Creation and Configuration of MAC Based Access Control List (ACL) on the WAP121 and WAP321 Access Points

Objective

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

This article explains how to create and configure MAC ACL on WAP121 and WAP321 Access Points (WAP).

Applicable Devices

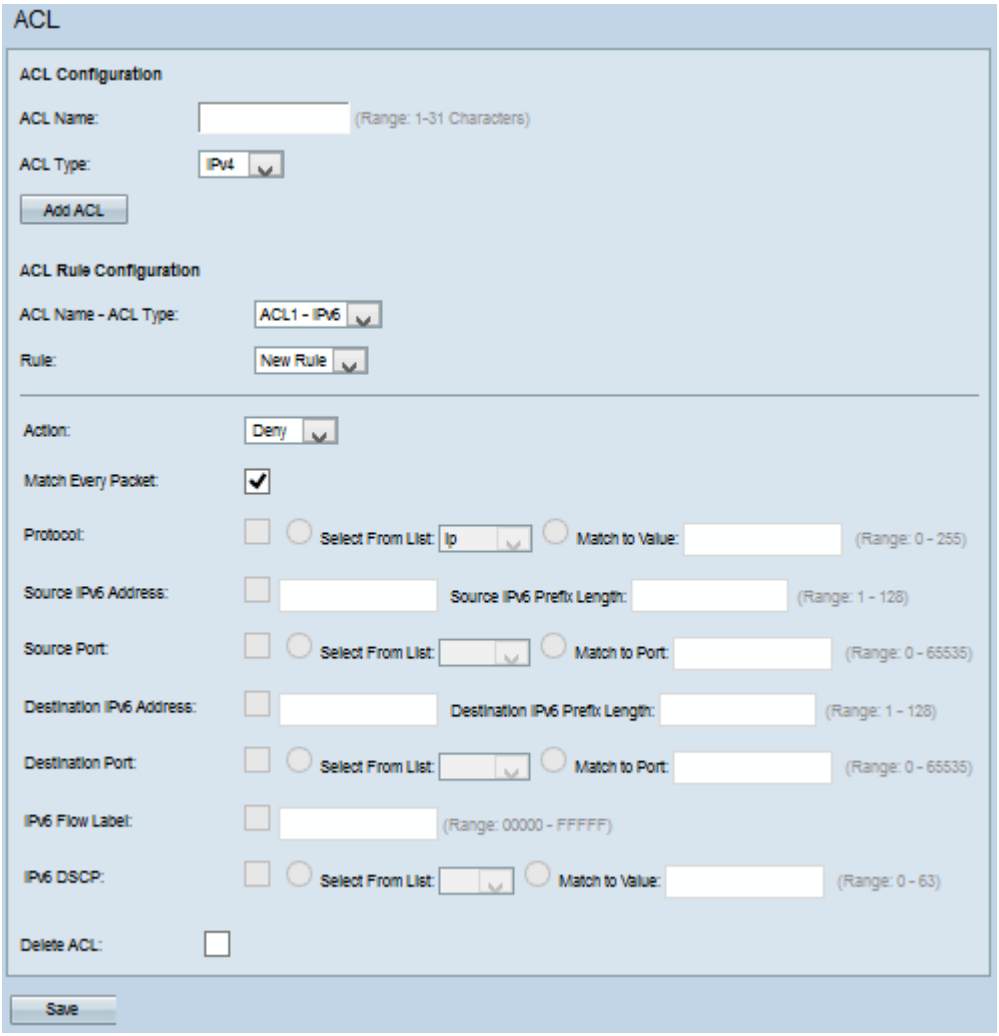
- WAP121
- WAP321

Software Version

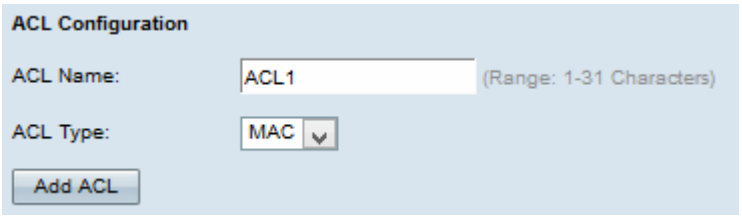
- v1.0.3.4

Creation of MAC based ACL

Step 1. Log in to the Access Point Configuration Utility and choose **Client QoS > ACL**. The *ACL* page opens:



Creation of a MAC based ACL

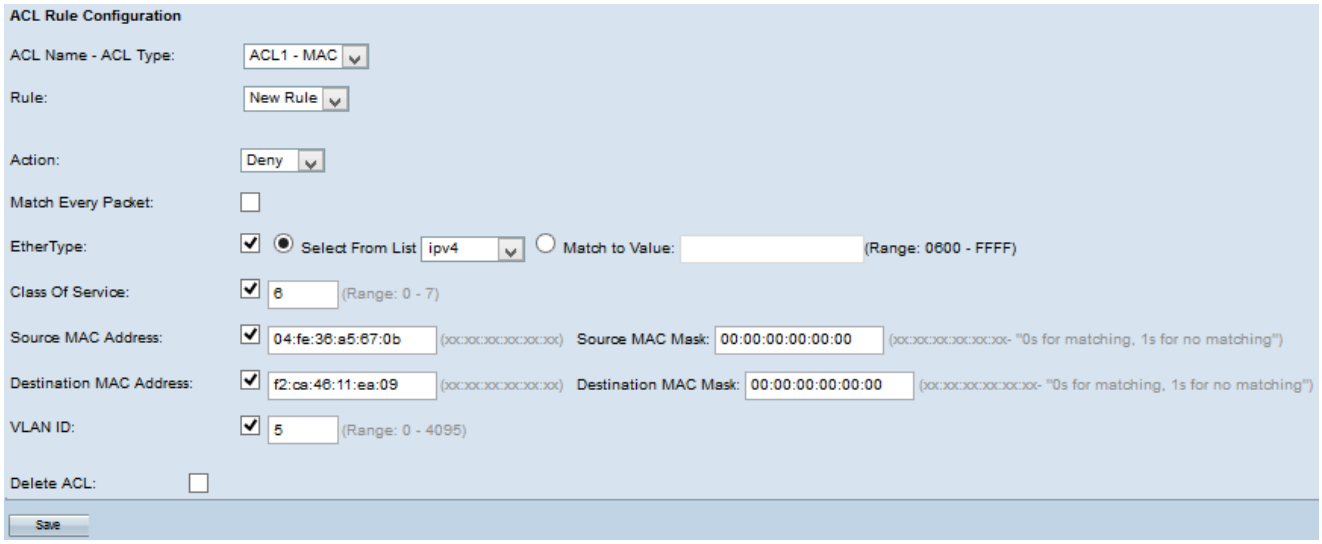


Step 1. Enter the name of the ACL in the *ACL Name* field.

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

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

Configuration of a Rule for MAC based ACL



Step 1. Choose the desired ACL from the *ACL Name - ACL Type* drop-down list.

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.

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.

- 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 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 **Match Every Packet** check box to configure any of the additional match criteria.

Timesaver: If **Match Every Packet** is checked then skip to Step 12.

Step 5. Check the **EtherType** check box to compare the match criteria against the value in the header of an Ethernet frame. If **EtherType** check box is checked, click one of these radio buttons.

- Select From List — Choose a protocol from the drop-down list. The drop-down list has appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe.
- Match to Value — For the custom protocol identifier. Enter the identifier which ranges from 0600 to FFFF.

Step 6. Check the **Class of Service** check box to enter 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.

Step 7. 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.

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

Step 9. 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.

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. 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.

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

Note: For information on how to create a new VLAN, refer the article *Configuration of Management and Untagged VLAN IDs on WAP121 and WAP321.*

Step 12. Click **Save** to save the settings.

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