WAP371上的ACL規則配置

目標

網路訪問控制清單(ACL)是可選的安全層，充當防火牆，用於控制進出子網的流量。訪問清單是出於多種原因提供安全性的允許和拒絕條件或規則的集合。例如，這些規則可以阻止未經授權的使用者，允許授權使用者訪問特定資源，並阻止任何訪問網路資源的無保證嘗試。

本文檔的目標是向您展示如何在WAP 371上配置ACL規則。

適用裝置

·WAP371

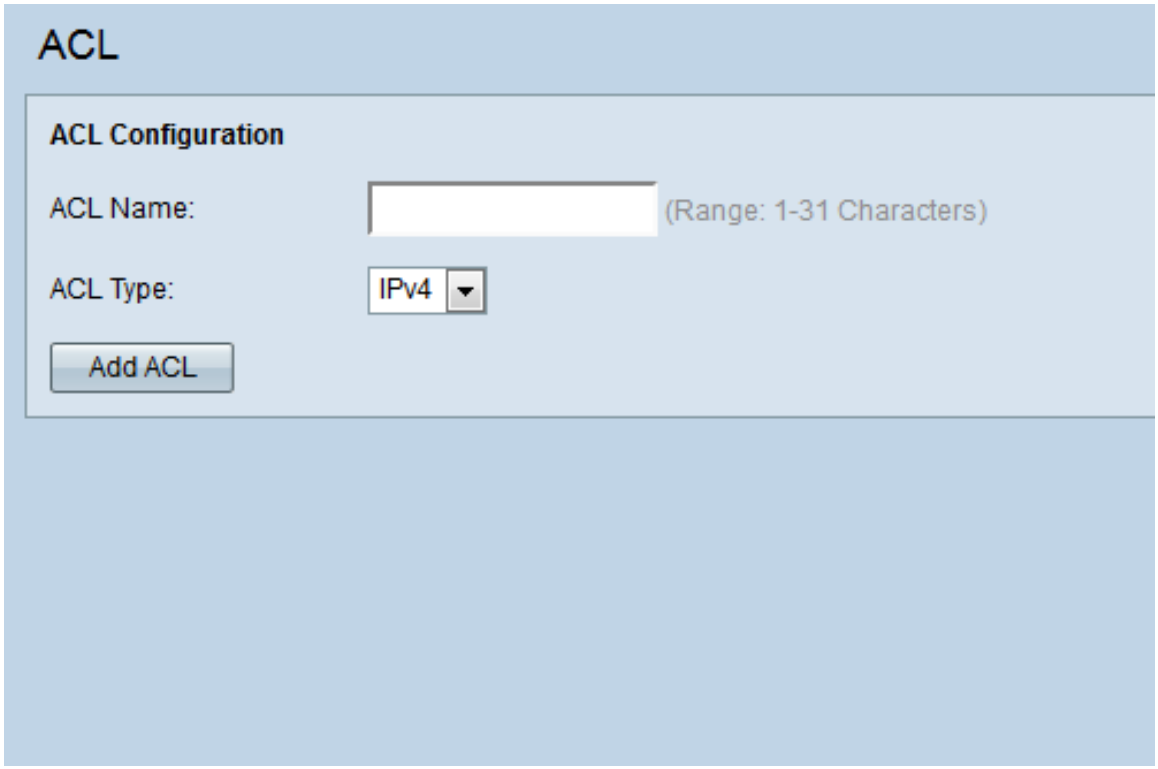
軟體版本

·v1.2.0.2

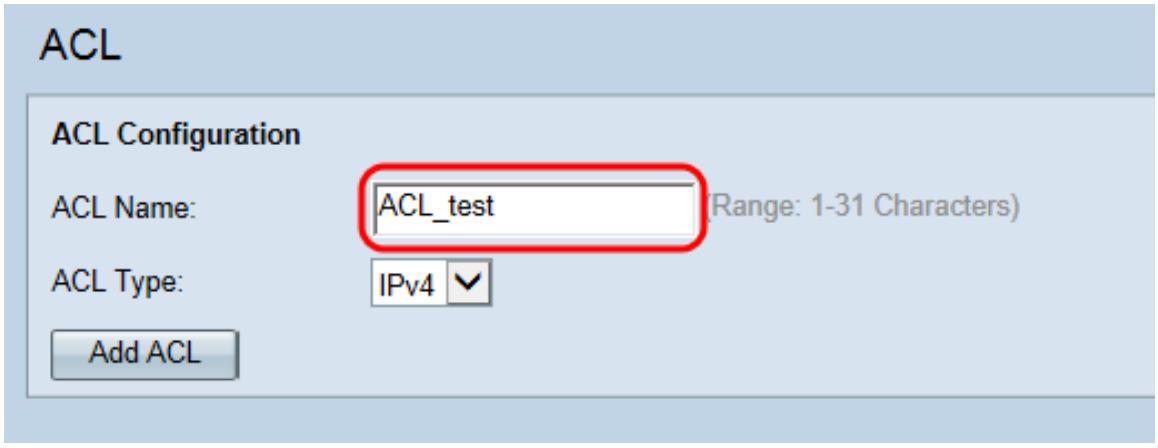
ACL規則配置

ACL配置

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：

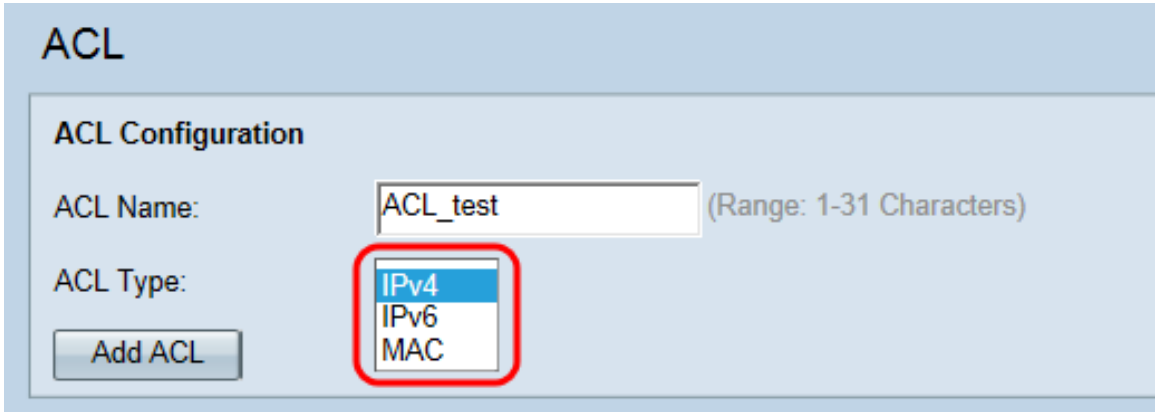


步驟2.在*ACL Name*欄位中輸入所需的ACL名稱。範圍為1-31個字元。



附註：ACL名稱是特定ACL的識別碼；對裝置的操作沒有影響。

步驟3.從*ACL Type*下拉選單中選擇ACL型別。



選項如下：

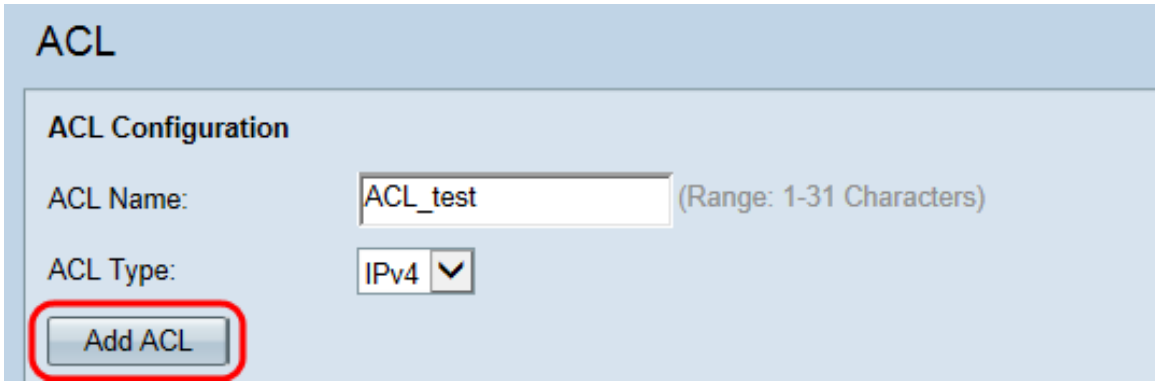
·IPv4 - 32位（4位元組）地址。

·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。

附註：IPv4和IPv6 ACL根據第3層和第4層標準控制對網路資源的訪問。MAC ACL根據第2層標準控制訪問。

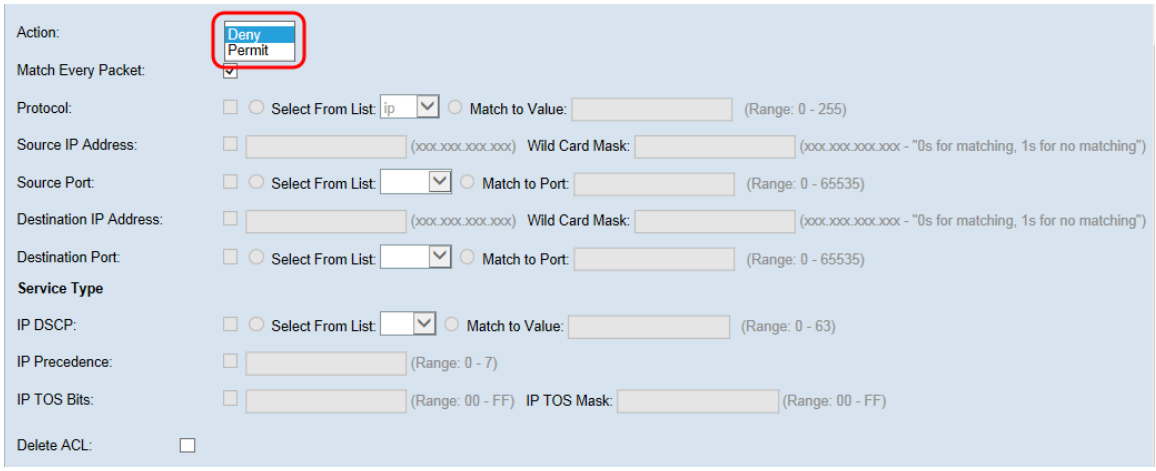
步驟4.按一下**Add ACL**以新增新的ACL。



IPv4和IPv6的ACL規則配置

附註：以下截圖用於IPv4 ACL規則，但可與IPv6 ACL規則互換。

步驟1.從*操作*下拉選單中選擇規則的操作。

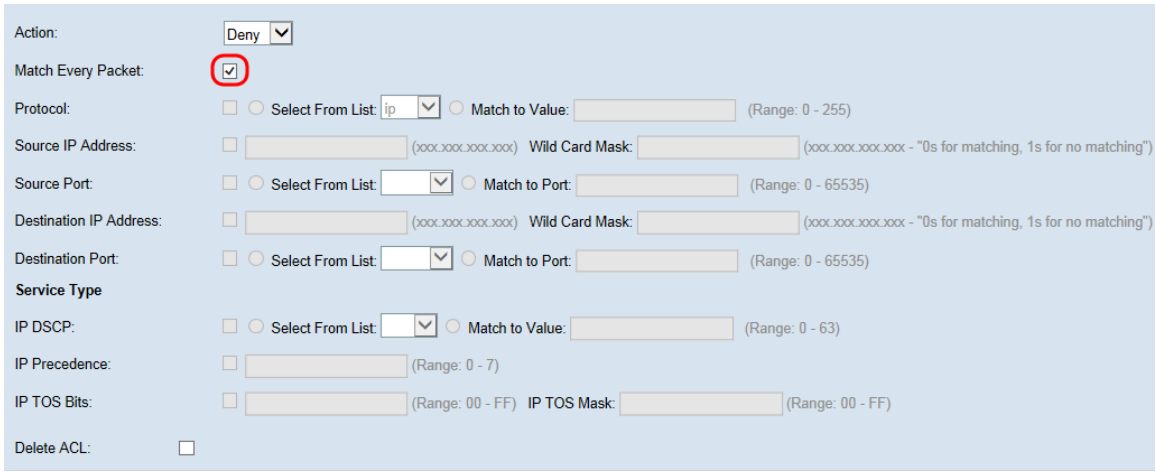


這些選項說明如下：

·允許 — 規則允許符合規則條件的所有流量進入或退出WAP裝置。不符合條件的流量將被丟棄。

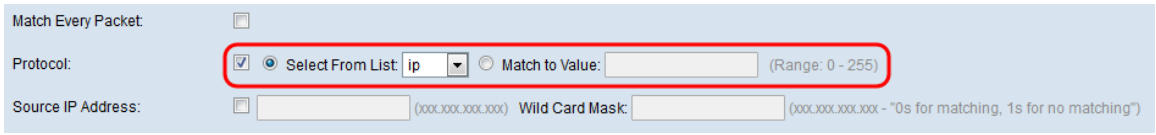
·拒絕 — 規則阻止符合規則標準的所有流量進入或退出WAP裝置。不符合標準的流量將轉發到下一個規則。如果這是最終規則，則不會明確允許的流量會遭到捨棄。

步驟2.選中或取消選中**Match Every Packet**覈取方塊。如果選中該選項，則無論幀或資料包的內容如何，該規則都會與幀或資料包匹配，其中包含permit或deny操作。



附註：如果選擇此欄位，則無法配置任何其他匹配條件。預設情況下，會為新規則選擇**Match Every Packet**選項。必須清除該選項才能配置其他匹配欄位。

步驟3.選中**Protocol** 覈取方塊，根據IPv4資料包中的IP協定欄位值或IPv6資料包中的Next Header欄位值使用L3或L4協定匹配條件。如果選中「協定」覈取方塊，請選擇以下單選按鈕之一。



這些選項說明如下：

·從清單中選擇 — 從*從清單中選擇*下拉選單中選擇協定。選項如下：

- IP - Internet協定(IP)是Internet協定套件中的主要通訊協定，用於通過網路中繼資料。

- ICMP — 網際網路控制訊息通訊協定(ICMP)是網際網路通訊協定套件中的通訊協定，路由器等裝置使用該通訊協定來傳送錯誤訊息。

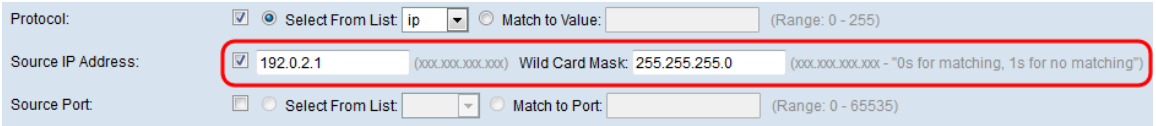
- IGMP — 網際網路組管理協定(IGMP)是主機用於在IPv4網路上建立組播組成員資格的通訊協定。

- TCP — 傳輸控制協定(TCP)使兩台主機能夠建立連線並交換資料流。

- UDP — 使用者資料包協定是網際網路協定簇中使用無連線傳輸模型的協定。

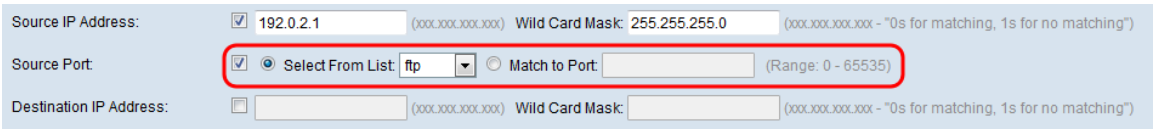
·與值匹配 — 為所有未列出的協定輸入標準IANA分配的協定ID，範圍從0到255。有關IANA分配的協定ID的詳細資訊，請參閱*分配的網際網路協定號*。

步驟4.選中**Source IP Address**覈取方塊以在匹配條件中包含源的IP地址。在各自的欄位中輸入源的IP地址和萬用字元掩碼。萬用字元掩碼確定使用源地址的哪些位以及忽略哪些位。可以將其視為反向子網掩碼。這對於指示某些路由協定的網路或子網大小，或者允許或拒絕IP地址範圍非常有用。



附註：如果選中了**Source IP Address** 覈取方塊，則需要Wild Card Mask欄位。

步驟5.勾選**Source Port** 覈取方塊以在匹配條件中包含來源連線埠。如果勾選「**Source Port**」覈取方塊，請選擇以下單選按鈕之一。



這些選項說明如下：

·從清單中選擇 — 從*從清單中選擇*下拉選單中選擇源埠。選項如下：

- FTP — 檔案傳輸通訊協定(FTP)是一種標準網路通訊協定，用於透過基於TCP的網路（例如網際網路）將檔案從一台主機傳輸到另一台主機。

- FTP資料 — 由連線到客戶端的伺服器啟動的資料通道，通常通過埠20。

- HTTP — 超文本傳輸協定(HTTP)是一種應用協定，它是全球資訊網資料通訊的基礎。

- SMTP — 簡單郵件傳輸協定(SMTP)是用於傳輸電子郵件（電子郵件）的Internet標準。

- SNMP — 簡單網路管理協定(SNMP)是Internet標準協定，用於管理IP網路上的裝置。

- Telnet — 在Internet或區域網中使用的會話層協定，用於提供雙向互動式面向文本的通訊。

- TFTP — 簡單式檔案傳輸通訊協定(TFTP)是一種用於傳輸檔案的Internet軟體公用程式，其使用比FTP更簡單，但功能更少。

- WWW — 全球資訊網是一個支援HTTP格式文檔的網際網路伺服器系統。

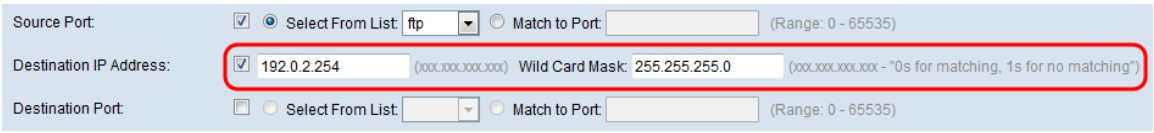
·Match to Port — 為未列出的源埠在*Match to Port*欄位中輸入範圍從0到65535的埠號。該範圍包括三種不同型別的埠。範圍描述如下：

- 0到1023 — 公認埠。

- 1024到49151 — 註冊埠。

- 49152 to 65535 — 動態和/或專用埠。

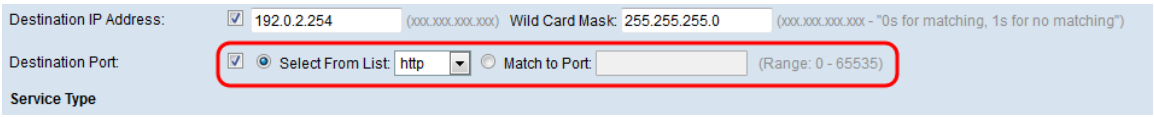
步驟6.選中**Destination IP Address**覈取方塊，將目標的IP地址包括在匹配條件中。在各自的欄位中輸入目標的IP地址和萬用字元掩碼。萬用字元掩碼確定使用源地址的哪些位以及忽略哪些位。可以將其視為反向子網掩碼。這對於指示某些路由協定的網路或子網大小，或者允許或拒絕IP地址範圍非常有用。



附註：如果選中**Destination IP Address**覈取方塊，則需要*Wild Card Mask*欄位。

附註：如果希望僅匹配單個IP地址，請使用萬用字元掩碼0.0.0.0。

步驟7.勾選「**Destination Port**」覈取方塊以在匹配條件中包含目的地連線埠。如果選中**Destination Port**覈取方塊，請選擇以下單選按鈕之一。



這些選項說明如下：

·從清單中選擇 — 從*從清單中選擇*下拉選單中選擇目標埠。下拉選單選項如下所示：

- FTP — 檔案傳輸通訊協定(FTP)是一種標準網路通訊協定，用於透過基於TCP的網路（例如網際網路）將檔案從一台主機傳輸到另一台主機。

- FTP資料 — 由連線到客戶端的伺服器啟動的資料通道，通常通過埠20。

- HTTP — 超文本傳輸協定(HTTP)是一種應用協定，它是全球資訊網資料通訊的基礎。

- SMTP — 簡單郵件傳輸協定(SMTP)是用於傳輸電子郵件（電子郵件）的Internet標準。

- SNMP — 簡單網路管理協定(SNMP)是Internet標準協定，用於管理IP網路上的裝置。

- Telnet — 在Internet或區域網中使用的會話層協定，用於提供雙向互動式面向文本的通訊。

- TFTP — 簡單式檔案傳輸通訊協定(TFTP)是一種用於傳輸檔案的Internet軟體公用程式，其使用比FTP更簡單，但功能更少。

- WWW — 全球資訊網是一個支援HTTP格式文檔的網際網路伺服器系統。

·與埠匹配 — 在未列出的目標埠的*與埠匹配*欄位中輸入範圍從0到65535的埠號。該範圍包括三種不同型別的埠。範圍描述如下：

- 0到1023 — 公認埠。

- 1024到49151 — 註冊埠。

- 49152 to 65535 — 動態和/或專用埠。

附註：只能從「服務型別」區域選擇一項服務，並且只能為匹配條件新增這些服務。

IPv4的ACL規則服務型別配置

步驟1.選中**IP DSCP**覈取方塊以根據IP DSCP值匹配資料包。DSCP用於指定幀的IP報頭上的流量優先順序。這將使用您從清單中選擇的IP DSCP值對關聯流量流的所有資料包進行分類。如果選中IP DSCP覈取方塊，請選擇以下單選按鈕之一。

這些選項說明如下：

·從清單中選擇 — 從*從清單中選擇*下拉選單中選擇IP DSCP值。選項如下：

- DSCP保證轉發(AS) — 允許運營商提供傳送保證，只要流量不超過某個訂閱速率。

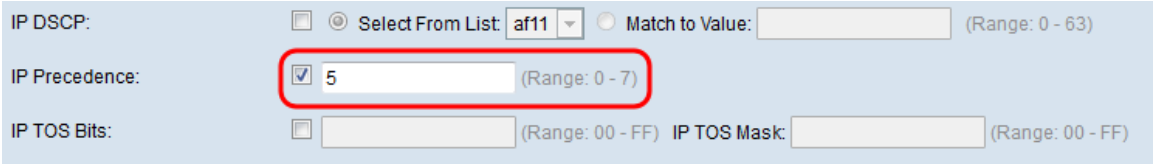
— 服務類別(CS) — 允許與仍然使用「優先順序」欄位的網路裝置向後相容。

— 加速轉發(EF) — 用於通過DS(DiffServ)域構建低丟失、低延遲、低抖動、有保證的頻寬、端到端服務。

·Match to Value — 在*Match to Value*欄位中輸入範圍從0到63的DSCP值以自定義DSCP值。

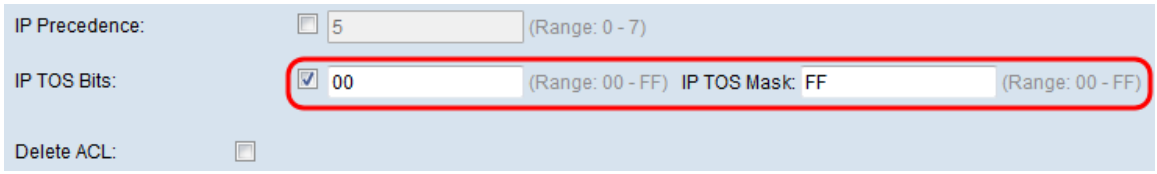
附註：有關DSCP的詳細資訊，請參閱*DSCP和優先順序值*。

步驟2.選中**IP Precedence復**選框以在匹配條件中包含IP Precedence值。這是一種為每個IP資料包分配優先順序的機制，其中0是最低優先順序，7是最高優先順序。如果勾選「**IP Precedence**」覈取方塊，請輸入一個範圍從0到7的IP優先順序值。



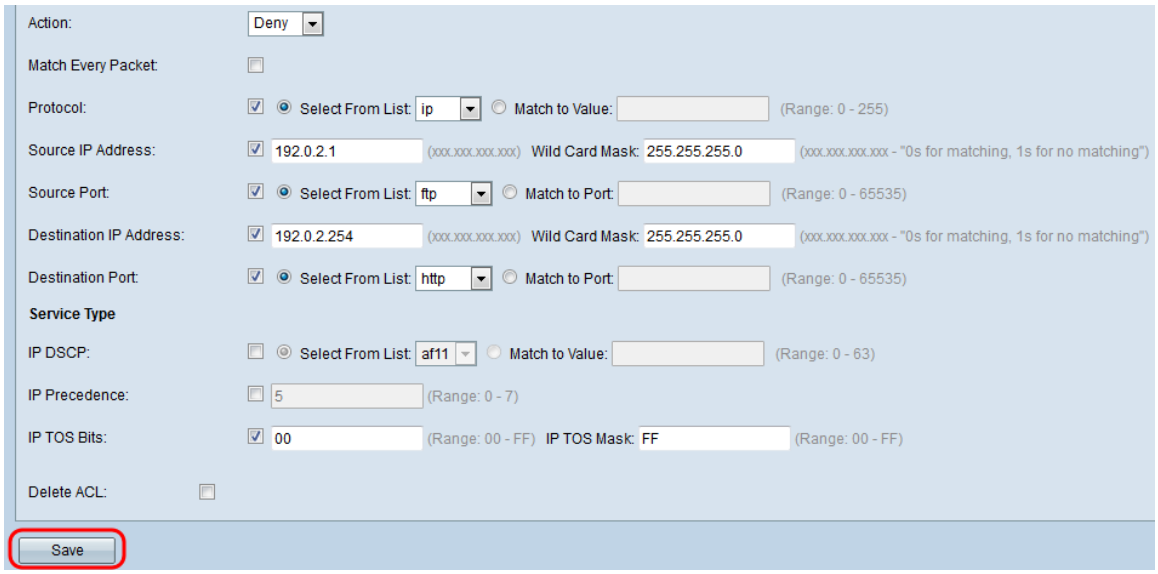
附註：有關IP優先*級的詳細資訊，請參閱DSCP和優先順序值*。

步驟3.選中**IP TOS Bits** 覈取方塊，將IP報頭中的資料包服務型別(TOS)位用作匹配條件。TOS欄位用於指定資料包的優先順序並相應地對其進行路由。如果選中IP TOS Bits覈取方塊，請在各自的欄位中輸入範圍介於00-FF和00-FF的IP TOS掩碼。



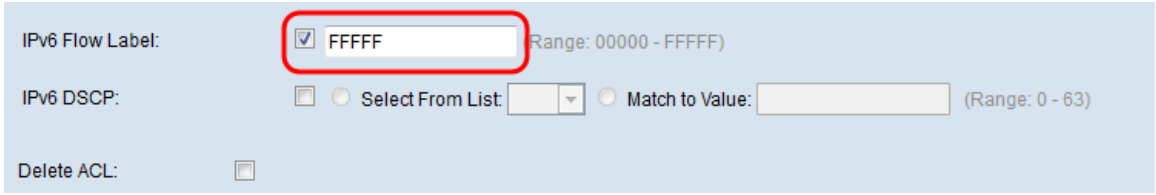
步驟4。（可選）如果要刪除已配置的ACL，請選中**Delete ACL**覈取方塊。

步驟5.按一下「**Save**」以儲存設定。

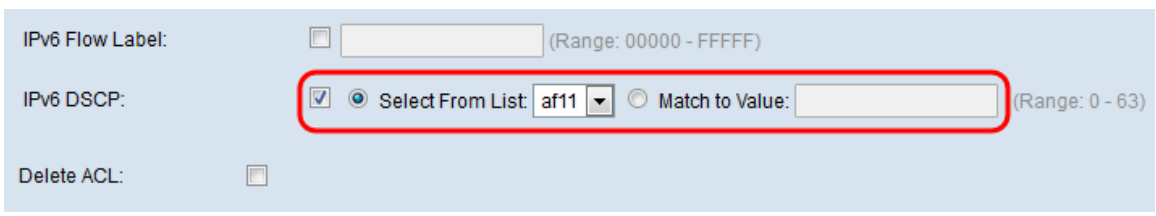


IPv6的ACL規則配置

步驟1.選中**IPv6流標籤**覈取方塊以設定IPv6資料包唯一的20位編號。終端站用它來表示路由器(範圍0到1048575)中的QoS處理。



步驟2.選中**IPv6 DSCP**覈取方塊以根據IP DSCP值匹配資料包。DSCP用於指定幀的IP報頭上的流量優先順序。這將使用您從清單中選擇的IP DSCP值對關聯流量流的所有資料包進行分類。如果選中**IPv6 DSCP**覈取方塊，請選擇以下單選按鈕之一。



這些選項說明如下：

·從清單中選擇 — 從*從清單中選擇*下拉選單中選擇IP DSCP值。選項如下：

- DSCP保證轉發(AS) — 允許運營商提供傳送保證，只要流量不超過某個訂閱速率。

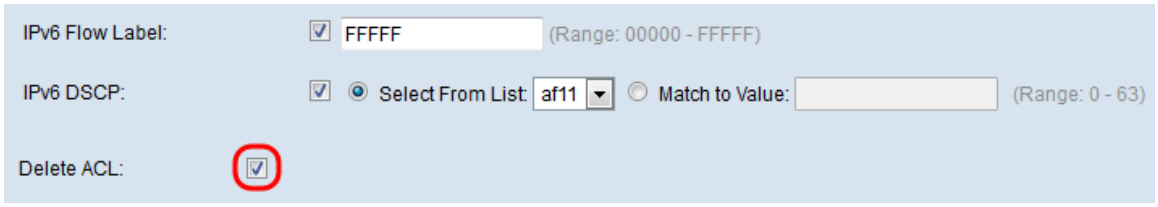
— 服務等級(CS) — 允許與仍然使用「優先順序」欄位的網路裝置向後相容。

— 加速轉發(EF) — 用於通過DS(DiffServ)域構建低丟失、低延遲、低抖動、有保證的頻寬、端到端服務。

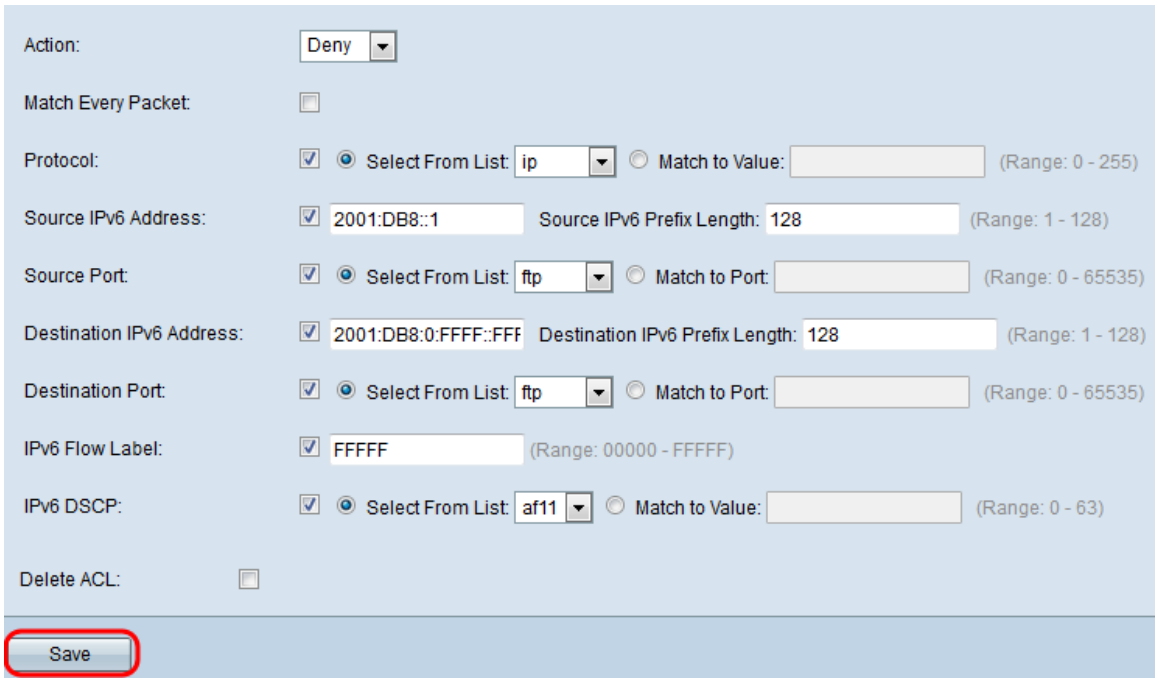
·Match to Value — 在*Match to Value*欄位中輸入範圍從0到63的DSCP值以自定義DSCP值。

附註：有關DSCP的*詳細資訊，請參閱DSCP和優先順序值*。

步驟3.（可選）如果要刪除已配置的ACL，請選中**Delete ACL**覈取方塊。

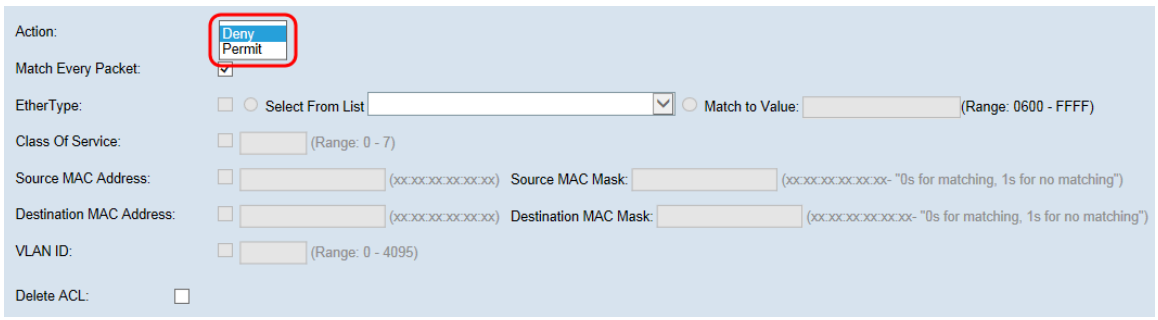


步驟4.按一下**Save**以儲存設定。



MAC的ACL規則配置

步驟1.從*操作*下拉選單中選擇規則的操作。

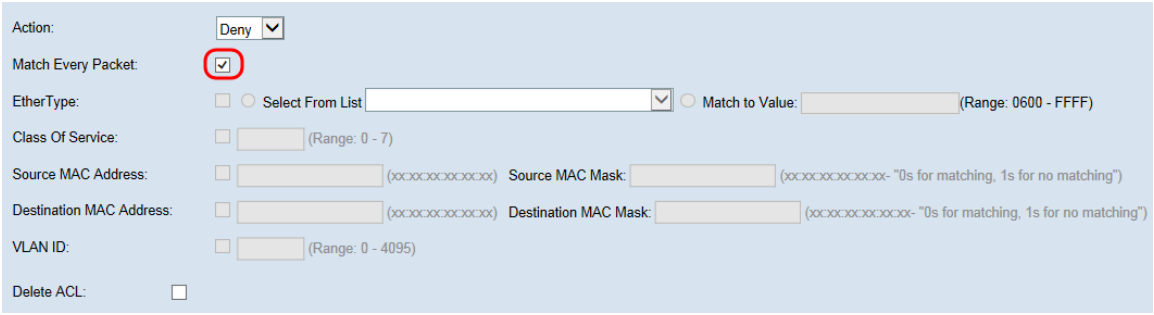


這些選項說明如下：

·允許 — 規則允許符合規則條件的所有流量進入或退出WAP裝置。不符合條件的流量將被丟棄。

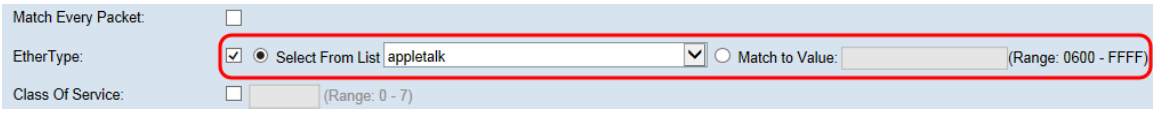
·拒絕 — 規則阻止符合規則標準的所有流量進入或退出WAP裝置。不符合標準的流量將轉發到下一個規則。如果這是最終規則，則不會明確允許的流量會遭到捨棄。

步驟2.選中或取消選中**Match Every Packet**覈取方塊。如果選中該選項，則無論幀或資料包的內容如何，該規則都會與幀或資料包匹配，其中包含permit或deny操作。



附註：如果選擇此欄位，則無法配置任何其他匹配條件。預設情況下，會為新規則選擇**Match Every Packet**選項。必須清除該選項才能配置其他匹配欄位。

步驟3.選中**Ether Type**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**Ether Type**覈取方塊，請選擇以下單選按鈕之一。



這些選項說明如下：

·從清單中選擇 — 從*從清單中選擇*下拉選單中選擇協定。選項如下：

- AppleTalk - AppleTalk是Apple Inc.為其Macintosh電腦開發的專有網路協定套件。AppleTalk包括許多功能，這些功能允許無需預先設定或需要任何型別的集中式路由器或伺服器即可連線區域網。

- ARP — 位址解析通訊協定(ARP)是一種電信通訊協定，用於將網路層位址解析為連結層位址，這是多重存取網路中的關鍵功能。

- IPv4 — 網際網路協定第4版(IPv4)是網際網路協定(IP)開發的第四個版本。 它是Internet中基於標準的互聯方法的核心協定之一。

- IPv6 - Internet協定第6版(IPv6)是Internet協定(IP)的最新版本，IP是一種通訊協定，為網路上的電腦提供識別和定位系統，並通過Internet路由流量。

- IPX — 網際網路資料包交換(IPX)是IPX/SPX協定簇中的網路層協定。IPX源自Xerox網路系統的IDP。它還可以充當傳輸層協定。

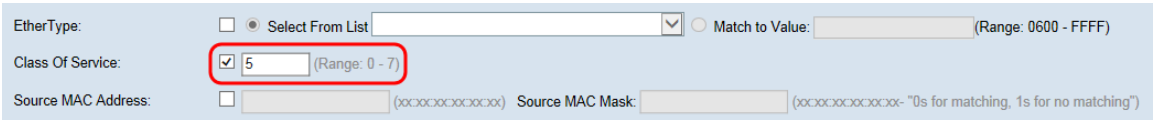
- NetBIOS - NetBIOS是網路基本輸入/輸出系統的縮寫。它提供與OSI模型的會話層相關的服務，允許不同電腦上的應用程式通過區域網進行通訊。嚴格來說，NetBIOS不是網路協定。

- PPPOE — 乙太網路上的點對點通訊協定(PPPoE)是一種網路通訊協定，用於將PPP訊框

封裝在乙太網路訊框內。

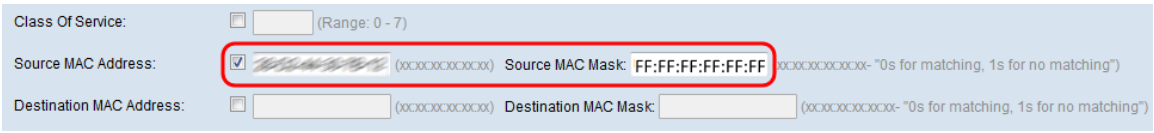
·與值匹配 — 輸入與資料包匹配的自定義協定識別符號。該值是一個四位數十六進位制數，範圍為0600到FFFF。

步驟4.選中**Class of Service復**選框以輸入802.1p使用者優先順序與乙太網幀進行比較。與IP優先順序一樣，0是最低優先順序，7是最高優先順序。有效範圍為0到7。

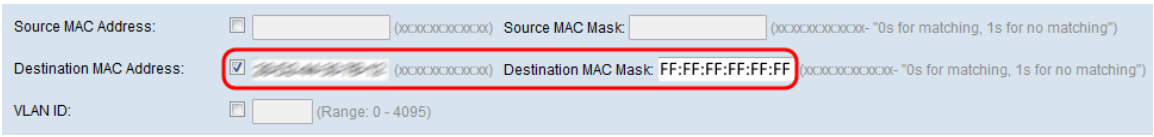


步驟5.選中**Source MAC Address**覈取方塊以輸入與乙太網幀進行比較的源MAC地址。如果選中源MAC地址覈取方塊，請在*源MAC地址*欄位中輸入源MAC地址。然後在*Source MAC Mask*欄位中輸入源MAC地址掩碼。這將指定將源MAC地址中的哪些位與乙太網幀進行比較。

附註：如果希望只匹配單個MAC地址，請使用萬用字元掩碼00:00:00:00:00:00。

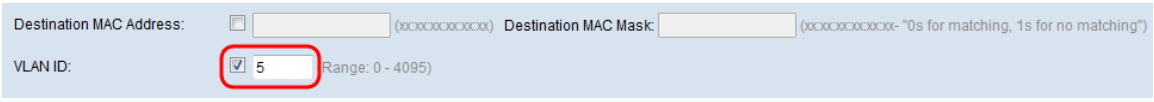


步驟6.選中**Destination MAC Address復**選框以輸入與乙太網幀比較的目標MAC地址。如果選中目標MAC地址覈取方塊，請在「目標MAC地址」欄位中輸入*目標MAC*地址。然後在*Destination MAC Mask*欄位中輸入*MAC地址掩*碼。這將指定將目標MAC地址中的哪些位與乙太網幀進行比較。

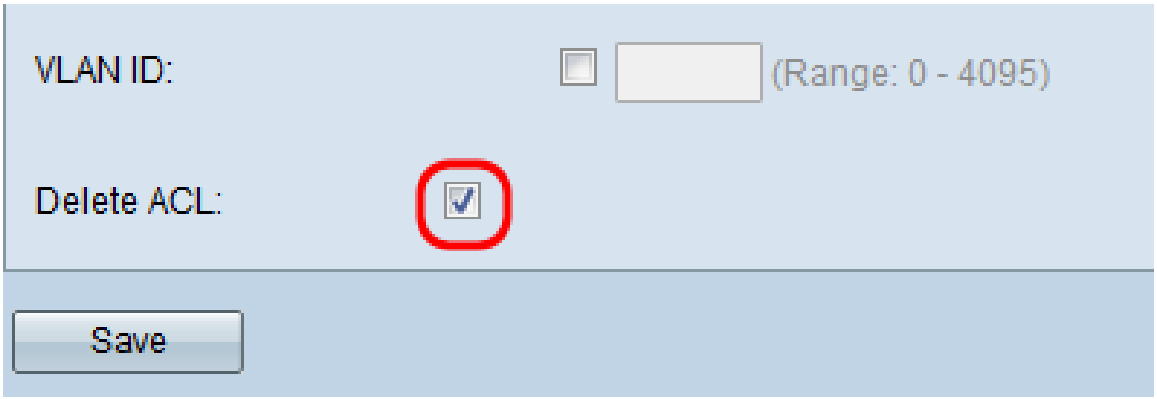


附註：如果希望只匹配單個MAC地址，請使用萬用字元掩碼00:00:00:00:00:00。

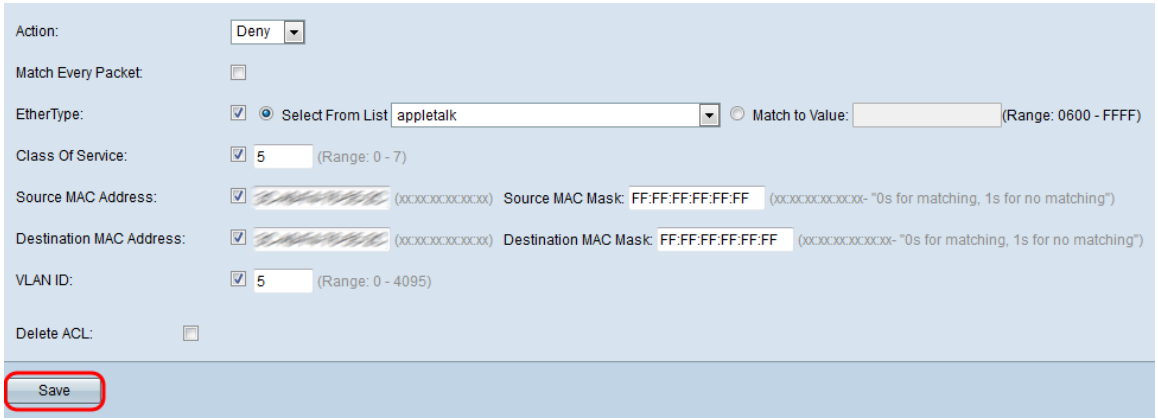
步驟7.選中**VLAN ID** 覈取方塊以輸入VLAN ID與乙太網幀進行比較。如果勾選「**VLAN ID**」覈取方塊，請在「*VLAN ID*」欄位中輸入VLAN ID。VLAN ID的範圍是從0到4095。



步驟8。（可選）如果要刪除已配置的ACL，請選中**Delete ACL**覈取方塊。



步驟9.按一下**Save**以儲存設定。


Action:
Deny
Match Every Packet:
EtherType:
Select From List
appletalk
Match to Value:
(Range: 0600 - FFFF)
Class Of Service:
5
(Range: 0 - 7)
Source MAC Address:
(xx:xx:xx:xx:xx:xx)
Source MAC Mask:
FF:FF:FF:FF:FF:FF
(xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
Destination MAC Address:
(xx:xx:xx:xx:xx:xx)
Destination MAC Mask:
FF:FF:FF:FF:FF:FF
(xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
VLAN ID:
5
(Range: 0 - 4095)
Delete ACL:
Save