•从列表挑选—从*挑选*选择协议*从列表*下拉列表。选项如下：

– AppleTalk - AppleTalk是网络协议一个所有权套件他们的Macintosh计算机的Apple Inc.开发的。AppleTalk包括了允许区域网连接没有前期设置或需要对于所有排序一个集中化路由器或服务器的一定数量的功能。

– ARP -地址解析服务(ARP)是用于网络层地址的解决方法的电信协议到链路层地址，一个重要功能在多个访问网络。

– IPv4 -互联网协议版本4 (IPv4)是在网络协议(IP)的发展的第四个版本。它是其中一个基于标准的互联网络方法核心协议在互联网里。

– IPv6 -互联网协议版本6 (IPv6)是网络协议(IP)的多数最新版本，为计算机提供一个证明和定位系统在网络并且路由在互联网间的数据流的通信协议。

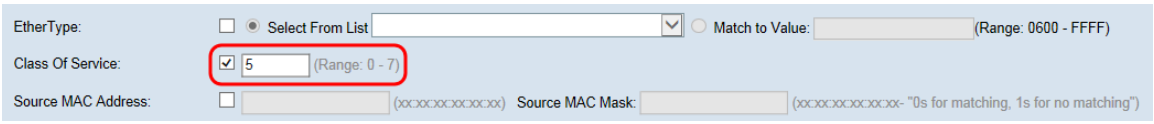
– IPX -网际分组交换(IPX)是网络层协议在IPX/SPX协议组。IPX从施乐网络系统的IDP派生。它可能作为传输层协议。

– NetBIOS - NetBIOS是网络基本输入/输出系统的一个缩写。它在独立的计算机提供服务与OSI模型的会话层有关允许应用程序在一个区域网沟通。作为严格API， NetBIOS不是网络协议。

– PPPOE -以太网点对点协议(PPPoE)是封装的PPP帧一个网络协议在以太网帧里面。

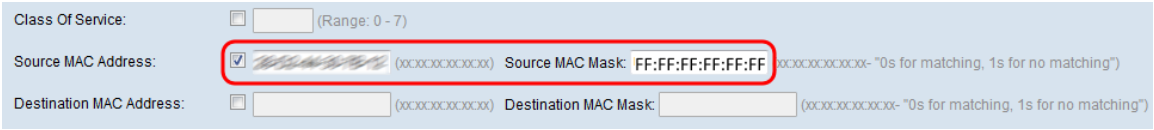
•重视的匹配—输入信息包被匹配的一个自定义协议标识符。值是一个四字节十六进制数字在0600范围内对FFFF。

第4.步。检查**业务类别**复选框输入802.1p用户优先级比较以太网帧。类似IP优先级， 0是最低优先级的，并且7最高。有效范围是从0到7。

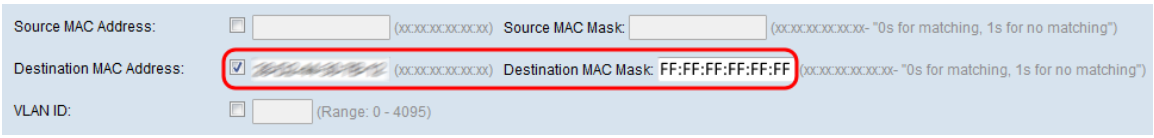


第5.步。检查**源MAC地址**复选框输入源MAC地址比较以太网帧。如果源MAC地址复选框被检查，请输入源MAC地址在*源MAC地址*地址字段。然后请输入源MAC地址网址遮罩在*源MAC掩码*字段。这将指定从源MAC地址的哪些位对以太网帧将比较。

Note:如果希望匹配仅单个MAC地址，请使用通配符掩码为00:00:00:00:00:00。

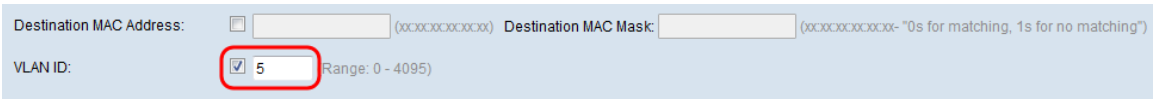


第6.步。检查**目的地MAC地址**复选框输入目的地MAC地址比较以太网帧。如果目的地MAC地址复选框被检查，请输入目的地MAC地址在*目的地MAC Address字段*。然后请输入MAC地址掩码在*目的地MAC掩码*字段。这将指定从目的地MAC地址的哪些位对以太网帧将比较。

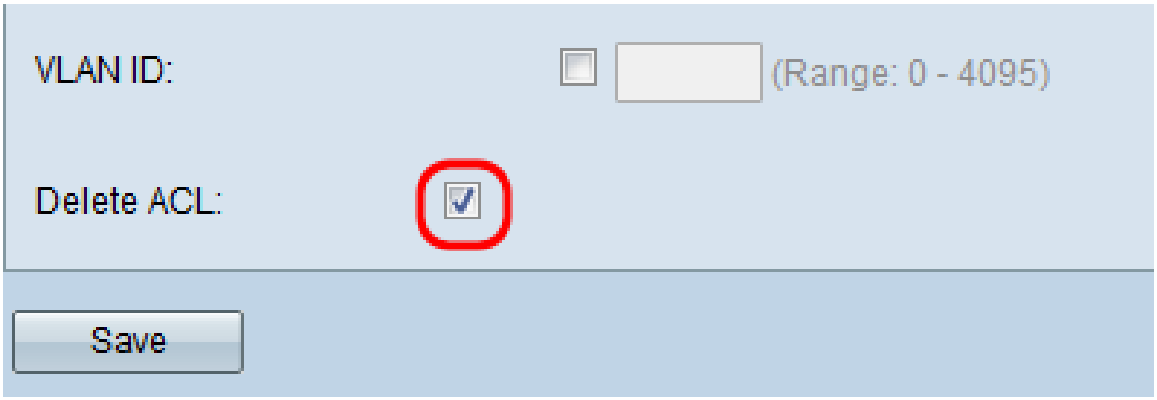


Note:如果希望匹配仅单个MAC地址，请使用通配符掩码为00:00:00:00:00:00。

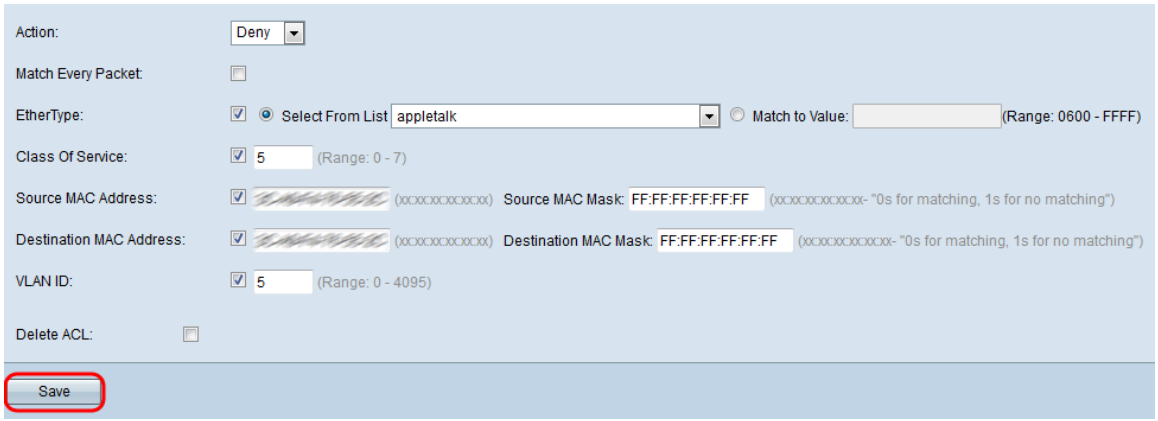
第7.步。检查**VLAN ID**复选框输入VLAN ID比较以太网帧。如果**VLAN ID**复选框被检查，请输入VLAN ID在*VLAN ID字段*。VLAN ID范围是从0-4095。



第8.步(可选)，如果要然后删除被配置的ACL，检查**删除ACL**复选框。



步骤9.点击**"Save"**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