

# 在無線接入點上配置MAC、IPv4和IPv6訪問控制清單

## 目標

訪問控制清單(ACL)是一個網路流量過濾器清單和相關操作清單，用於提高安全性。它阻止未經授權的使用者並允許授權的使用者訪問特定資源。ACL包含允許或拒絕訪問網路裝置的主機。ACL可以用以下兩種方式之一定義：通過IPv4地址或IPv6地址。

本文介紹如何在無線接入點(WAP)上成功建立ACL並配置基於IPv4、IPv6和媒體訪問控制(MAC)的ACL以提高網路安全性。

## 適用裝置

- WAP100系列
- WAP300系列
- WAP500系列

## 軟體版本

- 1.0.6.2 - WAP121、WAP321
- 1.2.0.2 - WAP371、WAP551、WAP561
- 1.0.1.4 - WAP131、WAP351
- 1.0.0.16 - WAP150、WAP361

## 建立ACL

附註：用於此配置的映像來自WAP150。

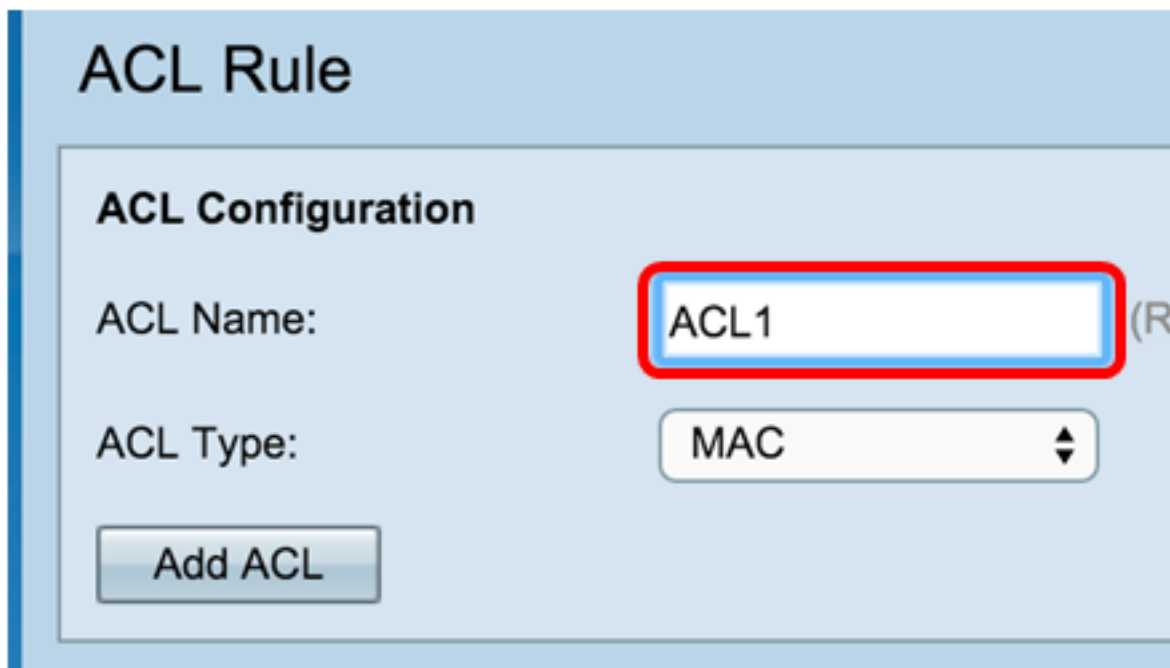
步驟1.登入到接入點基於Web的實用程式，然後選擇ACL > ACL Rule。



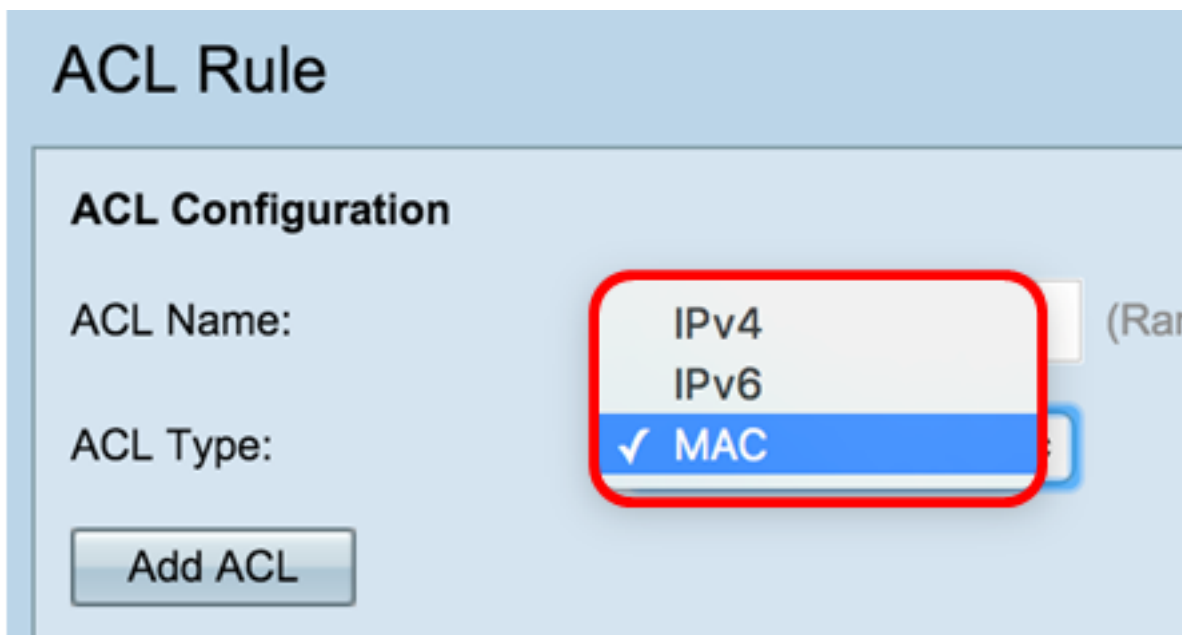
附註：對於WAP121、WAP321、WAP371、WAP551和WAP561:登入到接入點基於Web的實用程式，然後選擇Client QoS> ACL。



步驟2.開啟ACL Configuration頁面後，在ACL Name欄位中輸入ACL名稱。



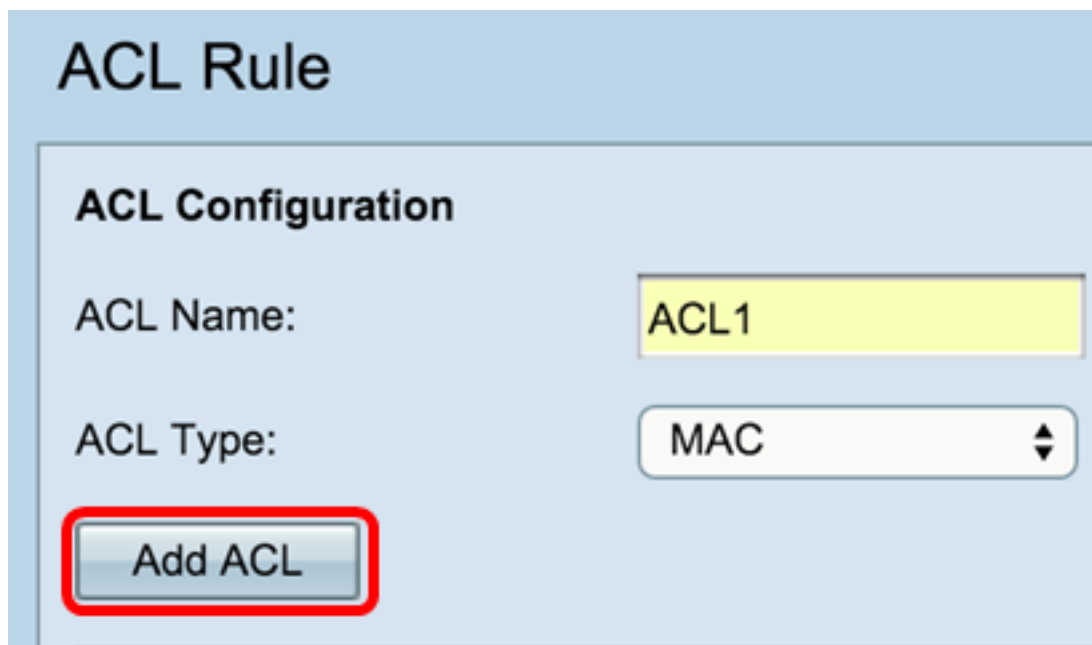
步驟3.從ACL Type下拉式清單中選擇ACL Type。



- IPv4 - 32位 ( 4位元組 ) 地址。

- IPv6 — IPv4的後繼路由器，由128位（8位元組）地址組成。
- MAC - MAC地址是分配給網路介面的唯一地址。

步驟4. 按一下Add ACL按鈕。



ACL Rule

ACL Configuration

ACL Name: ACL1

ACL Type: MAC

Add ACL

如果選擇MAC，請跳至[配置基於MAC的ACL](#)。

如果您選擇IPv4，請跳至[設定基於IPv4的ACL](#)。

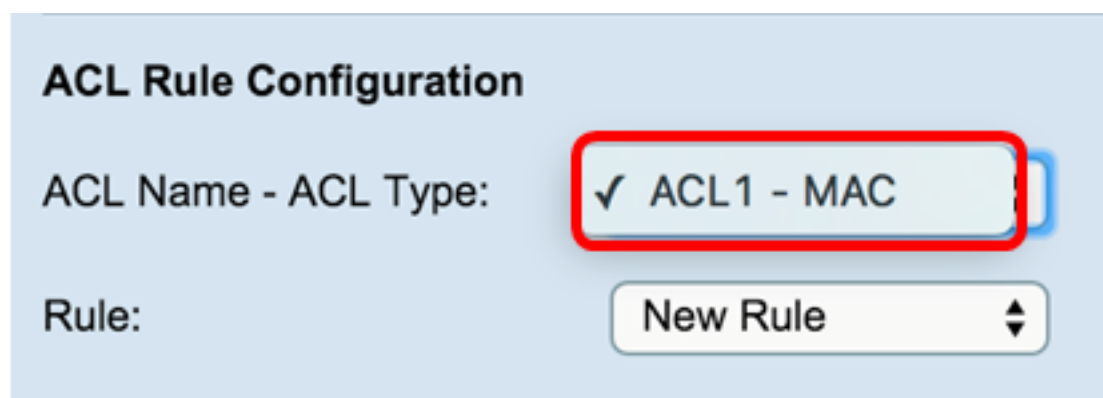
如果選擇IPv6，請跳至[配置基於IPv6的ACL](#)。

您現在應該已經成功建立了ACL。

## 配置基於MAC的ACL

步驟1. 從ACL Name - ACL Type下拉選單中選擇要新增規則的ACL。

附註：下圖選擇了ACL1 MAC作為示例。



ACL Rule Configuration

ACL Name - ACL Type: ✓ ACL1 - MAC

Rule: New Rule

步驟2. 如果必須為所選ACL配置新規則，請從Rule下拉選單中選擇New Rule。否則，請從Rule下拉選單中選擇一個當前規則。

注意：最多可以為單個ACL建立10個規則。

**ACL Rule Configuration**

ACL Name - ACL Type:

Rule:

步驟3.從Action下拉選單中選擇用於ACL規則的操作。

注意：在此示例中，建立了一個Deny語句。

Action:

Match Every Packet:

- 拒絕 — 阻止符合規則標準的所有流量進入或退出WAP。由於每個ACL的結尾都有一個隱含的deny-all規則，因此不會明確允許的流量會遭到捨棄。
- 允許 — 允許符合規則標準的所有流量進入或退出WAP。不符合條件的流量將被丟棄。

附註：步驟4到11是可選的。已啟用選中的篩選條件。取消選中您不希望過濾器應用於此特定規則的過濾器對應的覈取方塊。

步驟4.選中Match Every Packet覈取方塊以匹配每個幀或資料包的規則，無論其內容如何。取消選中此框可配置任何其他匹配條件。

提示：如果已選中Match Every Packet，請跳至步驟12。

Action:

Match Every Packet:

步驟5.在EtherType區域中，選擇單選按鈕，將匹配的標準與乙太網幀報頭中的值進行比較。您可以選擇以下選項之一或選擇任意：

- 從清單中選擇協定 — 從下拉選單中選擇協定。該清單具有以下選項：appletalk、arp、IPv4、IPv6、ipx、netbios、pppoe。
- 與值匹配 — 對於自定義協定識別符號，請輸入從0600到FFFF的識別符號。

Protocol:

Any

Select From List:

Match to Value:

icmp

0 (Range)

步驟6.在Class Of Service區域中，選擇單選按鈕以輸入802.1p使用者優先順序並與乙太網幀進行比較。可以選擇任意或使用者定義的優先順序。在 *User Defined* 欄位中輸入從0到7的優先順序。

Class Of Service:

Any

User Defined

6

步驟7.在Source MAC區域中，選擇單選按鈕將源MAC地址與乙太網幀進行比較。您可以選擇 **Any** 或 **User Defined**，然後在提供的欄位中輸入源MAC地址。

Source MAC:

Any

User Defined

Source MAC Address: 04:FE:36:A5:670B

Source MAC Mask:

步驟8.在 *Source MAC Mask* 欄位中輸入源MAC地址掩碼，指定源MAC中的哪些位與乙太網幀進行比較。

附註：如果MAC掩碼使用0位，則接受該地址；如果使用1位，則忽略該地址。

Source MAC:

Any

User Defined

Source MAC Address: 04:FE:36:A5:670B

Source MAC Mask: 00:00:00:00:00:00

步驟9.在Destination MAC區域中，選擇單選按鈕將目的MAC地址與乙太網幀進行比較。您可以選擇任意(Any)或選擇使用者定義(User Defined)，然後在提供的欄位中輸入目標MAC地址。

Destination MAC:

Any

User Defined

Destination MAC Address: F2:CA:46:11:EA:09

Destination MAC Mask:

步驟10.在 *Destination MAC Mask* 欄位中輸入目標MAC地址掩碼，指定目標MAC中的哪些位與乙太網幀進行比較。

附註：如果MAC掩碼使用0位，則接受該地址；如果使用1位，則忽略該地址。

Destination MAC:  Any  
 User Defined  
Destination MAC Address: F2:CA:46:11:EA:09  
Destination MAC Mask: 00:00:00:00:00:00

步驟11.在VLAN ID區域中，選擇單選按鈕將VLAN ID與乙太網幀進行比較。在提供的欄位中輸入範圍從0到4095的VLAN ID。

VLAN ID:  Any  
 User Defined 52 (Range: 0 - 4095)

步驟12.按一下「Save」。

VLAN ID:  Any  
 User Defined  
Delete ACL:

Save

步驟13。(可選)若要刪除已配置的ACL，請選中Delete ACL覈取方塊，然後按一下Save。

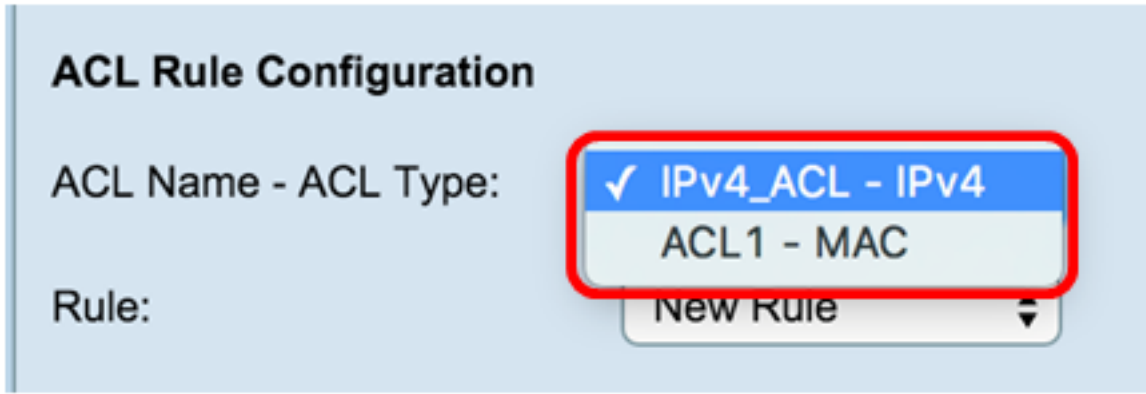
您現在應該已經在WAP上成功配置了MAC ACL。

## 配置基於IPv4的ACL

1.ACL Rule Configuration

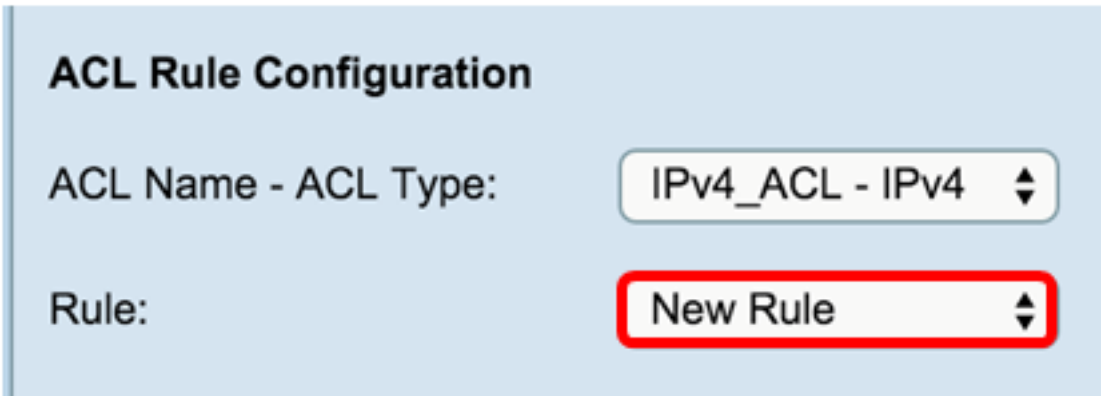
ACL — ACLACL

IPv4\_ACL-IPv4



2. ACL Rule New Rule Rule

ACL10



3. Action ACL

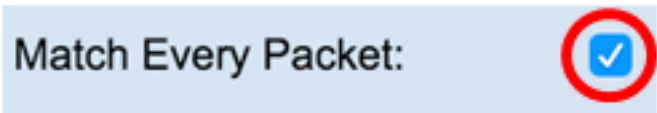
Permit

- — WAP ACL deny-all
- — WAP



49

4. Match Every Packet



Match Every Packet [11](#)

5. Protocol Any

- —

- IP - Internet
- ICMP — Internet

- IGMP — IPv4
- TCP —
- UDP — Internet

- — 0255IANAID

**Protocol:**

Any  
 **Select From List:**  
 Match to Value:

icmp (Range: 0 - 65535)

#### 6. Source IP

- IP (Source IP Address) — IP
- — IP 255.255.255.255 0.0.0.0 IP

0.0.0.0/24 (192.168.10.0/24) 0.0.0.255

**Source IP:**

Any  
 **User Defined**  
 Source IP Address: 192.168.1.100 (xxx.xxx.xxx.xxx)  
 Wild Card Mask: 0.0.0.255 (xxx.xxx.xxx.xxx)

#### 7. Source Port

- —

- (FTP) — FTP (TCP)
- FTP — 20
- (HTTP) — HTTP
- (SMTP) — SMTP Internet
- (SNMP) — SNMP IP Internet
- Telnet — Internet
- (TFTP) — TFTP Internet FTP
- (WWW) — WWW HTTP

- — 065535

- 01023 —
- 102449151 —
- 4915265535 — /

- — (0 - 0xFFFF) 01

**Source Port:**

Any  
 **Select From List:**  
 Match to Port:  
 Mask:

www (Range: 0 - 65535)

(Range: 0 ~ 0xffff, 0s)

#### 8. Destination IP

- IP — IP



- — IP255.255.255.2550.0.0.0IP

0.0.0.024(192.168.10.0/24)0.0.0.255

Destination IP:

Any  
 User Defined  
 Destination IP Address:  (xxx.xxx.xxx.xxx)  
 Wild Card Mask:  (xxx.xxx.xxx.xxx -

9.Destination PortAny

- —

- FTP — TCPInternet
- FTP — 20
- HTTP —
- SMTP — Internet
- SNMP — IPInternet
- Telnet — Internet
- TFTP — FTP
- WWW — HTTPInternet

- — 065535

- 01023 —
- 102449151 —
- 4915265535 — /

- — (0-0xFFFF)01

Destination Port:

Any  
 Select From List:  (Range: 0 - 65535)  
 Match to Port:  (Range: 0 - 65535)  
 Mask:  (Range: 0 ~ 0xFFFF)

10.Service Type

- IP DSCP Select From List — (DSCP)(AS)(CS)(EF)
- IP DSCP Match to Value — DSCP063
- IP — IP07IP
- IP TOS Bits — IPTOS
- IP TOSIPIP TOS Bits00ff3IP6IP DSCP
- IP TOS — IP TOSIP TOSIP TOS
- IP TOS Mask00FFIP TOSIP TOSIP TOS7517IP TOSIP TOS0IP TOS00

Service Type

Any  
 IP DSCP Select From List  (Range: 0 - 63)  
 IP DSCP Match to Value:  (Range: 0 - 63)  
 IP Precedence:  (Range: 0 - 7)  
 IP TOS Bits:  (Range: 00 - FF)  
 IP TOS Mask:  (Range: 00 - FF)

11.

VLAN ID:  Any  
 User Defined

Delete ACL:

Save

IPv4ACL

## 配置基於IPv6的ACL

1.ACL Rule Configuration

ACL Name - ACL Type — ACL

IPv6\_ACL - Pv6

**ACL Rule Configuration**

ACL Name - ACL Type: IPv6\_ACL - IPv6

Rule: New Rule

2.ACLRuleNew RuleRule

ACL10

**ACL Rule Configuration**

ACL Name - ACL Type: IPv6\_ACL - IPv6

Rule: New Rule

3.ActionACL

- — WAPACLdeny-all
- — WAP

Action: Deny

Permit

Match Every Packet:

#### 4. Match Every Packet

Match Every Packet:



Match Every Packet<sup>12</sup>

#### 5. Protocol

- —

— IP - Internet

— ICMP — Internet

— IGMP — IPv4

— TCP —

— UDP — Internet

- — 0255IANAID

Protocol:

- Any
- Select From List:
- Match to Value:

ipv6

0

(Range:)

#### 6. Source IPv6 IP Any User Defined IPv6 IPv6

- IPv6 — IPv6

- IPv6 — IPv6

Source IPv6:

- Any
  - User Defined
- Source IPv6 Address:
- Source IPv6 Prefix Length:

fd2d:43a5:25fe:9fef:ffff

64

(Range:)

Source Port:

- Any

#### 7. Source Port Any

- —

— FTP — TCP Internet

— FTP — 20

— HTTP —

— SMTP — Internet

— SNMP — IP Internet

— Telnet — Internet

- TFTP — FTP

— WWW — HTTP Internet

- — 065535

— 01023 —

— 102449151 —

— 4915265535 — /

- — â(0xFFFF)01

Source Port:

- Any
  - Select From List:
  - Match to Port:
- Mask:

www

(Range:)

(Range:)

#### 8. Destination IPv6 IP Any User Defined IPv6 IPv6

- IPv6 — IPv6

- IPv6 — IPv6

Destination IPv6:

Any

User Defined

Destination IPv6 Address:

Destination IPv6 Prefix Length:  (Range: 0-128)

#### 9. Destination Port Any

- — FTP
- — HTTP
- — HTTPS
- — SNMP
- — SMTP
- — FTP
- — Telnet
- — WWW
- — 065535

— 01023 —

— 102449151 —

— 4915265535 — /

- — (0-0xFFFF)01

Destination Port:

Any

Select From List:

Match to Port:

Mask:

#### 10. IPv6 Flow Label IPv6 IPv6 Any User Defined IPv6 200-0xffff

IPv6 Flow Label:

Any

User Defined:

#### 11. IPv6 DSCP IPv6 DSCP

- — DSCP(AF)(CS)(EF)
- — 063 DSCP

IPv6 DSCP:

Any

Select From List:

Match to Value:  (Range: 0 - 63)

Delete ACL:

#### 12. Save

IPv6 DSCP:  Any  
 Select From List:  
 Match to Value:

Delete ACL:

**Save**

13.ACLACL Name-ACL TypeACLDelete ACL

IPv6ACL