

Konfiguration einer MAC-basierten Zugriffskontrollliste (ACL) für Access Points der Serien WAP551 und WAP561

Ziel

Eine Zugriffskontrollliste (ACL) ist eine Sammlung 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. Eine MAC-ACL ist eine Layer-2-ACL. Das Netzwerkgerät überprüft den Frame und die ACL-Regeln auf den Inhalt des Frames. Wenn eine der Regeln mit dem Inhalt übereinstimmt, wird im Frame eine Aktion für "Zulassen" oder "Ablehnen" ausgeführt.

In diesem Dokument wird dem Benutzer gezeigt, wie MAC ACL auf WAP551- und WAP561-Access Points erstellt und konfiguriert werden.

Anwendbare Geräte

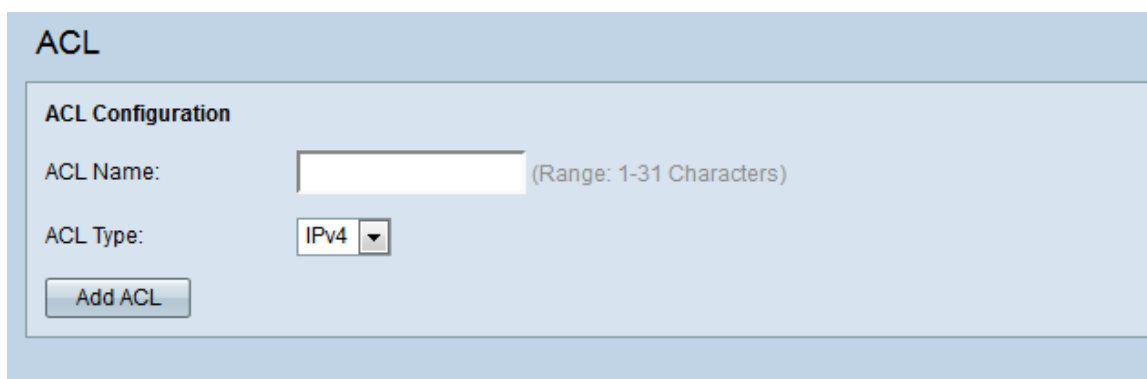
WAP551
WAP561

Softwareversion

·v1.0.4.2

Konfiguration von MAC-ACLs

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



The screenshot shows a web interface for configuring ACLs. The title is "ACL". Below it, there is a section titled "ACL Configuration". This section contains two input fields: "ACL Name:" with a text box and a note "(Range: 1-31 Characters)", and "ACL Type:" with a dropdown menu currently set to "IPv4". At the bottom of this section is a button labeled "Add ACL".

Erstellen einer MAC-ACL

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

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: ▼

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

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: ▼

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

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: ▼

Konfiguration einer Regel für eine MAC-ACL

Schritt 1: Wählen Sie die ACL aus der Dropdown-Liste *ACL Name-ACL Type (ACL-Namen-ACL-Typ)* aus, der Sie Regeln hinzufügen möchten.

ACL Rule Configuration

ACL Name - ACL Type: ▼

Rule: ▼

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

ACL Rule Configuration

ACL Name - ACL Type: ▼

Rule: ▼

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.

Action: **Deny** ▼

Match Every Packet: Deny Permit

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

Die verfügbaren Optionen sind wie folgt definiert:

- 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 auszusteuern.

Hinweis: Die Schritte 4 bis 9 sind optional. Wenn Sie einen Filter nicht auf eine ACL-Regel anwenden möchten, deaktivieren Sie das entsprechende Kontrollkästchen.

Schritt 4: (Optional) 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.

Action: ▼

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

Fahren Sie mit Schritt 11 fort, wenn das Kontrollkästchen *Jedes Paket zuordnen* aktiviert ist.

Schritt 5: (Optional) 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 entweder auf das Optionsfeld *Select From List* (*Von Liste auswählen*) oder *Match to Value* (*Dem Wert zuordnen*).

Action: ▼

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

appletalk
arp
ipv4
ipv6
ipx
netbios
pppoe

Die verfügbaren Optionen sind wie folgt definiert:

·Aus Liste auswählen - Ermöglicht die Auswahl eines Protokolls aus der Dropdown-Liste. Die verfügbaren Optionen sind appletalk, arp, ipv4, ipv6, ipx, netbios und pppoe. Bei Auswahl einer Option wird die Regel auf Pakete des ausgewählten Protokolls angewendet.

- appletalk - Dies ist ein Netzwerkprotokoll, das von Apple Inc. für ihre Macintosh-Computer entwickelt wurde. Appletalk ist ein Plug-in-Play-System. Er weist automatisch Adressen zu und verarbeitet alle anderen Netzwerkkonfigurationen ohne Benutzereingabe.

- arp - ARP (Address Resolution Protocol) ist ein wichtiges Protokoll, das verwendet wird, um IP-Adressen in MAC-Adressen zu übersetzen.

- ipv4 - IPv4 (Internet Protocol Version 4) ist ein wichtiges Protokoll, das für den Großteil des Internetverkehrs verantwortlich ist. Es verarbeitet die IP-Adressen von Geräten.

- ipv6 - IPv6 ist die Nachfolgerversion von IPv4 und der neuesten Version des Internetprotokolls. Sie wurde als Reaktion auf die Erschöpfung der meisten vorhandenen IPv4-IP-Adressen entwickelt.

- ipx - IPX (Internetwork Packet Exchange) ist ein Netzwerk-/Transportprotokoll. Obwohl das Protokoll nicht auch in großen Netzwerken funktioniert, hat IPX gegenüber TCP/IP einen Vorteil, wenn nur wenig Speicher verwendet wird.

- netbios - NetBIOS (Network Basic Input/Output System) ist eine API (Application Programming Interface), die in modernen Netzwerken normalerweise neben TCP/IP ausgeführt wird.

- pppoe - PPPoE (Point-to-Point Protocol over Ethernet) ist ein Netzwerkprotokoll, das verwendet wird, um PPP-Pakete in Ethernet-Paketen zu kapseln.

·Match to Value (Dem Wert zuordnen): Ermöglicht die Eingabe einer benutzerdefinierten Protokollkennung im Feld *Zuordnen zu Wert*. Diese Option ist nützlich, wenn Sie Pakete nach einem Protokoll filtern möchten, das nicht in der Dropdown-Liste *Select From List (Von Liste auswählen)* enthalten ist. Gültige benutzerdefinierte Protokoll-IDs liegen zwischen 0600 und FFFF.

Schritt 6: (Optional) Aktivieren Sie das Kontrollkästchen **Class of Service** (Serviceklasse), um eine 802.1p-Benutzerpriorität für den Vergleich mit einem Ethernet-Frame einzugeben. Geben Sie im Feld *Class of Service (Serviceklasse)* die Priorität ein, die zwischen 0 und 7 liegt.

The screenshot shows a configuration panel for an ACL rule. The 'Action' is set to 'Deny'. The 'Match Every Packet' checkbox is unchecked. Under 'EtherType', the 'Select From List' radio button is selected, and the dropdown menu shows 'ipv4'. The 'Match to Value' radio button is unselected. The 'Class Of Service' checkbox is checked, and the input field next to it contains the number '6', which is circled in red. Below this, there are fields for 'Source MAC Address', 'Source MAC Mask', 'Destination MAC Address', and 'Destination MAC Mask', all of which are currently empty. There is also a 'VLAN ID' field with a range of 0-4095 and a 'Delete ACL' checkbox at the bottom.

Schritt 7: (Optional) 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.

Action:

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

Schritt 8: (Optional) Geben Sie im Feld *Quell-MAC-Maske* die Quell-MAC-Adressenmaske ein, die angibt, welche Bits in der Quell-MAC-Adresse mit einem Ethernet-Frame verglichen werden sollen.

Action:

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

Schritt 9: (Optional) 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 *Ziel-MAC-Adresse*-Feld ein.

Action:

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

Schritt 10: (Optional) Geben Sie die MAC-Zieladressenmaske im Feld *Ziel-MAC-Maske* ein, das angibt, welche Bits in der Ziel-MAC-Adresse mit einem Ethernet-Frame verglichen werden sollen.

Action:

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

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

Action: ▼

Match Every Packet:

EtherType: Select From List ▼ Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

Schritt 12: (Optional) Um die konfigurierte ACL zu löschen, aktivieren Sie das Kontrollkästchen **ACL löschen**.

Schritt 13: Klicken Sie auf **Speichern**.