Configuration of IPv4 and IPv6 based Access Control List (ACL) on WAP551 and WAP561 Access Points

Objective

Access Lists (ACLs) are collections of permit and deny conditions, called rules, that provide security to block unauthorized users and allow authorized users to access specific resources. ACLs can block any unwarranted attempts to reach network resources. The QoS feature contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

This article explains how to create and configure IPv4 and IPv6 based ACL on WAP551 and WAP561 Access Points (WAP).

Applicable Devices

- WAP551
- WAP561

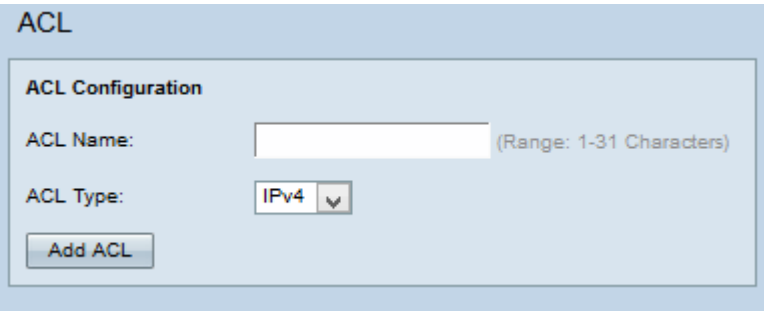
Software Version

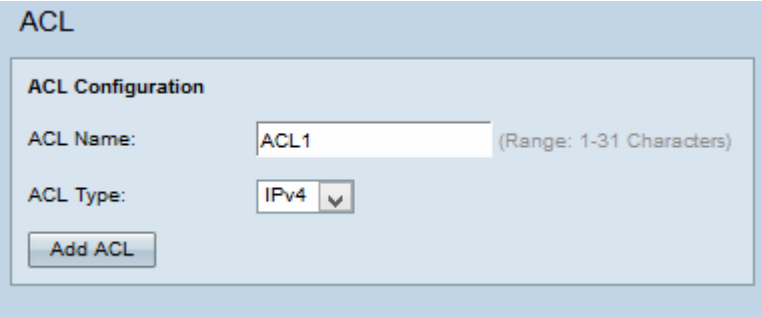
- v1.0.4.2

ACL Configuration

IP ACLs classify traffic for Layer 3 in the IP stack. Each ACL is a set of up to 10 rules applied to traffic sent from a wireless client or to be received by a wireless client. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network. Rules can be based on various criteria and may apply to one or more fields within a packet, such as the source or destination IP address, the source or destination port, or the protocol carried in the packet.

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





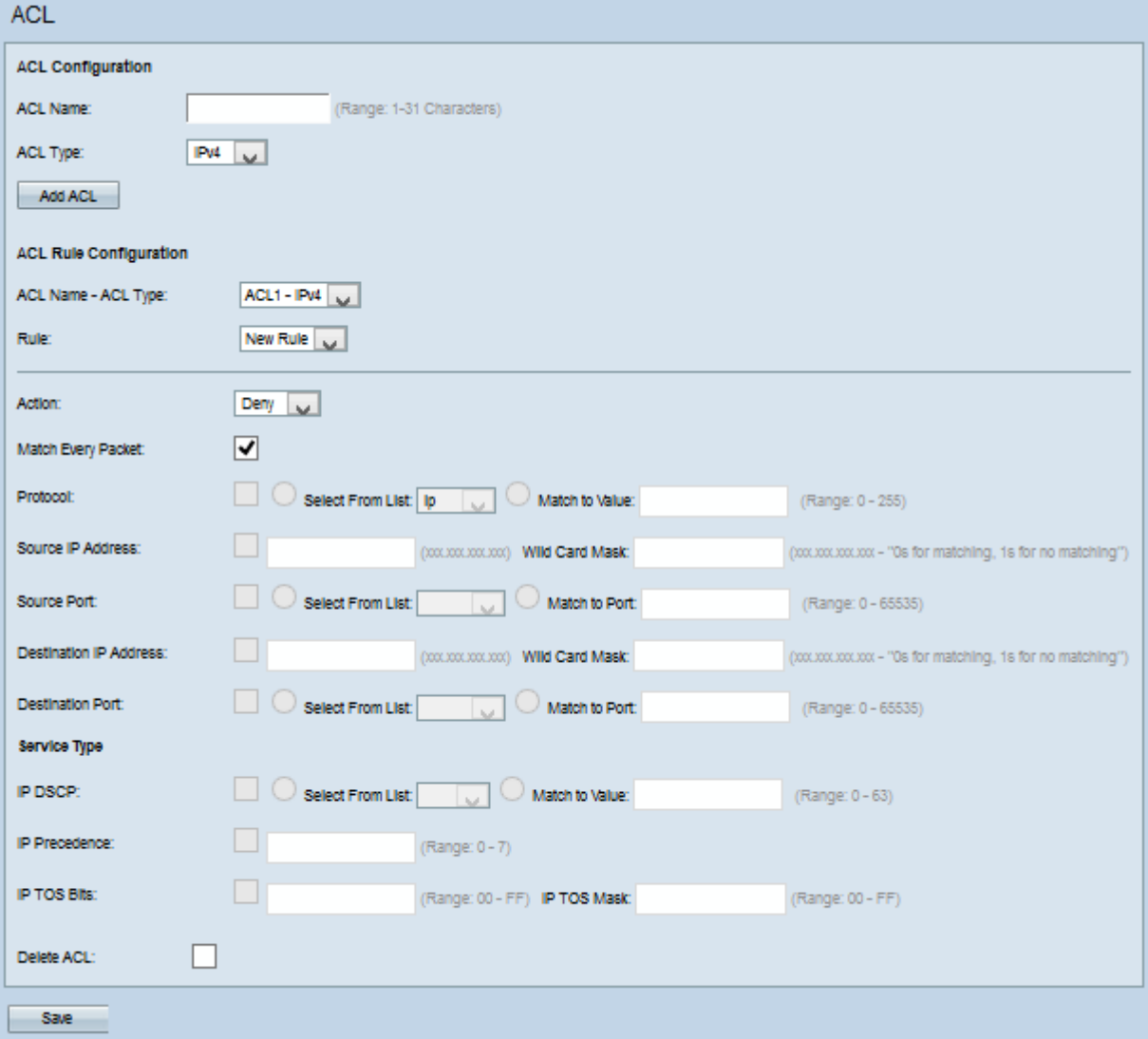
Step 2. Enter the name of the ACL in the ACL Name field.

Step 3. Choose the desired type of ACL from the ACL Type drop-down list. If IPv6 is chosen refer to the *IPv6 ACL Configuration* section. If MAC Based ACL is chosen from the ACL Type drop-down list refer to article *Configuration of MAC Based Access Control List (ACL) on WAP551 and WAP561 Access Points*.

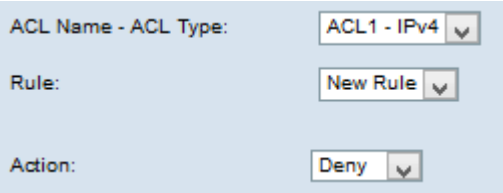
Step 4. Click **Add ACL** to create a new ACL.

IPv4 ACL Configuration

Note: If IPv4 is chosen from the ACL Type drop-down list, follow the steps below to configure the IPv4 ACL Rules.



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

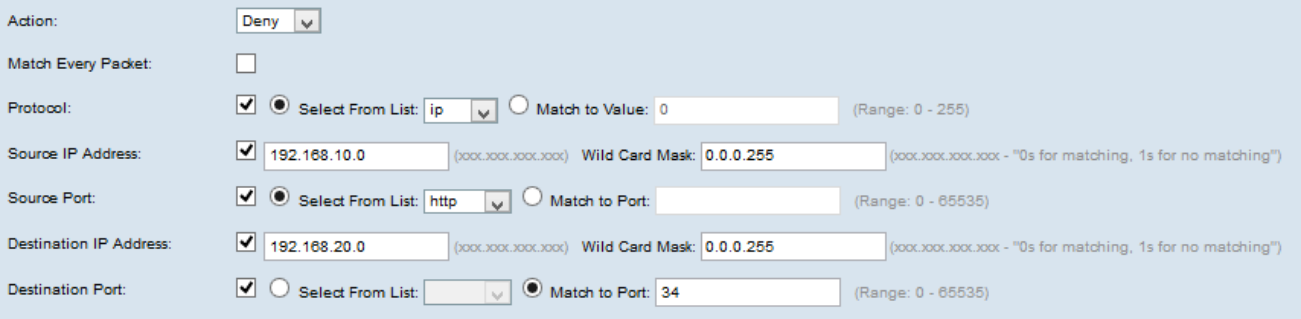


Step 2. If a new rule has to be configured, and if there are less than 10 rules for the selected ACL, choose **New Rule** from the Rule drop-down list. Otherwise, choose one of the present rules from the Rule drop-down list.

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: All of the following steps are optional. Boxes that are checked will be enabled. Uncheck the box if you do not want to apply a 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 additional match criteria.

Timesaver: If Match Every Packet is checked then skip to Step 10.

Step 5. Check the **Protocol** check box to use an L3 or L4 protocol match condition based on the value of the IP Protocol field in IPv4 packets. If the Protocol check box is checked, click one of the these radio buttons:

- Select From List — Protocol to choose from the Select From List drop-down list.
- Match to Value — For protocol not presented in the list. Enter a standard IANA-assigned protocol ID ranges from 0 to 255.

Step 6. Check the **Source IP Address** check box to include the IP address of the source in the match condition. Enter the IP address and wild card mask of the source in the respective fields.

Step 7. Check the **Source Port** check box to include a source port in the match condition. If the Source Port check box is checked, click one of these radio buttons:

- Select From List — Source port to choose from the Select From List drop-down list.
- Match to Port — For source port not presented in the list. Enter the port number which

ranges 0 to 65535 and includes three different types of ports.

– 0 to 1023 — Well known ports.

– 1024 to 49151 — Registered ports.

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

Step 8. Check the **Destination IP Address** check box to include the IP address of the destination in the match condition. Enter the IP address and wild card mask of the destination in the respective fields.

Step 9. Check the **Destination Port** check box to include a destination port in the match condition. If the Destination Port check box is checked, click one of these radio buttons.

• Select From List — Destination port to choose from the Select From List drop-down list.

• Match to Port — For destination port not presented in the list. Enter the port number which ranges from 0 to 65535 in the Match to Port field. The range includes three different types of ports.

– 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.

Step 10. Check the **IP DSCP** check box to match the packets based on IP DSCP values. If IP DSCP check box is checked, click one of these radio buttons:

• Select From List — Choose the desired IP DSCP value from the Select From List drop-down list.

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

Step 11. Check the **IP Precedence** check box to include a IP Precedence value in the match condition. If IP Precedence check box is checked, enter an IP precedence value which ranges from 0 to 7. The IP precedence values and the corresponding value description can be explained as follows:

• 0 — Routine or Best Effort

• 1 — Priority

• 2 — Immediate

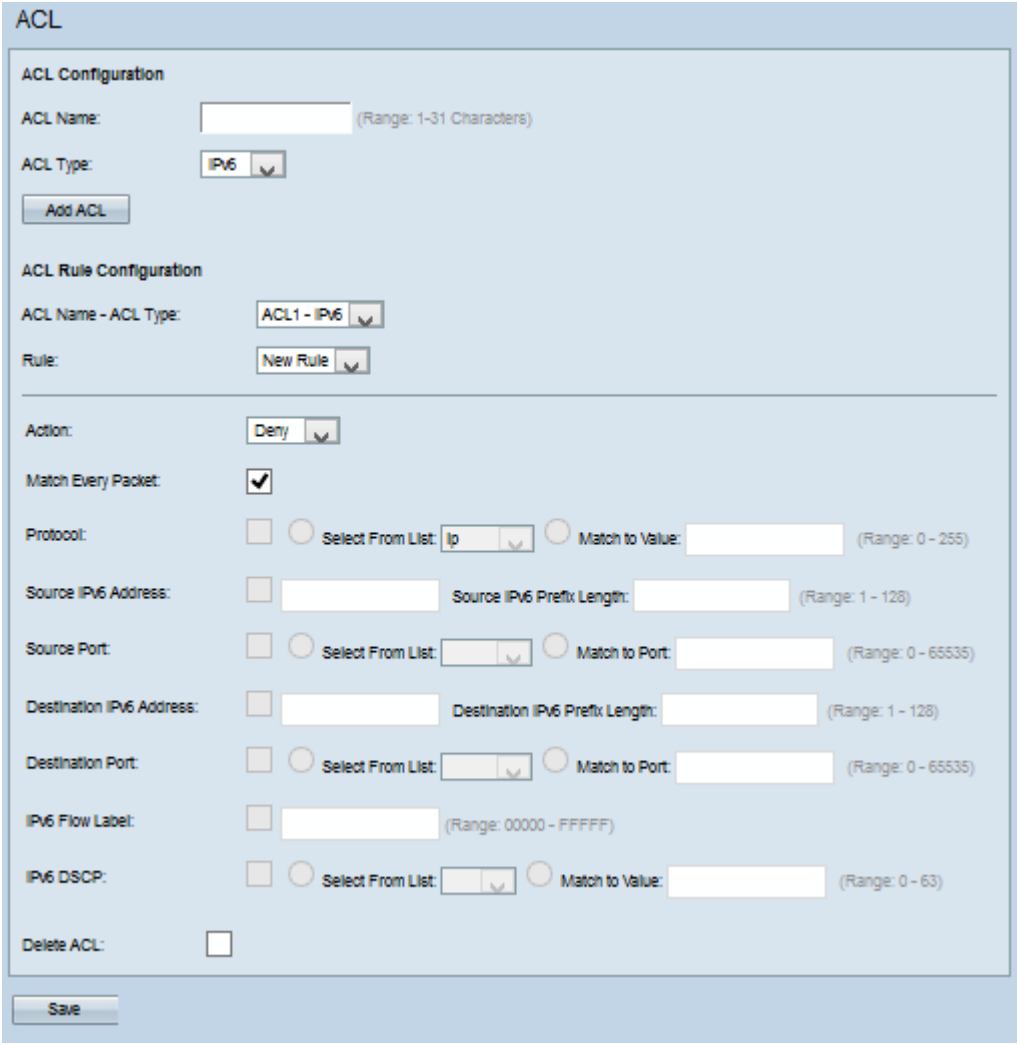
- 3 — Flash (mainly used for voice signaling or for video)
- 4 — Flash Override
- 5 — Critical (mainly used for voice RTP)
- 6 — Internet
- 7 — Network

Step 12. Check the **IP TOS Bits** check box to use the Type of Service bits in the IP header as match criteria. If the IP TOS Bits check box is checked, enter the IP TOS bits which range from 00 to FF and IP TOS mask which ranges from 00 to FF in the respective fields.

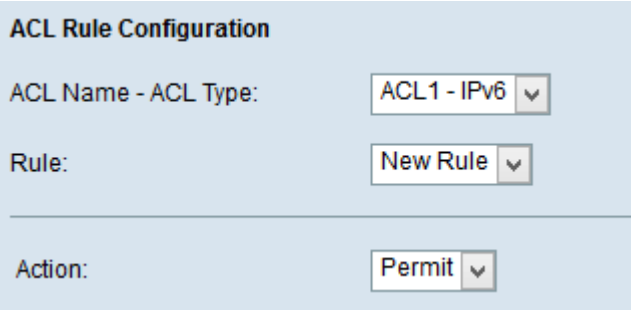
Step 13. To delete the configured ACL, check the **Delete ACL** check box and then click **Save**.

IPv6 ACL Configuration

Note: If IPv6 is chosen from the ACL Type drop-down list, follow the steps below to configure the IPv6 ACL Rules.



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

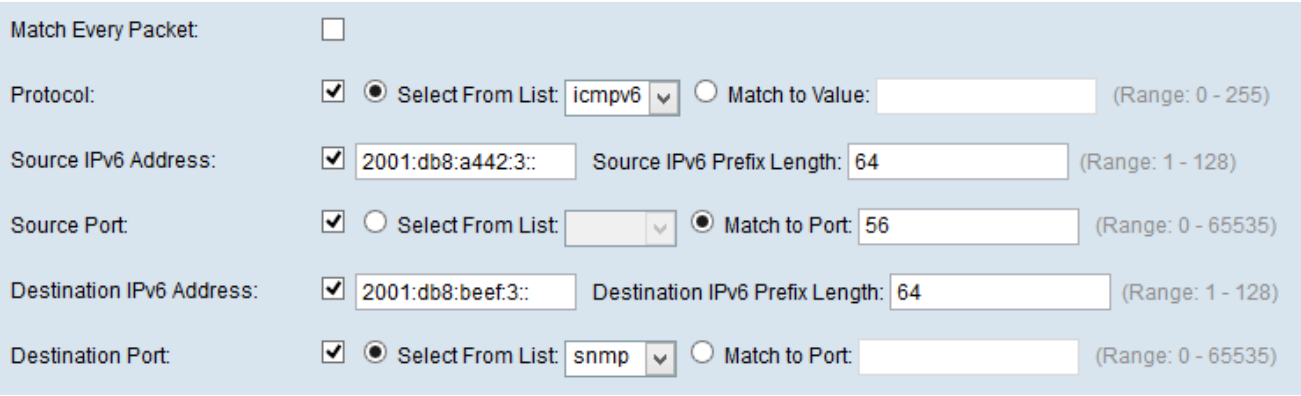


Step 2. If new rule has to be configured for the selected ACL, choose **New Rule** from the Rule drop-down list. Otherwise choose one of the present rules from the Rule drop-down list.

Note: 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: All of the following steps are optional. Boxes that are checked will be enabled. Uncheck the box if you do not want to apply a 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 additional match criteria.

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

Step 5. Check the **Protocol** check box to use an L3 or L4 protocol match condition based on the value of the IP Protocol field in IPv6 packets. If the Protocol check box is checked, click one of the these radio buttons.

- Select From List — Protocol to choose from the Select From List drop-down list.
- Match to Value — For protocol not presented in the list. Enter a standard IANA-assigned protocol ID ranges from 0 to 255.

Step 6. Check the **Source IP Address** check box to include a IP address of the source in the match condition. Enter the IP address and wild card mask of the source in the respective fields.

Step 7. Check the **Source Port** check box to include a source port in the match condition. If the Source Port check box is checked, click one of the following radio buttons:

• Select From List — Source port to choose from the Select From List drop-down list.

• Match to Port — For source ports not presented in the list. Enter the port number which ranges 0 to 65535 and includes three different types of ports.

– 0 to 1023 — Well known ports.

– 1024 to 49151 — Registered ports.

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

Step 8. Check the **Destination IP Address** check box to include the IP address of the destination in the match condition. Enter the IP address and wild card mask of the destination in the respective fields.

Step 9. Check the **Destination Port** check box to include a destination port in the match condition. If the Destination Port check box is checked, click one of these radio buttons:

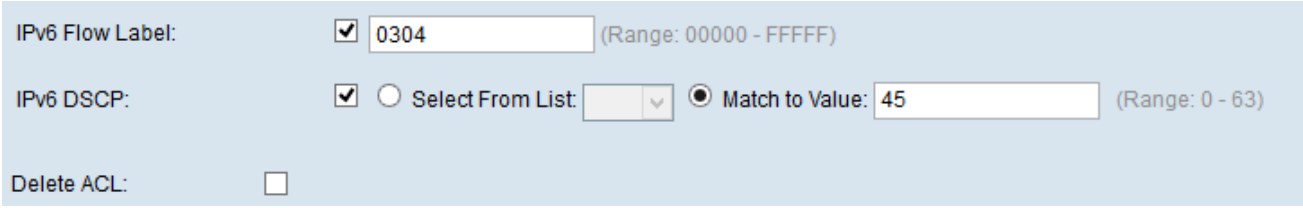
• Select From List — Destination port to choose from the Select From List drop-down list.

• Match to Port — For destination port not presented in the list. Enter the port number which ranges from 0 to 65535 in the Match to Port field. The range includes three different types of ports.

– 0 to 1023 — Well Known Ports.

– 1024 to 49151 — Registered Ports.

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



Step 10. Check the **IPv6 Flow label** check box to include the IPv6 flow label in the match condition. The 20-bit flow label field in the IPv6 header can be used by a source to label a set of packets belonging to the same flow. Enter the number which ranges from 00000 to FFFFF in the IPv6 Flow label field.

Step 11. Check the **IPv6 DSCP** check box to include the IP DSCP values in the match condition. If IP DSCP check box is checked, click one of these radio buttons.

• Select From List — IP DSCP value to choose from the Select From List drop-down list.

• Match to Value — To customize DSCP value which ranges from 0 to 63.

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

Step 13. Click **Save**.