Client Quality Of Service (QoS) Association Configuration on the WAP121 and WAP321 Access Points

Objective

Client Quality Of Service (QoS) Association is used to control the wireless clients connected to the network, and allows you to manage bandwidth that the clients can use. Client QoS Association also allows you to control the traffic such as the HTTP traffic or traffic from a specific subnet by the use of Access Control Lists (ACLs). An 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. ACLs can block any unwarranted attempts to reach network resources.

This document explains how to configure the Client QoS Association settings on WAP121 and WAP321 access points.

Applicable Devices

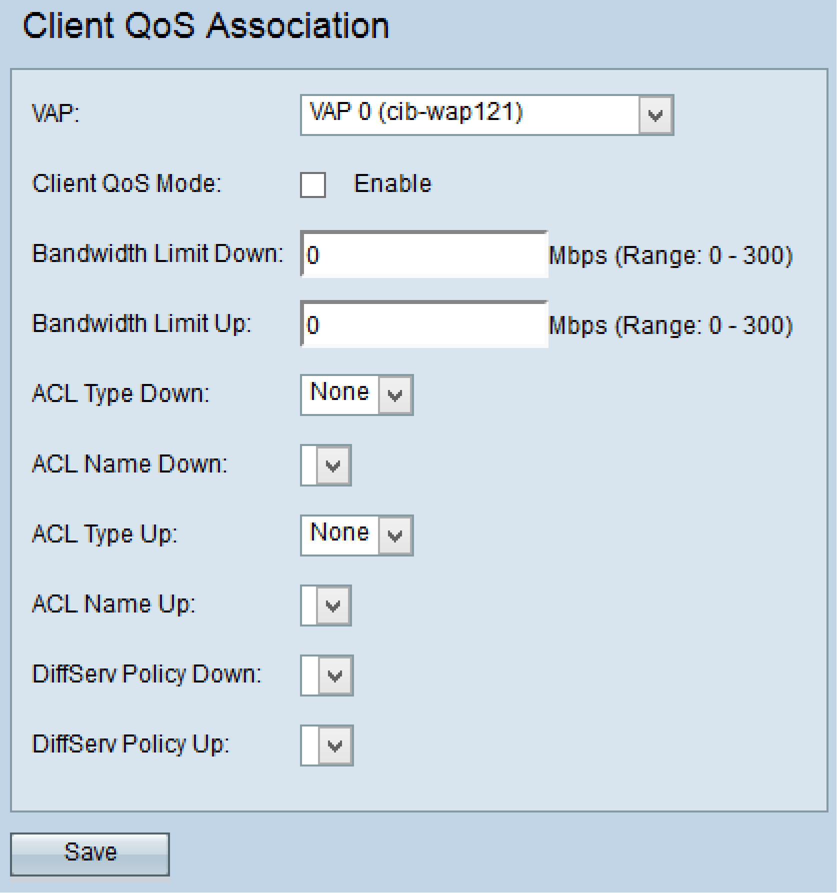
- WAP121
- WAP321

Software Version

- 1.0.3.4

Client QoS Association

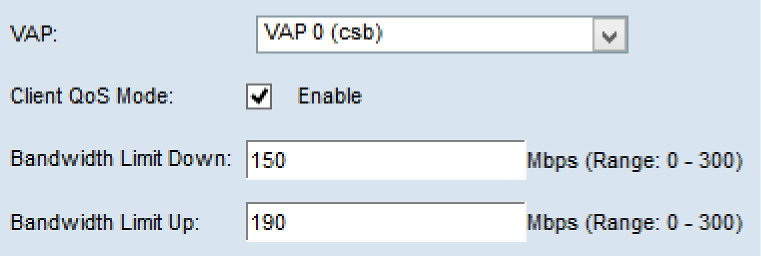
Step 1. Log in to the Access Point Configuration Utility and choose **Client QoS > Client QoS Association**. The *Client QoS Association* page opens:



Client QoS Association

VAP:	VAP 0 (cib-wap121)
Client QoS Mode:	□ Enable
Bandwidth Limit Down:	0 Mbps (Range: 0 - 300)
Bandwidth Limit Up:	0 Mbps (Range: 0 - 300)
ACL Type Down:	None
ACL Name Down:	
ACL Type Up:	None
ACL Name Up:	
DiffServ Policy Down:	
DiffServ Policy Up:	

Step 2. From the VAP drop-down list, choose the VAP for which you want to configure the Client QoS parameters. A Virtual Access Point (VAP) is used to segment the wireless LAN into multiple broadcast domains. Each radio can contain up to a maximum of 16 VAPs.

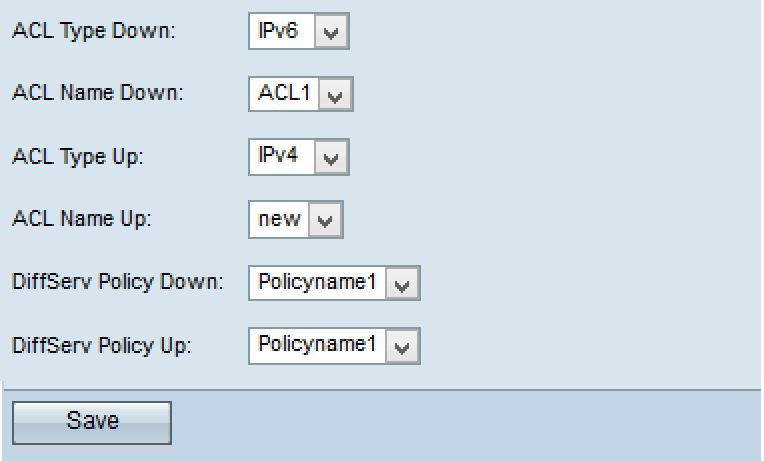


VAP:	VAP 0 (csb)
Client QoS Mode:	☑ Enable
Bandwidth Limit Down:	150 Mbps (Range: 0 - 300)
Bandwidth Limit Up:	190 Mbps (Range: 0 - 300)

Step 3. Check **Enable** for the Client QoS Mode check box to enable Client QoS Mode. This enables QoS service for the chosen VAP.

Step 4. In the Bandwidth Limit Down field, enter the number of Mbps permitted for transmission from the device to the client.

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



ACL Type Down:	IPv6
ACL Name Down:	ACL1
ACL Type Up:	IPv4
ACL Name Up:	new
DiffServ Policy Down:	Policyname1
DiffServ Policy Up:	Policyname1

Step 6. From the ACL Type Down drop-down list, choose an option 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.

Note: To know how to create an IPv4 rule, refer to the article, *Creation and Configuration of a Rule for IPv4 Based Access Control List (ACL) on WAP121 and WAP321 Access Points* *and* *Creation and Configuration of IPv4 Based Class Map on WAP121 and WAP321 Access Points*. To know how to create an IPv6 rule, refer to the article, *Creation and Configuration of a Rule for IPv6 Based Access Control List (ACL) on WAP121 and WAP321 Access Points* *and* *Creation and Configuration of IPv6 Based Class Map on WAP121 and WAP321 Access Points*.

Step 7. From the ACL Name Down drop-down list, choose the ACL that will be applied to outbound traffic.

Step 8. From the ACL Type Up drop-down list, choose an option 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 9. From the ACL Name Up drop-down list, choose your ACL that will be applied to inbound traffic.

Note: Please refer the article *Creation and Configuration of IPv4 Based Class Map on WAP121 and WAP321 Access Points* *and* *Creation and Configuration of IPv6 Based Class Map on WAP121 and WAP321 Access Points* for details on Class Map.

Step 10. From the DiffServ Policy Down drop-down list, choose your policy map that will be applied to outbound traffic. The Differentiated Services (DiffServ) policy is used to categorize the wireless clients based on inbound and outbound traffic. The configuration of Diffserv begins with configuration of class map, which classifies traffic with respect to the IP protocol and other parameters.

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

Note: To know how to add a policy map, refer to the article, *Add Policy Map on WAP121 and WAP321 Access Points*.

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