ACL Rule Configuration on the WAP371

Objective

A network access control list (ACL) is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. Access lists are collections of permit and deny conditions, or rules, that provide security for a number of reasons. For example, these rules can block unauthorized users, allow authorized users to access specific resources, and block any unwarranted attempts to reach network resources.

The objective of this document is to show you how to configure ACL rules on the WAP 371.

Applicable Devices

- WAP371

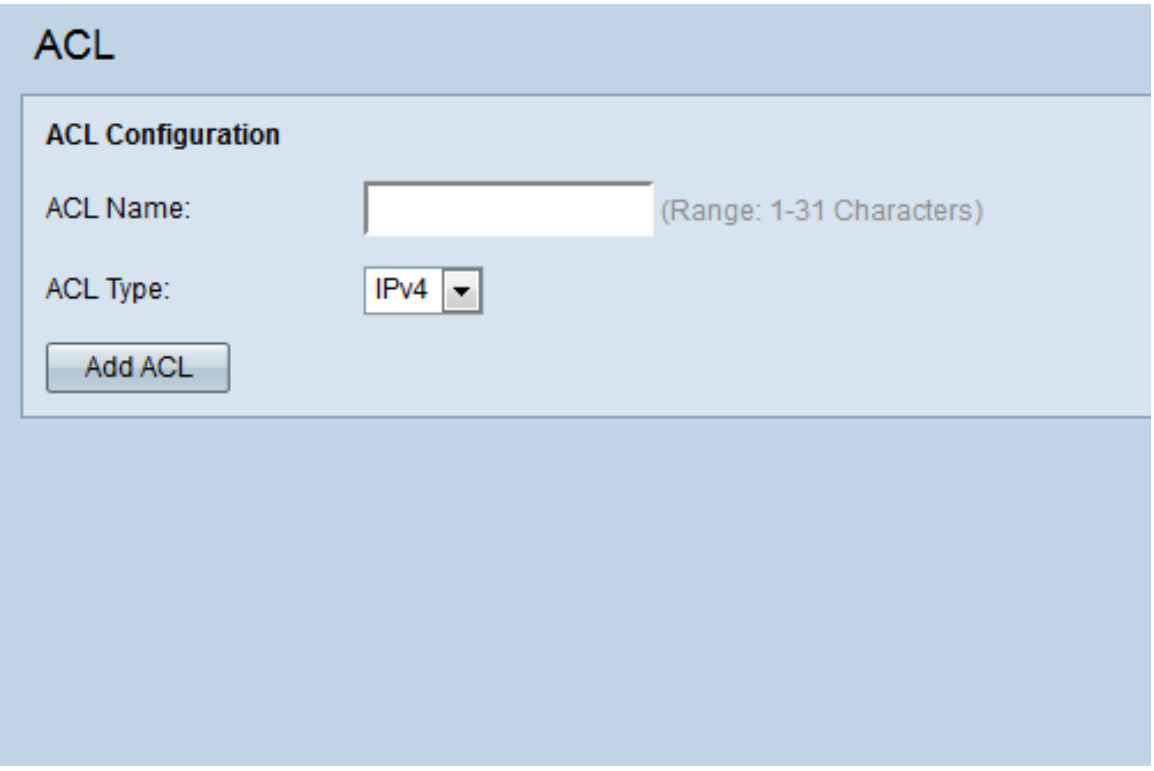
Software Version

- v1.2.0.2

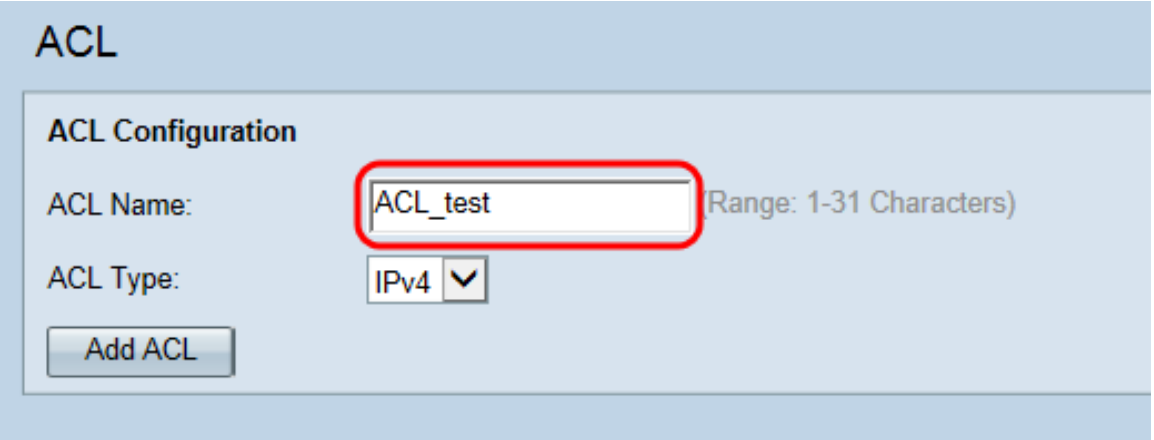
ACL Rule Configuration

ACL Configuration

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

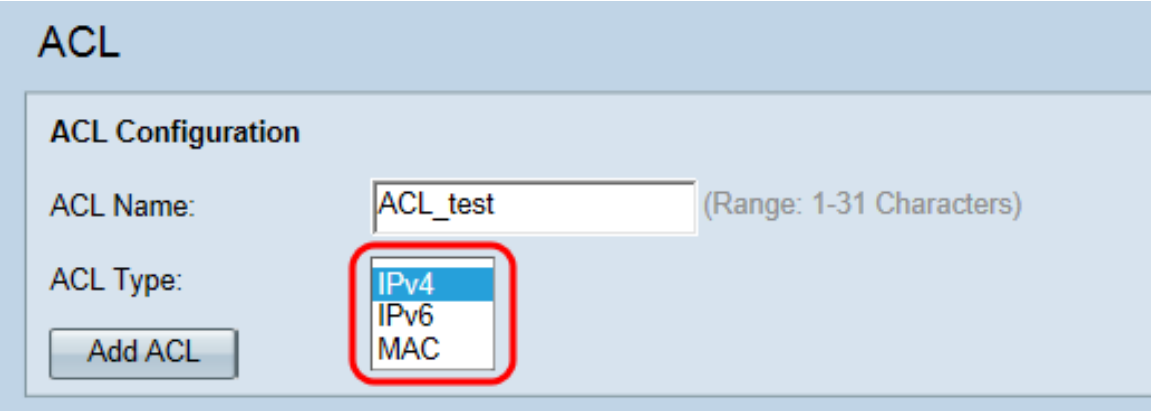


Step 2. Enter the desired ACL name in the *ACL Name* field. The range is from 1-31 characters.



Note: The ACL name is an identifier for the particular ACL; it has no impact on the operation of the device.

Step 3. Select the ACL type from the *ACL Type* drop-down list.

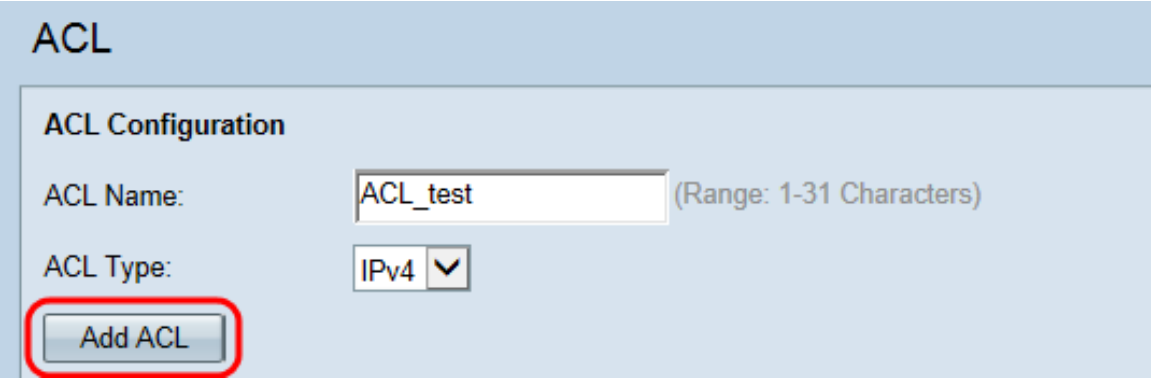


The options are as follows:

- IPv4 – A 32-bit (four-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.

Note: IPv4 and IPv6 ACLs control access to network resources based on Layer 3 and Layer 4 criteria. MAC ACLs control access based on Layer 2 criteria.

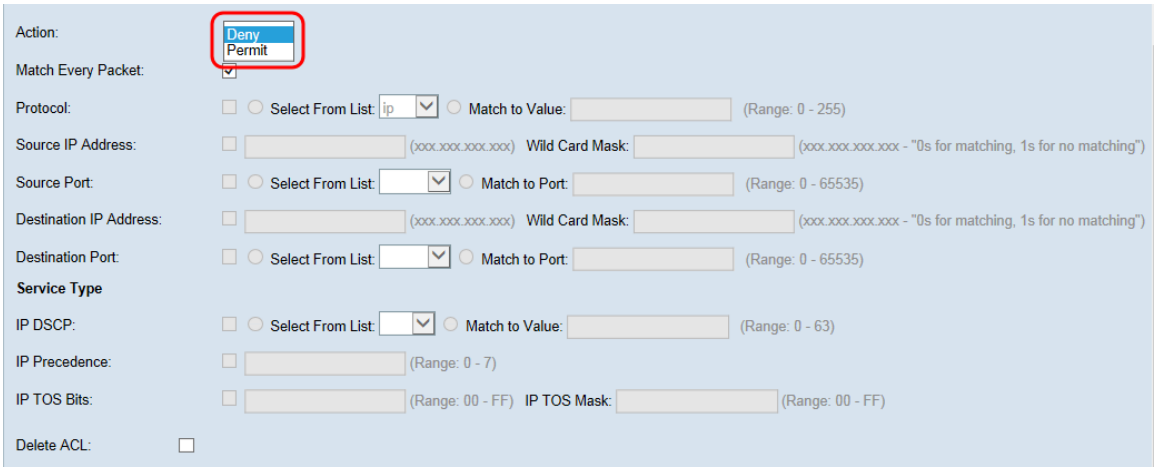
Step 4. Click **Add ACL** to add the new ACL.



ACL Rule Configuration for IPv4 and IPv6

Note: The following screenshots are for IPv4 ACL rules but are interchangeable with IPv6 ACL rules.

Step 1. Select an action for the rule from the *Action* drop-down list.

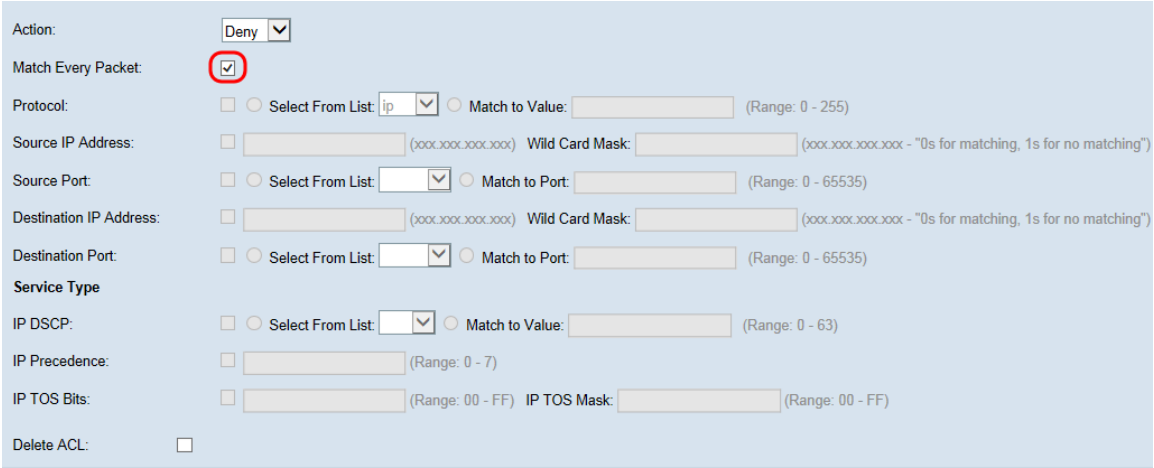


The options are described as follows:

- Permit – The rule allows all traffic that meets the rule criteria to enter or exit the WAP device. Traffic that does not meet the criteria is dropped.

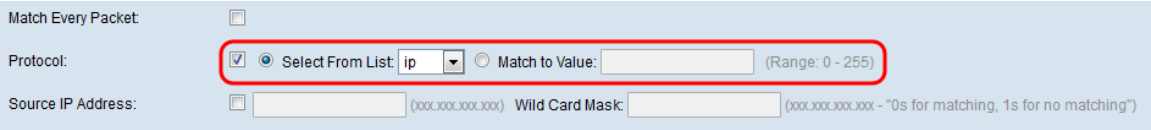
- Deny – The rule blocks all traffic that meets the rule criteria from entering or exiting the WAP device. Traffic that does not meet the criteria is forwarded to the next rule. If it is the final rule, the traffic that is not explicitly permitted is dropped.

Step 2. Check or uncheck the **Match Every Packet** checkbox. If selected, the rule, which either has a permit or deny action, matches the frame or packet regardless of its contents.



Note: If you select this field, you cannot configure any additional match criteria. The **Match Every Packet** option is selected by default for a new rule. You must clear the option to configure other match fields.

Step 3. Check the **Protocol** checkbox to use a L3 or L4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field in IPv6 packets. If the Protocol checkbox is checked, select one of the following radio buttons.



The options are described as follows:

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

  – IP – The Internet Protocol (IP) is the principle communications protocol in the Internet Protocol Suite for relaying data across networks.

  – ICMP – The Internet Control Message Protocol (ICMP) is a protocol in the Internet Protocol Suite that is used by devices like routers to send error messages.

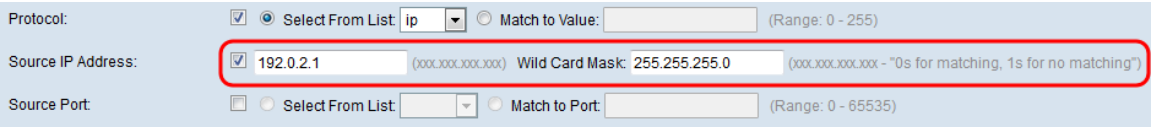
  – IGMP – The Internet Group Management Protocol (IGMP) is a communications protocol used by host to establish multicast group memberships on IPv4 networks.

  – TCP – The Transmission Control Protocol (TCP) enables two hosts to establish a connection and exchange streams of data.

  – UDP –The User Datagram Protocol is a protocol in the Internet Protocol Suite that uses a connectionless transmission model.

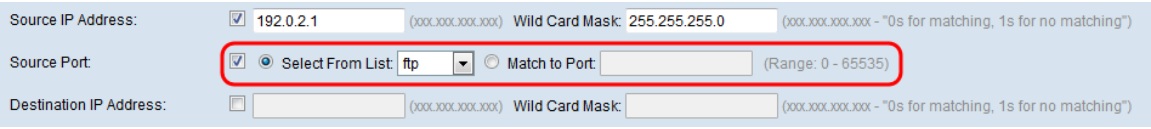
- Match to Value — Enter a standard IANA-assigned protocol ID which ranges from 0 to 255 for all unlisted protocols. Refer to *Assigned Internet Protocol Numbers* for more information on IANA-assigned protocol IDs.

Step 4. Check the **Source IP Address** checkbox to include an IP address of the source in the match condition. Enter the IP address and wild card mask of the source in their respective fields. The wild card mask determines which bits of the source address are used and which are ignored. It can be thought of as an inverted subnet mask. This is useful for indicating the size of a network or subnet for some routing protocols or to permit or deny a range of IP addresses.



Note: The Wild Card Mask field is required if the **Source IP Address** checkbox is checked.

Step 5. Check the **Source Port** checkbox to include a source port in the match condition. If the **Source Port** checkbox is checked, select one of the following radio buttons.



The options are described as follows:

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

  – FTP – The File Transfer Protocol (FTP) is 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 – The Hypertext Transfer Protocol (HTTP) is an application protocol that is the foundation of data communication for the World Wide Web.

– SMTP – The Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission.

– SNMP – The Simple Network Management Protocol (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.

– TFTP – The Trivial File Transfer Protocol (TFTP) is an Internet software utility for transferring files that is simpler to use than FTP but less capable.

– WWW – The World Wide Web is a system of Internet servers that support HTTP formatted documents.

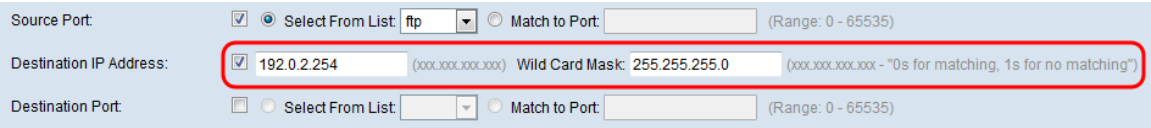
- Match to Port — Enter the port number which ranges from 0 to 65535 in the *Match to Port* field for unlisted source ports. The range includes three different types of ports. The ranges are described as follows:

  – 0 to 1023 — Well known ports.

  – 1024 to 49151 — Registered ports.

  – 49152 to 65535 — Dynamic and/or Private ports.

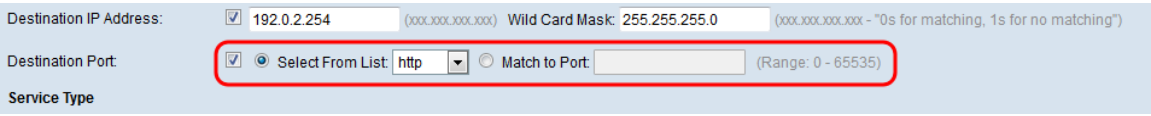
Step 6. Check the **Destination IP Address** checkbox to include the IP address of the destination in the match condition. Enter the IP address and wild card mask of the destination in their respective fields. The wild card mask determines which bits of the source address are used and which are ignored. It can be thought of as an inverted subnet mask. This is useful for indicating the size of a network or subnet for some routing protocols or to permit or deny a range of IP addresses.



Note: The *Wild Card Mask* field is required if the **Destination IP Address** checkbox is checked.

Note: If you wish to match only a single IP address, use the wild card mask of 0.0.0.0.

Step 7. Check the **Destination Port** checkbox to include a destination port in the match condition. If the **Destination Port** check box is checked, select one of the following radio buttons.



The options are described as follows:

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

  – FTP – The File Transfer Protocol (FTP) is 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 – The Hypertext Transfer Protocol (HTTP) is an application protocol that is the foundation of data communication for the World Wide Web.

  – SMTP – The Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission.

  – SNMP – The Simple Network Management Protocol (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.

  – TFTP – The Trivial File Transfer Protocol (TFTP) is an Internet software utility for transferring files that is simpler to use than FTP but less capable.

  – WWW – The World Wide Web is a system of Internet servers that support HTTP formatted documents.

- Match to Port — Enter the port number which ranges from 0 to 65535 in the *Match to Port* field for unlisted destination 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.

Note: Only one of the services can be selected from the Service Type area and can be added for the match condition.

ACL Rule Service Type Configuration for IPv4

Step 1. Check the **IP DSCP** checkbox to match the packets based on IP DSCP values. DSCP is used to specify the traffic priorities over the IP header of the frame. This categorizes all packets for the associated traffic stream with the IP DSCP value that you select from the list. If the IP DSCP checkbox is checked, select one of the following radio buttons.

The options are described as follows:

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

  – DSCP Assured Forwarding (AS) - Allows the operator to provide assurance of delivery as long as the traffic does not exceed some subscribed rate.

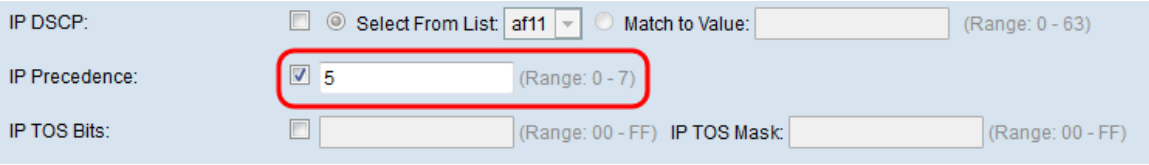
  – Class of Service (CS) – Allows backward compatibility with network devices that still use the Precedence field.

  – Expedited Forwarding (EF) - Used to build a low loss, low latency, low jitter, assured bandwidth, end-to-end service through DS (DiffServ) domains.

- Match to Value — Enter the DSCP value which ranges from 0 to 63 in the *Match to Value* field to customize DSCP values.

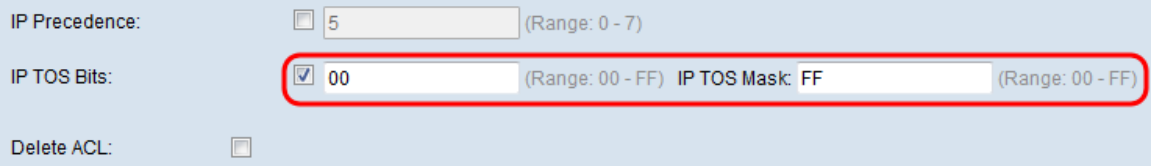
Note: Refer to *DSCP and Precedence Values* for further details on DSCP.

Step 2. Check the **IP Precedence** checkbox to include an IP Precedence value in the match condition. This is a mechanism for assigning a priority to each IP packet where 0 is the lowest priority and 7 is the highest. If the **IP Precedence** checkbox is checked, enter an IP precedence value which ranges from 0 to 7.



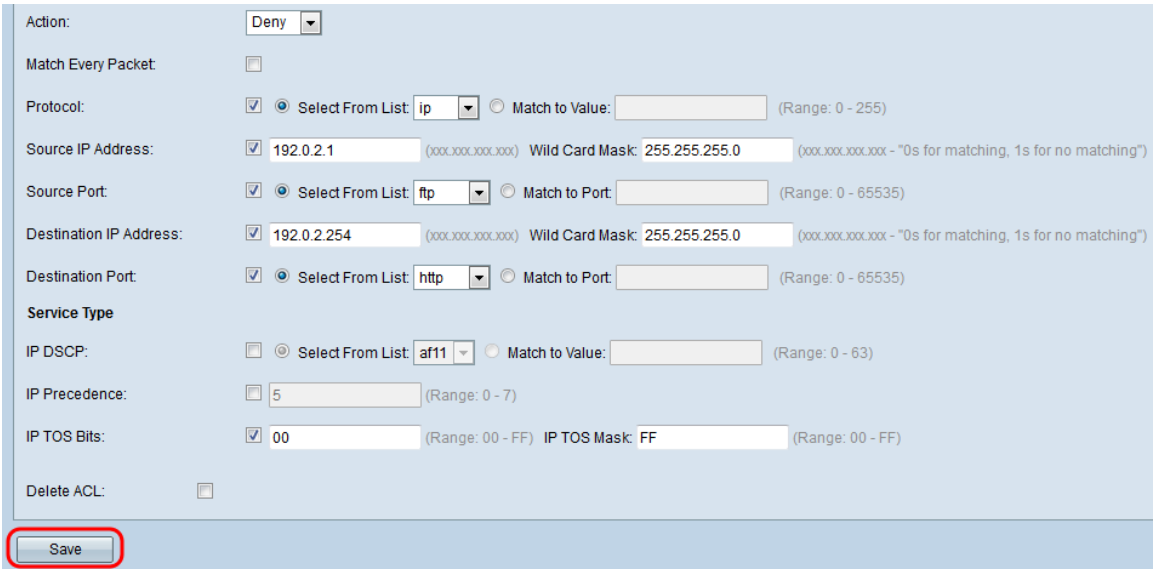
Note: Refer to *DSCP and Precedence Values* for further details on IP Precedence.

Step 3. Check the **IP TOS Bits** checkbox to use the packet's Type of Service (TOS) bits in the IP header as match criteria. A TOS field is used to specify a datagram's priority and route it accordingly. If the IP TOS Bits checkbox is checked, enter the IP TOS bits which ranges from 00-FF and IP TOS mask which ranges from 00-FF in their respective fields.



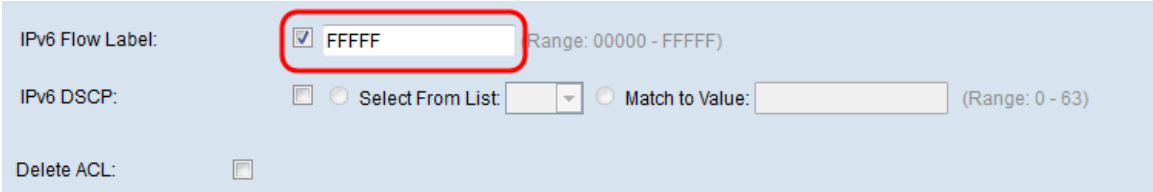
Step 4. (Optional) If you want to delete the configured ACL then, check the **Delete ACL** checkbox.

Step 5. Click **Save** to save the settings.

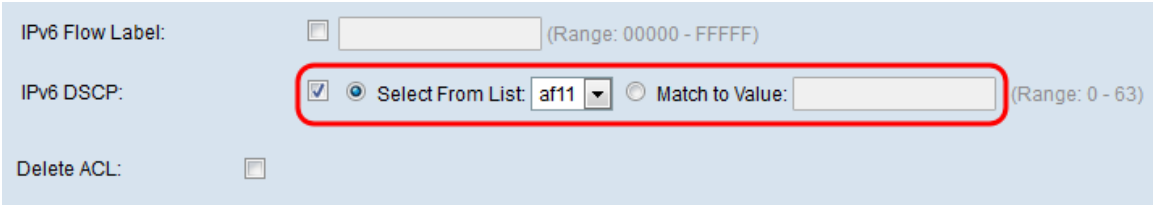


ACL Rule Configuration for IPv6

Step 1. Check the **IPv6 Flow Label** checkbox to set a 20-bit number that is unique to an IPv6 packet. It is used by end stations to signify QoS handling in routers (range 0 to 1048575).



Step 2. Check the **IPv6 DSCP** checkbox to match the packets based on IP DSCP values. DSCP is used to specify the traffic priorities over the IP header of the frame. This categorizes all packets for the associated traffic stream with the IP DSCP value that you select from the list. If the **IPv6 DSCP** checkbox is checked, select one of the following radio buttons.



The options are described as follows:

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

  – DSCP Assured Forwarding (AS) - allows the operator to provide assurance of delivery as long as the traffic does not exceed some subscribed rate.

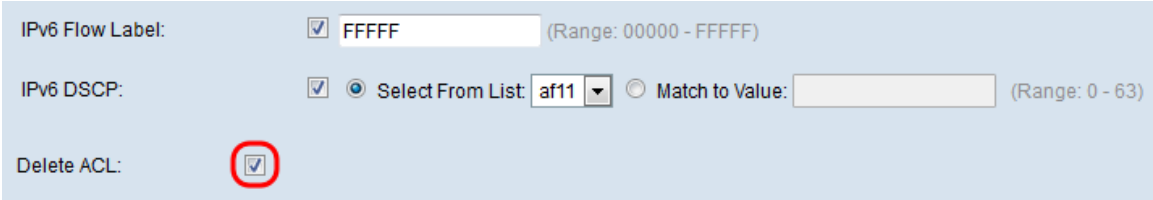
  – Class of Service (CS) – allows backward compatibility with network devices that still use the Precedence field.

  – Expedited Forwarding (EF) - Is used to build a low loss, low latency, low jitter, assured bandwidth, end-to-end service through DS (DiffServ) domains.

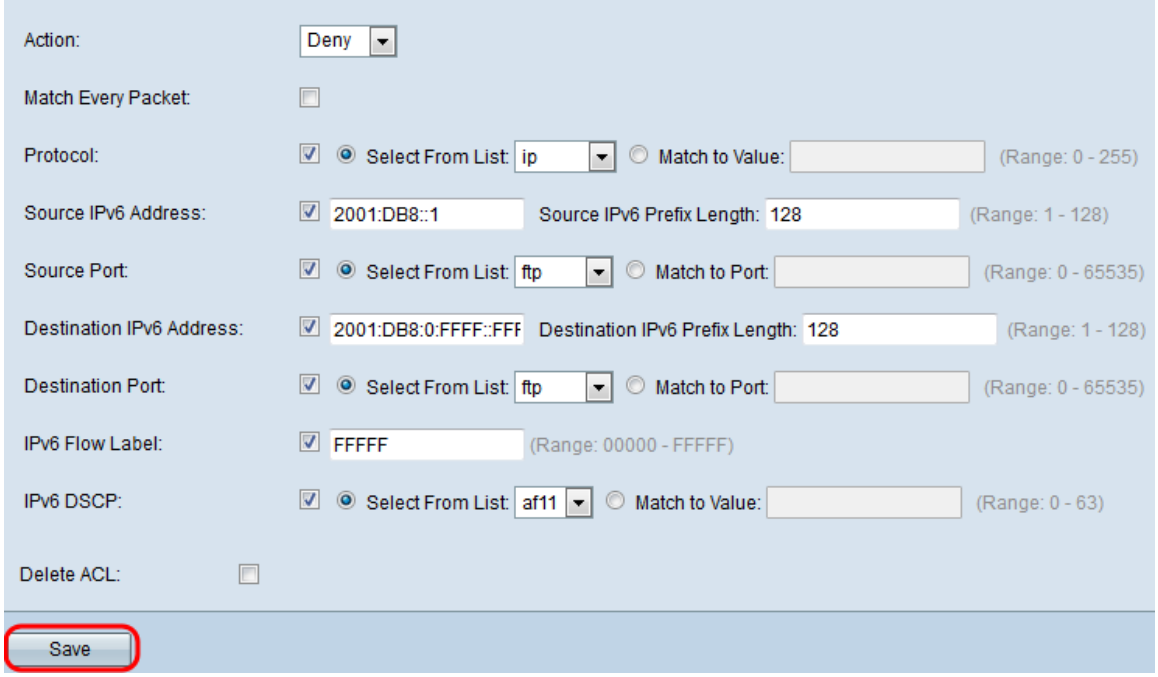
• Match to Value — Enter the DSCP value which ranges from 0 to 63 in the *Match to Value* field to customize DSCP values.

Note: Refer to *DSCP and Precedence Values* for further details on DSCP.

Step 3. (Optional) If you want to delete the configured ACL then, check the **Delete ACL** checkbox.

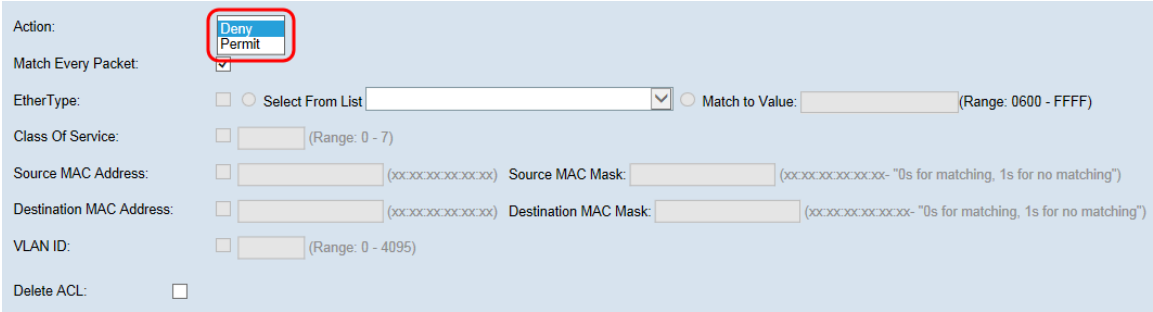


Step 4. Click **Save** to save the settings.



ACL Rule Configuration for MAC

Step 1. Select an action for the rule from the *Action* drop-down list.

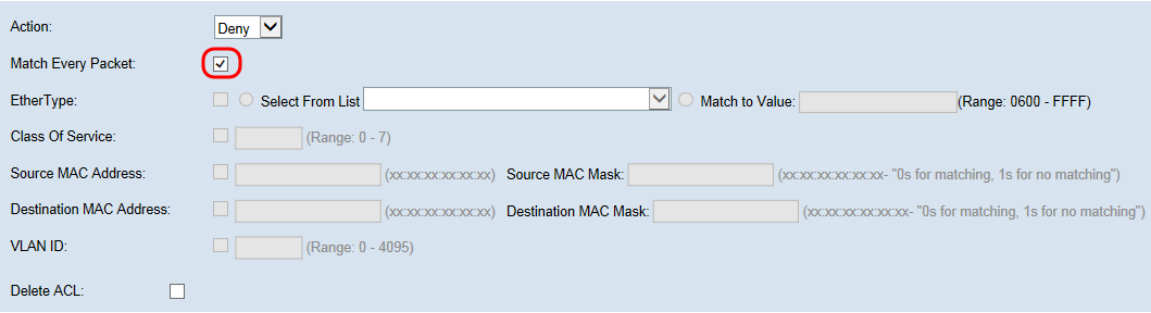


The options are described as follows:

• Permit – The rule allows all traffic that meets the rule criteria to enter or exit the WAP device. Traffic that does not meet the criteria is dropped.

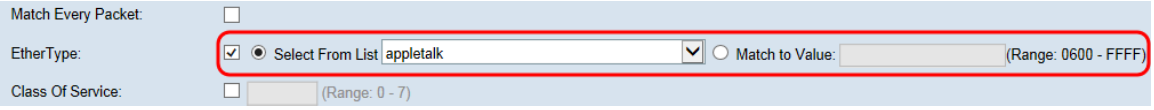
• Deny – The rule blocks all traffic that meets the rule criteria from entering or exiting the WAP device. Traffic that does not meet the criteria is forwarded to the next rule. If it is the final rule, the traffic that is not explicitly permitted is dropped.

Step 2. Check or uncheck the **Match Every Packet** checkbox. If selected, the rule, which either has a permit or deny action, matches the frame or packet regardless of its contents.



Note: If you select this field, you cannot configure any additional match criteria. The **Match Every Packet** option is selected by default for a new rule. You must clear the option to configure other match fields.

Step 3. Check the **Ether Type** checkbox to compare the match criteria against the value in the header of an Ethernet frame. If the **Ether Type** checkbox is checked, select one of the following radio buttons.



The options are described as follows:

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

– AppleTalk - AppleTalk is a proprietary suite of networking protocols developed by Apple Inc. for their Macintosh computers. AppleTalk included a number of features that allowed local area networks to be connected with no prior setup or the need for a centralized router or server of any sort.

– ARP - The Address Resolution Protocol (ARP) is a telecommunication protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks.

– IPv4 - Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet.

– IPv6 - Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

– IPX - Internetwork Packet Exchange (IPX) is the network layer protocol in the IPX/SPX protocol suite. IPX is derived from Xerox Network Systems' IDP. It may act as a transport layer protocol as well.

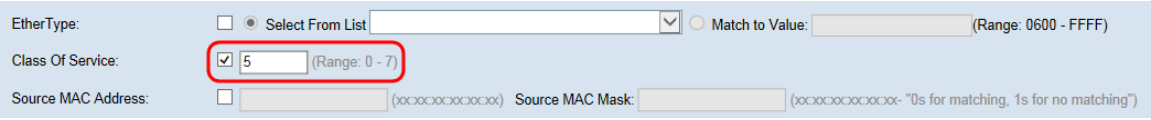
– NetBIOS - NetBIOS is an acronym for Network Basic Input/Output System. It provides

services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network. As strictly an API, NetBIOS is not a networking protocol.

– PPPOE - The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames.

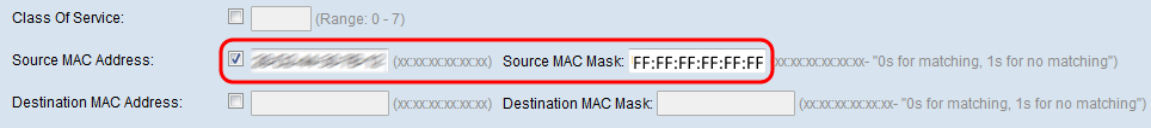
- Match to Value—Enter a custom protocol identifier to which packets are matched. The value is a four-digit hexadecimal number in the range of 0600 to FFFF.

Step 4. Check the **Class of Service** checkbox to enter an 802.1p user priority to compare against an Ethernet frame. Like IP Precedence, 0 is the lowest priority and 7 is the highest. The valid range is from 0 to 7.

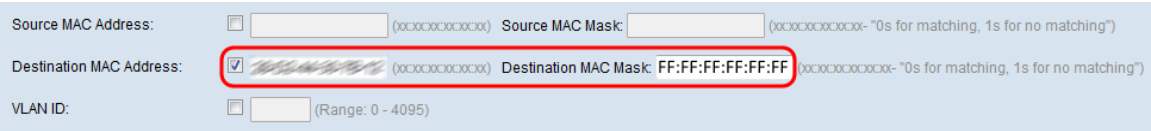


Step 5. Check the **Source MAC Address** checkbox to enter a source MAC address to compare against an Ethernet frame. If the Source MAC Address checkbox is checked, enter the source MAC address in the *Source MAC Address* field. Then enter the source MAC address mask in the *Source MAC Mask* field. This will specify which bits from the source MAC address will be compared against an Ethernet frame.

Note: If you wish to match only a single MAC address, use the wild card mask of 00:00:00:00:00:00.

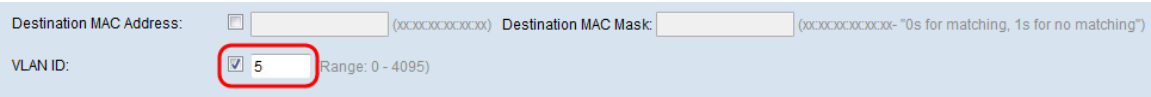


Step 6. Check the **Destination MAC Address** checkbox to enter a destination MAC address to compare against an Ethernet frame. If the Destination MAC Address checkbox is checked, enter the destination MAC address in the *Destination MAC Address* field. Then enter the MAC address mask in the *Destination MAC Mask* field. This will specify which bits from the destination MAC address will be compared against an Ethernet frame.

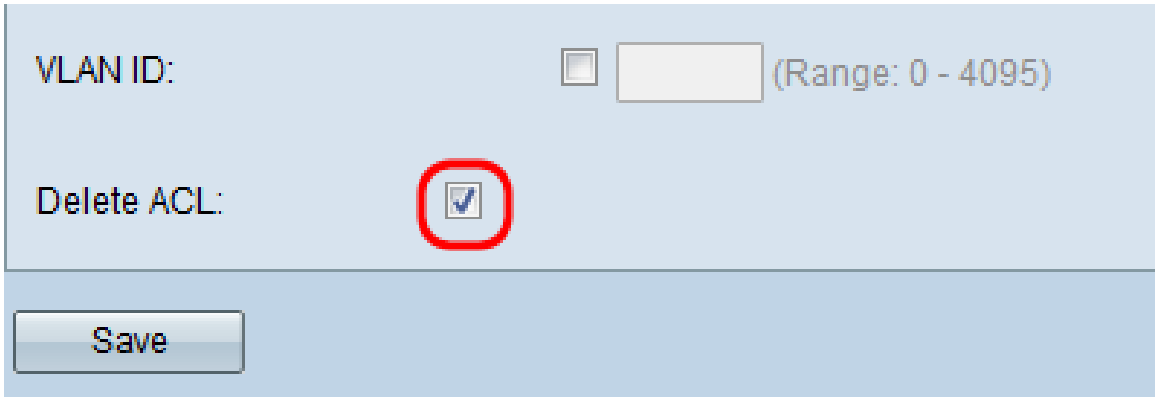


Note: If you wish to match only a single MAC address, use the wild card mask of 00:00:00:00:00:00.

Step 7. Check the **VLAN ID** checkbox to enter a VLAN ID to compare against an Ethernet frame. If the **VLAN ID** checkbox is checked, enter the VLAN ID in the *VLAN ID* field. The VLAN ID range is from 0-4095.



Step 8. (Optional) If you want to delete the configured ACL then, check the **Delete ACL** checkbox.



Step 9. Click **Save** to save the settings.