

Configurazione della regola ACL su WAP371

Obiettivo

Un elenco di controllo di accesso (ACL, Network Access Control List) è un livello di protezione facoltativo che funge da firewall per il controllo del traffico in entrata e in uscita da una subnet. Gli elenchi di accesso sono raccolte di condizioni di autorizzazione e negazione, o regole, che offrono protezione per diversi motivi. Queste regole possono ad esempio bloccare utenti non autorizzati, consentire agli utenti autorizzati di accedere a risorse specifiche e bloccare qualsiasi tentativo non giustificato di raggiungere risorse di rete.

Lo scopo di questo documento è mostrare come configurare le regole ACL su WAP 371.

Dispositivi interessati

·WAP371

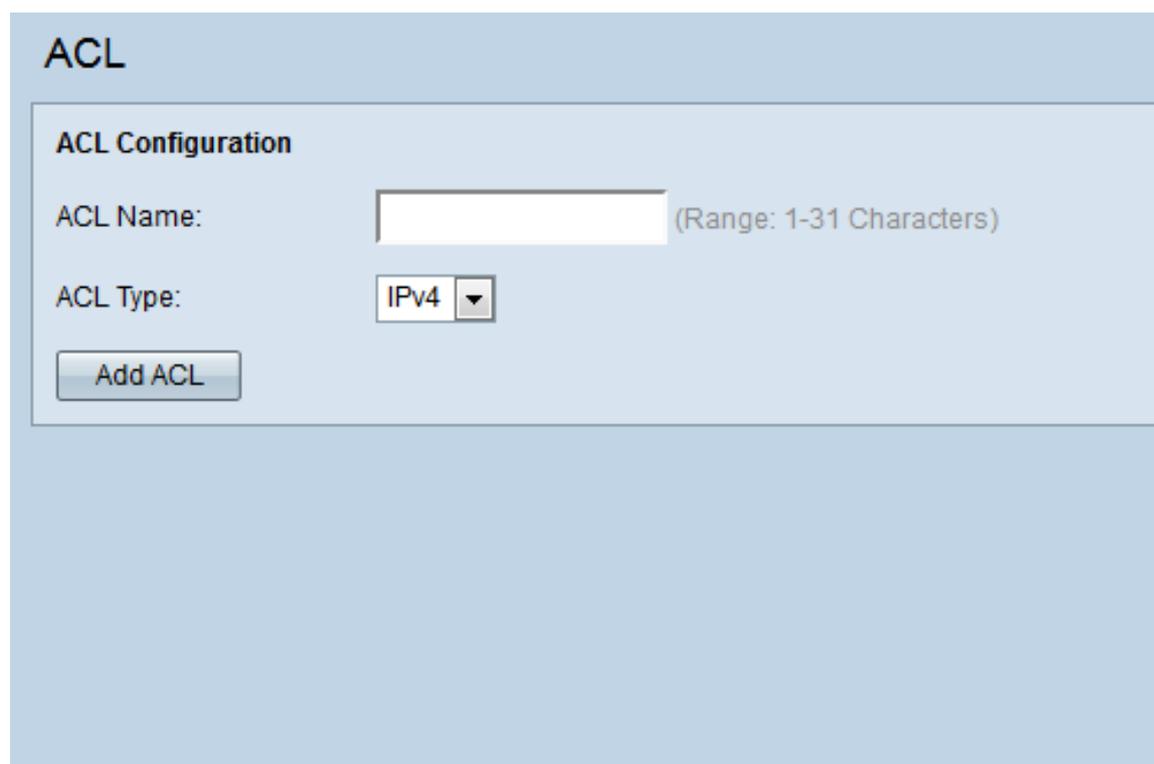
Versione del software

·v1.2.0.2

Configurazione regola ACL

Configurazione ACL

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **QoS client > ACL**. Viene visualizzata la pagina *ACL*:



The screenshot shows a web interface for configuring ACLs. The page title is "ACL". Below the title, there is a section titled "ACL Configuration". This section contains two input fields: "ACL Name:" with a text box and a note "(Range: 1-31 Characters)", and "ACL Type:" with a dropdown menu currently set to "IPv4". At the bottom of this section, there is a button labeled "Add ACL".

Passaggio 2. Inserire il nome dell'ACL desiderato nel campo *Nome ACL*. L'intervallo è

compreso tra 1 e 31 caratteri.

The screenshot shows the 'ACL Configuration' section of a network device's web interface. The 'ACL Name' field contains the text 'ACL_test' and is circled in red. To its right, the text '(Range: 1-31 Characters)' is displayed. Below this, the 'ACL Type' dropdown menu is set to 'IPv4'. At the bottom left of the configuration area, there is a button labeled 'Add ACL'.

Nota: Il nome ACL è un identificatore dell'ACL specifico; non ha alcun impatto sul funzionamento del dispositivo.

Passaggio 3. Selezionare il tipo di ACL dall'elenco a discesa *ACL Type (Tipo di ACL)*.

This screenshot shows the 'ACL Configuration' section with the 'ACL Name' field set to 'ACL_test'. The 'ACL Type' dropdown menu is open, showing three options: 'IPv4', 'IPv6', and 'MAC'. The 'IPv4' option is highlighted with a blue background and is circled in red. The 'Add ACL' button is visible at the bottom left.

Le opzioni sono le seguenti:

- IPv4 - Un indirizzo a 32 bit (quattro byte).
- IPv6 - Successore di IPv4, costituito da un indirizzo a 128 bit (8 byte).
- MAC - L'indirizzo MAC è l'indirizzo univoco assegnato a un'interfaccia di rete.

Nota: Gli ACL IPv4 e IPv6 controllano l'accesso alle risorse di rete in base ai criteri di layer 3 e layer 4. Gli ACL MAC controllano l'accesso in base ai criteri del layer 2.

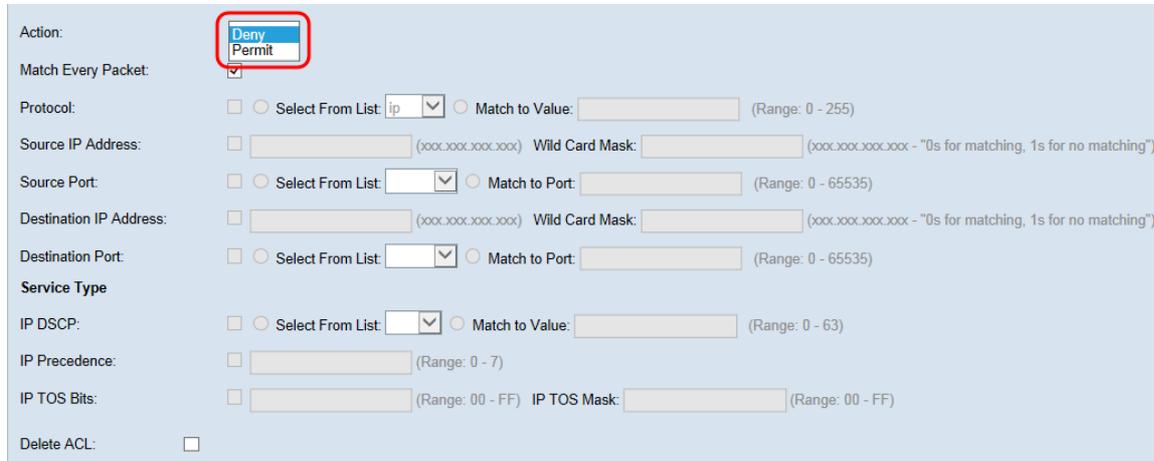
Passaggio 4. Per aggiungere il nuovo ACL, fare clic su **Add ACL**.

This screenshot shows the 'ACL Configuration' section with the 'ACL Name' field set to 'ACL_test' and the 'ACL Type' dropdown set to 'IPv4'. The 'Add ACL' button at the bottom left is circled in red.

Configurazione regola ACL per IPv4 e IPv6

Nota: Le schermate seguenti fanno riferimento alle regole ACL IPv4 ma sono intercambiabili con le regole ACL IPv6.

Passaggio 1. Selezionare un'azione per la regola dall'elenco a discesa *Azione*.



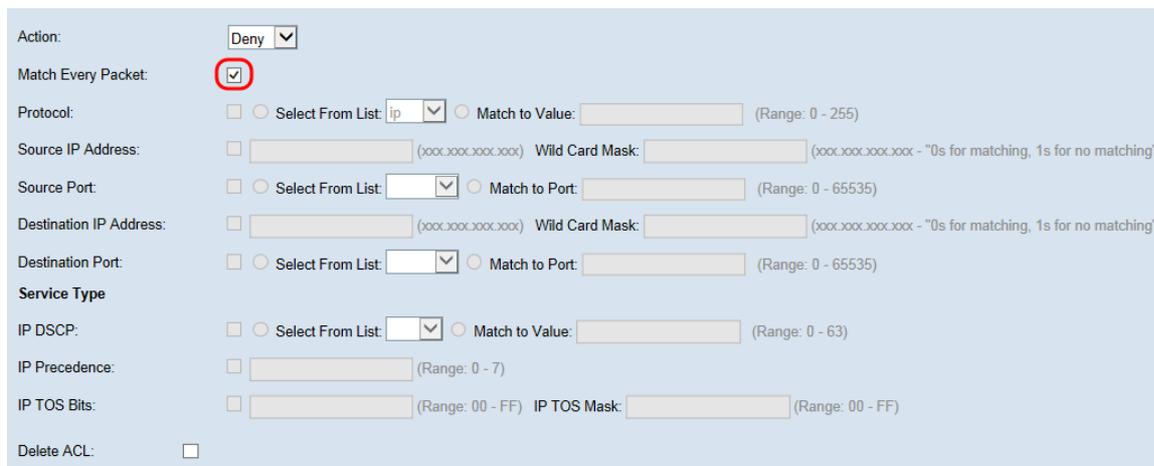
The screenshot shows the configuration interface for an ACL rule. The 'Action' dropdown menu is open, showing 'Deny' and 'Permit' options. The 'Deny' option is highlighted with a red box. Below the 'Action' dropdown, there are several configuration fields: 'Match Every Packet' (checked), 'Protocol' (ip), 'Source IP Address' (with Wild Card Mask), 'Source Port' (with Match to Port), 'Destination IP Address' (with Wild Card Mask), 'Destination Port' (with Match to Port), 'Service Type' (IP DSCP, IP Precedence, IP TOS Bits), and 'Delete ACL' (unchecked).

Le opzioni sono descritte come segue:

·Permit (Autorizzazione) - La regola consente a tutto il traffico che soddisfa i criteri della regola di entrare o uscire dal dispositivo WAP. Il traffico che non soddisfa i criteri viene eliminato.

·Nega - La regola impedisce l'ingresso o l'uscita dal dispositivo WAP a tutto il traffico che soddisfa i criteri della regola. Il traffico che non soddisfa i criteri viene inoltrato alla regola successiva. Se si tratta della regola finale, il traffico non autorizzato esplicitamente viene interrotto.

Passaggio 2. Selezionare o deselezionare la casella di controllo **Confronta ogni pacchetto**. Se l'opzione è selezionata, la regola, che prevede un'azione di autorizzazione o rifiuto, corrisponde al frame o al pacchetto indipendentemente dal relativo contenuto.



The screenshot shows the configuration interface for an ACL rule. The 'Match Every Packet' checkbox is checked and highlighted with a red box. The 'Action' dropdown menu is set to 'Deny'. Below the 'Match Every Packet' checkbox, there are several configuration fields: 'Protocol' (ip), 'Source IP Address' (with Wild Card Mask), 'Source Port' (with Match to Port), 'Destination IP Address' (with Wild Card Mask), 'Destination Port' (with Match to Port), 'Service Type' (IP DSCP, IP Precedence, IP TOS Bits), and 'Delete ACL' (unchecked).

Nota: Se si seleziona questo campo, non sarà possibile configurare ulteriori criteri di corrispondenza. L'opzione **Corrispondenza ogni pacchetto** è selezionata per impostazione predefinita per una nuova regola. È necessario deselezionare l'opzione per configurare altri campi di corrispondenza.

Passaggio 3. Selezionare la casella di controllo **Protocollo** per utilizzare una condizione di

corrispondenza del protocollo L3 o L4 in base al valore del campo Protocollo IP nei pacchetti IPv4 o al campo Intestazione successiva nei pacchetti IPv6. Se la casella di controllo Protocollo è selezionata, selezionare uno dei seguenti pulsanti di opzione.



Match Every Packet:

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

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Le opzioni sono descritte come segue:

· Select From List: consente di scegliere un protocollo dall'elenco a discesa *Select From List*. Le opzioni sono le seguenti:

- IP - Internet Protocol (IP) è il protocollo di comunicazione principale nella suite di protocolli Internet per il trasferimento di dati attraverso le reti.

- ICMP - Internet Control Message Protocol (ICMP) è un protocollo della Internet Protocol Suite utilizzato da dispositivi come i router per inviare messaggi di errore.

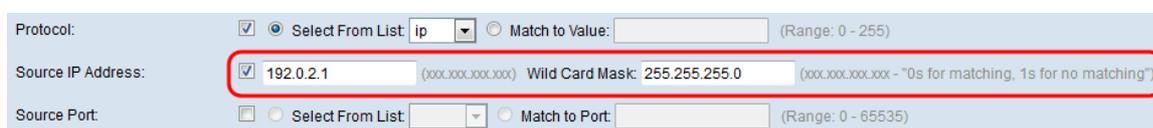
- IGMP - Internet Group Management Protocol (IGMP) è un protocollo di comunicazione utilizzato dall'host per stabilire l'appartenenza a gruppi multicast su reti IPv4.

- TCP - Il protocollo TCP (Transmission Control Protocol) consente a due host di stabilire una connessione e scambiare flussi di dati.

- UDP - User Datagram Protocol è un protocollo della suite di protocolli Internet che utilizza un modello di trasmissione senza connessione.

· Corrispondenza con il valore - Immettere un ID di protocollo standard assegnato da IANA compreso tra 0 e 255 per tutti i protocolli non elencati. Per ulteriori informazioni sugli ID di protocollo assegnati da IANA, fare riferimento a [Numeri di protocollo Internet assegnati](#).

Passaggio 4. Selezionare la casella di controllo **Source IP Address** (Indirizzo IP di origine) per includere un indirizzo IP dell'origine nella condizione di corrispondenza. Immettere l'indirizzo IP e la maschera con caratteri jolly dell'origine nei rispettivi campi. La maschera con caratteri jolly determina quali bit dell'indirizzo di origine vengono utilizzati e quali vengono ignorati. una subnet mask invertita. Questa opzione permette di indicare le dimensioni di una rete o di una subnet per alcuni protocolli di routing o di autorizzare o negare un intervallo di indirizzi IP.



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

Source IP Address: **192.0.2.1** (xxx.xxx.xxx.xxx) Wild Card Mask: **255.255.255.0** (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

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

Nota: Il campo Maschera con caratteri jolly è obbligatorio se la casella di controllo **Source IP Address** (Indirizzo IP di origine) è selezionata.

Passaggio 5. Selezionare la casella di controllo **Porta di origine** per includere una porta di origine nella condizione di corrispondenza. Se la casella di controllo **Porta di origine** è selezionata, selezionare uno dei seguenti pulsanti di opzione.

Source IP Address:	<input checked="" type="checkbox"/> 192.0.2.1	<small>(xxx.xxx.xxx.xxx)</small>	Wild Card Mask:	255.255.255.0	<small>(xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")</small>
Source Port:	<input checked="" type="checkbox"/> Select From List:	ftp	<input type="checkbox"/> Match to Port:		<small>(Range: 0 - 65535)</small>
Destination IP Address:	<input type="checkbox"/>	<small>(xxx.xxx.xxx.xxx)</small>	Wild Card Mask:		<small>(xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")</small>

Le opzioni sono descritte come segue:

·Select From List (Seleziona dall'elenco) - Consente di scegliere una porta di origine dall'elenco a discesa *Select From List (Seleziona dall'elenco)*. Le opzioni sono le seguenti:

- FTP - File Transfer Protocol (FTP) è un protocollo di rete standard utilizzato per trasferire file da un host all'altro su una rete basata su TCP come Internet.
- Dati FTP - Canale dati avviato dal server collegato a un client, in genere tramite la porta 20.
- HTTP - Il protocollo HTTP (Hypertext Transfer Protocol) è un protocollo applicativo alla base della comunicazione dei dati per il World Wide Web.
- SMTP - Il protocollo SMTP (Simple Mail Transfer Protocol) è uno standard Internet per la trasmissione della posta elettronica.
- SNMP - Il protocollo SNMP (Simple Network Management Protocol) è un protocollo Internet standard per la gestione di dispositivi su reti IP.
- Telnet - Protocollo a livello di sessione utilizzato su Internet o nelle reti locali per fornire comunicazioni bidirezionali interattive orientate al testo.
- TFTP - Il protocollo TFTP (Trivial File Transfer Protocol) è un'utility software per il trasferimento di file su Internet, più semplice da utilizzare rispetto al protocollo FTP, ma meno capace.
- WWW - Il World Wide Web è un sistema di server Internet che supportano documenti in formato HTTP.

·Corrispondenza con porta: immettere il numero di porta compreso tra 0 e 65535 nel campo *Corrispondenza con porta* per le porte di origine non elencate. L'intervallo include tre tipi diversi di porte. Gli intervalli sono descritti come segue:

- da 0 a 1023 — Porte conosciute.
- da 1024 a 49151 — Porti registrati.
- da 49152 a 65535 — porte dinamiche e/o private.

Passaggio 6. Selezionare la casella di controllo **Indirizzo IP di destinazione** per includere l'indirizzo IP della destinazione nella condizione di corrispondenza. Immettere l'indirizzo IP e la maschera con caratteri jolly della destinazione nei rispettivi campi. La maschera con caratteri jolly determina quali bit dell'indirizzo di origine vengono utilizzati e quali vengono ignorati. una subnet mask invertita. Questa opzione permette di indicare le dimensioni di una rete o di una subnet per alcuni protocolli di routing o di autorizzare o negare un intervallo di indirizzi IP.

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

Destination IP Address: Wild Card Mask:

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

Nota: Il campo *Maschera con caratteri jolly* è obbligatorio se la casella di controllo **Indirizzo IP di destinazione** è selezionata.

Nota: Se si desidera ottenere una corrispondenza solo per un singolo indirizzo IP, utilizzare la maschera con caratteri jolly 0.0.0.

Passaggio 7. Selezionare la casella di controllo **Porta di destinazione** per includere una porta di destinazione nella condizione di corrispondenza. Se la casella di controllo **Porta di destinazione** è selezionata, selezionare uno dei seguenti pulsanti di opzione.

Destination IP Address: Wild Card Mask:

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

Service Type

Le opzioni sono descritte come segue:

- Select From List (Seleziona dall'elenco) - Consente di scegliere una porta di destinazione dall'elenco a discesa *Select From List (Seleziona dall'elenco)*. Le opzioni dell'elenco a discesa sono le seguenti:

- FTP - File Transfer Protocol (FTP) è un protocollo di rete standard utilizzato per trasferire file da un host all'altro su una rete basata su TCP come Internet.

- Dati FTP - Canale dati avviato dal server collegato a un client, in genere tramite la porta 20.

- HTTP - Il protocollo HTTP (Hypertext Transfer Protocol) è un protocollo applicativo alla base della comunicazione dei dati per il World Wide Web.

- SMTP - Il protocollo SMTP (Simple Mail Transfer Protocol) è uno standard Internet per la trasmissione della posta elettronica.

- SNMP - Il protocollo SNMP (Simple Network Management Protocol) è un protocollo Internet standard per la gestione di dispositivi su reti IP.

- Telnet - Protocollo a livello di sessione utilizzato su Internet o nelle reti locali per fornire comunicazioni bidirezionali interattive orientate al testo.

- TFTP - Il protocollo TFTP (Trivial File Transfer Protocol) è un'utility software per il trasferimento di file su Internet, più semplice da utilizzare rispetto al protocollo FTP, ma meno capace.

- WWW - Il World Wide Web è un sistema di server Internet che supportano documenti in formato HTTP.

- Corrispondenza con porta: immettere il numero di porta compreso tra 0 e 65535 nel campo *Corrispondenza con porta* per le porte di destinazione non elencate. L'intervallo include tre tipi diversi di porte. Gli intervalli sono descritti come segue:

- Da 0 a 1023 — Porte conosciute.

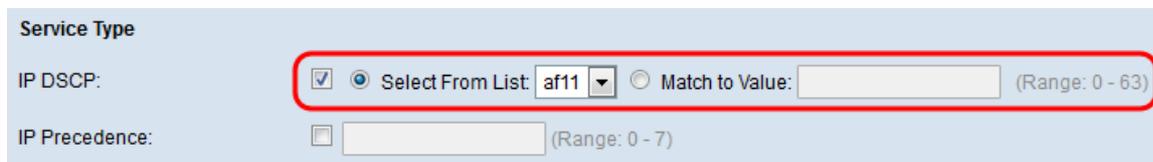
- da 1024 a 49151 — Porte registrate.

da 49152 a 65535 — porte dinamiche e/o private.

Nota: Solo uno dei servizi può essere selezionato dall'area Tipo di servizio e può essere aggiunto per la condizione di corrispondenza.

Configurazione tipo di servizio regola ACL per IPv4

Passaggio 1. Selezionare la casella di controllo **IP DSCP** per trovare una corrispondenza con i pacchetti basati sui valori IP DSCP. Il protocollo DSCP viene usato per specificare le priorità del traffico sull'intestazione IP del frame. In questo modo tutti i pacchetti per il flusso di traffico associato vengono classificati con il valore IP DSCP selezionato dall'elenco. Se la casella di controllo DSCP IP è selezionata, selezionare uno dei seguenti pulsanti di opzione.



Le opzioni sono descritte come segue:

·Select From List (Seleziona da elenco) - Consente di scegliere un valore DSCP IP dall'elenco a discesa *Select From List* (Seleziona da elenco). Le opzioni sono le seguenti:

- DSCP Assured Forwarding (AS) - Consente all'operatore di garantire la consegna, a condizione che il traffico non superi la velocità sottoscritta.

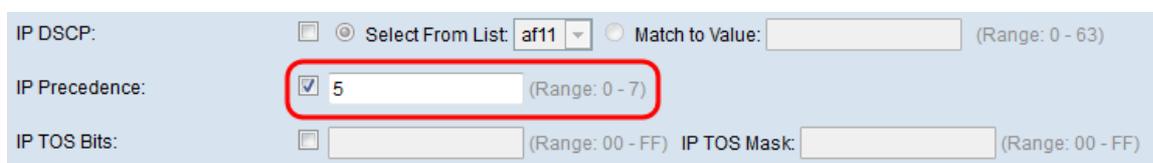
- Class of Service (CS) - Consente la compatibilità con dispositivi di rete che ancora utilizzano il campo Precedence.

- Expedited Forwarding (EF) - Utilizzato per creare una bassa perdita, bassa latenza, un basso jitter, una larghezza di banda garantita, un servizio end-to-end attraverso i domini DS (DiffServ).

·Corrispondenza con valore — immettere il valore DSCP compreso tra 0 e 63 nel campo *Corrispondenza con valore* per personalizzare i valori DSCP.

Nota: Per ulteriori informazioni su DSCP, fare riferimento a [DSCP e valori di precedenza](#).

Passaggio 2. Selezionare la casella di controllo **Precedenza IP** per includere un valore di Precedenza IP nella condizione di corrispondenza. Questo è un meccanismo che permette di assegnare una priorità a ciascun pacchetto IP dove 0 corrisponde alla priorità più bassa e 7 alla priorità più alta. Se la casella di controllo **Precedenza IP** è selezionata, immettere un valore di precedenza IP compreso tra 0 e 7.



Nota: Per ulteriori informazioni sulla [precedenza](#) IP, fare riferimento ai [valori DSCP e di precedenza](#).

Passaggio 3. Selezionare la casella di controllo **IP TOS Bits** per utilizzare i bit TOS (Type of Service) del pacchetto nell'intestazione IP come criteri di corrispondenza. Un campo TOS viene utilizzato per specificare la priorità di un datagramma e instradarlo di conseguenza. Se la casella di controllo Bit IP TOS è selezionata, immettere nei rispettivi campi i bit IP TOS compresi tra 00-FF e la maschera IP TOS compresa tra 00-FF.

IP Precedence: 5 (Range: 0 - 7)

IP TOS Bits: 00 (Range: 00 - FF) IP TOS Mask: FF (Range: 00 - FF)

Delete ACL:

Passaggio 4. (Facoltativo) Se si desidera eliminare l'ACL configurato, selezionare la casella di controllo **Elimina ACL**.

IP TOS Bits: 00 (Range: 00 - FF) IP TOS Mask: FF (Range: 00 - FF)

Delete ACL:

Passaggio 5. Fare clic su **Save** per salvare le impostazioni.

Action: Deny

Match Every Packet:

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

Source IP Address: 192.0.2.1 Wild Card Mask: 255.255.255.0

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

Destination IP Address: 192.0.2.254 Wild Card Mask: 255.255.255.0

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

Service Type

IP DSCP: Select From List: af11 Match to Value: (Range: 0 - 63)

IP Precedence: 5 (Range: 0 - 7)

IP TOS Bits: 00 (Range: 00 - FF) IP TOS Mask: FF (Range: 00 - FF)

Delete ACL:

Save

Configurazione regola ACL per IPv6

Passaggio 1. Selezionare la casella di controllo **Etichetta flusso IPv6** per impostare un numero a 20 bit univoco per un pacchetto IPv6. Viene utilizzato dalle stazioni terminali per indicare la gestione QoS nei router (intervallo da 0 a 1048575).

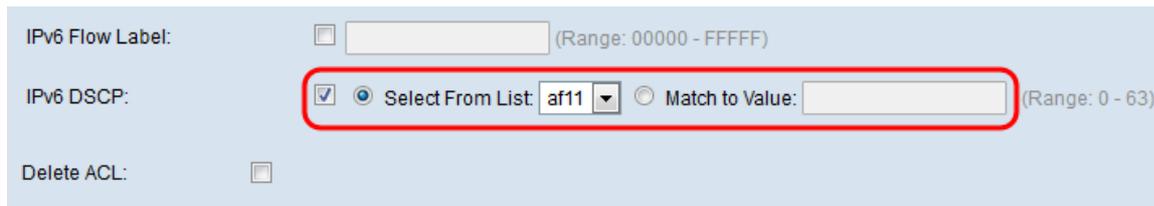
IPv6 Flow Label: FFFFF (Range: 00000 - FFFFF)

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

Delete ACL:

Passaggio 2. Selezionare la casella di controllo **DSCP IPv6** per trovare una corrispondenza con i pacchetti basati sui valori DSCP IP. Il protocollo DSCP viene usato per specificare le priorità del traffico sull'intestazione IP del frame. In questo modo tutti i pacchetti per il flusso di traffico associato vengono classificati con il valore IP DSCP selezionato dall'elenco. Se la

casella di controllo **DSCP IPv6** è selezionata, selezionare uno dei pulsanti di opzione seguenti.



The screenshot shows a configuration panel for IPv6. It includes three rows: 'IPv6 Flow Label' with a checkbox and an empty text field (range 00000 - FFFFF); 'IPv6 DSCP' with a checked checkbox, a radio button selected for 'Select From List' (dropdown menu showing 'af11'), and a radio button for 'Match to Value' with an empty text field (range 0 - 63); and 'Delete ACL' with an unchecked checkbox. A red rectangle highlights the 'Select From List' radio button and its dropdown menu.

Le opzioni sono descritte come segue:

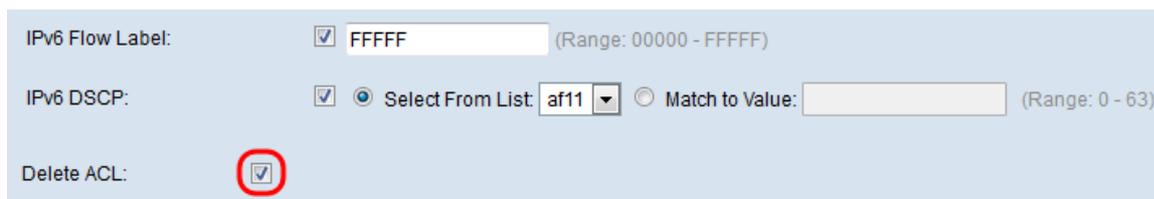
·Select From List (Seleziona da elenco) - Consente di scegliere un valore DSCP IP dall'elenco a discesa *Select From List* (Seleziona da elenco). Le opzioni sono le seguenti:

- DSCP Assured Forwarding (AS) - consente all'operatore di garantire la consegna, a condizione che il traffico non superi la velocità sottoscritta.
- Class of Service (CS) - Consente la compatibilità con dispositivi di rete che ancora utilizzano il campo Precedence.
- Expedited Forwarding (EF) - Viene utilizzato per creare una bassa perdita, bassa latenza, basso jitter, larghezza di banda garantita, servizio end-to-end attraverso i domini DS (DiffServ).

·Corrispondenza con valore — immettere il valore DSCP compreso tra 0 e 63 nel campo *Corrispondenza con valore* per personalizzare i valori DSCP.

Nota: Per ulteriori informazioni su DSCP, fare riferimento a [DSCP e valori di precedenza](#).

Passaggio 3. (Facoltativo) Se si desidera eliminare l'ACL configurato, selezionare la casella di controllo **Elimina ACL**.



The screenshot shows the same configuration panel as above, but with the 'Delete ACL' checkbox checked. A red circle highlights this checked checkbox.

Passaggio 4. Fare clic su **Save** per salvare le impostazioni.

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:

Configurazione regola ACL per MAC

Passaggio 1. Selezionare un'azione per la regola dall'elenco a discesa *Azione*.

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:

Le opzioni sono descritte come segue:

- Permit (Autorizzazione) - La regola consente a tutto il traffico che soddisfa i criteri della regola di entrare o uscire dal dispositivo WAP. Il traffico che non soddisfa i criteri viene eliminato.

- Nega - La regola impedisce l'ingresso o l'uscita dal dispositivo WAP a tutto il traffico che soddisfa i criteri della regola. Il traffico che non soddisfa i criteri viene inoltrato alla regola successiva. Se si tratta della regola finale, il traffico non autorizzato esplicitamente viene interrotto.

Passaggio 2. Selezionare o deselezionare la casella di controllo **Confronta ogni pacchetto**. Se l'opzione è selezionata, la regola, che prevede un'azione di autorizzazione o rifiuto, corrisponde al frame o al pacchetto indipendentemente dal relativo contenuto.

Action: Deny Allow

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:

Nota: Se si seleziona questo campo, non sarà possibile configurare ulteriori criteri di corrispondenza. L'opzione **Corrispondenza ogni pacchetto** è selezionata per impostazione predefinita per una nuova regola. È necessario deselectionare l'opzione per configurare altri campi di corrispondenza.

Passaggio 3. Selezionare la casella di controllo **Ether Type** per confrontare i criteri di corrispondenza con il valore nell'intestazione di un frame Ethernet. Se la casella di controllo **Tipo Ether** è selezionata, selezionare uno dei seguenti pulsanti di opzione.

Match Every Packet:

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

Class Of Service: (Range: 0 - 7)

Le opzioni sono descritte come segue:

·Selezionare dall'elenco — Scegliere un protocollo dall'elenco a discesa *Seleziona da elenco*. Le opzioni sono le seguenti:

- AppleTalk - AppleTalk è una suite proprietaria di protocolli di rete sviluppata da Apple Inc. per i loro computer Macintosh. AppleTalk includeva una serie di funzioni che consentivano di collegare le reti locali senza alcuna configurazione precedente o la necessità di un router o server centralizzato di alcun tipo.
- ARP - Address Resolution Protocol (ARP) è un protocollo di telecomunicazione utilizzato per la risoluzione degli indirizzi a livello di rete in indirizzi a livello di collegamento, una funzione critica nelle reti ad accesso multiplo.
- IPv4 - Internet Protocol versione 4 (IPv4) è la quarta versione nello sviluppo del protocollo Internet (IP). È uno dei protocolli principali dei metodi di internetworking basati su standard in Internet.
- IPv6 - Internet Protocol versione 6 (IPv6) è la versione più recente di Internet Protocol (IP), il protocollo di comunicazione che fornisce un sistema di identificazione e di localizzazione per i computer sulle reti e instrada il traffico attraverso Internet.
- IPX - Internetwork Packet Exchange (IPX) è il protocollo a livello di rete della suite di protocolli IPX/SPX. Il protocollo IPX deriva dall'IDP di Xerox Network Systems. Può fungere anche da protocollo del livello trasporto.
- NetBIOS - NetBIOS è l'acronimo di Network Basic Input/Output System. Fornisce servizi correlati al livello di sessione del modello OSI, consentendo alle applicazioni in computer separati di comunicare su una rete locale. Essendo strettamente un'API, NetBIOS non è un protocollo di rete.
- PPPOE - Il protocollo PPPoE (Point-to-Point over Ethernet) è un protocollo di rete per l'incapsulamento dei frame PPP all'interno di frame Ethernet.

·Corrispondenza con valore (Match to Value) - Consente di immettere un identificativo di protocollo personalizzato al quale devono corrispondere i pacchetti. Il valore è un numero esadecimale a quattro cifre compreso tra 0600 e FFFF.

Passaggio 4. Selezionare la casella di controllo **Classe di servizio** per immettere una priorità utente 802.1p da confrontare con un frame Ethernet. Analogamente a IP Precedence, 0 rappresenta la priorità più bassa e 7 la priorità più alta. L'intervallo valido è compreso tra 0 e 7.

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)
Class Of Service: 5 (Range: 0 - 7)
Source MAC Address: Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Passaggio 5. Selezionare la casella di controllo **Indirizzo MAC di origine** per immettere un indirizzo MAC di origine da confrontare con un frame Ethernet. Se la casella di controllo Indirizzo MAC di origine è selezionata, immettere l'indirizzo MAC di origine nel campo *Indirizzo MAC di origine*. Immettere quindi la maschera dell'indirizzo MAC di origine nel campo *Maschera MAC di origine*. Consente di specificare i bit dell'indirizzo MAC di origine da confrontare con un frame Ethernet.

Nota: Se si desidera ottenere una corrispondenza solo per un singolo indirizzo MAC, utilizzare la maschera con caratteri jolly 00:00:00:00:00:00.

Class Of Service: (Range: 0 - 7)
Source MAC Address: 00:00:00:00:00:00 (xxxxxxxxxxxx) Source MAC Mask: FF:FF:FF:FF:FF:FF (xxxxxxxxxxxx- "0s for matching, 1s for no matching")
Destination MAC Address: Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Passaggio 6. Selezionare la casella di controllo **Indirizzo MAC di destinazione** per immettere un indirizzo MAC di destinazione da confrontare con un frame Ethernet. Se la casella di controllo Indirizzo MAC di destinazione è selezionata, immettere l'indirizzo MAC di destinazione nel campo *Indirizzo MAC di destinazione*. Immettere quindi la maschera dell'indirizzo MAC nel campo *Maschera MAC di destinazione*. Consente di specificare i bit dell'indirizzo MAC di destinazione da confrontare con un frame Ethernet.

Source MAC Address: Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")
Destination MAC Address: 00:00:00:00:00:00 (xxxxxxxxxxxx) Destination MAC Mask: FF:FF:FF:FF:FF:FF (xxxxxxxxxxxx- "0s for matching, 1s for no matching")
VLAN ID: (Range: 0 - 4095)

Nota: Se si desidera ottenere una corrispondenza solo per un singolo indirizzo MAC, utilizzare la maschera con caratteri jolly 00:00:00:00:00:00.

Passaggio 7. Selezionare la casella di controllo **VLAN ID** per immettere un ID VLAN da confrontare con un frame Ethernet. Se la casella di controllo ID VLAN è selezionata, immettere l'ID VLAN nel campo *ID VLAN*. L'intervallo di ID della VLAN è compreso tra 0 e 4095.

Destination MAC Address: Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")
VLAN ID: 5 (Range: 0 - 4095)

Passaggio 8. (Facoltativo) Se si desidera eliminare l'ACL configurato, selezionare la casella di controllo **Elimina ACL**.

VLAN ID: (Range: 0 - 4095)

Delete ACL:

Passaggio 9. Fare clic su **Save** per salvare le impostazioni.

Action: ▾

Match Every Packet:

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

Class Of Service: (Range: 0 - 7)

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

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

VLAN ID: (Range: 0 - 4095)

Delete ACL: