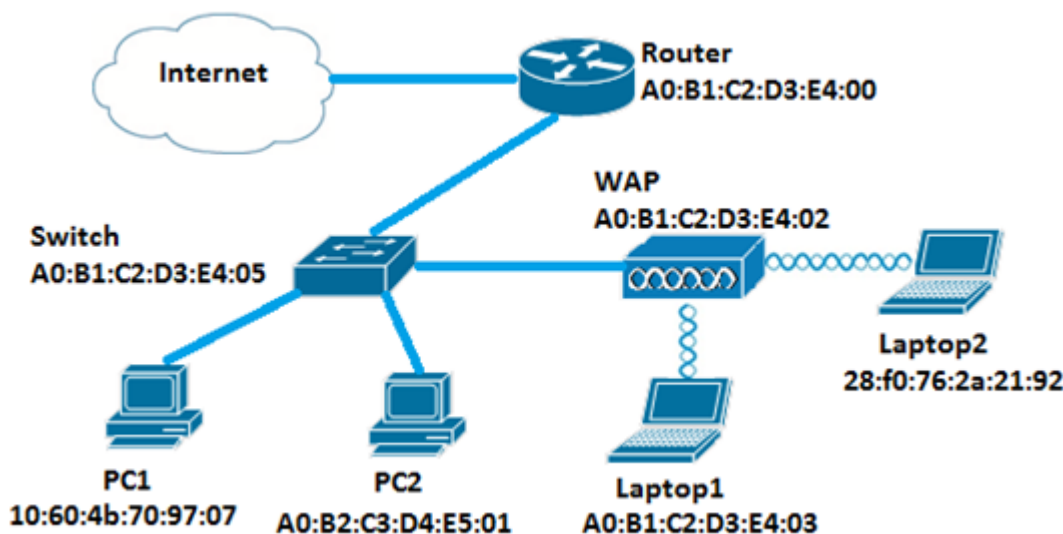


# 在WAP125和WAP581上配置MAC ACL

## 簡介

媒體存取控制(MAC)存取控制清單(ACL)是第2層ACL。每個ACL都是應用於無線接入點(WAP)接收的流量的一組規則。規則指定應使用給定欄位的內容來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MAC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MAC ACL通常用於授權對網路資源的訪問，以便選擇網路中的裝置。

**附註：**每個建立的規則的結尾都有一個隱含的deny。



在此場景中，將允許網路中的所有裝置訪問WAP後面的Laptop2 ( PC1除外 )。

## 目標

本文旨在展示如何在WAP125或WAP581接入點上配置基於MAC的ACL，以防止PC1訪問WAP後面的Laptop2。

## 適用裝置

- WAP125
- WAP581

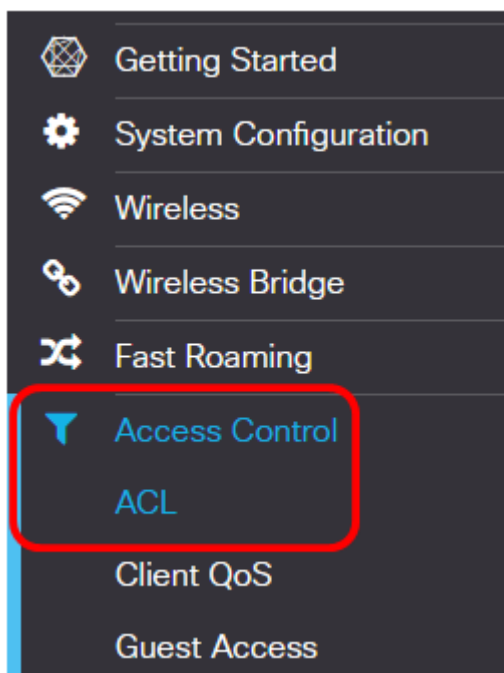
## 軟體版本

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

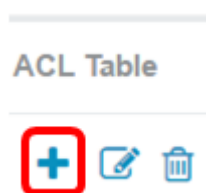
## 配置客戶端過濾器清單

**附註：**選單選項可能會隨您使用的WAP確切型號而有所不同。以下影象來自WAP125。

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



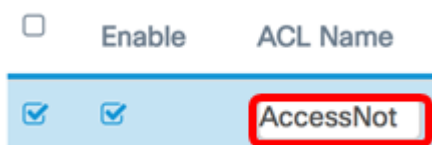
步驟2.按一下按 **+** 鈕。



步驟3.檢驗是否已選中Enable覆取方塊以確保ACL處於活動狀態。預設情況下選中此選項。

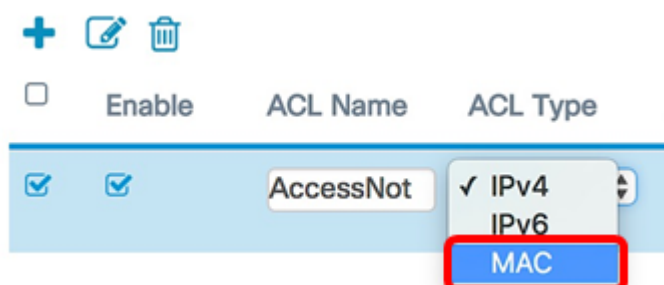


步驟4.在ACL Name欄位中輸入ACL名稱以識別ACL。



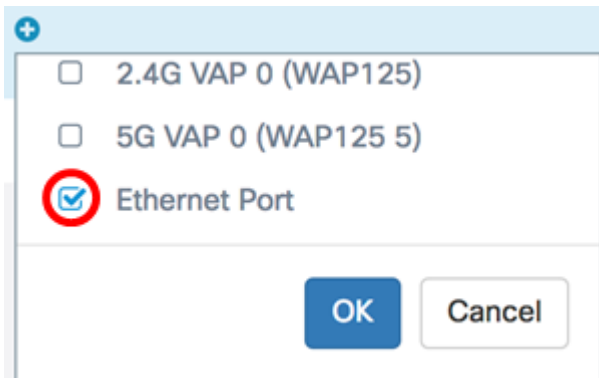
附註：在本示例中，輸入了AccessNot。

步驟5.從ACL Type下拉選單中選擇MAC。



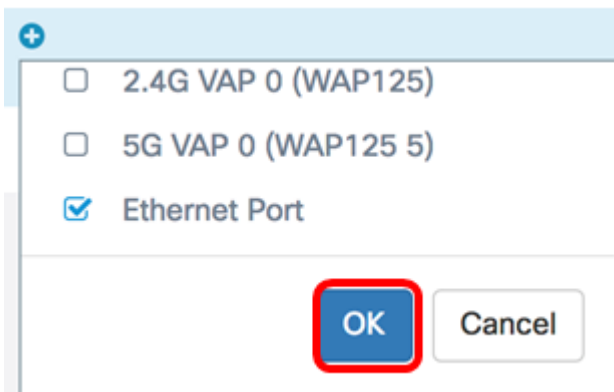
步驟6.點選按  鈕，並從Associated Interface下拉選單中選擇一個介面。選項包括：

- 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 VAP0 ( 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。

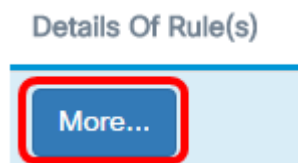


**附註：**可將多個介面關聯到一個ACL。選中相應介面的覈取方塊，將介面與ACL相關聯。取消選中此框可將介面與ACL取消關聯。在本範例中，乙太網路連線埠與ACL相關聯。

步驟7.按一下OK。



步驟8.按一下More...按鈕以設定ACL的引數。

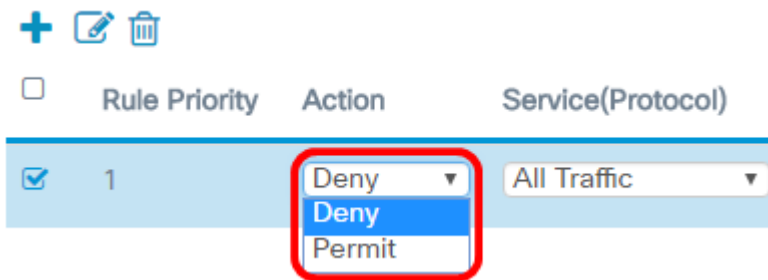


步驟9.按一下  按鈕新增新規則。



步驟10.從「操作」下拉選單中選擇操作。選項包括：

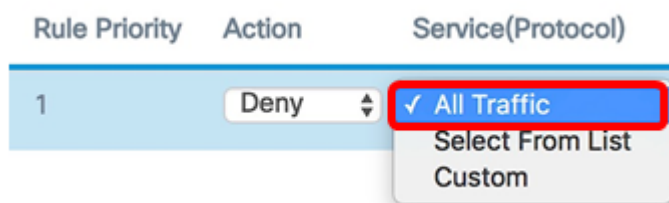
- Permit — 此選項將允許符合ACL條件的資料包連線到網路。
- 拒絕 — 此選項將阻止符合ACL標準的資料包連線到網路。



**附註：**在此示例中，選擇Deny。

步驟11.從Service(Protocol)下拉選單中選擇要過濾的服務或協定。選項包括：

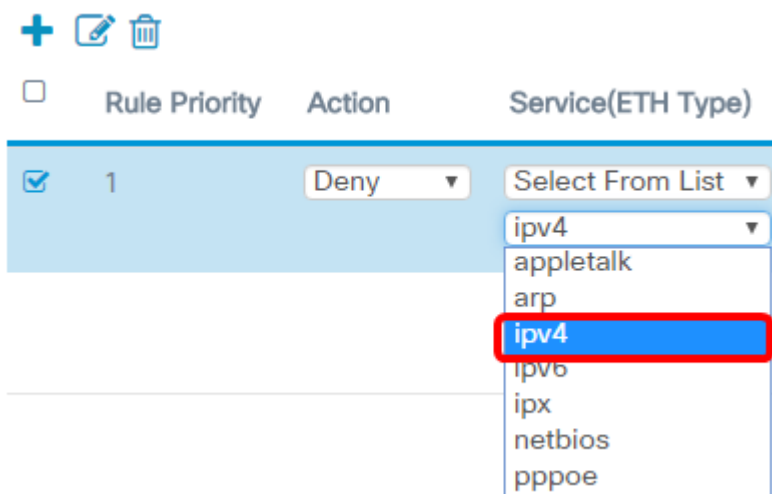
- 所有流量 — 此選項會將所有封包視為與ACL過濾器的相符。
- Select From List — 此選項將允許您選擇appletalk、arp、ipv4、ipv6、ipx、netbios和pppoe作為ACL的過濾器。如果選擇此選項，請跳至[步驟12](#)。
- 自定義 — 此選項將允許您輸入自定義協定識別符號作為資料包的過濾器。值為四位十六進位制數。範圍為0600到FFFF。



**附註：**在本例中，選擇了All Traffic。

[步驟12.](#)(可選)如果選擇「從清單中選擇」，請選擇以下任一選項：

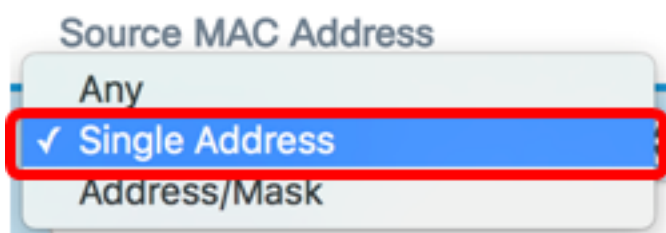
- appletalk — 此選項根據ACL的語句過濾appletalk資料包。Appletalk是蘋果為其Mac電腦開發的一組網路協定。其中一個功能允許無需中央路由器或伺服器即可連線區域網(LAN)。
- arp — 此選項根據ACL的陳述過濾位址解析通訊協定(ARP)封包。ARP維護一個表，其中的MAC地址對映到IP地址。
- ipv4 — 此選項根據ACL的陳述過濾ipv4封包。
- ipv6 — 此選項根據ACL的語句過濾ipv6資料包。IPv6是網路定址中IPv6的後繼者。
- ipx — 此選項根據ACL的陳述過濾網際網路封包交換(IPX)封包。與appletalk一樣，IPX也是一種專有網路協定。它連線使用Novell客戶端和伺服器的網路。
- netbios — 此選項根據ACL的語句過濾網路基本輸入和輸出系統(NetBIOS)資料包。NetBIOS通過為不同電腦上的應用程式提供通訊服務來允許它們進行通訊。
- pppoe — 此選項根據ACL的陳述過濾乙太網路上的點對點通訊協定(PPPoE)封包。它主要用於數字使用者線路(DSL)服務。



**附註：**在此範例中，選擇了ipv4。

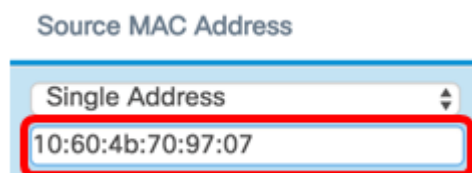
步驟13.從Source MAC Address下拉選單中定義源MAC地址。選項包括：

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



**附註：**在本例中，選擇了Single Address。

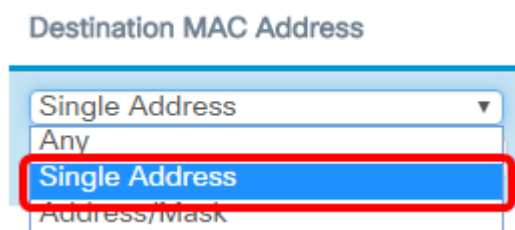
步驟14.在Source MAC Address欄位中輸入源MAC地址。



**附註：**在本示例中，輸入了10:60:4b:70:97:07。這是PC1的MAC地址。

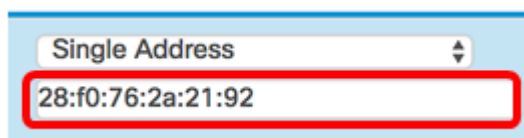
步驟15.從Destination MAC Address下拉選單中定義目標MAC地址。選項包括：

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



**附註：**在本例中，選擇了Single Address。

步驟16.在Destination MAC Address欄位中輸入目的MAC地址。



**附註：**在本示例中，輸入了28:f0:76:2a:21:92。這是Laptop2的MAC地址。

步驟17.從下拉選單中選擇VLAN ID。

- Any — 此選項允許任何VLAN ID通過網路。
- 自定義 — 此選項將允許您輸入特定VLAN ID。如果選擇此選項，請跳至[步驟18](#)。

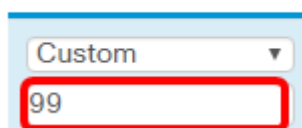
VLAN ID



**附註：**在此示例中，選擇了Any。

[步驟18](#). (可選) 如果您選擇自定義，請在VLAN ID欄位中輸入VLAN ID。

VLAN ID



**附註：**在此示例中，輸入99。

步驟19. (可選) 從下拉式清單中選擇服務類別。選項包括：

- Any — 此選項允許具有任何優先順序的資料包連線到網路。
- 自定義 — 此選項將允許您在特定優先順序級別過濾資料包。

Class Of Service



**附註：**在此示例中，選擇了Any。如果選擇自定義，請在Class of Service(服務類別)欄位中輸入優先順序。

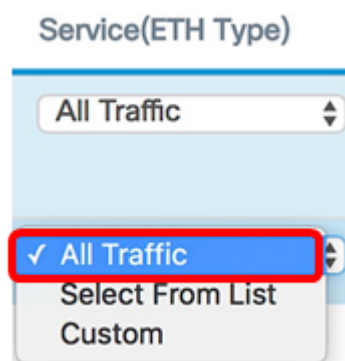
步驟20.再次單 **+** 擊該按鈕以新增允許規則。

**附註：**由於建立的每個規則的結尾都有一個隱含的deny，因此強烈建議向ACL新增允許規則，以允許來自網路中其他裝置的流量。

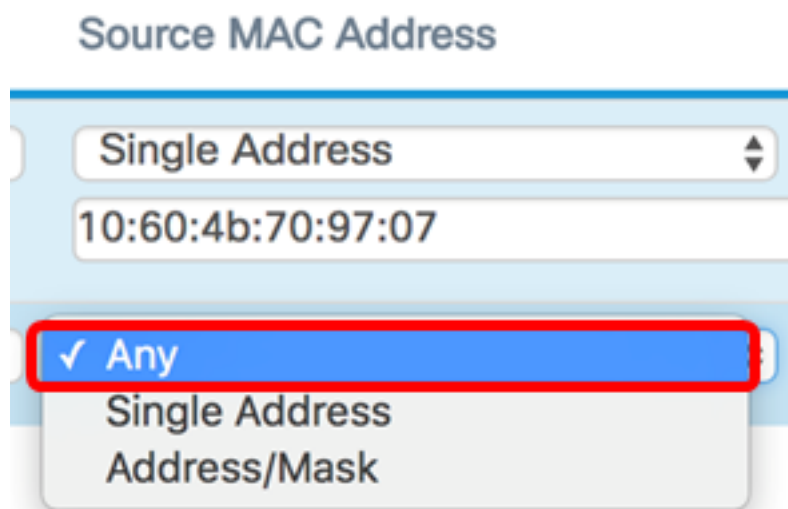
步驟21.點選Action下拉箭頭並選擇Permit。



步驟22.點選Service(ETH Type)下拉箭頭並選擇All Traffic。



步驟23.按一下Source MAC Address下拉選單，然後選擇Any。這將允許來自網路中除第一條規則中指示的PC1 MAC地址以外的任何其他MAC地址的流量。



步驟24.按一下Destination MAC Address下拉選單，然後選擇Any。這將允許流量流向網路中的任何MAC地址。

## Destination MAC Address

Single Address

28:f0:76:2a:21:92

✓ Any

Single Address

Address/Mask

步驟25. ( 可選 ) 通過按一下向上和向下箭頭直到規則到位，更改規則的優先順序。

+ ✎ 🗑

Rule Priority

---

1 ▼

2 ▲

步驟26. 按一下OK。

Action	Service(ETH Type)	Source MAC Address	Destination MAC Address
Deny	All Traffic	Single Address 10:60:4b:70:97:07	Single Address 28:f0:76:2a:21:92
Permit	All Traffic	Any	Any

OK Cancel

步驟27. 按一下「Save」。

ACL

Save

ACL Table

+ ✎ 🗑

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

現在，您應該已經在WAP125或WAP581接入點上配置了MAC ACL。

[檢視與本文相關的影片.....](#)



[按一下此處檢視思科的其他技術對話](#)