Konfiguration der Client Quality of Service (QoS) Association auf den Access Points WAP121 und WAP321

Ziel

Die Client Quality of Service (QoS)-Zuordnung wird verwendet, um die mit dem Netzwerk verbundenen Wireless-Clients zu kontrollieren. Sie ermöglicht die Verwaltung der Bandbreite, die die Clients verwenden können. Die Client-QoS-Zuordnung ermöglicht Ihnen auch die Steuerung des Datenverkehrs, z. B. des HTTP-Datenverkehrs oder des Datenverkehrs von einem bestimmten Subnetz mithilfe von Zugriffskontrolllisten (Access Control Lists, ACLs). Eine ACL ist eine Zusammenstellung von Zulassen- und Ablehnungsbedingungen (auch als Regeln bezeichnet), die Sicherheit bieten, nicht autorisierte Benutzer blockieren und autorisierten Benutzern den Zugriff auf bestimmte Ressourcen ermöglichen. ACLs können alle ungerechtfertigten Versuche blockieren, Netzwerkressourcen zu erreichen.

In diesem Dokument wird erläutert, wie die Client QoS Association-Einstellungen für WAP121- und WAP321-Access Points konfiguriert werden.

Anwendbare Geräte

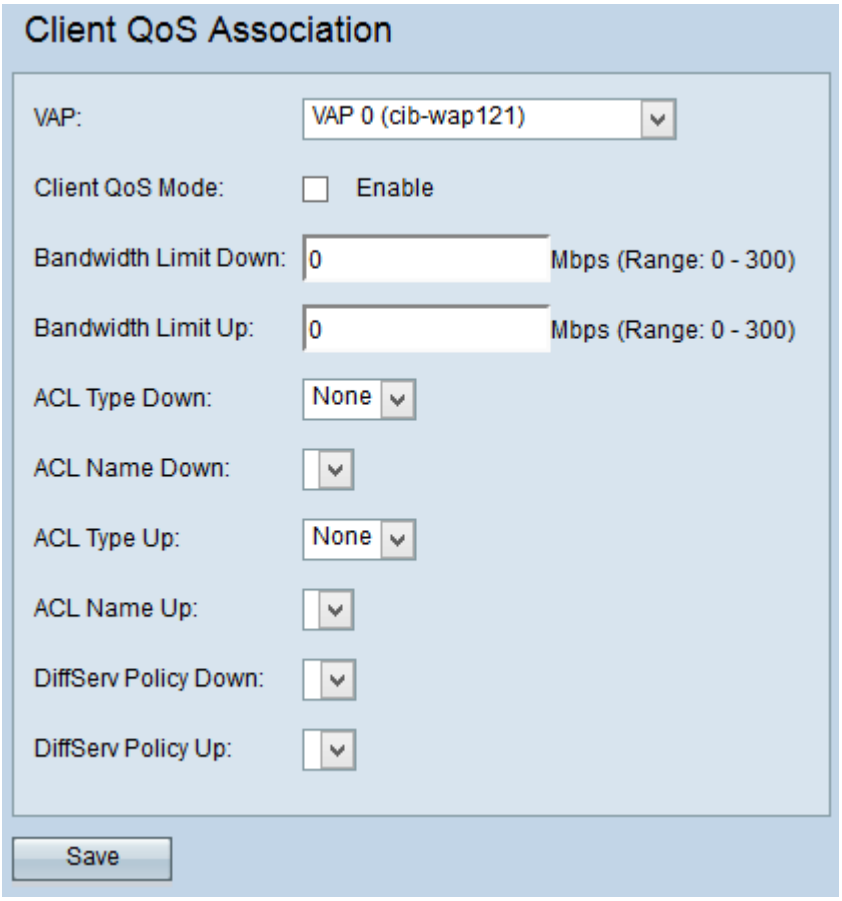
WAP121
WAP321

Softwareversion

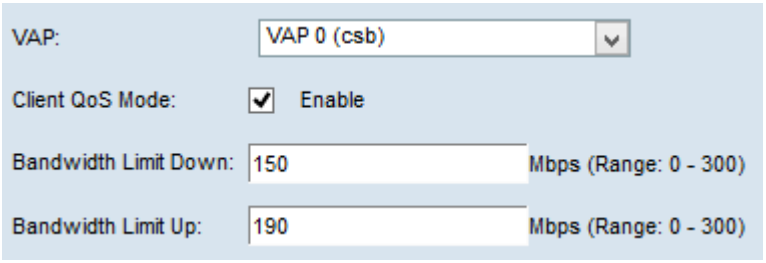
·1,0/3,4

Client-QoS-Zuordnung

Schritt 1: Melden Sie sich beim Konfigurationsprogramm für Access Points an, und wählen Sie **Client QoS > Client QoS Association aus**. Die Seite *Client QoS Association* wird geöffnet:



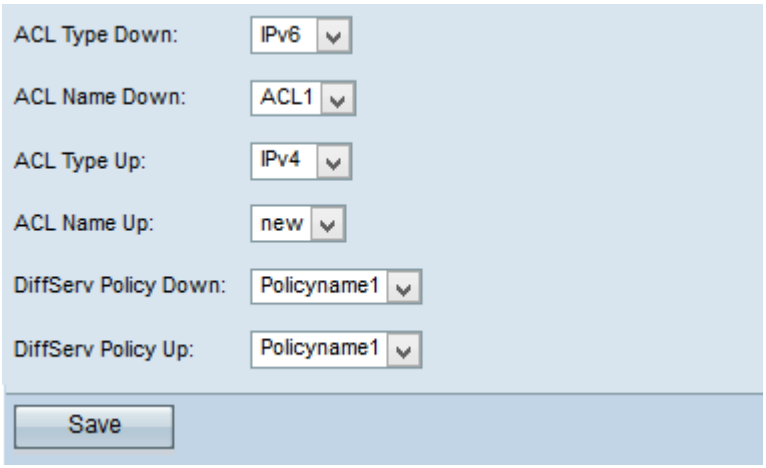
Schritt 2: Wählen Sie aus der VAP-Dropdown-Liste den VAP aus, für den Sie die Client QoS-Parameter konfigurieren möchten. Ein Virtual Access Point (VAP) dient zum Segmentieren des WLAN in mehrere Broadcast-Domänen. Jede Funkeinheit kann maximal 16 VAPs enthalten.



Schritt 3: Aktivieren Sie das Kontrollkästchen **Aktivieren** für den Client-QoS-Modus, um den Client-QoS-Modus zu aktivieren. Dadurch wird der QoS-Service für den ausgewählten VAP aktiviert.

Schritt 4: Geben Sie im Feld "Bandwidth Limit Down" (Bandbreitenlimit nach unten) die Anzahl der Mbit/s ein, die für die Übertragung vom Gerät zum Client zulässig sind.

Schritt 5: Geben Sie im Feld "Bandwidth Limit Up" (Bandbreitenlimit nach oben) die Anzahl der Mbit/s ein, die für die Übertragung vom Client zum Gerät zulässig sind.



Schritt 6: Wählen Sie in der Dropdown-Liste ACL Type Down (ACL-Typ-Down) eine Option für ausgehenden Datenverkehr aus.

·IPv4 - IPv4-Pakete werden auf Übereinstimmungen mit den ACL-Regeln geprüft.

·IPv6 - IPv6-Pakete werden auf Übereinstimmungen mit den ACL-Regeln geprüft.

·MAC - Layer-2-Frames werden auf Übereinstimmungen mit den ACL-Regeln geprüft.

Hinweis: Informationen zum Erstellen einer IPv4-Regel finden Sie im Artikel *Erstellen und Konfigurieren einer Regel für eine IPv4-basierte Zugriffskontrollliste (ACL) auf WAP121 und WAP321 Access Points* sowie *Erstellen und Konfigurieren einer IPv4-basierten Klassenzuordnung auf WAP121 und WAP322. 1 Access Points*. Weitere Informationen zum Erstellen einer IPv6-Regel finden Sie im Artikel *Erstellen und Konfigurieren einer Regel für eine IPv6-basierte Zugriffskontrollliste (ACL) für WAP121 und WAP321 Access Points* sowie *Erstellen und Konfigurieren einer IPv6-basierten Klassenzuordnung für WAP121 und WAP321*. ...

Schritt 7: Wählen Sie in der Dropdown-Liste "ACL Name Down" (ACL-Name) die ACL aus, die auf ausgehenden Datenverkehr angewendet wird.

Schritt 8: Wählen Sie in der Dropdown-Liste "ACL Type Up" (ACL-Typ nach oben) eine Option für eingehenden Datenverkehr aus.

·IPv4 - IPv4-Pakete werden auf Übereinstimmungen mit den ACL-Regeln geprüft.

·IPv6 - IPv6-Pakete werden auf Übereinstimmungen mit den ACL-Regeln geprüft.

·MAC - Layer-2-Frames werden auf Übereinstimmungen mit den ACL-Regeln geprüft.

Schritt 9: Wählen Sie aus der Dropdown-Liste "ACL Name Up" (ACL-Name nach oben) die ACL aus, die auf eingehenden Datenverkehr angewendet wird.

Hinweis: Weitere Details zur Klassenzuordnung finden Sie im Artikel *Erstellen und Konfigurieren von IPv4-basierten Klassenzuordnungen auf WAP121- und WAP321-Zugangspunkten* und *Erstellen und Konfigurieren von IPv6-basierter Klassenzuordnung auf WAP121- und WAP321-Access Points.*

Schritt 10: Wählen Sie aus der Dropdown-Liste DiffServ Policy (DiffServ-Richtlinie) die Richtlinienzuordnung aus, die auf ausgehenden Datenverkehr angewendet wird. Die Differentiated Services (DiffServ)-Richtlinie dient zur Kategorisierung der Wireless-Clients anhand des ein- und ausgehenden Datenverkehrs. Die Konfiguration von Diffserv beginnt

mit der Konfiguration der Klassenzuordnung, die den Datenverkehr in Bezug auf das IP-Protokoll und andere Parameter klassifiziert.

Schritt 11: Wählen Sie aus der Dropdown-Liste DiffServ Policy Up (DiffServ-Richtlinie nach oben) Ihre Richtlinienzuordnung für eingehenden Datenverkehr aus.

Hinweis: Weitere Informationen zum Hinzufügen einer Richtlinienzuordnung finden Sie im Artikel *Add Policy Map on WAP121 and WAP321 Access Points.*

Schritt 12: Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.