

在WAP125上配置IPv6访问控制列表(ACL)

目标

Internet协议第4版(IPv4)和Internet协议第6版(IPv6)访问控制列表(ACL)是应用于无线接入点(WAP)接收的数据包的一组规则。每条规则用于确定是允许还是拒绝访问网络。ACL可以配置为检查帧的字段，如源或目标IP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ACL通常用于授权对网络资源的访问。在公司设置中，通常是经理或授权访问资源的管理员，授予他们访问资源的权限以选择网络中的设备。这使资源服务器更高效，网络更安全。

本文旨在向您展示如何在WAP125接入点上配置IPv6 ACL。

注意：在本示例中，将允许来自IP地址为2001:DB8::22:F673:FF3B:AC99/10的选定主机的所有流量访问网络。来自其他主机的所有其他流量将被拒绝。

适用设备

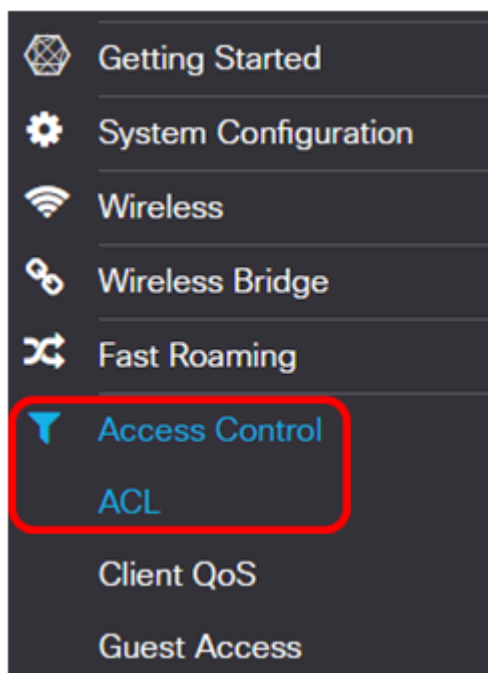
- WAP125

软件版本

- 1.0.0.3

配置IPv6 ACL

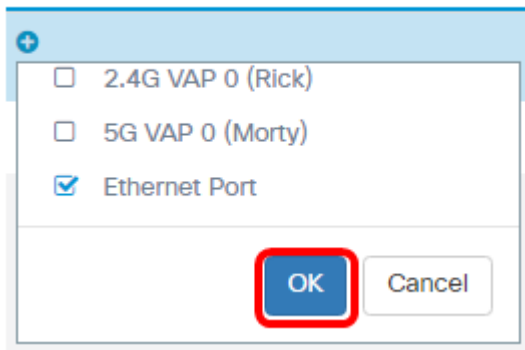
步骤1.登录WAP125的基于Web的实用程序，然后选择**Access Control > ACL**。



步骤2.单击  按钮添加ACL。

步骤6.单击OK。

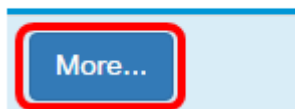
Associated Interface



A dialog box titled "Associated Interface" with a blue header bar containing a plus icon. Below the header is a list of three items: "2.4G VAP 0 (Rick)", "5G VAP 0 (Morty)", and "Ethernet Port". The "Ethernet Port" item is selected with a blue checkmark. At the bottom right of the dialog are two buttons: "OK" (highlighted with a red rectangle) and "Cancel".

步骤7.单击**More...**按钮配置ACL的参数。

Details Of Rule(s)



A dialog box titled "Details Of Rule(s)" with a blue header bar. Below the header is a single button labeled "More..." which is highlighted with a red rectangle.

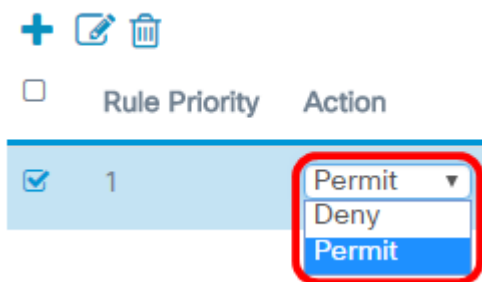
步骤8.单击  按钮添加新规则。



A toolbar with three icons: a plus sign (highlighted with a red rectangle), a pencil, and a trash can. Below the icons is a checkbox labeled "Rule Priority".

步骤9.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。



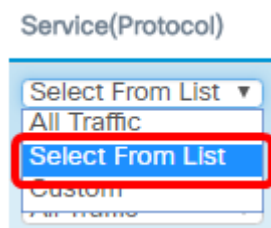
A table with two columns: "Rule Priority" and "Action". The first row is selected with a blue checkmark. The "Rule Priority" value is "1". The "Action" dropdown menu is open, showing three options: "Permit" (selected), "Deny", and "Permit" (highlighted with a red rectangle).

Rule Priority	Action
1	Permit

注意：在本例中，选择Permit。

步骤10.从Service(Protocol)下拉列表中选择要过滤的服务或协议。选项有：

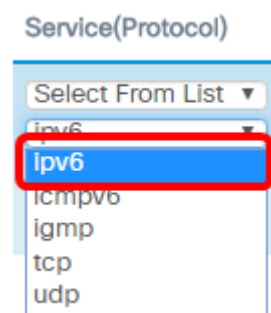
- 所有流量 — 此选项将所有数据包视为与ACL过滤器的匹配项。
- Select From List — 此选项允许您选择ipv6、icmpv6、igmp、tcp或udp作为ACL的过滤器。如果选择此选项，请继续[步骤11](#)。
- 自定义 — 此选项允许您输入自定义协议标识符作为数据包的过滤器。该值是一个四位十六进制数。范围是0到255。



注意：在本例中，选择从列表中选择。

步骤11.从Service(Protocol)下拉列表中选择协议。选项有：

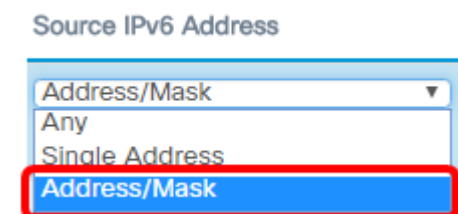
- ipv6 — 此选项将允许接入点使用其IPv6地址作为过滤器过滤访问网络的主机。
- icmpv6 — 此选项将允许接入点过滤通过接入点进入网络的互联网控制消息协议第6版(ICMPv6)数据包。
- igmp — 此选项将允许接入点过滤通过接入点进入网络的互联网组管理协议(IGMP)数据包。
- tcp — 此选项将允许接入点过滤通过接入点进入网络的传输控制协议(TCP)数据包。
- udp — 此选项将允许接入点过滤通过接入点进入网络的用户数据报协议(UDP)数据包。



注意：在本例中，选择ipv6。

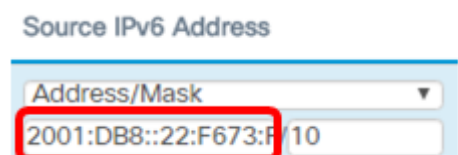
步骤12.从Source IPv6 Address下拉列表定义Source IPv6 Address。选项有：

- Any — 此选项将允许WAP将过滤器应用于来自任何IP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IP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IP地址和IP掩码。



注意：在本例中，选择Address/Mask。

步骤13.在Source IPv6 Address字段中输入源IPv6地址。



注意：在本例中，输入2001:DB8::22:F673:FF3B:AC20。

步骤14.在掩码字段中输入IPv6掩码。

Source IPv6 Address

Address/Mask

2001:DB8::22:F376:F 10

注意：在本例中，输入10。

步骤15.为条件选择源端口。选项有：

- Any — 此选项将允许来自源端口的符合条件的所有数据包。
- Select From List — 此选项允许您选择ftp、ftp data、http、smtp、snmp、telnet、tftp和www。
- 自定义 — 此选项允许您输入IANA端口号，以匹配数据报报头中标识的源端口。端口范围为0到65535，包括以下内容：
 - 0到1023 — 公认端口
 - 1024 — 49151 — 注册端口。
 - 49152 — 65535 — 动态和/或专用端口

Source Port

Any

Select From List

Custom

注意：在本例中，选择Any。

步骤16.从Destination IPv6 Address下拉列表中选择目标地址。选项有：

- Any — 此选项将任何IP地址视为与ACL语句匹配。
- Single Address — 此选项允许您为ACL条件输入特定IP地址。
- 地址/掩码 — 此选项允许您输入IP地址范围。

Destination IPv6 Address

Single Address

Any

Single Address

Address/Mask

注意：在本例中，选择了Single Address。

步骤17.在Destination IPv6 Address字段中输入目的IPv6地址。

Destination IPv6 Address

Single Address

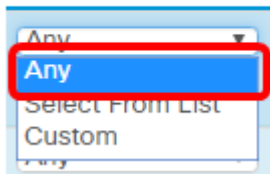
2001:DB8::22:F376:FF3B:AC99

注意：在本例中，输入2001:DB8::22:F376:FF3B:AC99。

步骤18.从Destination Port下拉列表中选择目标端口。选项有：

- Any — 此选项将数据包的所有目的端口视为与ACL中的语句匹配。
- 从列表中选择 — 此选项允许您选择与要匹配的目标端口关联的关键字。选项有：ftp、ftpdata、http、smtp、snmp、telnet、tftp和www。这些关键字转换为相应的端口号。
- 自定义 — 此选项允许您输入IANA端口号，以匹配数据报报头中标识的源端口。端口范围为0到65535，包括以下内容：
 - 0到1023 — 公认端口
 - 1024 — 49151 — 注册端口。
 - 49152 — 65535 — 动态和/或专用端口

Destination Port

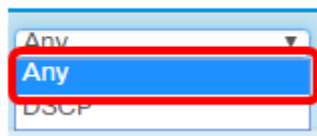


注意：在本例中，选择Any。

步骤19.从Flow Label下拉列表中选择IPv6流标签。这指定IPv6数据包唯一的20位数。选项有：

- Any — 此选项指定任何20位数字。
- DSCP值 — 此选项根据数据包的自定义DSCP值匹配数据包。选择此选项时，在DSCP值字段中输入0到63之间的值。

Flow Label

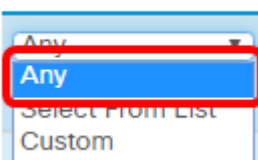


注意：在本例中，选择Any。

步骤20.从DSCP下拉列表中选择差分服务代码点(DSCP)设置。选项有：

- Any — 此选项将任何类型的服务视为匹配。
- Select From List — 此选项允许您从DSCP列表中选择DSCP过滤器。选择取决于DSCP配置。
- 自定义 — 此选项允许您输入从0到63的自定义DSCP值。

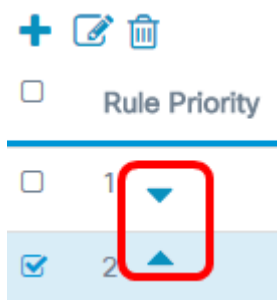
DSCP



注意：在本例中，选择Any。

第21步。（可选）重复第8步到第20步，直到ACL完成。

步骤22.（可选）通过单击上下按钮更改ACL上条件的顺序，直到它们按正确顺序排列。

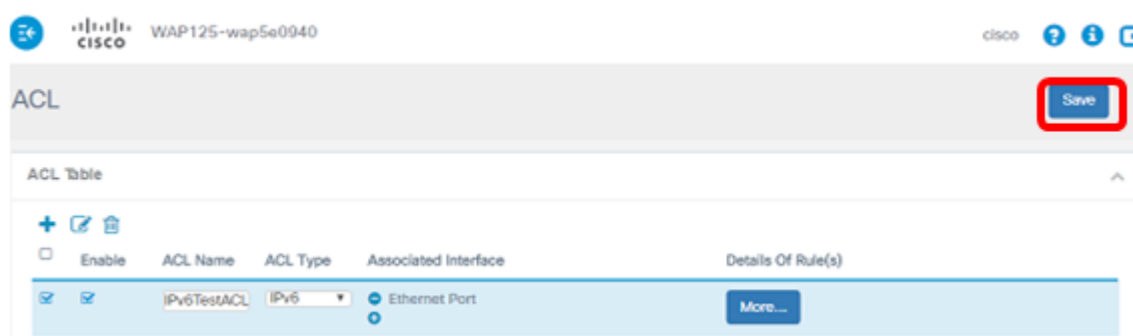


步骤23.单击OK。

Source Port	Destination IPv6 Address
Any	Single Address
	2001:DB8::22:F376:FF3B:AC99
Any	Any



步骤24.单击“保存”。



您现在应该已在WAP125接入点上完成IPv6 ACL。