在WAP121和WAP321接入点上创建和配置基于MAC的访问控制列表(ACL)

目标

访问控制列表(ACL)是允许和拒绝条件（称为规则）的集合，提供安全性并阻止未授权用户并允许授权用户访问特定资源。ACL可以阻止任何不必要的访问网络资源的尝试。MAC ACL是第2层ACL。网络设备检查帧并根据帧的内容（例如源MAC地址和目的MAC地址）检查ACL规则。如果任何规则与内容匹配，则对帧执行允许或拒绝操作。

本文介绍如何在WAP121和WAP321接入点(WAP)上创建和配置MAC ACL。

适用设备

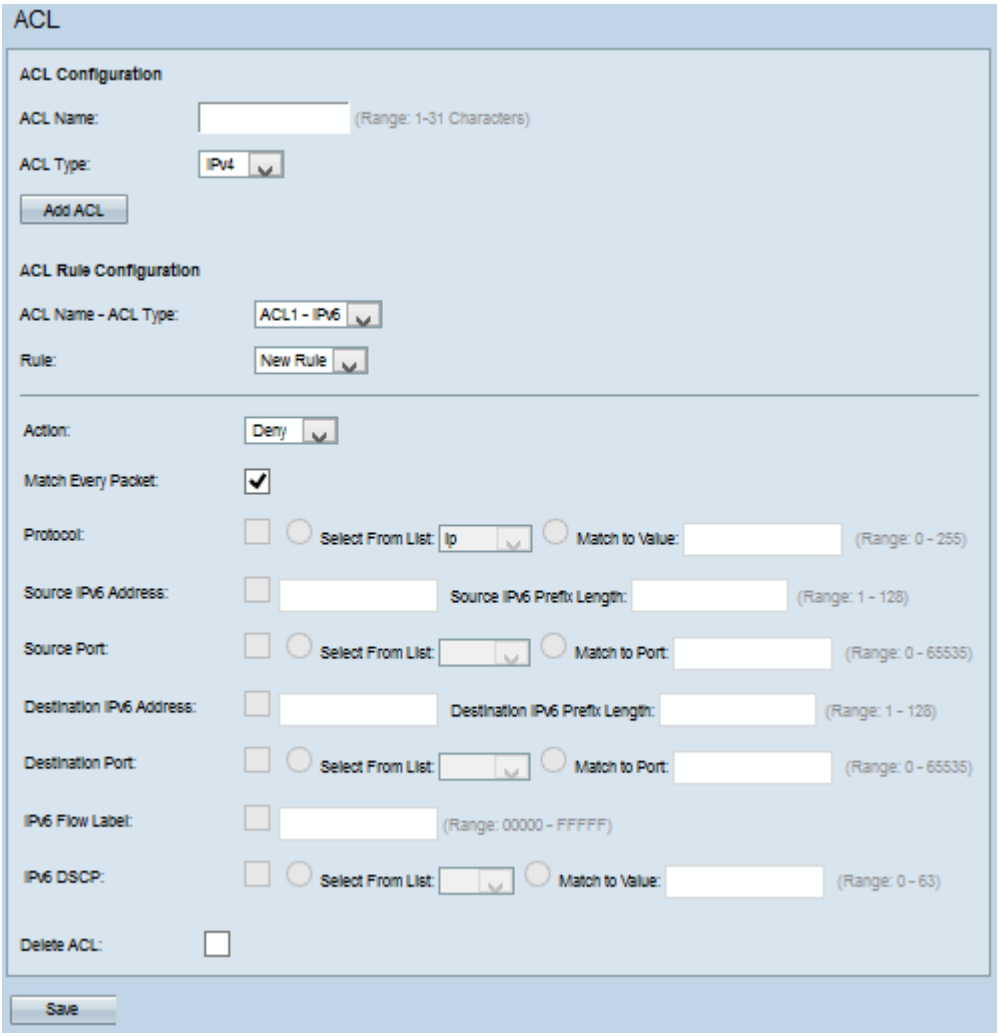
·WAP121
· WAP321

软件版本

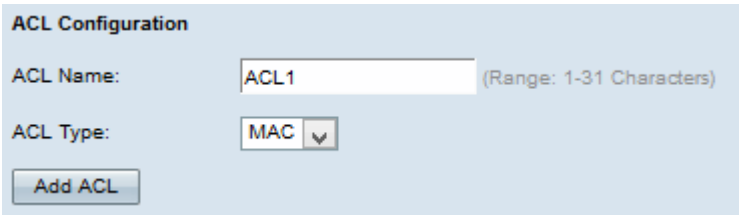
•v1.0.3.4

创建基于MAC的ACL

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



创建基于MAC的ACL

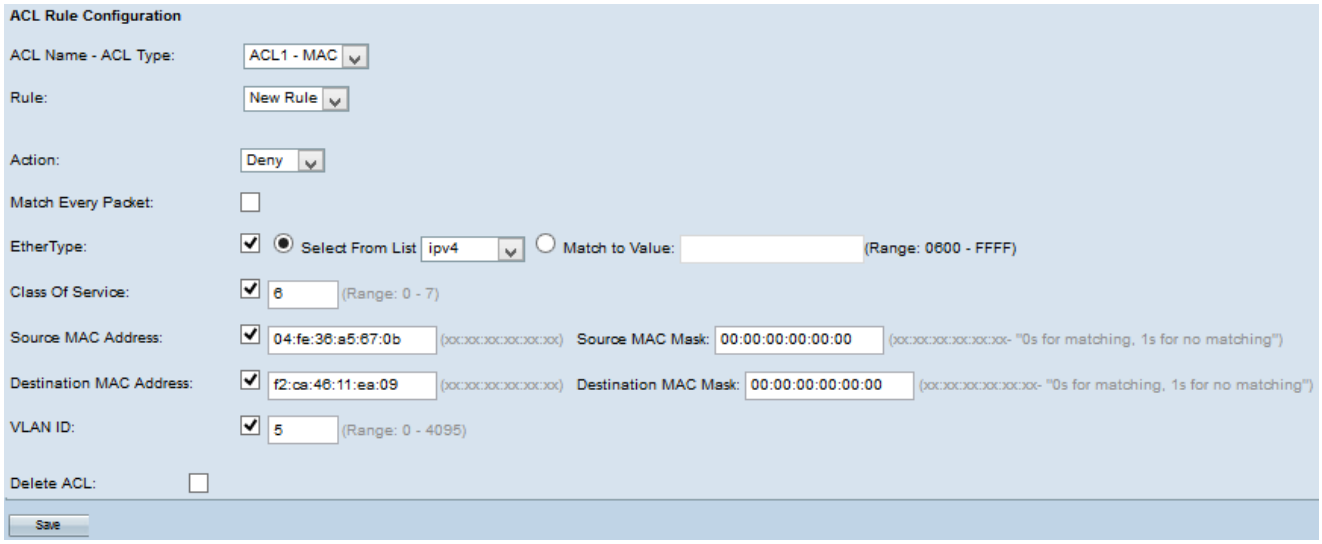


步骤1.在ACL Name字段中输入ACL*的名*称。

步骤2.从**ACL Type**下拉列表中为*ACL*类型选择MAC。

步骤3.单击**Add ACL**创建新的MAC ACL。

基于MAC的ACL的规则配置



步骤1.从ACL Name - ACL Type下*拉列表中选择*所需的ACL。

步骤2.如果必须为所选ACL配置新规则，请从“规则”下**拉列**表中选*择*“新建规则”；否则，从“规则”(Rule)下拉列*表中*选择一个当前规则。

注意：一个ACL最多可创建10个规则。

步骤3.从Action下拉列表中选择ACL规则*的*操作。

·拒绝 — 阻止符合规则条件的所有流量进入或退出WAP设备。

·允许 — 允许符合规则条件的所有流量进入或退出WAP设备。

注意：步骤4至11为可选步骤。已启用选中的过滤器。如果不希望过滤器应用于此特定规则，请取消选中该过滤器的复选框。

步骤4.选中**匹配每个数据包**复选框以匹配每个帧或数据包的规则，而不考虑其内容。取消选中**匹配每个数据**包复选框以配置任何附加匹配条件。

节省时间：如果选**中“匹配每**个数据包”，则跳至步骤12。

步骤5.选中**EtherType**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EtherType**复选框，请单击其中一个单选按钮。

·从列表中选择 — 从下拉列表中选择协议。下拉列表包含appletalk、arp、ipv4、ipv6、ipx、netbios、pppoe。

·与值匹配 — 用于自定义协议标识符。输入范围从0600到FFFF的标识符。

步骤6.选中**Class of Service**复选框以输入802.1p用户优先级，以与以太网帧进行比较。在Class of Service（服务类别）字段中，输入介*于0到7之间的*优先级。

步骤7.选中**源MAC地址**复选框，将源MAC地址与以太网帧进行比较，并在源MAC地址字*段中输入源*MAC地址。

步骤8.在源MAC掩码字段中输入源MAC地址掩码，该字*段指定源MAC中*要与以太网帧进行比较的位。如果MAC掩码使用0位，则接受该地址，如果它使用1位，则忽略该地址。

步骤9.选中**Destination MAC Address（目标MAC地址）**复选框，将目标MAC地址与以太网帧进行比较，并在Destination MAC Address（目标MAC地址）字*段中输入目*标MAC地址。

步骤10.在Destination MAC Mask字段中输入目的MAC地址掩码，该字段指定目的MAC中要与以太网帧进行比较的位。如果MAC掩码使用0位，则接受该地址，如果它使用1位，则忽略该地址。

步骤11.选中**VLAN ID**复选框，将VLAN ID与以太网帧进行比较。在VLAN ID字段中输入范围为0到4095*的VLAN* ID。

注意：有关如何创建新VLAN的信息，请参阅*WAP121和WAP321上管理和无标记VLAN ID的配置文章。*

步骤12.单击**Save**保存设置。

步骤13.（可选）要删除已配置的ACL，请选中**Delete ACL**复选框，然后单击**Save**。