Configuration of MAC Based Access Control List (ACL) on WAP551 and WAP561 Access Points

Objective

An Access Control List (ACL) is a collection of permit and deny conditions, called rules, that provide security, block unauthorized users, and allow authorized users to access specific resources. ACLs can block any unwarranted attempts to reach network resources. A MAC ACL is a Layer 2 ACL. The network device inspects the frame and checks the ACL rules against the content of the frame. If any of the rules match the content, a permit or deny action is taken on the frame.

The objective of this document is to show the user how to create and configure MAC ACL on WAP551 and WAP561 Access Points.

Applicable Devices

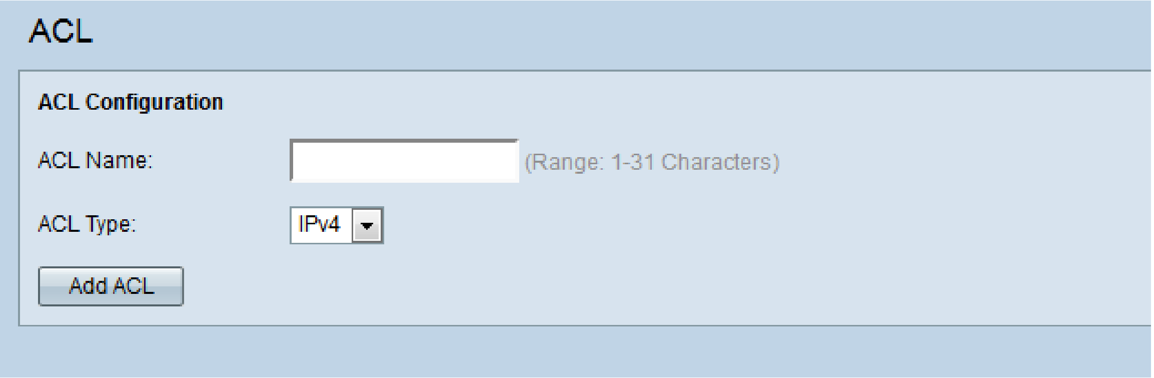
- WAP551
- WAP561

Software Version

- v1.0.4.2

Configuration of MAC ACLs

Step 1. Log in to the web configuration utility and choose **Client QoS > ACL**. The *ACL* page opens:



ACL

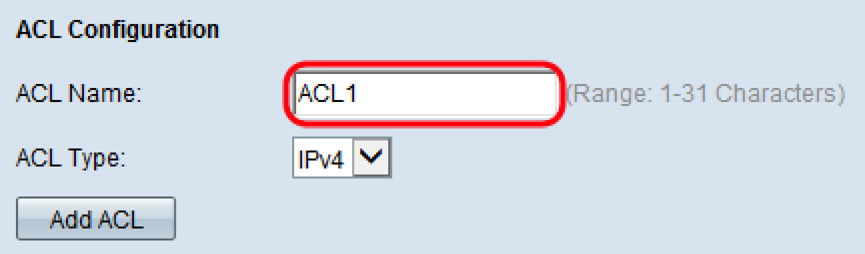
ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: IPv4

Creation of a MAC ACL

Step 1. Enter the name of the ACL in the *ACL Name* field.

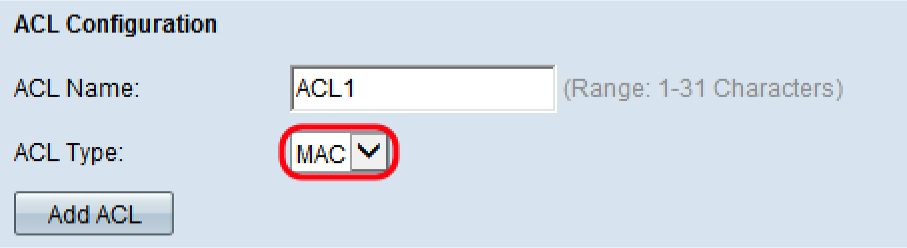


ACL Configuration

ACL Name: ACL1 (Range: 1-31 Characters)

ACL Type: IPv4

Step 2. Choose **MAC** for the ACL type from the *ACL Type* drop-down list.

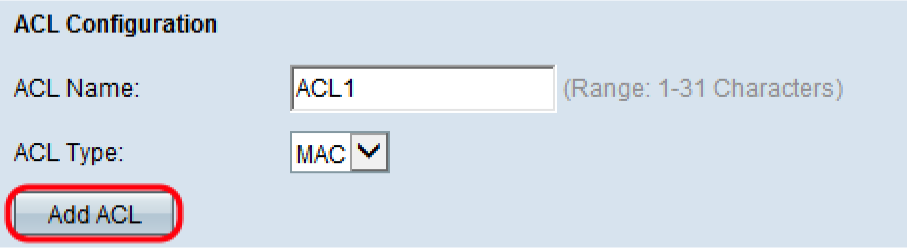


ACL Configuration

ACL Name: ACL1 (Range: 1-31 Characters)

ACL Type: MAC

Step 3. Click **Add ACL** to create a new MAC ACL.



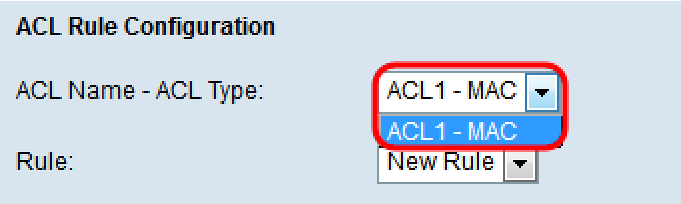
ACL Configuration

ACL Name: ACL1 (Range: 1-31 Characters)

ACL Type: MAC

Configuration of a Rule for a MAC ACL

Step 1. Choose the ACL from the *ACL Name-ACL Type* drop-down list to which you would like to add rules.

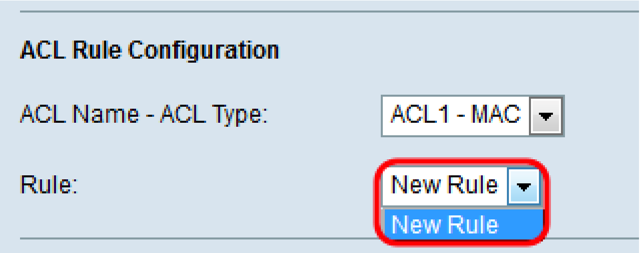


ACL Rule Configuration

ACL Name - ACL Type: ACL1 - MAC

Rule: New Rule

Step 2. If a new rule has to be configured for the selected ACL, choose **New Rule** from the *Rule* drop-down list. Otherwise, choose one of the present rules from the *Rule* drop-down list.



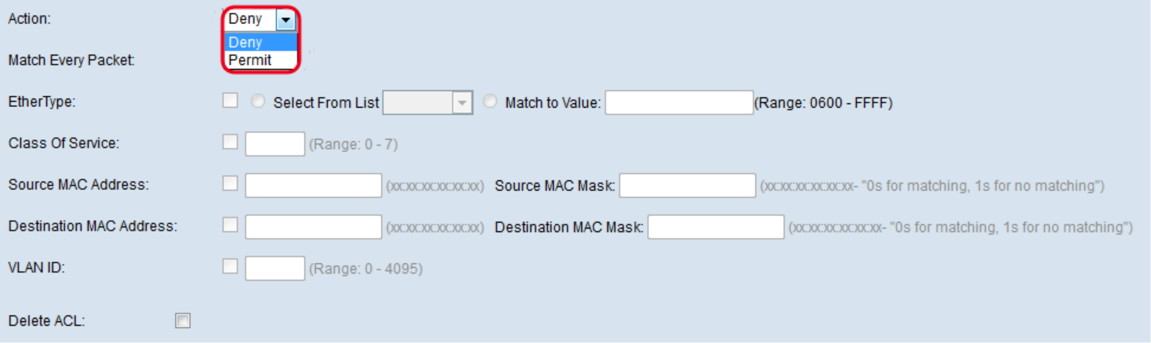
ACL Rule Configuration

ACL Name - ACL Type: ACL1 - MAC

Rule: New Rule

Note: A maximum of 10 rules can be created for a single ACL.

Step 3. Choose the action for the ACL rule from the *Action* drop-down list.



Action: Deny

Match Every Packet:

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

Class Of Service: □ (Range: 0 - 7)

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

VLAN ID: □ (Range: 0 - 4095)

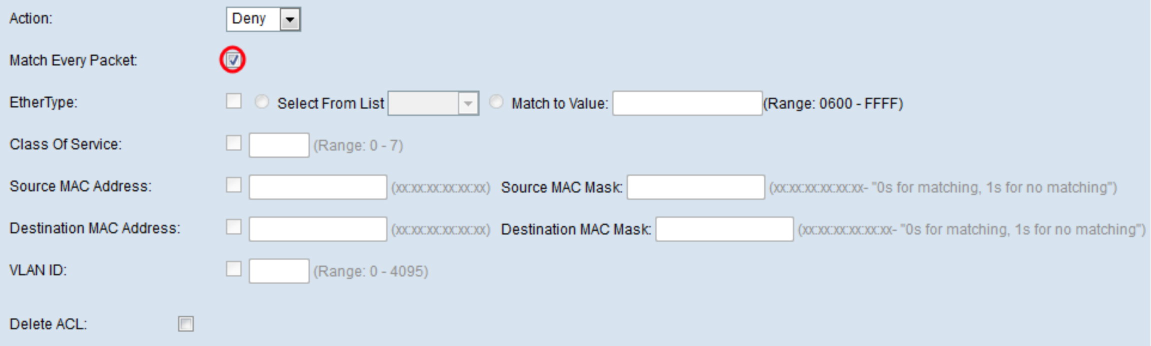
Delete ACL: □

The available options are defined as:

- Deny — Blocks all traffic that meets the rule criteria to enter or exit the WAP device.
- Permit — Allows all traffic that meets the rule criteria to enter or exit the WAP device.

Note: Steps 4 to 9 are optional. If you do not want to apply a filter to an ACL rule, uncheck its corresponding box.

Step 4. (Optional) Check the **Match Every Packet** check box to match the rule for every frame or packet regardless of its contents. Uncheck the **Match Every Packet** check box to configure any of the additional match criteria.



Action: Deny

Match Every Packet: ☑

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

Class Of Service: □ (Range: 0 - 7)

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

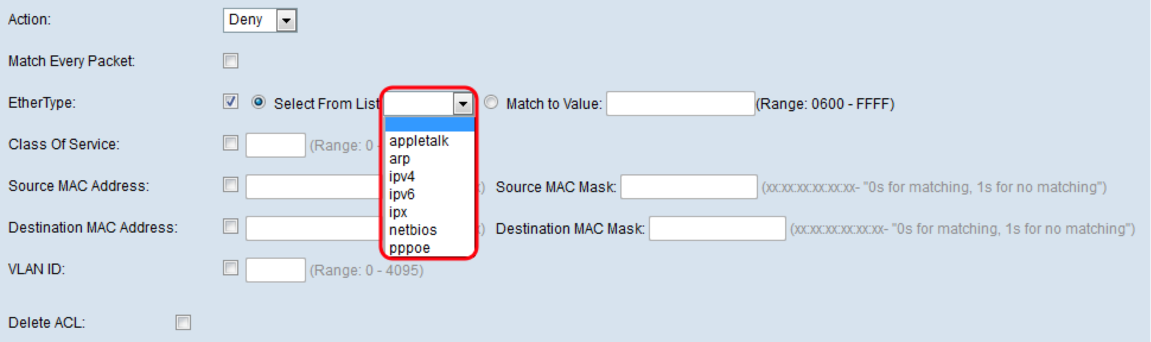
Destination MAC Address: □ (xx:xx:xx:xx:xx:xx) Destination MAC Mask: (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")

VLAN ID: □ (Range: 0 - 4095)

Delete ACL: □

Skip to Step 11 if the *Match Every Packet* box is checked.

Step 5. (Optional) Check the **EtherType** check box to compare the match criteria against the value in the header of an Ethernet frame. If the *EtherType* check box is checked, click either the *Select From List* or *Match to Value* radio buttons.



Action: Deny

Match Every Packet: □

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

Class Of Service: □ (Range: 0

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

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

VLAN ID: □ (Range: 0 - 4095)

Delete ACL: □

The available options are defined as follows:

- Select From List — Allows you to choose a protocol from the drop-down list. The available options are appletalk, arp, ipv4, ipv6, ipx, netbios, and pppoe. Choosing an option will apply the rule to packets of the selected protocol.

– appletalk — This is a network protocol designed by Apple Inc. for their Macintosh computers. Appletalk is a plug-n-play system; it automatically assigns addresses and handles any other network configurations without user input.

– arp — ARP (Address Resolution Protocol) is a critical protocol used to translate IP addresses into MAC addresses.

– ipv4 — IPv4 (Internet Protocol version 4) is an important protocol that is responsible for most traffic on the Internet. It handles the IP addresses of devices.

– ipv6 — IPv6 is the successor to IPv4 and the latest version of the Internet Protocol. It was developed in response to the exhaustion of most existing IPv4 IP addresses.

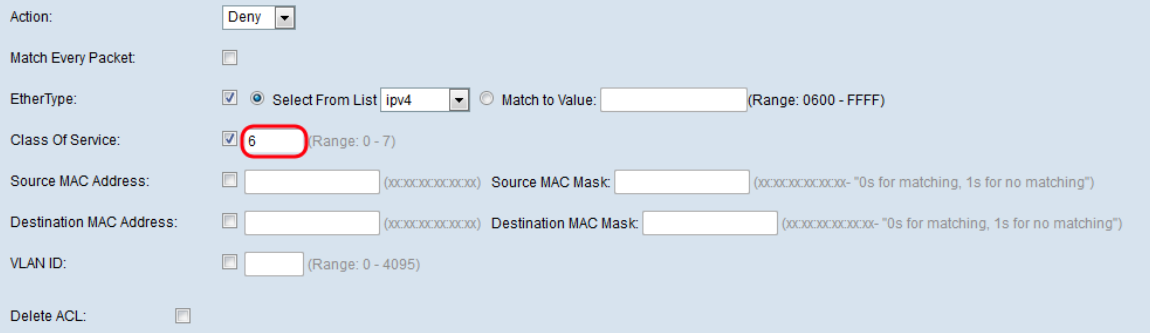
– ipx — IPX (Internetwork Packet Exchange) is a network/transport protocol. Although the protocol doesn't function as well in large networks, an advantage IPX has over TCP/IP is the small amount of memory it uses.

– netbios — NetBIOS(Network Basic Input/Output System) is an API (application programming interface) that typically runs alongside TCP/IP in modern networks.

– pppoe —PPPoE (Point-to-Point Protocol over Ethernet) is a network protocol used to encapsulate PPP packets inside Ethernet packets.

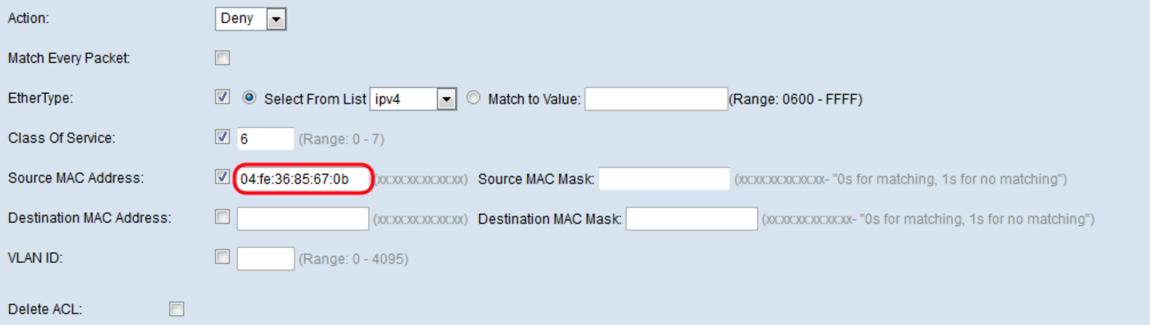
- Match to Value — Allows you to enter a custom protocol identifier in the *Match to Value* field. This option is useful if you want to filter packets by a protocol not included in the *Select From List* drop-down list. Valid custom protocol identifiers range from 0600 to FFFF.

Step 6. (Optional) Check the **Class of Service** check box to enter a 802.1p user priority to compare against an Ethernet frame. Enter the priority, which ranges from 0 to 7, in the *Class of Service* field.



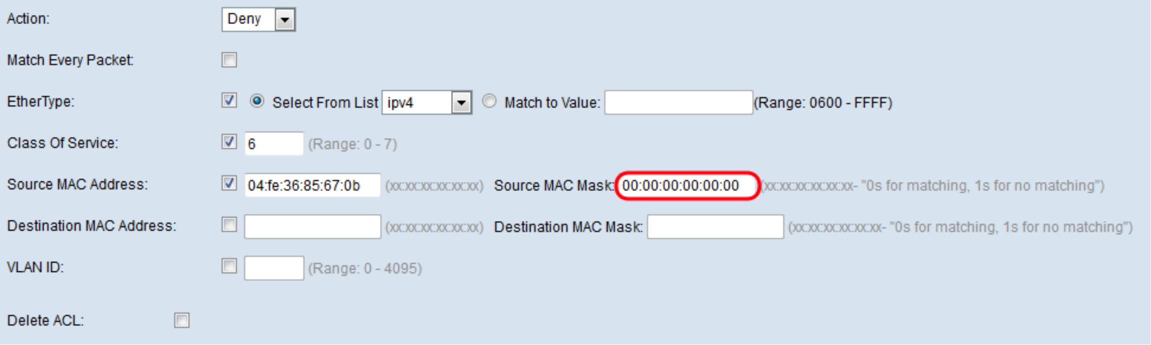
Action:	Deny
Match Every Packet:	□
EtherType:	☑ ● Select From List ipv4 ○ Match to Value: (Range: 0600 - FFFF)
Class Of Service:	☑ 6 (Range: 0 - 7)
Source MAC Address:	□ (xx:xx:xx:xx:xx:xx) Source MAC Mask: (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
Destination MAC Address:	□ (xx:xx:xx:xx:xx:xx) Destination MAC Mask: (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
VLAN ID:	□ (Range: 0 - 4095)
Delete ACL:	□

Step 7. (Optional) Check the **Source MAC Address** check box to compare the source MAC address against an Ethernet frame and enter the source MAC address in the *Source MAC Address* field.



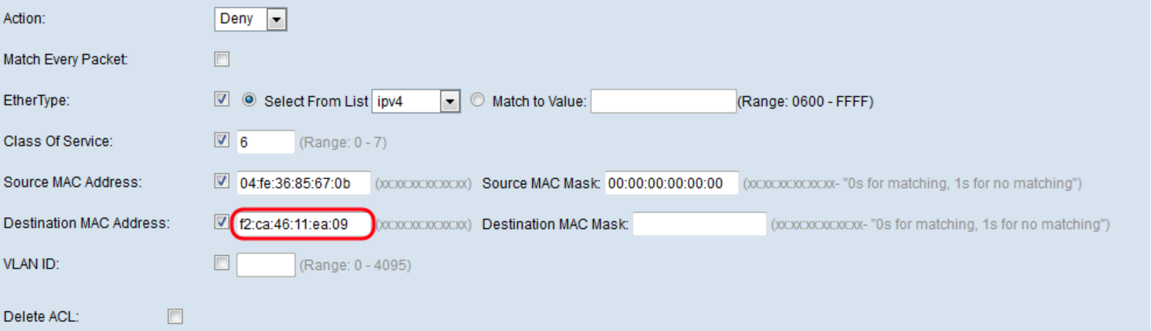
Action:	Deny
Match Every Packet:	□
EtherType:	☑ ● Select From List ipv4 ○ Match to Value: (Range: 0600 - FFFF)
Class Of Service:	☑ 6 (Range: 0 - 7)
Source MAC Address:	☑ 04:fe:36:85:67:0b (xx:xx:xx:xx:xx:xx) Source MAC Mask: (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
Destination MAC Address:	□ (xx:xx:xx:xx:xx:xx) Destination MAC Mask: (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
VLAN ID:	□ (Range: 0 - 4095)
Delete ACL:	□

Step 8. (Optional) Enter the source MAC address mask in the *Source MAC Mask* field that specifies which bits in the source MAC to compare against an Ethernet frame.



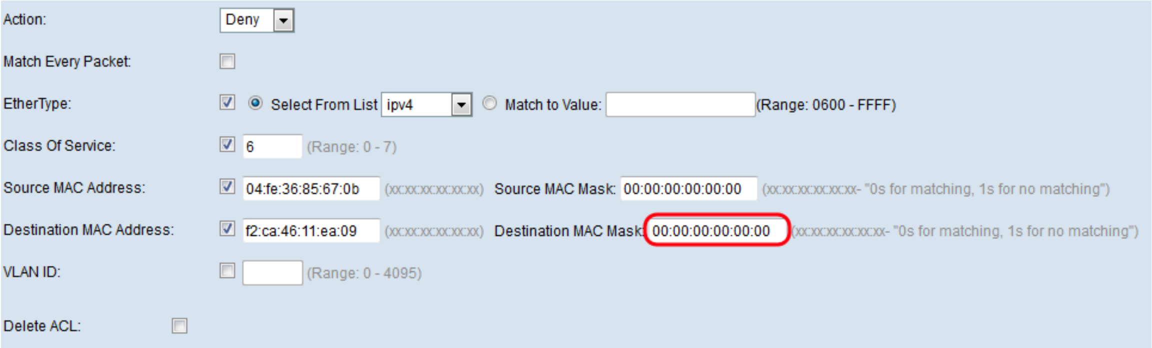
Action:	Deny ▾
Match Every Packet:	□
EtherType:	☑ ● Select From List ipv4 ▾ ○ Match to Value: (Range: 0600 - FFFF)
Class Of Service:	☑ 6 (Range: 0 - 7)
Source MAC Address:	☑ 04:fe:36:85:67:0b (xx:xx:xx:xx:xx:xx) Source MAC Mask: 00:00:00:00:00:00 (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
Destination MAC Address:	□ (xx:xx:xx:xx:xx:xx) Destination MAC Mask: (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
VLAN ID:	□ (Range: 0 - 4095)
Delete ACL:	□

Step 9. (Optional) Check the **Destination MAC Address** check box to compare destination MAC address against an Ethernet frame and enter the destination MAC address in the *Destination MAC Address* field.



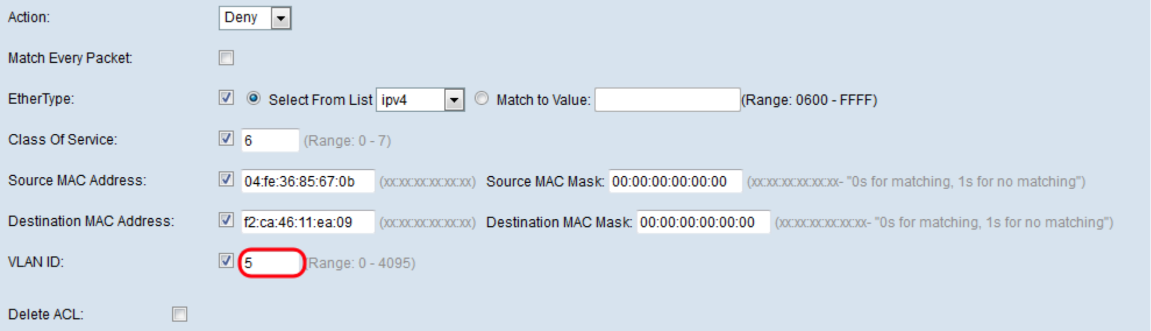
Action:	Deny ▾
Match Every Packet:	□
EtherType:	☑ ● Select From List ipv4 ▾ ○ Match to Value: (Range: 0600 - FFFF)
Class Of Service:	☑ 6 (Range: 0 - 7)
Source MAC Address:	☑ 04:fe:36:85:67:0b (xx:xx:xx:xx:xx:xx) Source MAC Mask: 00:00:00:00:00:00 (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
Destination MAC Address:	☑ f2:ca:46:11:ea:09 (xx:xx:xx:xx:xx:xx) Destination MAC Mask: (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
VLAN ID:	□ (Range: 0 - 4095)
Delete ACL:	□

Step 10. (Optional) Enter the destination MAC address mask in the *Destination MAC Mask* field that specifies which bits in the destination MAC to compare against an Ethernet frame.



Action:	Deny ▾
Match Every Packet:	□
EtherType:	☑ ● Select From List ipv4 ▾ ○ Match to Value: (Range: 0600 - FFFF)
Class Of Service:	☑ 6 (Range: 0 - 7)
Source MAC Address:	☑ 04:fe:36:85:67:0b (xx:xx:xx:xx:xx:xx) Source MAC Mask: 00:00:00:00:00:00 (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
Destination MAC Address:	☑ f2:ca:46:11:ea:09 (xx:xx:xx:xx:xx:xx) Destination MAC Mask: 00:00:00:00:00:00 (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
VLAN ID:	□ (Range: 0 - 4095)
Delete ACL:	□

Step 11. (Optional) Check the **VLAN ID** check box to compare the VLAN ID against an Ethernet frame. Enter the desired VLAN ID, which ranges from 0 to 4095, in the *VLAN ID* field.



Action:	Deny ▾
Match Every Packet:	□
EtherType:	☑ ● Select From List ipv4 ▾ ○ Match to Value: (Range: 0600 - FFFF)
Class Of Service:	☑ 6 (Range: 0 - 7)
Source MAC Address:	☑ 04:fe:36:85:67:0b (xx:xx:xx:xx:xx:xx) Source MAC Mask: 00:00:00:00:00:00 (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
Destination MAC Address:	☑ f2:ca:46:11:ea:09 (xx:xx:xx:xx:xx:xx) Destination MAC Mask: 00:00:00:00:00:00 (xx:xx:xx:xx:xx:xx- "0s for matching, 1s for no matching")
VLAN ID:	☑ 5 (Range: 0 - 4095)
Delete ACL:	□

Step 12. (Optional) To delete the configured ACL, check the **Delete ACL** check box.

Step 13. Click **Save**.