Erstellung und Konfiguration einer MAC-basierten Zugriffskontrollliste (ACL) für die WAP121- und WAP321-Access Points

Ziel

Eine Zugriffskontrollliste (Access Control List, ACL) ist eine Sammlung von Zulassen- und Ablehnungsbedingungen, die als Regeln bezeichnet werden und Sicherheit bieten, nicht autorisierte Benutzer blockieren und autorisierten Benutzern den Zugriff auf bestimmte Ressourcen ermöglichen. Die ACL kann alle ungerechtfertigten Versuche blockieren, Netzwerkressourcen zu erreichen. MAC ACL ist eine Layer-2-ACL. Das Netzwerkgerät überprüft den Frame und die ACL-Regeln auf den Inhalt des Frames, z. B. die Quell- und Ziel-MAC-Adresse. Wenn eine der Regeln mit dem Inhalt übereinstimmt, wird im Frame eine Aktion für "Zulassen" oder "Ablehnen" ausgeführt.

In diesem Artikel wird erläutert, wie MAC ACL auf WAP121 und WAP321 Access Points (WAP) erstellt und konfiguriert wird.

Anwendbare Geräte

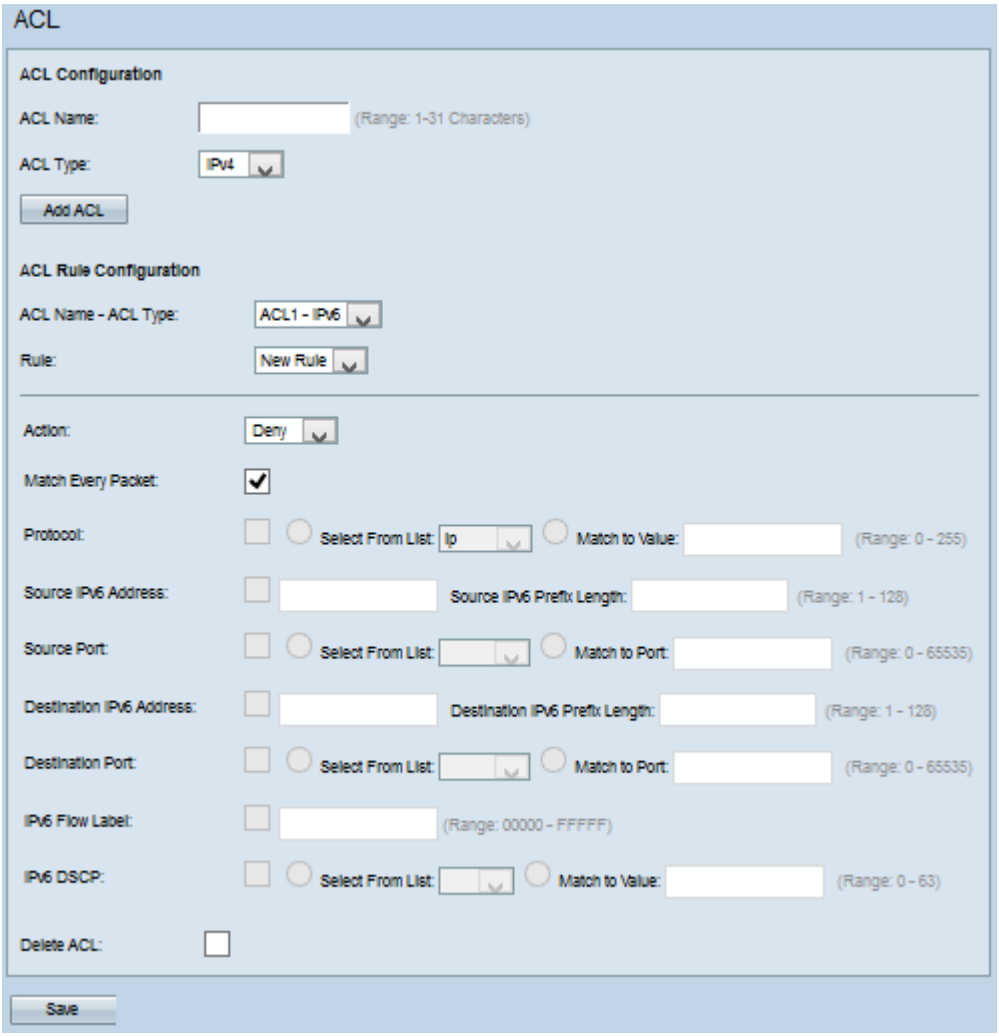
WAP121
WAP321

Softwareversion

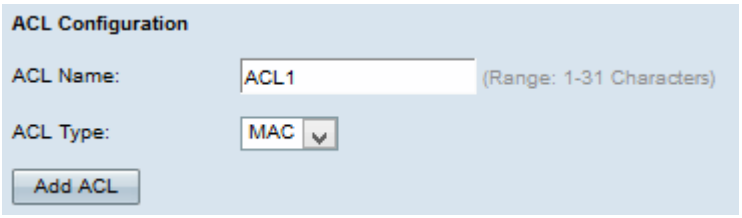
·v1.0.3.4

Erstellung MAC-basierter ACL

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



Erstellung einer MAC-basierten ACL

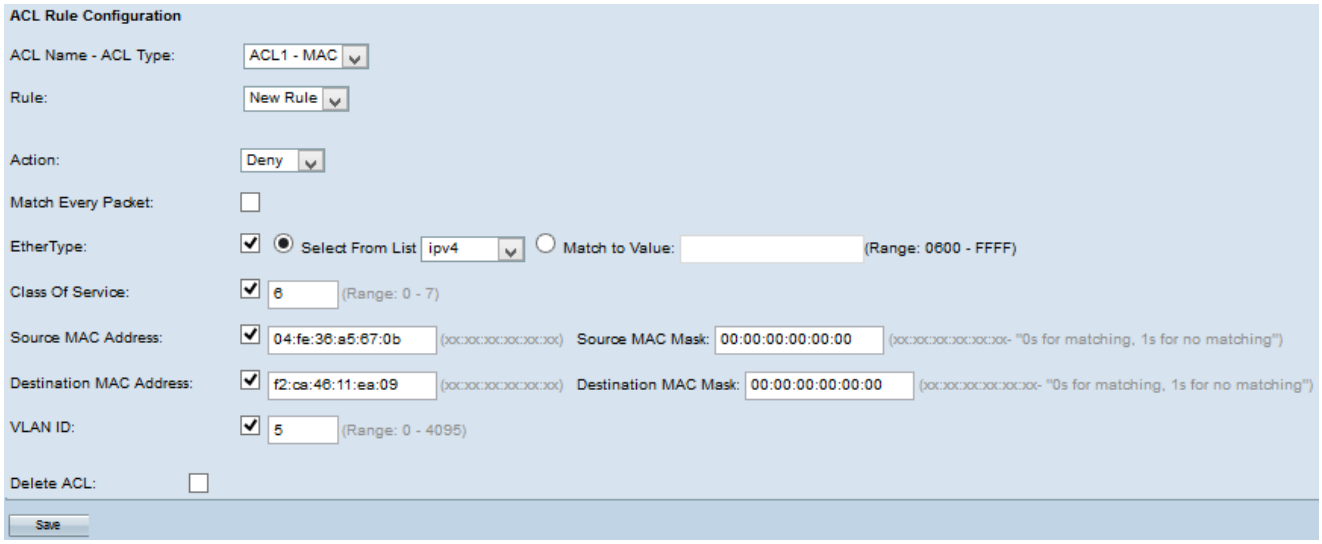


Schritt 1: Geben Sie im Feld *ACL Name* den Namen der ACL ein.

Schritt 2: Wählen Sie **MAC** für den ACL-Typ aus der Dropdown-Liste *ACL Type (ACL-Typ)* aus.

Schritt 3: Klicken Sie auf **ACL hinzufügen**, um eine neue MAC-ACL zu erstellen.

Konfiguration einer Regel für MAC-basierte ACL



Schritt 1: Wählen Sie die gewünschte ACL aus der Dropdown-Liste *ACL Name - ACL Type (ACL-Typ*) aus.

Schritt 2: Wenn für die ausgewählte ACL eine neue Regel konfiguriert werden muss, wählen Sie **Neue Regel** aus der *Regel*-Dropdown-Liste aus. Wählen Sie andernfalls eine der aktuellen Regeln aus der Dropdown-Liste *Regel*.

Hinweis: Es können maximal 10 Regeln für eine einzige ACL erstellt werden.

Schritt 3: Wählen Sie die Aktion für die ACL-Regel aus der Dropdown-Liste *Aktion* aus.

·Verweigern: Blockiert den gesamten Datenverkehr, der die Regelkriterien für die Ein- bzw. Ausfahrt des WAP-Geräts erfüllt.

·Zulassen - Ermöglicht allen Datenverkehr, der die Regelkriterien erfüllt, ein- oder auszusteigen.

Hinweis: Die Schritte 4 bis 11 sind optional. Aktivierte Filter sind aktiviert. Deaktivieren Sie das Kontrollkästchen für den Filter, wenn er nicht auf diese bestimmte Regel angewendet werden soll.

Schritt 4: Aktivieren Sie das Kontrollkästchen **Jedes Paket** zuordnen, um die Regel für jeden Frame oder jedes Paket zu übernehmen, unabhängig vom Inhalt. Deaktivieren Sie das Kontrollkästchen **Jedes Paket** zuordnen, um eines der zusätzlichen Anpassungskriterien zu konfigurieren.

Timesaver: Wenn **Jedes Paket zuordnen** aktiviert ist, fahren Sie mit Schritt 12 fort.

Schritt 5: Aktivieren Sie das Kontrollkästchen **EtherType**, um die Anpassungskriterien mit dem Wert im Header eines Ethernet-Frames zu vergleichen. Wenn das Kontrollkästchen **EtherType** aktiviert ist, klicken Sie auf eine dieser Optionsfelder.

·Aus Liste auswählen - Wählen Sie ein Protokoll aus der Dropdown-Liste aus. Die Dropdown-Liste enthält Appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe.

·Dem Wert zuordnen - Für die benutzerdefinierte Protokollkennung. Geben Sie die ID ein, die zwischen 0600 und FFFF liegt.

Schritt 6: Aktivieren Sie das Kontrollkästchen **Class of Service**, um die 802.1p-Benutzerpriorität einzugeben, um sie mit einem Ethernet-Frame zu vergleichen. Geben Sie

im Feld "*Class of Service"* die Priorität zwischen 0 und 7 ein.

Schritt 7: Aktivieren Sie das Kontrollkästchen **Quell-MAC-Adresse**, um die Quell-MAC-Adresse mit einem Ethernet-Frame zu vergleichen, und geben Sie die Quell-MAC-Adresse in das Feld *Quell-MAC-Adresse ein*.

Schritt 8: Geben Sie die Quell-MAC-Adressenmaske in das Feld *Quell-MAC-Maske ein*, das angibt, welche Bits in der Quell-MAC mit einem Ethernet-Frame verglichen werden sollen. Wenn die MAC-Maske 0 Bit verwendet, wird die Adresse akzeptiert, und wenn sie 1 Bit verwendet, wird die Adresse ignoriert.

Schritt 9: Aktivieren Sie das Kontrollkästchen **Ziel-MAC-Adresse**, um die Ziel-MAC-Adresse mit einem Ethernet-Frame zu vergleichen, und geben Sie die Ziel-MAC-Adresse im Feld *Ziel-MAC-Adresse ein*.

Schritt 10: Geben Sie die MAC-Zieladressenmaske im Feld *Ziel-MAC-Maske ein*, das angibt, welche Bits der MAC-Zieladresse mit einem Ethernet-Frame verglichen werden sollen. Wenn die MAC-Maske 0 Bit verwendet, wird die Adresse akzeptiert, und wenn sie ein 1 Bit verwendet, wird die Adresse ignoriert.

Schritt 11: Aktivieren Sie das Kontrollkästchen **VLAN-ID**, um die VLAN-ID mit einem Ethernet-Frame zu vergleichen. Geben Sie die VLAN-ID zwischen 0 und 4095 in das Feld *VLAN-ID ein*.

Hinweis: Weitere Informationen zum Erstellen eines neuen VLAN finden Sie im Artikel *Konfiguration von Management- und nicht getaggten VLAN-IDs auf WAP121 und WAP321.*

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

Schritt 13: (Optional) Um die konfigurierte Zugriffskontrollliste zu löschen, aktivieren Sie das Kontrollkästchen **Zugriffskontrollliste löschen** und klicken Sie anschließend auf **Speichern**.