

在WAP125上配置IPv6訪問控制清單(ACL)

目標

網際網路通訊協定第4版(IPv4)和網際網路通訊協定第6版(IPv6)存取控制清單(ACL)是一組應用於無線存取點(WAP)所接收封包的規則。每個規則用於確定應該允許還是拒絕對網路的訪問。可以將ACL配置為檢查幀的欄位，例如源或目標IP地址、虛擬區域網(VLAN)識別符號(ID)或服務類別(CoS)。當幀進入WAP裝置埠時，它會檢查該幀，並根據該幀的內容檢查ACL規則。如果任何規則與內容匹配，則對幀執行允許或拒絕操作。

配置ACL通常用於授權對網路資源的訪問。在企業設定中，被授權訪問資源以選擇網路中的裝置的通常是經理，或者被授權訪問資源的經理。這使得資源伺服器更加高效，並且使網路更加安全。

本文旨在展示如何在WAP125接入點上配置IPv6 ACL。

附註：在本示例中，將允許來自IP地址為2001:DB8::22:F673:FF3B:AC99/10的特定主機的所有流量訪問網路。來自其他主機的所有其他流量都將被拒絕。

適用裝置

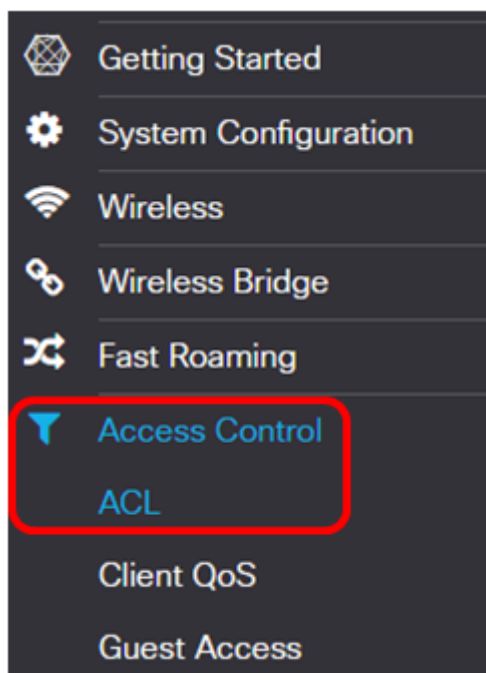
- WAP125

軟體版本

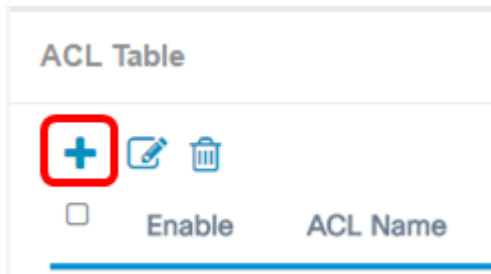
- 1.0.0.3

配置IPv6 ACL

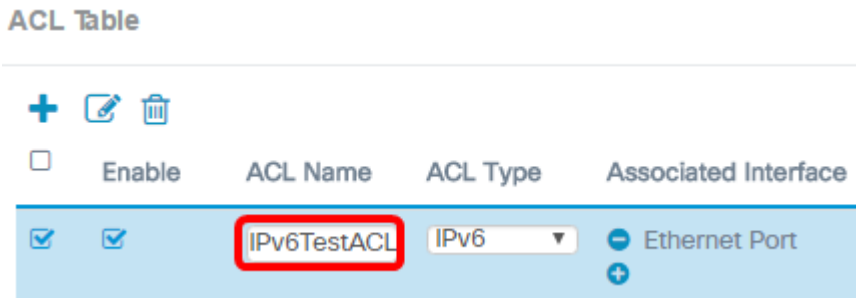
步驟1.登入到WAP125的基於Web的實用程式，然後選擇**Access Control > ACL**。



步驟2.按一下  按鈕新增ACL。

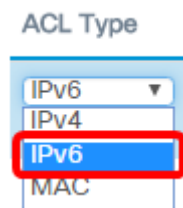


步驟3.在ACL Name欄位中輸入該ACL的名稱。



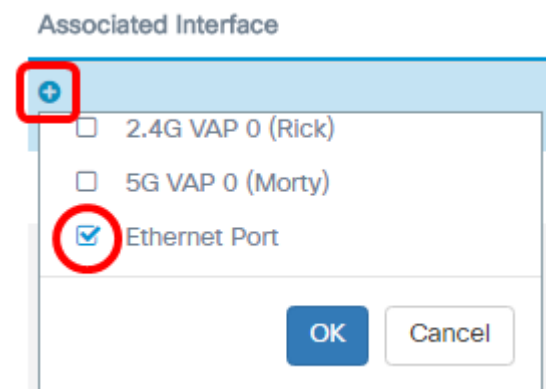
附註：在此示例中，輸入了IPv6TestACL。

步驟4.從ACL Type下拉選單中選擇IPv6。



步驟5.按一下  按鈕，並從Associated Interface下拉式清單中選擇一個介面。選項包括：

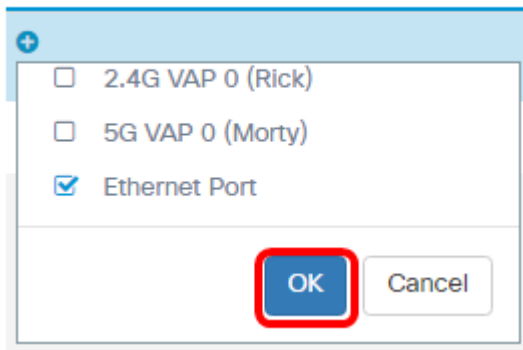
- 2.4G VAP 0 (SSID名稱) — 此選項將將MAC ACL應用於2.4 GHz虛擬接入點(VAP)。「SSID名稱」部分可能根據WAP上配置的SSID名稱而更改。
- 5G VAP 0 (SSID名稱) — 此選項將將MAC ACL應用於5 GHz VAP。
- Ethernet Port — 此選項會將MAC ACL應用於WAP的乙太網介面。



附註：可將多個介面關聯到一個ACL。但是，如果已將其與ACL關聯，則無法將其與另一個ACL關聯。在本示例中，乙太網埠與IPv6TestACL相關聯。取消選中此框可將介面與ACL取消關聯。

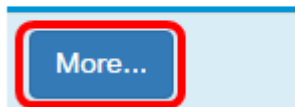
步驟6.按一下OK。

Associated Interface



步驟7.按一下**More...**按鈕配置ACL的引數。

Details Of Rule(s)

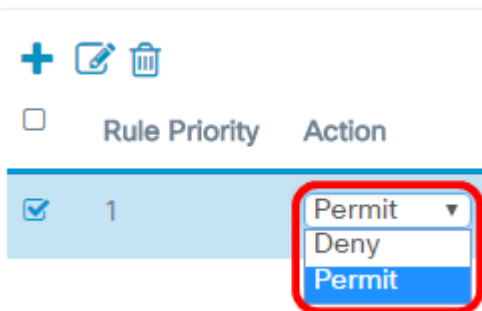


步驟8.按一下  按鈕新增新規則。



步驟9.從「操作」下拉選單中選擇操作。選項包括：

- Permit — 此選項將允許符合ACL條件的資料包連線到網路。
- 拒絕 — 此選項將阻止符合ACL標準的資料包連線到網路。



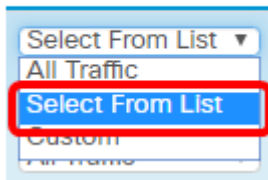
<input type="checkbox"/>	Rule Priority	Action
<input checked="" type="checkbox"/>	1	Permit

附註：在此示例中，選擇Permit。

步驟10.從Service(Protocol)下拉選單中選擇要過濾的服務或協定。選項包括：

- 所有流量 — 此選項會將所有封包視為與ACL過濾器的相符。
- Select From List — 此選項將允許您選擇ipv6、icmpv6、igmp、tcp或udp作為ACL的過濾器。如果選擇此選項，請繼續[步驟11](#)。
- 自定義 — 此選項將允許您輸入自定義協定識別符號作為資料包的過濾器。值為四位十六進位制數。範圍為0到255。

Service(Protocol)

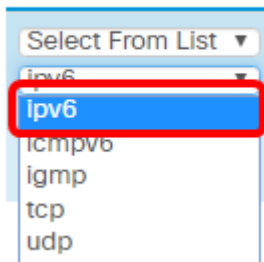


附註：在此示例中，選擇從清單中選擇。

步驟11.從Service(Protocol)下拉選單中選擇協定。選項包括：

- ipv6 — 此選項將允許接入點使用其IPv6地址作為過濾器來過濾訪問網路的主機。
- icmpv6 — 此選項將允許接入點過濾通過接入點進入網路的網際網路控制消息協定第6版(ICMPv6)資料包。
- igmp — 此選項可讓存取點過濾透過存取點進入網路的網際網路群組管理通訊協定(IGMP)封包。
- tcp — 此選項可讓存取點過濾透過存取點進入網路的傳輸控制通訊協定(TCP)封包。
- udp — 此選項將允許接入點過濾通過接入點進入網路的使用者資料包協定(UDP)資料包。

Service(Protocol)

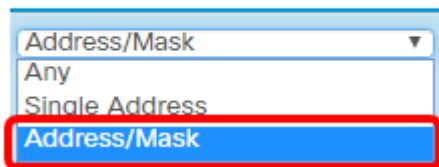


附註：在本示例中，選擇了ipv6。

步驟12.從Source IPv6 Address下拉選單中定義源IPv6地址。選項包括：

- Any — 此選項允許WAP對來自任何IP地址的資料包應用過濾器。
- Single Address — 此選項允許WAP對來自指定IP地址的資料包應用過濾器。
- Address/Mask — 此選項可讓WAP將過濾器應用於指向IP地址和IP掩碼的資料包。

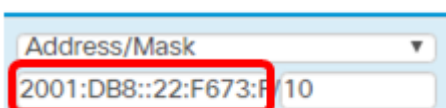
Source IPv6 Address



附註：在本示例中，選擇了Address/Mask。

步驟13.在源IPv6地址欄位中輸入源IPv6地址。

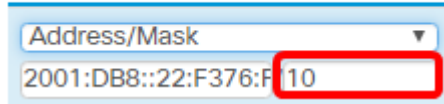
Source IPv6 Address



附註：在本示例中，輸入了2001:DB8::22:F673:FF3B:AC20。

步驟14.在*mask*欄位中輸入IPv6掩碼。

Source IPv6 Address

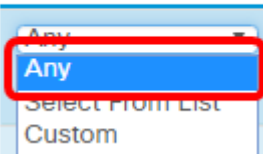


附註：在此示例中，輸入10。

步驟15.選擇條件的源埠。選項包括：

- Any — 此選項將允許來自源埠且符合條件的所有資料包。
- Select From List — 此選項可讓您選擇ftp、ftp資料、http、smtp、snmp、telnet、tftp和www。
- 自定義 — 此選項將允許您輸入IANA埠號以匹配資料包報頭中標識的源埠。埠範圍從0到65535，包括以下內容：
 - 0到1023 — 公認埠
 - 1024 — 49151 — 註冊埠。
 - 49152 - 65535 — 動態和/或專用埠

Source Port



附註：在此示例中，選擇了Any。

步驟16.從Destination IPv6 Address下拉選單中選擇一個目標地址。選項包括：

- Any — 此選項將任何IP地址視為與ACL語句的匹配項。
- Single Address — 此選項可讓您為ACL條件輸入特定IP地址。
- 地址/掩碼 — 此選項可讓您輸入IP地址範圍。

Destination IPv6 Address



附註：在本例中，選擇了Single Address。

步驟17.在*Destination IPv6 Address* 欄位中輸入目的IPv6地址。

Destination IPv6 Address

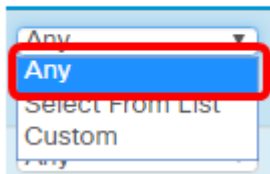


附註：在本示例中，輸入了2001:DB8::22:F376:FF3B:AC99。

步驟18.從Destination Port下拉選單中選擇目的地連線埠。選項包括：

- Any — 此選項將封包的所有目的地連線埠視為與ACL中的語句相符。
- 從清單中選擇 — 此選項可讓您選擇與要匹配的目的地埠關聯的關鍵字。選項包括：ftp、ftpdata、http、smtp、snmp、telnet、tftp和www。這些關鍵字轉換為它們對應的埠號。
- 自定義 — 此選項將允許您輸入IANA埠號以匹配資料包報頭中標識的源埠。埠範圍從0到65535，包括以下內容：
 - 0到1023 — 公認埠
 - 1024 — 49151 — 註冊埠。
 - 49152 - 65535 — 動態和/或專用埠

Destination Port

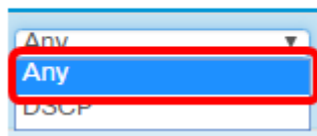


附註：在此示例中，選擇了Any。

步驟19.從Flow Label下拉選單中選擇IPv6流標籤。指定IPv6資料包唯一的20位編號。選項包括：

- Any — 此選項指定任何20位數字。
- DSCP值 — 此選項根據資料包的自定義DSCP值來匹配資料包。選擇此選項時，在「DSCP值」欄位中輸入從0到63的值。

Flow Label

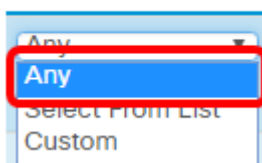


附註：在此示例中，選擇了Any。

步驟20.從DSCP下拉選單中選擇差異化服務代碼點(DSCP)設定。選項包括：

- Any — 此選項將任何型別的服務視為匹配項。
- Select From List — 此選項允許您從DSCP清單中選擇DSCP過濾器。這些選項取決於DSCP配置。
- 自定義 — 此選項可讓您輸入從0到63的自定義DSCP值。

DSCP



附註：在此示例中，選擇了Any。

步驟21. (可選) 重複步驟8到步驟20，直到ACL完成。

步驟22. (可選) 按一下up和down按鈕更改ACL上條件的順序，直到它們的順序正確。



Rule Priority

<input type="checkbox"/>	1	▼
<input checked="" type="checkbox"/>	2	▲

步驟23. 按一下OK。

Source Port	Destination IPv6 Address
<input type="text" value="Any"/>	<input type="text" value="Single Address"/> <input type="text" value="2001:DB8::22:F376:FF3B:AC99"/>
<input type="text" value="Any"/>	<input type="text" value="Any"/>



步驟24. 按一下「Save」。

WAP125-wap5e0940

ACL Save

ACL Table

Enable	ACL Name	ACL Type	Associated Interface	Details Of Rule(s)
<input checked="" type="checkbox"/>	IPv6TestACL	IPv6	Ethernet Port	More...

現在，您應該已經在WAP125接入點上完成了IPv6 ACL。