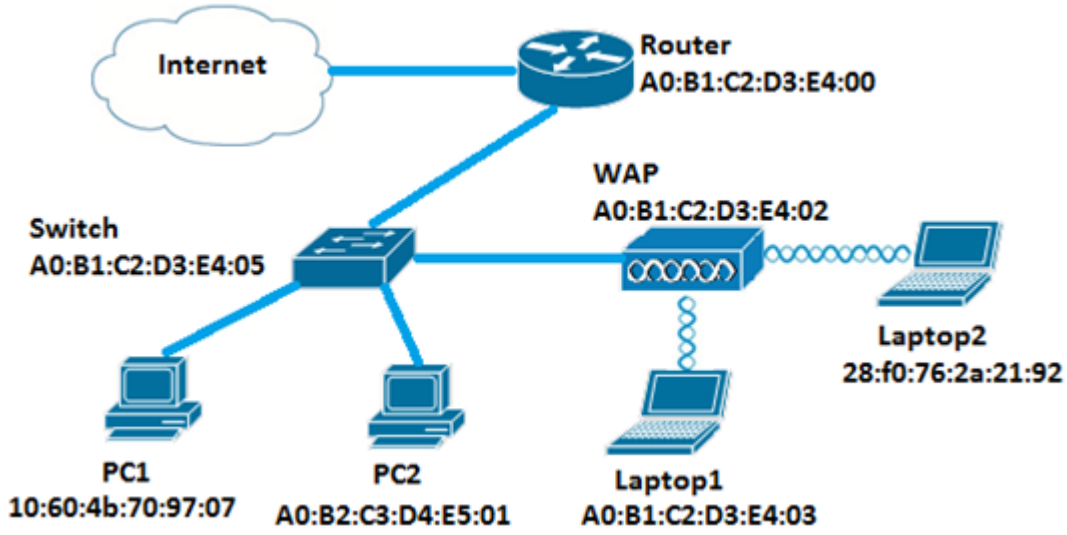
在WAP125和WAP581上配置MAC ACL

简介

介质访问控制(MAC)访问控制列表(ACL)是第2层ACL。每个ACL都是一组应用于无线接入点(WAP)接收的流量的规则。 该规则指定是否应使用给定字段的内容来允许或拒绝对网络的访问。ACL可以配置为检查帧的字段，如源或目标MAC地址、虚拟局域网(VLAN)标识符(ID)或服务类别(CoS)。 当帧进入WAP设备端口时，它会检查帧并根据帧的内容检查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。配置MAC ACL通常用于授权访问网络资源以选择网络中的设备。

注意：在创建的每条规则的末尾都有一个隐式拒绝。



在此场景中，除PC1外，网络中的所有设备都将被允许访问WAP后面的Laptop2。

目标

本文旨在向您展示如何在WAP125或WAP581接入点上配置基于MAC的ACL，以防止PC1访问WAP后面的Laptop2。

适用设备

- WAP125
- WAP581

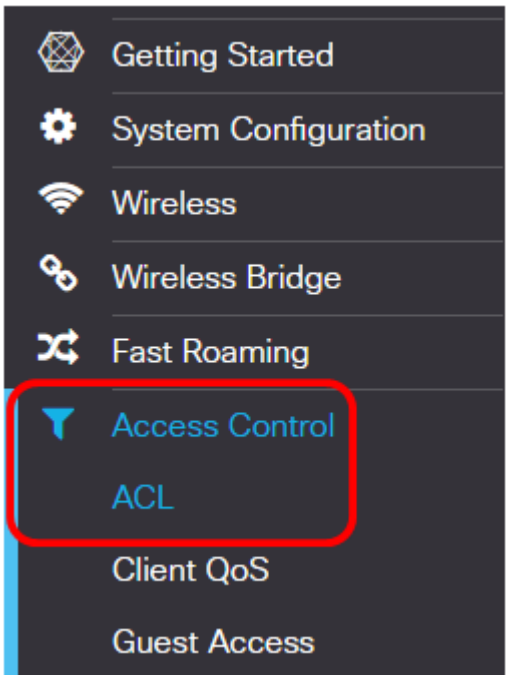
软件版本

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

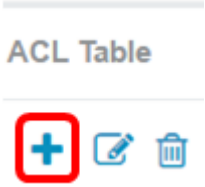
配置客户端过滤器列表

注意：菜单选项可能因您使用的WAP的确切型号而异。以下图像从WAP125拍摄。

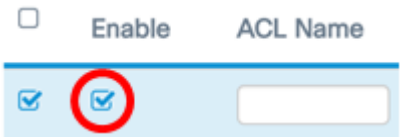
步骤1.登录WAP的基于Web的实用程序，然后选择**Access Control > ACL**。



步骤2.单击按 ✚ 钮。



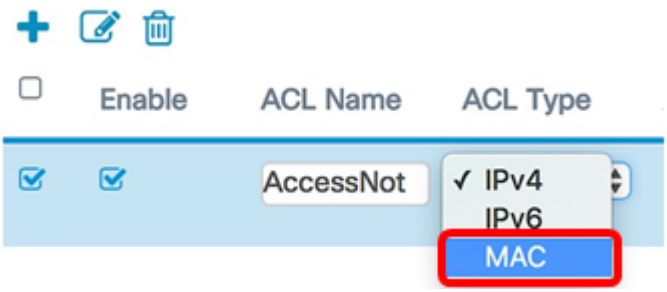
步骤3.检验Enable复选**框**是否选中，以确保ACL处于活动状态。默认情况下，选中此选项。



步骤4.在ACL Name字段中输入ACL*的名称*以标识ACL。

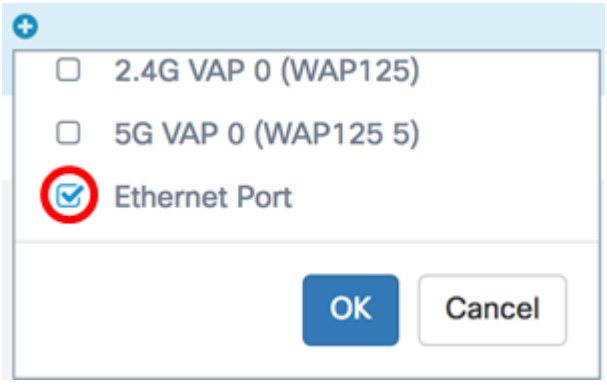
注意：在本例中，输入AccessNot。

步骤5.从ACL Type下拉列表中选择MAC。



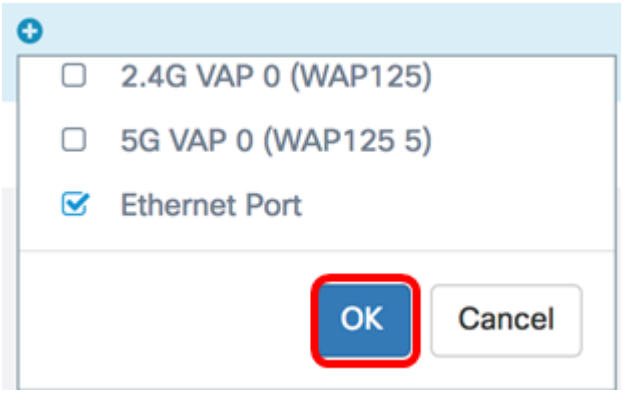
步骤6.单击按  钮，然后从Associated Interface下拉列表中选择接口。选项有：

- 2.4G VAP 0（SSID名称）— 此选项将MAC ACL应用于2.4 GHz虚拟接入点(VAP)。SSID Name部分可能会根据WAP上配置的SSID名称而更改。
- 5G VAP0（SSID名称）— 此选项将MAC ACL应用到5 GHz VAP。
- 以太网端口 — 此选项将MAC ACL应用到WAP的以太网接口。



注意：多个接口可以与ACL关联。选中相应接口的复选框，将接口与ACL关联。取消选中此框可取消接口与ACL的关联。在本例中，以太网端口与ACL关联。

步骤7.单击**OK**。

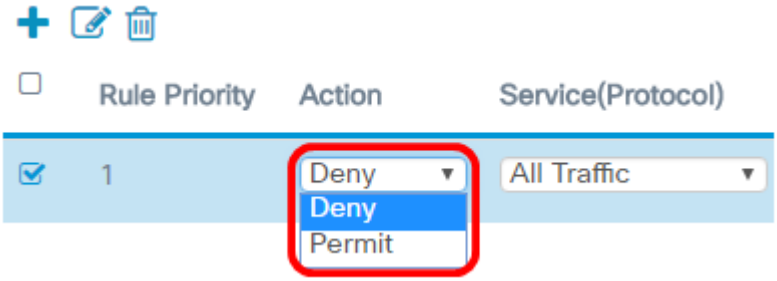


步骤8.单击**More...**按钮配置ACL的参数。

步骤9.单击  按钮添加新规则。

步骤10.从Action下拉列表中选择操作。选项有：

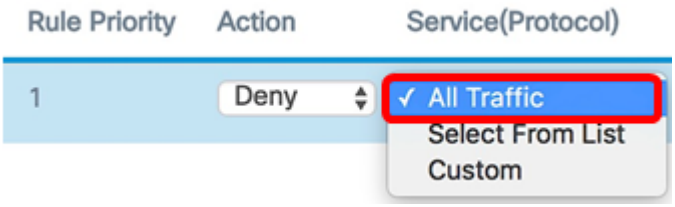
- 允许 — 此选项允许与ACL条件匹配的数据包连接到网络。
- 拒绝 — 此选项将阻止符合ACL条件的数据包连接到网络。



注意：在本例中，选择“拒绝”。

步骤11.从Service(Protocol)下拉列表中选择要过滤的服务或协议。选项有：

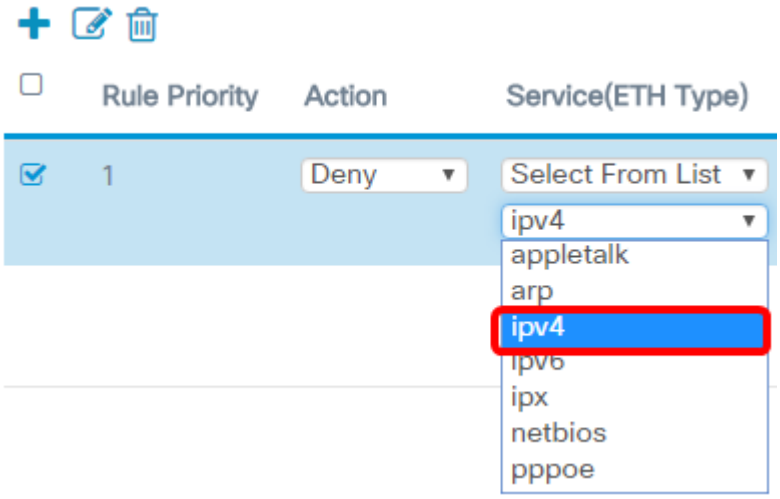
- 所有流量 — 此选项将所有数据包视为与ACL过滤器的匹配项。
- Select From List — 此选项允许您选择appletalk、arp、ipv4、ipv6、ipx、netbios和pppoe作为ACL的过滤器。如果选择此选项，请跳至步骤12。
- 自定义 — 此选项允许您输入自定义协议标识符作为数据包的过滤器。该值是一个四位十六进制数。范围为0600至FFFF。



注意：在本例中，选**择“所**有流量”。

第12步。（可选）如果选择“从列表中选择”，请选择以下任一选项：

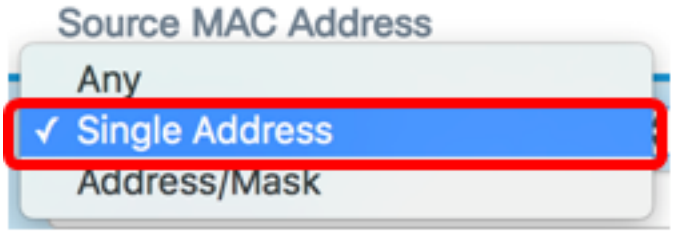
- appletalk — 此选项根据ACL的语句过滤appletalk数据包。Appletalk是Apple为其Mac计算机开发的一组网络协议。其中一项功能允许连接局域网(LAN)，而无需中央路由器或服务器。
- arp — 此选项根据ACL的语句过滤地址解析协议(ARP)数据包。ARP维护一个表，其中MAC地址映射到IP地址。
- ipv4 — 此选项根据ACL的语句过滤ipv4数据包。
- ipv6 — 此选项根据ACL的语句过滤ipv6数据包。IPv6是网络编址中IPv6的后继。
- ipx — 此选项根据ACL的语句过滤网际数据包交换(IPX)数据包。与appletalk一样，IPX也是专有网络协议。它连接使用Novell客户端和服务器的网络。
- netbios — 此选项根据ACL的语句过滤网络基本输入和输出系统(NetBIOS)数据包。NetBIOS允许独立计算机上的应用程序通过提供服务进行通信。
- pppoe — 此选项根据ACL的语句过滤以太网点对点协议(PPPoE)数据包。它主要用于数字用户线路(DSL)服务。



注意：在本例中，选择ipv4。

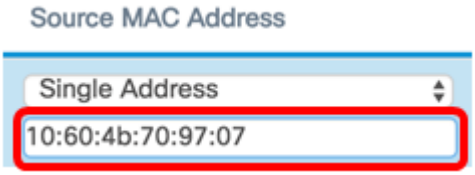
步骤13.从Source MAC Address下拉列表定义源MAC地址。选项有：

- Any — 此选项将允许WAP将过滤器应用于来自任何MAC地址的数据包。
- Single Address — 此选项将允许WAP将过滤器应用于来自指定MAC地址的数据包。
- 地址/掩码 — 此选项将允许WAP将过滤器应用于数据包的MAC地址和WAP的掩码。



注意：在本例中，选择了Single Address。

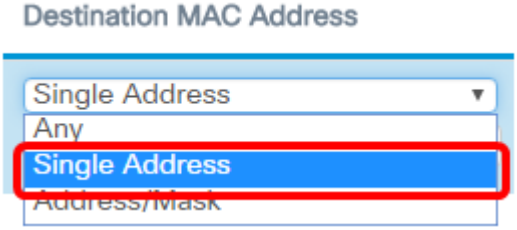
步骤14.在Source MAC Address字段中输入*源MAC*地址。



注意：在本例中，输入10:60:4b:70:97:07。这是PC1的MAC地址。

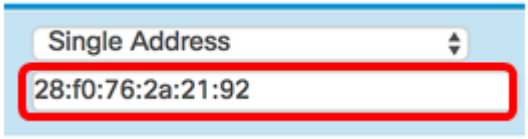
步骤15.从Destination MAC Address下拉列表定义目的MAC地址。选项有：

- Any — 此选项将允许WAP将过滤器应用于来自任何MAC地址的数据包。
- Single Address — 此选项将允许WAP将过滤器应用于来自指定MAC地址的数据包。
- 地址/掩码 — 此选项将允许WAP将过滤器应用于数据包的MAC地址和WAP的掩码。



注意：在本例中，选择了Single Address。

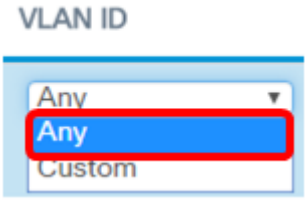
步骤16.在Destination MAC Address字段中输入**目的MAC**地址。



注意：在本例中，输入28:f0:76:2a:21:92。这是Laptop2的MAC地址。

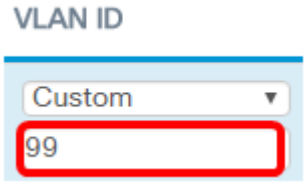
步骤17.从下拉列表中选择VLAN ID。

- Any — 此选项允许通过网络的任何VLAN ID。
- 自定义 — 此选项将允许您输入特定VLAN ID。如果选择此选项，请跳至步骤18。



注意：在本例中，选择Any。

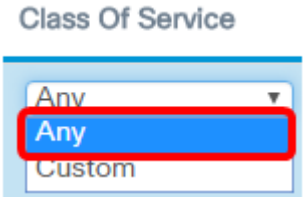
第18步。（可选）如果选择自定义，请在VLAN ID字段中*输入VLAN* ID。



注意：在本例中，输入99。

步骤19.（可选）从下拉列表中选择服务类别。选项有：

- Any — 此选项允许具有任何优先级的数据包连接到网络。
- 自定义 — 此选项将允许您过滤特定优先级的数据包。



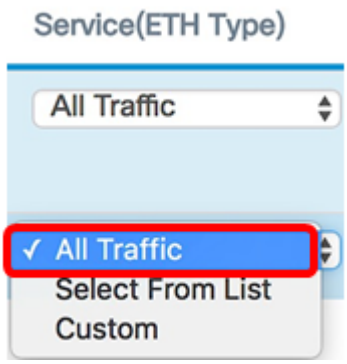
注意：在本例中，选择Any。如果选择自定义，请在服务类别字*段中输入优*先级。

步骤20.再次单 ✚ 击按钮以添加允许规则。

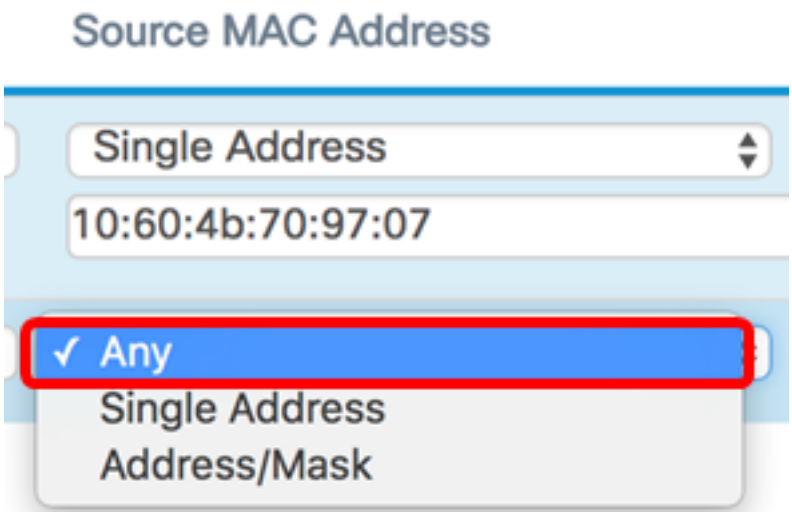
注意：由于在创建的每条规则末尾都存在隐式拒绝，因此强烈建议向ACL添加允许规则以允许来自网络中其他设备的流量。

步骤21.点击Action下拉箭头并选择**Permit**。

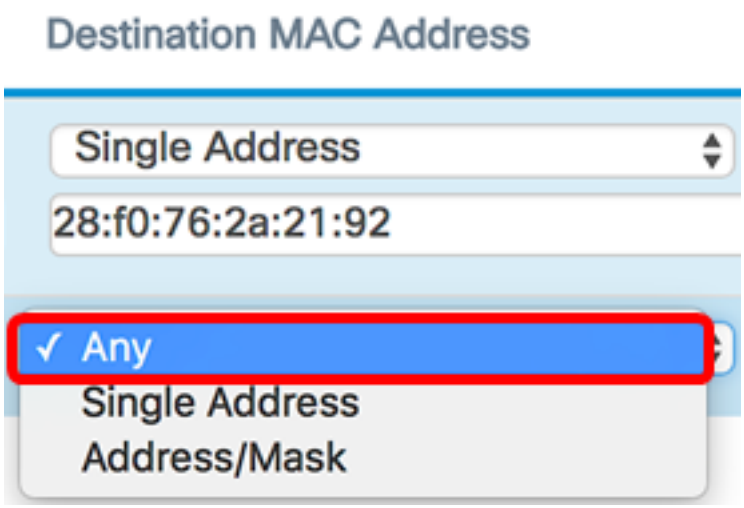
步骤22.点击Service(ETH Type)下拉箭头并选择All Traffic(所**有流量)**。



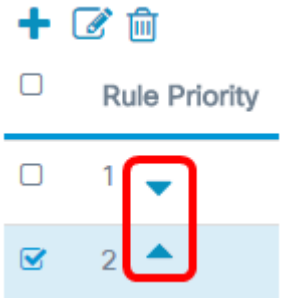
步骤23.单击“源MAC地址”下拉菜单，然后选择“任**何”**。这将允许来自网络中除第一条规则中指示的PC1 MAC地址外的任何其他MAC地址的流量。



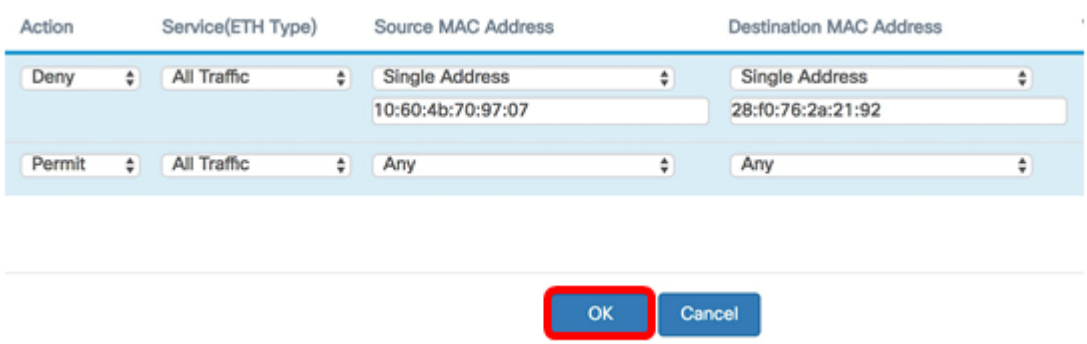
步骤24.单击Destination MAC Address下拉菜单并选择**Any**。这将允许流向网络中任何MAC地址的流量。



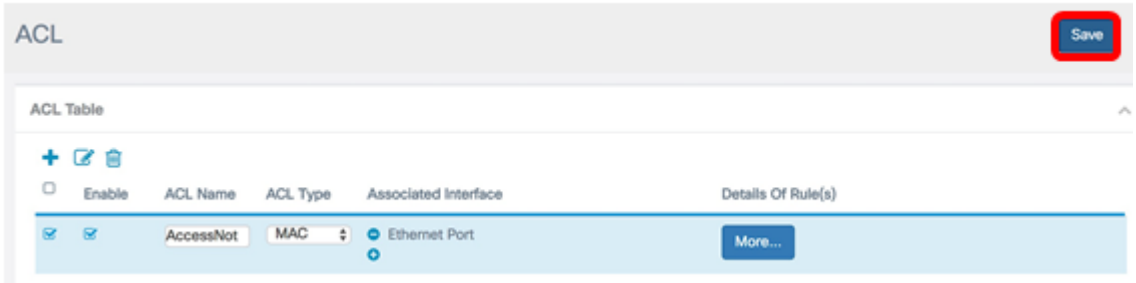
第25步。（可选）通过点击向上和向下箭头更改规则的优先级，直到规则到位。



步骤26.单击**OK**。



步骤27.单击“**保存**”。



您现在应该已在WAP125或WAP581接入点上配置MAC ACL。

查看与本文相关的视频……

[单击此处查看思科提供的其他技术讲座]