

在WAP551和WAP561存取點上設定基於MAC的存取控制清單(ACL)

目標

訪問控制清單(ACL)是允許和拒絕條件（稱為規則）的集合，它們提供安全性、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可以阻止任何未授權的嘗試訪問網路資源。MAC ACL是第2層ACL。網路裝置檢查幀並根據幀的內容檢查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。

本文檔的目的是向使用者展示如何在WAP551和WAP561接入點上建立和配置MAC ACL。

適用裝置

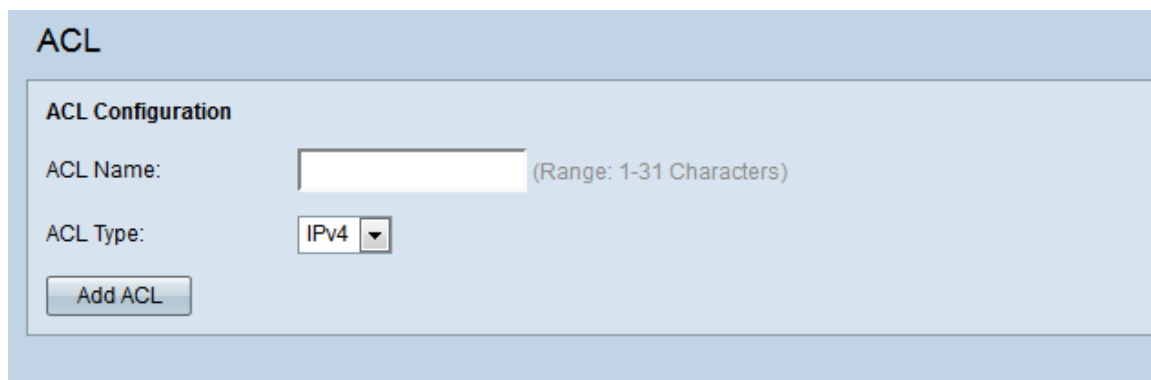
- WAP551
- WAP561

軟體版本

- v1.0.4.2

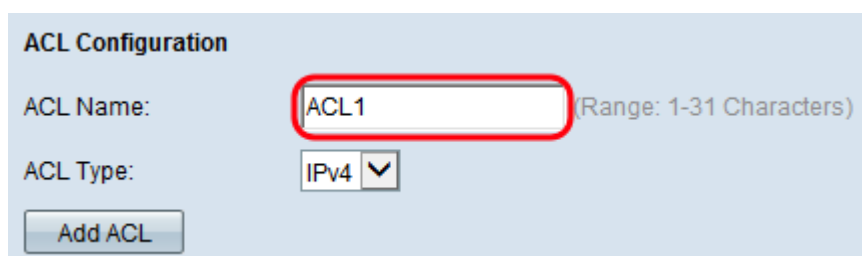
配置MAC ACL

步驟1.登入到Web配置實用程式並選擇客戶端QoS > ACL。ACL頁面隨即開啟：



建立MAC ACL

步驟1.在ACL Name欄位中輸入ACL的名稱。



步驟2.從ACL Type下拉式清單中選擇MAC作為ACL型別。

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: MAC ▼

步驟3.按一下Add ACL建立新的MAC ACL。

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: ▼

Add ACL

為MAC ACL配置規則

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

ACL Rule Configuration

ACL Name - ACL Type: ACL1 - MAC ▼
ACL1 - MAC
New Rule ▼

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。

ACL Rule Configuration

ACL Name - ACL Type: ▼

Rule: New Rule ▼
New Rule

附註：最多可為單個ACL建立10個規則。

步驟3.從Action下拉選單中選擇用於ACL規則的操作。

Action: Deny ▼
Deny
Permit

Match Every Packet: Select From List ▼ Match to Value: (Range: 0600 - FFFF)

EtherType: (Range: 0 - 7) Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

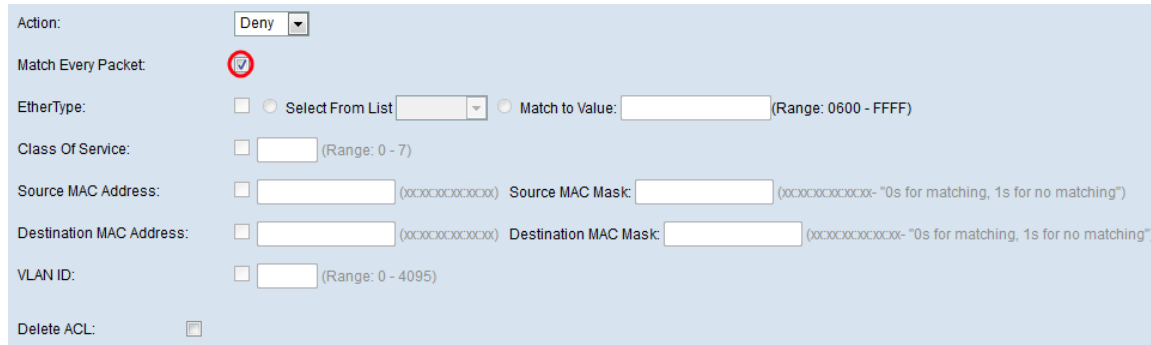
可用選項定義如下：

·拒絕 — 阻止符合規則標準的所有流量進入或退出WAP裝置。

·允許 — 允許符合規則條件的所有流量進入或退出WAP裝置。

附註：步驟4到9是可選的。如果不希望將過濾器應用於ACL規則，請取消選中其對應的框。

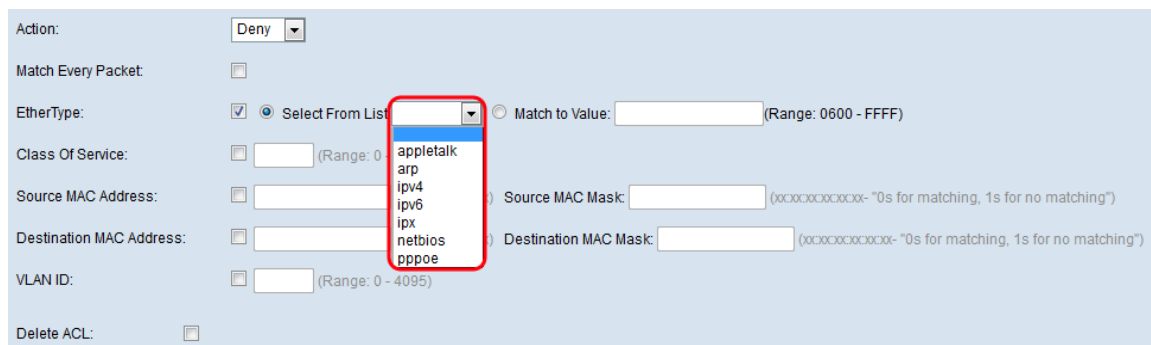
步驟4. (可選) 選中**Match Every Packet**覈取方塊以匹配每個幀或資料包的規則，而不管其內容如何。取消選中**Match Every Packet**覈取方塊以配置任何附加匹配條件。



The screenshot shows the configuration interface for an ACL rule. The 'Action' is set to 'Deny'. The 'Match Every Packet' checkbox is checked and highlighted with a red circle. Other options like 'EtherType', 'Class Of Service', 'Source MAC Address', 'Destination MAC Address', and 'VLAN ID' are present but not selected.

如果選中**Match Every Packet**框，請跳至步驟11。

步驟5. (可選) 勾選**EtherType**覈取方塊，將匹配條件與乙太網幀報頭中的值進行比較。如果勾選了**EtherType**覈取方塊，請按一下**Select From List**或**Match to Value**單選按鈕。



The screenshot shows the configuration interface with the 'EtherType' checkbox checked. The 'Select From List' dropdown menu is open, showing a list of protocols: appletalk, arp, ipv4, ipv6, ipx, netbios, and pppoe. The dropdown is highlighted with a red box.

可用選項定義如下：

·從清單中選擇協定 — 用於從下拉選單中選擇協定。可用的選項包括appletalk、arp、ipv4、ipv6、ipx、netbios和pppoe。選擇選項會將規則應用於所選協定的資料包。

- appletalk — 這是由Apple Inc.為其Macintosh電腦設計的網路協定。Appletalk是一個即插即用系統；它自動分配地址和處理任何其他網路配置，而無需使用者輸入。

- arp — ARP (地址解析協定) 是用於將IP地址轉換為MAC地址的關鍵協定。

- ipv4 - IPv4 (Internet協定版本4) 是負責網際網路上大部分流量的重要協定。處理裝置的IP地址。

- ipv6 — IPv6是IPv4的後繼者和最新版本的Internet協定。它是針對大多數現有IPv4 IP地址耗盡而開發的。

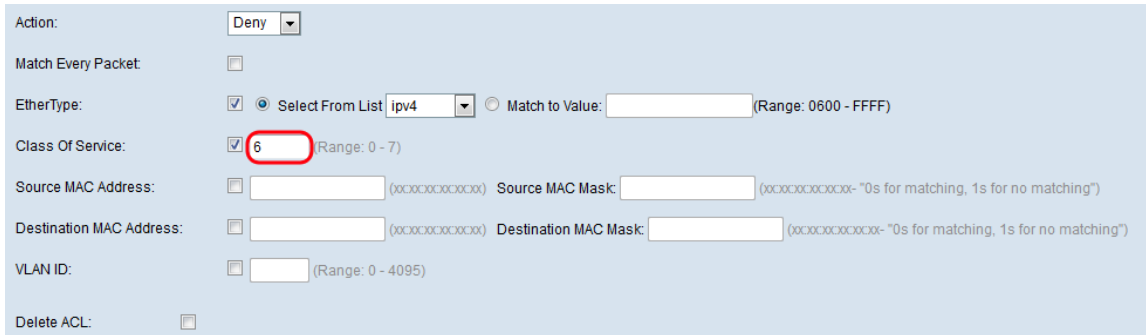
- ipx - IPX (網際網路資料包交換) 是一種網路/傳輸協定。雖然該協定在大型網路中效果不佳，但是IPX與TCP/IP相比有一個優勢，就是它使用的記憶體量很小。

- netbios — NetBIOS (Network Basic Input/Output System, 網路基本輸入/輸出系統) 是API (應用程式程式設計介面)，在現代網路中通常與TCP/IP一起運行。

- pppoe - PPPoE (乙太網路上的點對點通訊協定) 是一種網路通訊協定，用於將PPP封包封裝在乙太網路封包中。

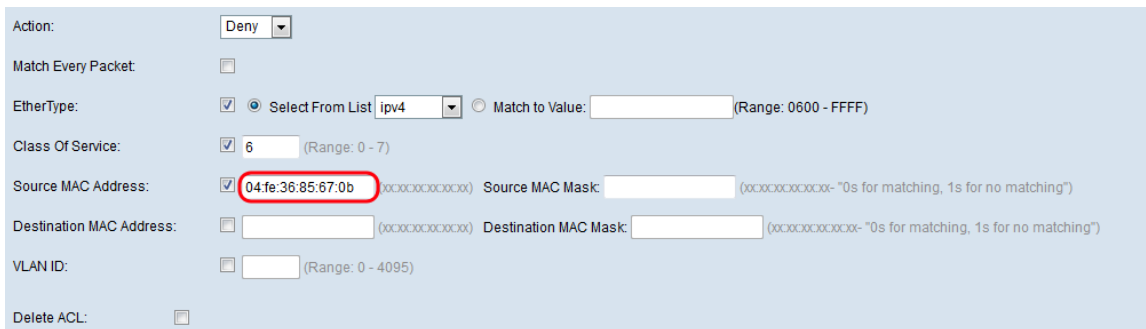
·Match to Value — 允許您在 *Match to Value* 欄位中輸入自定義協定標識符。如果要按 *Select From List* 下拉選單中未包含的協定過濾資料包，此選項非常有用。有效的自定義協定識別符號範圍為0600到FFFF。

步驟6. (可選) 選中 **Class of Service** 覈取方塊以輸入802.1p使用者優先順序，以便與乙太網幀進行比較。在 *Class of Service* 欄位中輸入優先順序，範圍為0至7。



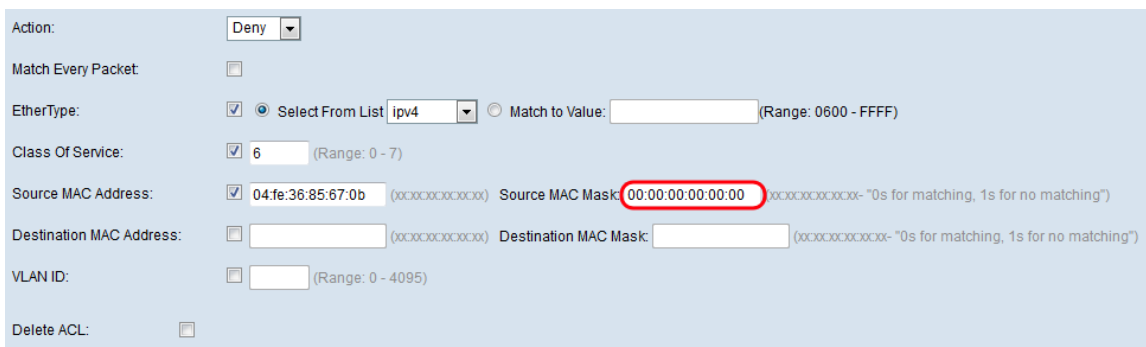
The screenshot shows the configuration interface for an ACL rule. The 'Action' is set to 'Deny'. The 'Match Every Packet' checkbox is unchecked. The 'EtherType' is set to 'Select From List' with 'ipv4' selected. The 'Class Of Service' checkbox is checked, and the value '6' is entered in the adjacent text box. The 'Source MAC Address' and 'Destination MAC Address' fields are empty. The 'VLAN ID' field is also empty. The 'Delete ACL' checkbox is unchecked.

步驟7. (可選) 選中 **Source MAC Address** 覈取方塊，將源MAC地址與乙太網幀進行比較，並在 *Source MAC Address* 欄位中輸入源MAC地址。



The screenshot shows the configuration interface for an ACL rule. The 'Action' is set to 'Deny'. The 'Match Every Packet' checkbox is unchecked. The 'EtherType' is set to 'Select From List' with 'ipv4' selected. The 'Class Of Service' checkbox is checked, and the value '6' is entered. The 'Source MAC Address' checkbox is checked, and the value '04:fe:36:85:67:0b' is entered in the adjacent text box. The 'Source MAC Mask' field is empty. The 'Destination MAC Address' and 'VLAN ID' fields are empty. The 'Delete ACL' checkbox is unchecked.

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



The screenshot shows the configuration interface for an ACL rule. The 'Action' is set to 'Deny'. The 'Match Every Packet' checkbox is unchecked. The 'EtherType' is set to 'Select From List' with 'ipv4' selected. The 'Class Of Service' checkbox is checked, and the value '6' is entered. The 'Source MAC Address' checkbox is checked, and the value '04:fe:36:85:67:0b' is entered. The 'Source MAC Mask' checkbox is checked, and the value '00:00:00:00:00:00' is entered. The 'Destination MAC Address' and 'VLAN ID' fields are empty. The 'Delete ACL' checkbox is unchecked.

步驟9. (可選) 選中 **Destination MAC Address** 覈取方塊，將目標MAC地址與乙太網幀進行比較，然後在 *Destination MAC Address* 欄位中輸入目標MAC地址。

Action:

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

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

Action:

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

步驟11。(可選)選中VLAN ID覈取方塊以將VLAN ID與乙太網幀進行比較。在VLAN ID欄位中輸入所需的VLAN ID，範圍從0到4095。

Action:

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

步驟12。(可選)若要刪除已設定的ACL，請勾選Delete ACL 覈取方塊。

步驟13.按一下「Save」。