

# Configure MAC, IPv4, and IPv6 Access Control List on a Wireless Access Point

## Objective

An Access Control List (ACL) is a list of network traffic filters and correlated actions used to improve security. It blocks unauthorized users and allow authorized users to access specific resources. An ACL contains the hosts that are allowed or denied access to the network device. ACLs can be defined in one of two ways: by IPv4 address or by IPv6 address.

This article guides you on how to successfully create an ACL and configure IPv4, IPv6 and Media Access Control (MAC)-based ACLs on your Wireless Access Point (WAP) to improve network security.

## Applicable Devices

- WAP100 Series
- WAP300 Series
- WAP500 Series

## Software Version

- 1.0.6.2 - WAP121, WAP321
- 1.2.0.2 - WAP371, WAP551, WAP561
- 1.0.1.4 - WAP131, WAP351
- 1.0.0.16 - WAP150, WAP361

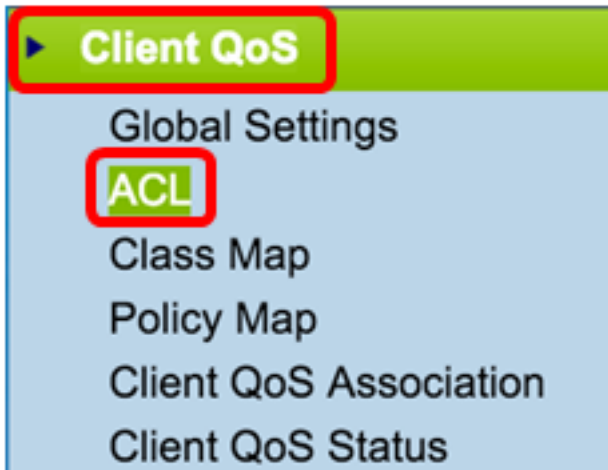
## Create ACL

**Note:** Images used for this configuration are from WAP150.

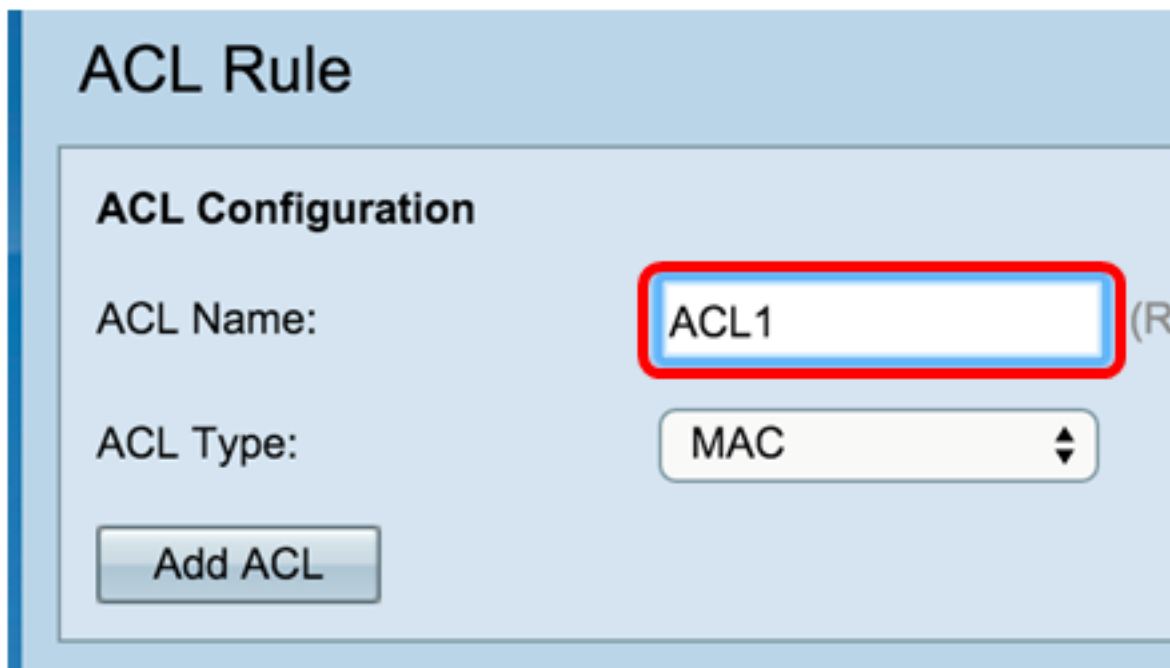
Step 1. Log in to the access point web-based utility and choose **ACL > ACL Rule**.



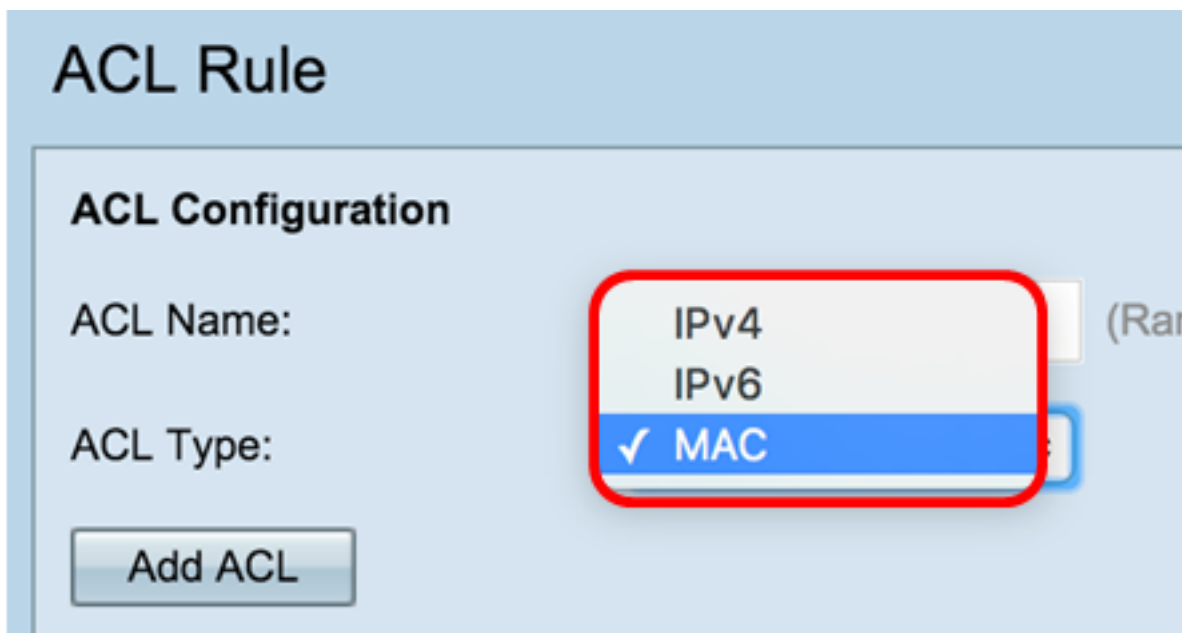
**Note:** For WAP121, WAP321, WAP371, WAP551, and WAP561: Log in to the access point web-based utility and choose Client QoS > ACL.



Step 2. Once the ACL Configuration page opens, enter the ACL name in the *ACL Name* field.



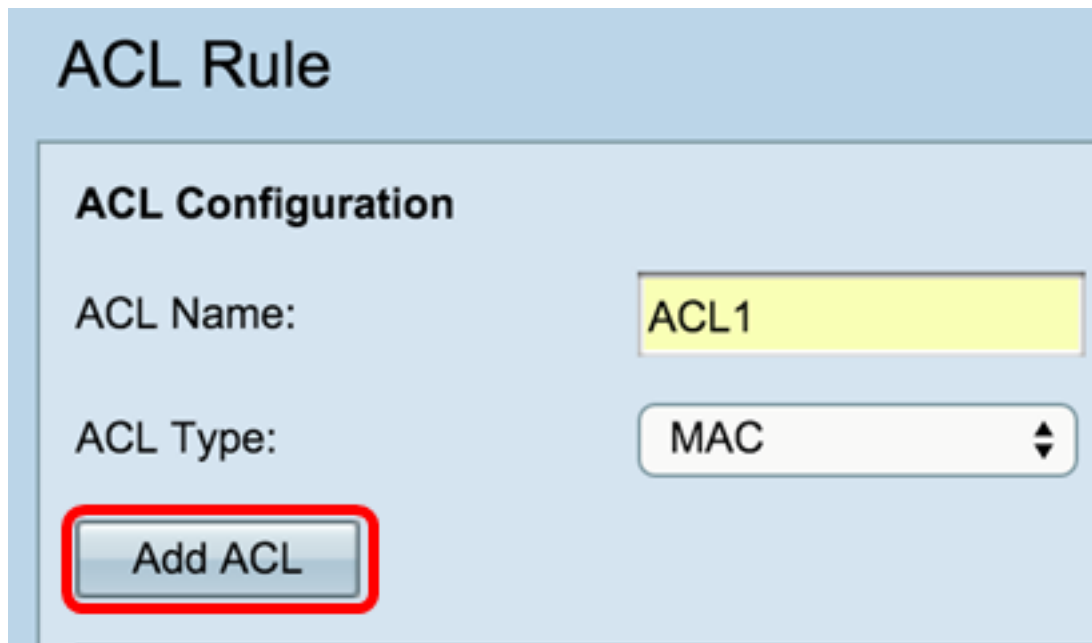
Step 3. Choose an **ACL Type** from the ACL Type drop-down list.



- IPv4 — A 32-bit (4-byte) address.

- IPv6 — A successor to IPv4, consists of a 128-bit (8-byte) address.
- MAC — The MAC address is the unique address assigned to a network interface.

Step 4. Click the **Add ACL** button.



**ACL Rule**

**ACL Configuration**

ACL Name:

ACL Type:

If you chose MAC, skip to [Configure MAC-based ACL](#).

If you chose IPv4, skip to [Configure IPv4-based ACL](#).

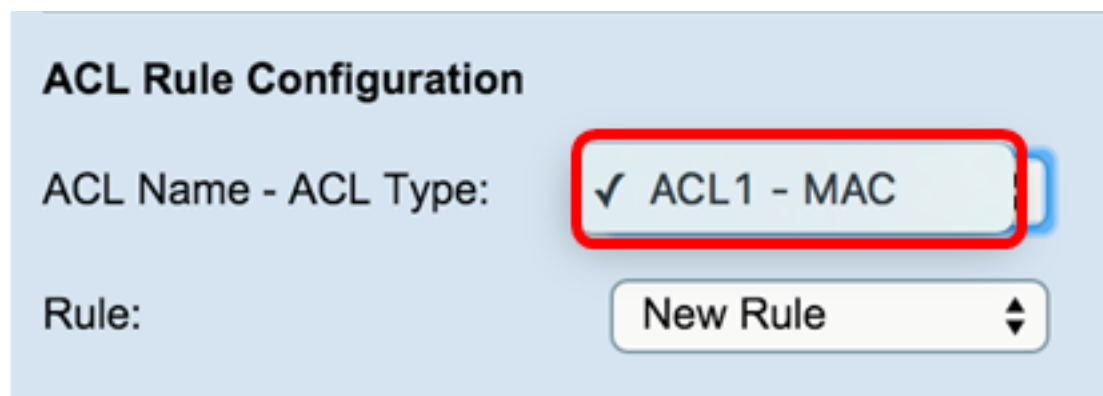
If you chose IPv6, skip to [Configure IPv6-based ACL](#).

You should now have successfully created an ACL.

## Configure MAC-based ACL

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

**Note:** In the image below, ACL1 MAC was chosen as an example.



**ACL Rule Configuration**

ACL Name - ACL Type:

Rule:

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

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

### ACL Rule Configuration

ACL Name - ACL Type:

Rule:

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

**Note:** In this example, a Deny statement is created.

Action:

Match Every Packet:

- Deny — Blocks all traffic that meets the rule criteria to enter or exit the WAP. Because there is an implicit deny-all rule at the end of every ACL, traffic that is not explicitly permitted is dropped.
- Permit — Allows all traffic that meets the rule criteria to enter or exit the WAP. Traffic that does not meet the criteria is dropped.

**Note:** Steps 4 to 11 are optional. Filters that are checked are enabled. Uncheck the check box for the filter that you do not want it to apply to this specific rule.

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

**Tip:** If Match Every Packet is already checked, skip to [Step 12](#).

Action:

Match Every Packet:

Step 5. In the EtherType area, choose a radio button to compare the matched criteria against the value in the header of an Ethernet frame. You can choose one of these options or choose Any:

- Select From List — Choose a protocol from the drop-down list. The list has the following options: appletalk, arp, IPv4, IPv6, ipx, netbios, pppoe.
- Match to Value — For the custom protocol identifier, enter the identifier which ranges from 0600 to FFFF.

Protocol:

Any

Select From List:

Match to Value:

icmp

0 (Range)

Step 6. In the Class Of Service area, choose a radio button to enter 802.1p user priority to compare against an Ethernet frame. You can either choose Any or a User Defined priority. Enter the priority which ranges from 0 to 7 in the *User Defined* field.

Class Of Service:

Any

User Defined

6

Step 7. In the Source MAC area, choose a radio button to compare the source MAC address against an Ethernet frame. You can choose **Any** or choose **User Defined** and enter the source MAC address in the field provided.

Source MAC:

Any

User Defined

Source MAC Address: 04:FE:36:A5:670B

Source MAC Mask:

Step 8. 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.

**Note: If the MAC mask uses a 0 bit, then the address is accepted, and if it uses 1 bit, then the address is ignored.**

Source MAC:

Any

User Defined

Source MAC Address: 04:FE:36:A5:670B

Source MAC Mask: 00:00:00:00:00:00

Step 9. In the Destination MAC area, choose a radio button to compare the destination MAC address against an Ethernet frame. You can choose Any or choose User Defined and enter the destination MAC address in the field provided.

Destination MAC:

Any

User Defined

Destination MAC Address: F2:CA:46:11:EA:09

Destination MAC Mask:

Step 10. 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.

**Note: If the MAC mask uses a 0 bit, then the address is accepted, and if it uses a 1 bit, then the address is ignored.**

Destination MAC:  Any  
 User Defined  
Destination MAC Address: F2:CA:46:11:EA:09  
Destination MAC Mask: 00:00:00:00:00:00

Step 11. In the **VLAN ID** area, choose a radio button to compare the VLAN ID against an Ethernet frame. Enter the VLAN ID which ranges from 0 to 4095 in the field provided.

VLAN ID:  Any  
 User Defined 52 (Range: 0 - 4095)

Step 12. Click **Save**.

VLAN ID:  Any  
 User Defined

Delete ACL:

Save

Step 13. (Optional) To delete the configured ACL, check the **Delete ACL** check box and then click **Save**.

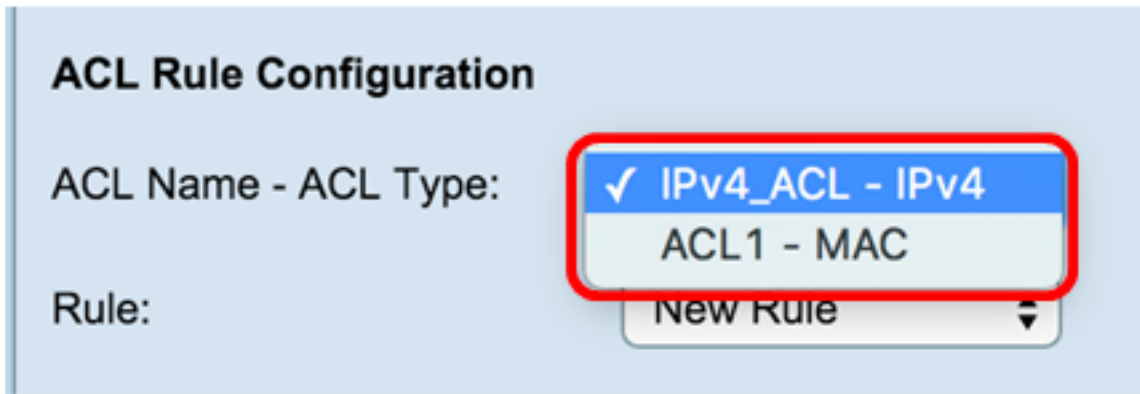
You should now have successfully configured MAC ACL on your WAP.

## Configure IPv4-based ACL

Step 1. In the ACL Rule Configuration area, configure these rule parameters:

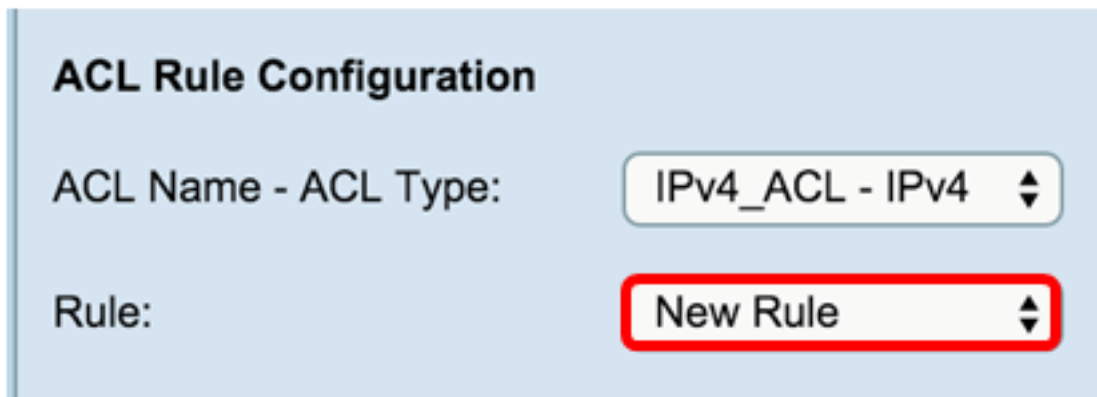
ACL Name - ACL Type Choose the ACL to configure with the new rule.

**Note:** In the image below, IPv4\_ACL-IPv4 was chosen as an example.



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

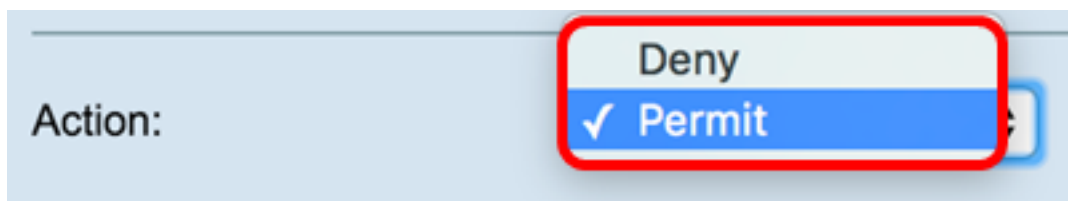
**Note:** A maximum of 10 rules can be created for a single ACL.



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

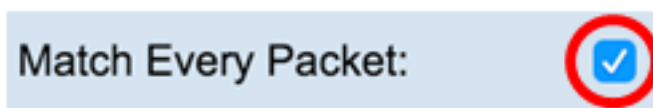
**Note:** In this example, a Permit statement is created.

- Deny — Blocks all traffic that meets the rule criteria to enter or exit the WAP. Because there is an implicit deny-all rule at the end of every ACL, traffic that is not explicitly permitted is dropped.
- Permit — Allows all traffic that meets the rule criteria to enter or exit the WAP. Traffic that does not meet the criteria is dropped.



**Note:** Steps 4 to 9 are optional. Filters that are checked are enabled. Uncheck the check box for the filter if you do not want it to apply to this specific rule.

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



**Tip:** Match Every Packet is enabled by default. If you wish to keep this setting, skip to [Step 11](#).

Step 5. In the Protocol area, choose a radio button to compare the matched criteria against the value in the header of an Ethernet frame. You can choose Any or select from the drop-down list

- Select From List — Choose one of these protocols:

- IP — The principle communications protocol in the Internet Protocol Suite for relaying data across networks.
- ICMP — A protocol in the Internet Protocol Suite that is used by devices like routers to send error messages.
- IGMP — A communications protocol used by host to establish multicast group memberships on IPv4 networks.
- TCP — Enables two hosts to establish a connection and exchange streams of data.
- UDP — A protocol in the Internet Protocol Suite that uses a connectionless transmission model.

- Match to Value — Enter a standard IANA-assigned protocol ID from 0 to 255. Choose this method to identify a protocol not listed by name in the Select From List.

Step 6. In the Source IP area, choose a radio button to include the IP address of the source in the match condition. You can choose Any or User Defined then enter the IP address and wild card mask of the source in the respective fields.

- Source IP Address — Enter an IP address to apply this criteria.
- Wild Card Mask — Enter the destination IP address wild card mask. The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wild card of 0.0.0.0 indicates that all bits are important. This field is required when Source IP Address is selected.

**Note:** A wild card mask is basically the inverse of a subnet mask. For example, to match the criteria to a single host address, use a wild card mask of 0.0.0.0. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a wild card mask of 0.0.0.255.

Step 7. In the Source Port area, choose a radio button to include a source port in the match condition. You can choose Anyto match to any source port or you can choose the following:

- Select From List — Choose a source port from the Select From List drop-down list. The options are as follows:

- File Transfer Protocol (FTP) — FTP is a standard network protocol used to transfer files from one host to another over a Transmission Control Protocol (TCP)-based network such as the Internet.
- FTP data — A data channel initiated by the server connected to a client, typically via port 20.
- Hypertext Transfer Protocol (HTTP) — HTTP is an application protocol that is the foundation of data communication for the World Wide Web.
- Simple Mail Transfer Protocol (SMTP) — SMTP is an Internet standard for electronic mail (email) transmission.
- Simple Network Management Protocol (SNMP) — SNMP is an Internet standard protocol for managing devices on IP networks.
- Telnet — A session layer protocol used on the Internet or local area networks to provide bidirectional interactive text-oriented communication.
- Trivial File Transfer Protocol (TFTP) — TFTP is an Internet software utility for transferring files that is simpler to use than FTP but less capable.
- World Wide Web (WWW) — WWW is a system of Internet servers that support HTTP formatted documents.



- Match to Port — Enter the port number that is not presented in the list. Port numbers range from 0 to 65535 in the *Match to Port* field for unlisted source ports. The range includes three different types of ports. The ranges are described as follows

- 0 to 1023 — Well-known ports
- 1024 to 49151 — Registered ports
- 49152 to 65535 — Dynamic and/or Private ports

- Mask — Enter the port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0 — 0xFFFF) is allowed. 0 means the bit matters and 1 means that you should ignore this bit.

Step 8. In the Destination IP area, choose a radio button to include the IP address of the destination in the match condition. You can choose Any or User Defined then enter the IP address and wild card mask of the destination in the respective fields.

- Destination IP Address — Enter an IP address to apply this criteria.
- Wild Card Mask — Enter the destination IP address wild card mask. The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wild card of 0.0.0.0 indicates that all bits are important. This field is required when destination IP Address is selected.

**Note:** A wild card mask is basically the inverse of a subnet mask. For example, to match the criteria to a single host address, use a wild card mask of 0.0.0.0. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a wild card mask of 0.0.0.255.

Step 9. In the Destination Port area, choose a radio button to include a destination port in the match condition. You can choose Any to match to any destination port or you can choose the following:

- Select From List — Choose a destination port from the drop-down list. The options are as follows

- FTP — A standard network protocol used to transfer files from one host to another over a TCP-based network such as the Internet.
- FTP data — A data channel initiated by the server connected to a client, typically via port 20.
- HTTP — An application protocol that is the foundation of data communication for the World Wide Web.
- SMTP — An Internet standard for electronic mail (email) transmission.
- SNMP — An Internet standard protocol for managing devices on IP networks.
- Telnet — A session layer protocol used on the Internet or local area networks to provide bidirectional interactive text-oriented communication.
- TFTP — An Internet software utility for transferring files that is simpler to use than FTP but less capable.
- WWW — A system of Internet servers that support HTTP formatted documents.

- Match to Port — Enter the port number that is not presented in the list. Port numbers range from 0 to 65535 in the *Match to Port* field for unlisted source ports. The range includes three different types of ports. The ranges are described as follows:

- 0 to 1023 — Well known ports
- 1024 to 49151 — Registered ports
- 49152 to 65535 — Dynamic and/or Private ports

- Mask — Enter the port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0-0xFFFF) is allowed. 0 means the bit matters and 1 means that you should ignore this bit.

**Destination Port:**

Any  
 **Select From List:**  (Range: 0 - 65535)  
 Match to Port:  (Range: 0 - 65535)  
 Mask:  (Range: 0 ~ 0xFFFF)

Step 10. In the Service Type area, choose a radio button to match packets based on specific service type. You can choose Any or you can choose from the following:

- IP DSCP Select From List — Matches the packets based on their Differentiated Services Code Point (DSCP) Assured Forwarding (AF), Class of Service (CS), or Expedited Forwarding (EF) values.
- IP DSCP Match to Value — Matches the packets based on a custom DSCP value. If chosen, enter a value from 0 to 63 in this field.
- IP Precedence — Matches the packets based on their IP precedence value. If chosen, enter an IP Precedence value from 0 to 7.
- IP TOS Bits — Specifies a value to use the TOS bits of the packets in the IP header as match criteria.
- The IP TOS field in a packet is defined as all eight bits of the Service Type octet in the IP header. The IP TOS Bits value is a two-digit hexadecimal number from 00 to ff. The high-order three bits represent the IP precedence value. The high-order six bits represent the IP DSCP value.
- IP TOS Mask — Enter an IP TOS Mask value to identify the bit positions in the IP TOS Bits value that are used for comparison against the IP TOS field in a packet.
- The IP TOS Mask value is a two-digit hexadecimal number from 00 to FF, representing an inverted (that is, wild card) mask. The zero-valued bits in the IP TOS Mask denote the bit positions in the IP TOS Bits value that are used for comparison against the IP TOS field of a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use an IP TOS Bits value of 0 and an IP TOS Mask of 00.

**Service Type**

Any  
 **IP DSCP Select From List:**  (Range: 0 - 63)  
 IP DSCP Match to Value:  (Range: 0 - 63)  
 IP Precedence:  (Range: 0 - 7)  
 IP TOS Bits:  (Range: 00 - FF)  
 IP TOS Mask:  (Range: 00 - FF)

Step 11. Click Save.

VLAN ID:  Any  
 User Defined

Delete ACL:

**Save**

You should now have successfully configured an IPv4-based ACL.

## Configure IPv6-based ACL

Step 1. In the ACL Rule Configuration area, configure these rule parameters:

ACL Name - ACL Type — Choose the ACL to configure with the new rule.

**Note:** In the image below, IPv6\_ACL — Pv6 was chosen as an example.

**ACL Rule Configuration**

ACL Name - ACL Type: **IPv6\_ACL - IPv6**

Rule: **New Rule**

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

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

**ACL Rule Configuration**

ACL Name - ACL Type: IPv6\_ACL - IPv6

Rule: **New Rule**

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

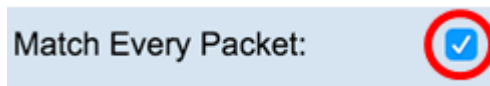
- Deny — Blocks all traffic that meets the rule criteria to enter or exit the WAP. Because there is an implicit deny-all rule at the end of every ACL, traffic that is not explicitly permitted is dropped.
- Permit — Allows all traffic that meets the rule criteria to enter or exit the WAP. Traffic that does not meet the criteria is dropped.

Action: **Deny**

Match Every Packet:

**Note:** Steps 4 to 11 are optional. Filters that are checked are enabled. Uncheck the check box for the filter if you do not want it to apply to this specific rule.

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



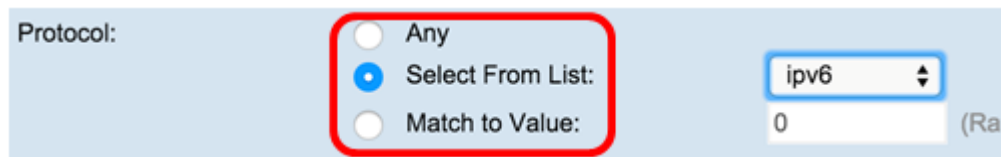
**Tip:** Match Every Packet is enabled by default. If you wish to keep this setting, skip to [Step 12](#).

Step 5. In the Protocol area, choose a radio button to compare the matched criteria against the value in the header of an Ethernet frame. You can choose one of these options or choose Any:

- Select From List — Choose one of these protocols:

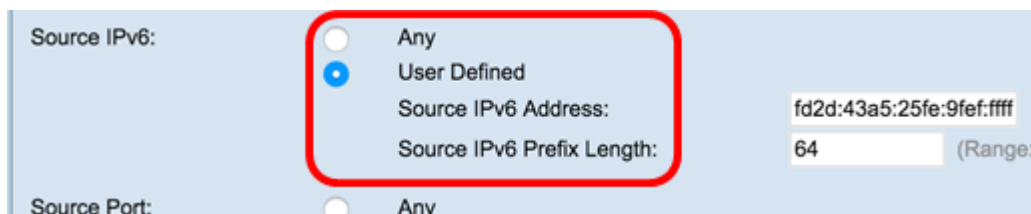
- IP — The principle communications protocol in the Internet Protocol Suite for relaying data across networks.
- ICMP — A protocol in the Internet Protocol Suite that is used by devices like routers to send error messages.
- IGMP — A communications protocol used by host to establish multicast group memberships on IPv4 networks.
- TCP — Enables two hosts to establish a connection and exchange streams of data.
- UDP — A protocol in the Internet Protocol Suite that uses a connectionless transmission model.

- Match to Value — Enter a standard IANA-assigned protocol ID from 0 to 255. Choose this method to identify a protocol not listed by name in the Select From List.



Step 6. In the Source IPv6 area, choose a radio button to include the IP address of the source in the match condition. You can choose Any or User Defined then enter the IPv6 address and source IPv6 Prefix Length.

- Source IPv6 Address — Enter an IPv6 address to apply this criteria.
- Source IPv6 Prefix Length — Enter the prefix length of the source IPv6 address.



Step 7. In the *Source Port* area, choose a radio button to include a source port in the match condition. You can choose Any to match to any source port or you can choose the following:

- Select From List — Choose a source port from the *Select From List* drop-down list. The options are as follows:

- FTP — A standard network protocol used to transfer files from one host to another over a TCP-based network such as the Internet.
- FTP data — A data channel initiated by the server connected to a client, typically via port 20.
- HTTP — An application protocol that is the foundation of data communication for the World Wide Web.
- SMTP — An Internet standard for electronic mail (email) transmission.
- SNMP — An Internet standard protocol for managing devices on IP networks.
- Telnet — A session layer protocol used on the Internet or local area networks to provide bidirectional interactive text-oriented communication.
- TFTP — An Internet software utility for transferring files that is simpler to use than FTP but less capable.
- WWW — A system of Internet servers that support HTTP formatted documents.

- Match to Port — Enter the port number that is not presented in the list. Port numbers range from 0 to 65535 in the *Match to Port* field for unlisted source ports. The range includes three different types of ports. The ranges are described as follows:

- 0 to 1023 — Well known ports
- 1024 to 49151 — Registered ports
- 49152 to 65535 — Dynamic and/or Private ports

- Mask — Enter the port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0 to 0xFFFF) is allowed. 0 means the bit matters and 1 means that you should ignore this bit.

Source Port:

Any  
 Select From List:  (Range: )  
 Match to Port:  (Range: )  
 Mask:  (Range: )

Step 8. In the Destination IPv6 area, choose a radio button to include the IP address of the destination in the match condition. You can choose Any or choose User Defined enter the IPv6 address and Destination IPv6 Prefix Length.

- Destination IPv6 Address — Enter an IPv6 address to apply this criteria.
- Destination IPv6 Prefix Length — Enter the prefix length of the destination IPv6 address.

Destination IPv6:

Any  
 User Defined  
 Destination IPv6 Address:   
 Destination IPv6 Prefix Length:  (Range: )

Step 9. In the Destination Port area, choose a radio button to include a destination port in the match condition. You can choose Any to match to any destination port or you can choose the following:

- Select From List — Choose a destination port from the *Select From List* drop-down list. The options are FTP, FTP data, HTTP, SNMP, SMTP, TFTP, Telnet, WWW.
- Match to Port — Enter the port number that is not presented in the list. Port numbers range from 0 to 65535 in the *Match to Port* field for unlisted source ports. The range includes three different types of ports. The ranges are described as follows:

— 0 to 1023 — Well known ports

— 1024 to 49151 — Registered ports

— 49152 to 65535 — Dynamic and/or Private ports

- Mask — Enter the port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0-0xFFFF) is allowed. 0 means the bit matters and 1 means that you should ignore this bit.

Destination Port:

Any  
 Select From List:  (Ra  
 Match to Port:  (Ra  
 Mask:  (Ra

Step 10. In the IPv6 Flow Label area, choose a radio button to include the IPv6 flow label in the match condition. You can choose Any or User Defined and enter a 20-bit number that is unique to an IPv6 packet. The range is from 0-0xffff.

IPv6 Flow Label:

Any  
 User Defined:  (

Step 11. In the IPv6 DSCP area, choose a radio button to match packets against their IP DSCP value. You can choose Any or you can choose the following:

- Select from list — Choose one of these values: DSCP Assured Forwarding (AF), Class of Service (CS), or Expedited Forwarding (EF).
- Match to Value — enter a custom DSCP value ranging from 0 to 63.

IPv6 DSCP:

Any  
 Select From List:  
 Match to Value:

(Range: 0 - 63)

Delete ACL:

Save

[Step 12.](#) Click Save.

IPv6 DSCP:

Any  
 Select From List:  
 Match to Value:

Delete ACL:

Save

Step 13. (Optional) To delete an ACL, ensure that the ACL name is selected in the ACL Name-ACL Type list then check Delete ACL.

You should have now successfully configured an IPv6-based ACL.