

在WAP121和WAP321存取點上建立和設定基於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，這些條件提供安全保護並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可以阻止任何訪問網路資源的無保證嘗試。MAC ACL是第2層ACL。網路裝置檢查幀並檢查ACL規則，以檢查幀內容，如源MAC地址和目的MAC地址。如果任何規則與內容匹配，則對幀執行允許或拒絕操作。

本文說明如何在WAP121和WAP321存取點(WAP)上建立和設定MAC ACL。

適用裝置

- WAP121
- WAP321

軟體版本

- v1.0.3.4

建立基於MAC的ACL

步驟1.登入到Access Point Configuration Utility，然後選擇Client QoS > ACL。ACL頁面隨即開啟：

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type:

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 255)

Source IPv6 Address: Source IPv6 Prefix Length: (Range: 1 - 128)

Source Port: Select From List: Match to Port: (Range: 0 - 65535)

Destination IPv6 Address: Destination IPv6 Prefix Length: (Range: 1 - 128)

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

IPv6 Flow Label: (Range: 00000 - FFFFF)

IPv6 DSCP: Select From List: Match to Value: (Range: 0 - 63)

Delete ACL:

建立基於MAC的ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type:

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。

步驟3.按一下Add ACL建立新的MAC ACL。

為基於MAC的ACL配置規則

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

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1.從ACL Name - ACL Type 下拉選單中選擇所需的ACL。

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，從Rule下拉式清單中選擇其中一個目前規則。

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。

- 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11是可選的。已啟用選中的篩選條件。如果您不希望過濾器應用於此特定規則，請取消選中該過濾器的覈取方塊。

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，而不管其內容如何。取消選中Match Every Packet覈取方塊以配置任何其他匹配條件。

Timesaver：如果選中Match Every Packet，則跳至[步驟12](#)。

步驟5.選中EtherType覈取方塊，將匹配條件與乙太網幀報頭中的值進行比較。如果選中EtherType覈取方塊，請按一下以下單選按鈕之一。

- 從清單中選擇 — 從下拉選單中選擇協定。下拉選單中包含appletalk、arp、ipv4、ipv6、ipx、netbios、pppoe。
- 與值匹配 — 用於自定義協定識別符號。輸入從0600到FFFF的識別符號。

步驟6.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「服務類別」欄位中輸入從0到7的優先順序。

步驟7.選中源MAC地址覈取方塊以將源MAC地址與乙太網幀進行比較，並在源MAC地址欄位中輸入源MAC地址。

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。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。

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

步驟10.在 *目標MAC掩碼* 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。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。

步驟11.選中 **VLAN ID** 覈取方塊以將VLAN ID與乙太網幀進行比較。在 *VLAN ID* 欄位中輸入範圍從0到4095的VLAN ID。

附註：有關如何建立新VLAN的資訊，請參閱在 *WAP121* 和 *WAP321* 上 *配置管理和未標籤的VLAN ID*。

[步驟12](#).按一下 **Save** 以儲存設定。

步驟13。（可選）若要刪除已設定的ACL，請勾選 **Delete ACL** 覈取方塊，然後按一下 **Save**。