Configuration of Client Quality Of Service (QoS) Association on WAP551 and WAP561 Access Points

Objective

Client QoS Association provides control over certain QoS aspects of wireless clients connected to the network. These QoS aspects include the amount of bandwidth allowed to a client, the ACL type that is required to control general categories of traffic like HTTP traffic, and the DiffServ policy. All of these are useful tools to characterize each wireless client that goes both inbound and outbound when it is authenticated on the network.

The article explains how to configure the Client QoS Association on WAP551 and WAP561 access points.

Applicable Devices

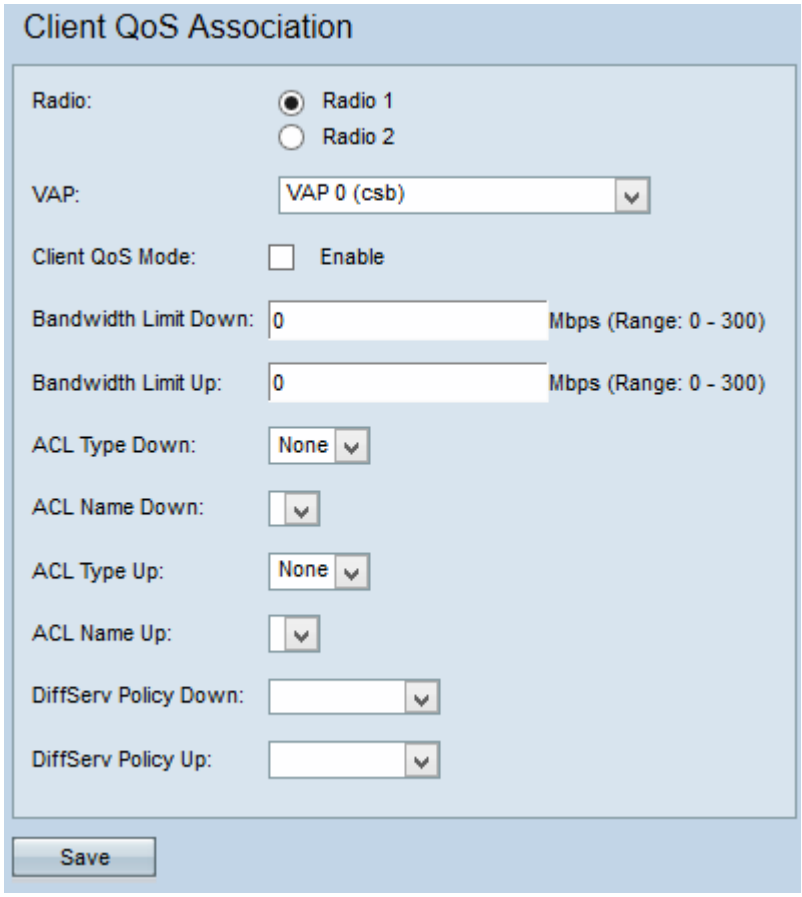
- WAP551
- WAP561

Software Version

- v1.0.4.2

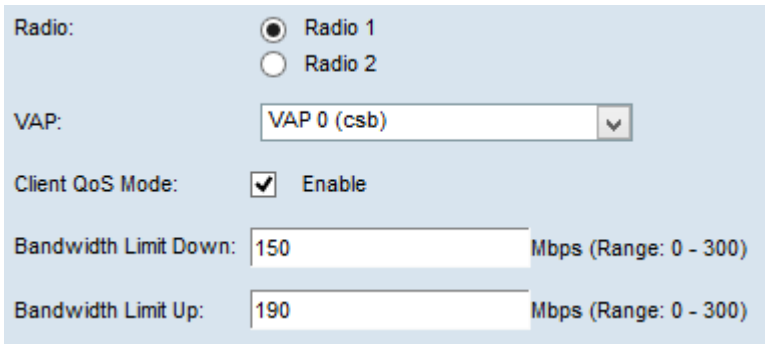
Client QoS Association

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



Step 2. Click the desired radio button for the configuration to apply to from the Radio field.

Note: Step 2 is available only for the WAP561 Access Point as the WAP551 has only one radio.

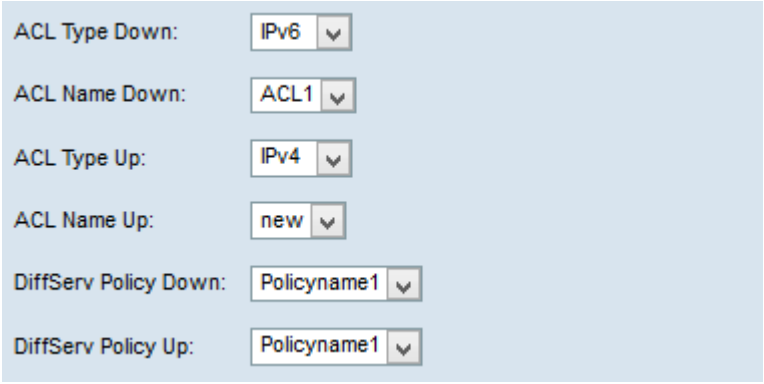


Step 3. From the VAP drop-down list, choose the VAP for which you want to configure the Client QoS parameters.

Step 4. Check **Enable** for the Client QoS Mode check box to enable Client QoS Mode.

Step 5. In the Bandwidth Limit Down field, enter the number of Mbps for transmission from the device to the client.

Step 6. In the Bandwidth Limit Up field, enter the number of Mbps for transmission from the client to the device.



Note: To find out how to create an IPv4 and IPv6 rule, refer to the article, *Configuration of IPv4 and IPv6 Based Access Control List (ACL) on WAP551 and WAP561 Access Points*.

Step 7. From the ACL Type Down drop-down list, choose either **IPv4**, **IPv6**, or **MAC** for inbound traffic.

- IPv4 — IPv4 packets will be examined for matches to the ACL rules.
- IPv6 — IPv6 packets will be examined for matches to the ACL rules.
- MAC — Layer 2 frames will be examined for matches to the ACL rules.

Step 8. From the ACL Name Down drop-down list, choose your ACL that will be applied to outbound traffic.

Step 9. From the ACL Type Up drop-down list, choose either **IPv4**, **IPv6**, or **MAC** for outbound traffic.

- IPv4 — IPv4 packets will be examined for matches to the ACL rules.
- IPv6 — IPv6 packets will be examined for matches to the ACL rules.
- MAC — Layer 2 frames will be examined for matches to the ACL rules.

Step 10. From the ACL Name Up drop-down list, choose your ACL that will be applied to inbound traffic.

Step 11. From the DiffServ Policy Down drop-down list, choose your policy map that will be applied to outbound traffic.

Step 12. From the DiffServ Policy Up drop-down list, choose your policy map that will be applied to inbound traffic.

Note: To find out how to add policy, refer to the article, *Policy Map Configuration on WAP551 and WAP561 Access Points*.

Step 13. Click **Save**.