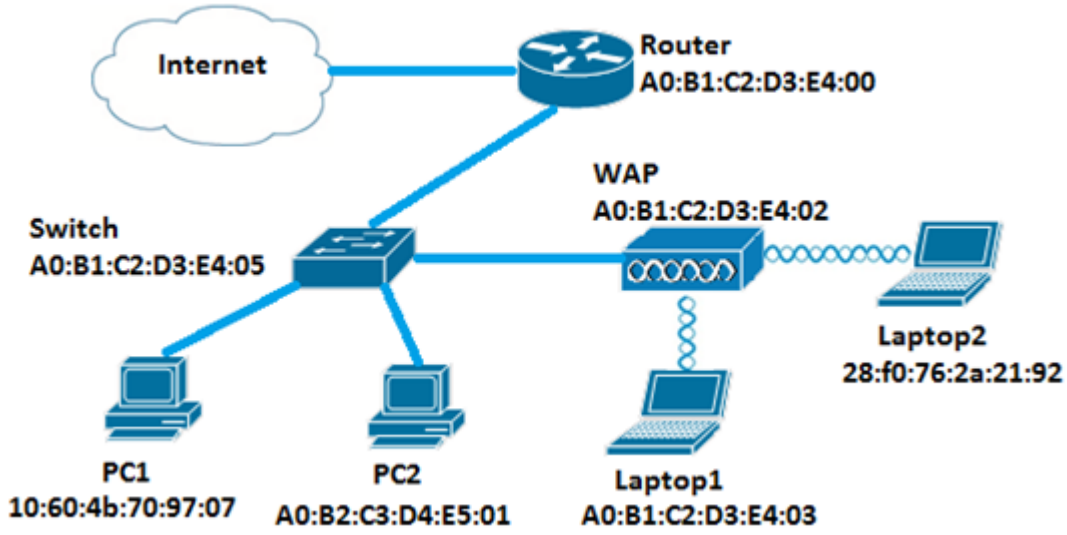
Konfigurieren einer MAC-ACL auf einem WAP125 und WAP581

Einführung

MAC-Zugriffskontrolllisten (ACLs) sind Layer-2-ACLs. Jede ACL ist ein Regelsatz, der auf den Datenverkehr angewendet wird, der vom Wireless Access Point (WAP) empfangen wird. Die Regel gibt an, ob der Inhalt eines Felds verwendet werden soll, um den Zugriff auf das Netzwerk zu ermöglichen oder zu verweigern. Die ACLs können so konfiguriert werden, dass sie Felder eines Frames wie die Quell- oder Ziel-MAC-Adresse, den Virtual Local Area Network (VLAN) Identifier (ID) oder die Class of Service (CoS) überprüfen. Wenn ein Frame in den WAP-Geräteport eingeht, prüft er den Frame und überprüft 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. Die Konfiguration von MAC-ACLs wird in der Regel verwendet, um den Zugriff auf Netzwerkressourcen zu autorisieren, um Geräte im Netzwerk auszuwählen.

Hinweis: Am Ende jeder erstellten Regel wird eine implizite Ablehnung ausgegeben.



In diesem Szenario dürfen alle Geräte im Netzwerk mit Ausnahme von PC1 Zugriff auf Laptop2 hinter dem WAP haben.

Ziel

Dieser Artikel soll Ihnen zeigen, wie Sie eine MAC-basierte ACL auf einem WAP125 oder WAP581 Access Point konfigurieren, um zu verhindern, dass PC1 auf Laptop2 hinter dem WAP zugreift.

Anwendbare Geräte

- WAP125
- WAP581

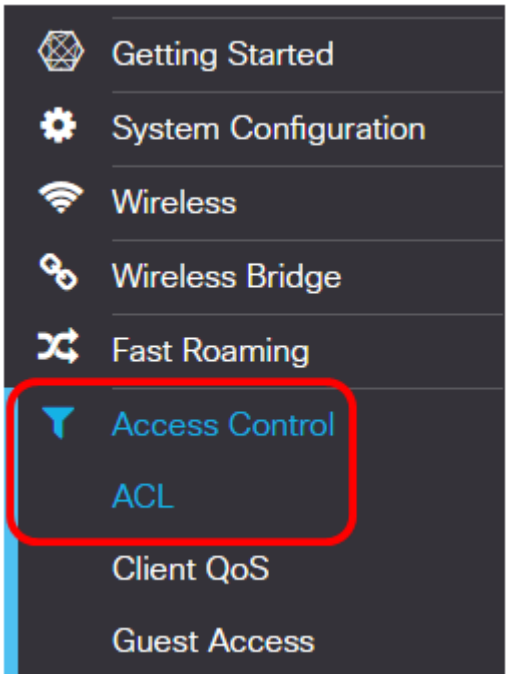
Softwareversion

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

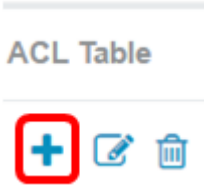
Konfigurieren einer Clientfilterliste

Hinweis: Die Menüoptionen können je nach dem verwendeten WAP-Modell variieren. Die folgenden Bilder stammen aus dem WAP125.

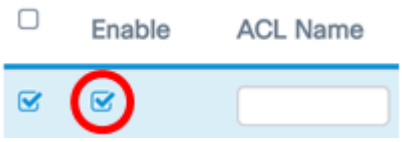
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des WAP an, und wählen Sie **Access Control > ACL aus**.



Schritt 2: Klicken Sie auf die + Schaltfläche.



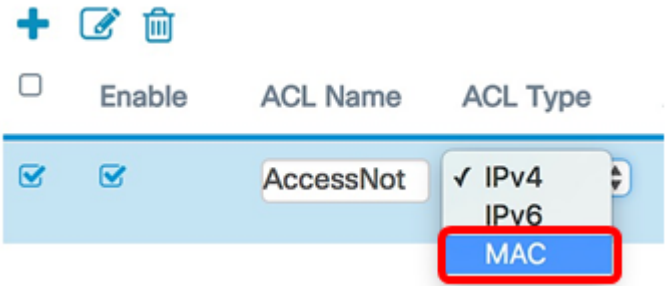
Schritt 3: Überprüfen Sie, ob das Kontrollkästchen **Aktivieren** aktiviert ist, um sicherzustellen, dass die Zugriffskontrollliste aktiviert ist. Diese Option ist standardmäßig aktiviert.



Schritt 4: Geben Sie einen Namen für die ACL im Feld *ACL Name* ein, um die ACL zu identifizieren.

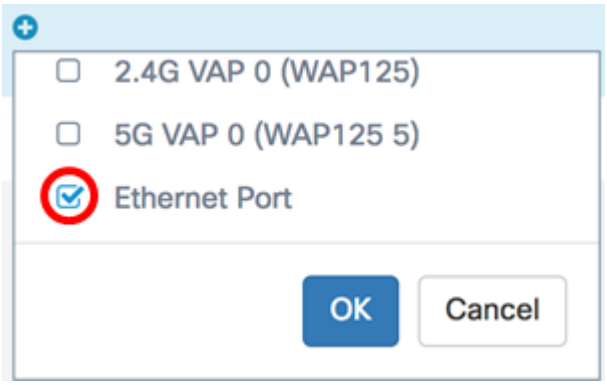
Hinweis: In diesem Beispiel wird AccessNot eingegeben.

Schritt 5: Wählen Sie **MAC** aus der Dropdown-Liste ACL Type (ACL-Typ) aus.



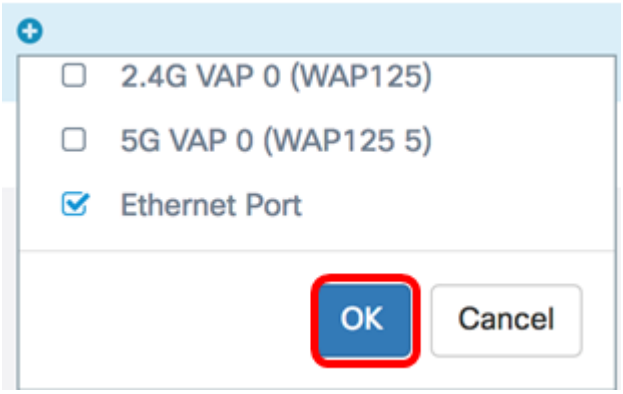
Schritt 6: Klicken Sie auf die Schaltfläche, und wählen Sie in der Dropdown-Liste Associated Interface (Zugeordnete Schnittstelle) eine Schnittstelle aus. Folgende Optionen stehen zur Verfügung:

- 2.4G VAP 0 (SSID-Name): Mit dieser Option wird die MAC-ACL auf den 2,4 GHz Virtual Access Point (VAP) angewendet. Der Abschnitt "SSID Name" kann sich je nach dem auf dem WAP konfigurierten SSID-Namen ändern.
- 5G VAP0 (SSID-Name): Mit dieser Option wird die MAC-ACL auf den 5-GHz-VAP angewendet.
- Ethernet Port (Ethernet-Port): Mit dieser Option wird die MAC-ACL auf die Ethernet-Schnittstelle des WAP angewendet.



Hinweis: Mehrere Schnittstellen können einer ACL zugeordnet werden. Aktivieren Sie das Kontrollkästchen der entsprechenden Schnittstelle, um die Schnittstelle der ACL zuzuordnen. Deaktivieren Sie das Kontrollkästchen, um die Schnittstelle von der ACL zu trennen. In diesem Beispiel wird der Ethernet-Port der ACL zugeordnet.

Schritt 7: Klicken Sie auf **OK**.

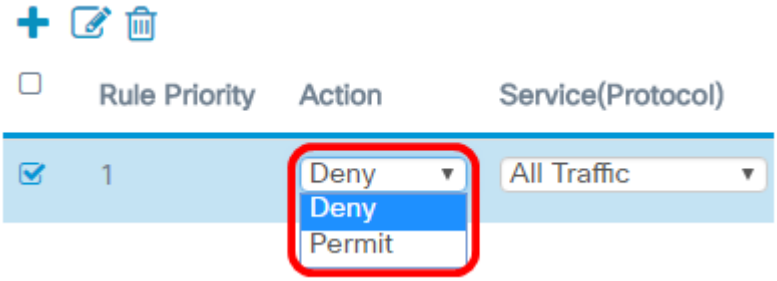


Schritt 8: Klicken Sie auf die Schaltfläche **More..**, um die Parameter der ACL zu konfigurieren.

Schritt 9: Klicken Sie auf die + Schaltfläche, um eine neue Regel hinzuzufügen.

Schritt 10: Wählen Sie eine Aktion aus der Dropdown-Liste Aktion aus. Folgende Optionen stehen zur Verfügung:

- Zulassen: Mit dieser Option können Pakete, die die ACL-Kriterien erfüllen, eine Verbindung zum Netzwerk herstellen.
- Verweigern: Diese Option verhindert, dass Pakete, die die ACL-Kriterien erfüllen, eine Verbindung zum Netzwerk herstellen.

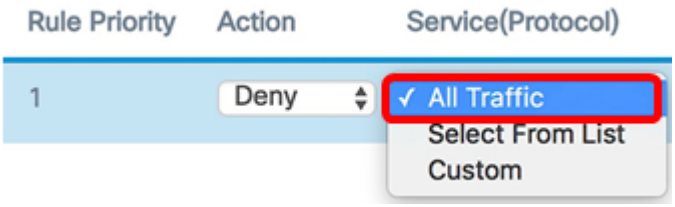


Hinweis: In diesem Beispiel wird Verweigern ausgewählt.

Schritt 11: Wählen Sie aus der Dropdown-Liste Service (Protocol) einen Service oder ein Protokoll aus, der bzw. das gefiltert werden soll. Folgende Optionen stehen zur Verfügung:

- Gesamter Datenverkehr: Diese Option behandelt alle Pakete als Übereinstimmung mit dem ACL-Filter.
- Wählen Sie From List (Von Liste auswählen): Mit dieser Option können Sie appletalk, arp, ipv4, ipv6, ipx, netbios und pppoe als Filter für die ACL auswählen. Wenn Sie diese Option auswählen, fahren Sie mit Schritt 12 fort.
- Custom (Benutzerdefiniert): Mit dieser Option können Sie eine benutzerdefinierte

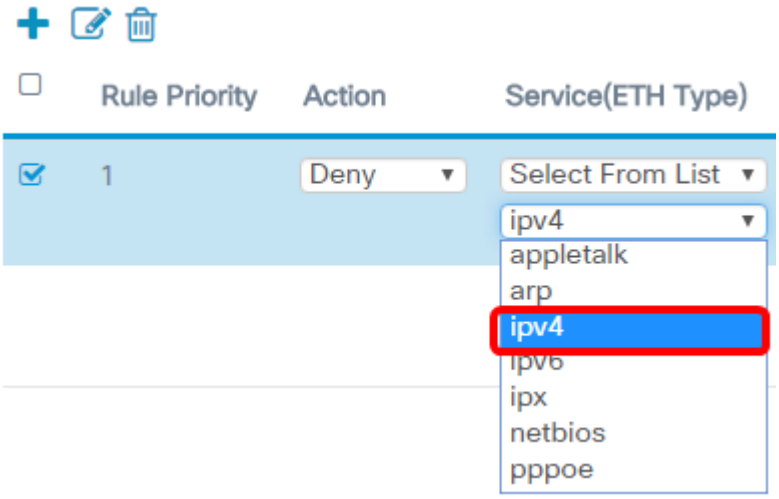
Protokoll-ID als Filter für die Pakete eingeben. Der Wert ist eine vierstellige Hexadezimalzahl. Der Bereich liegt zwischen 0600 und FFFF.



Hinweis: In diesem Beispiel wird **All Traffic (Gesamter Datenverkehr)** ausgewählt.

Schritt 12: (Optional) Wählen Sie Wählen Sie Wählen Sie eine der folgenden Optionen aus:

- appletalk: Mit dieser Option werden Appletalk-Pakete basierend auf der ACL-Anweisung gefiltert. Appletalk ist ein Satz von Netzwerkprotokollen, die von Apple für ihre Mac-Computer entwickelt wurden. Eine der Funktionen ermöglicht die Verbindung von LANs (Local Area Networks) ohne einen zentralen Router oder Server.
- arp - Diese Option filtert ARP-Pakete (Address Resolution Protocol) auf Basis der ACL-Anweisung. ARP unterhält eine Tabelle, in der MAC-Adressen IP-Adressen zugeordnet sind.
- ipv4: Diese Option filtert IPv4-Pakete auf Basis der ACL-Anweisung.
- ipv6 - Diese Option filtert IPv6-Pakete auf Basis der ACL-Anweisung. IPv6 ist der Nachfolger von IPv6 bei der Netzwerkadressierung.
- ipx - Diese Option filtert Internetwork Packet Exchange (IPX)-Pakete auf Basis der ACL-Anweisung. Wie bei AppletTalk ist IPX auch ein proprietäres Netzwerkprotokoll. Es verbindet Netzwerke, die Novell-Clients und -Server nutzen.
- netbios - Diese Option filtert NetBIOS-Pakete (Network Basic Input and Output System) auf Basis der ACL-Anweisung. NetBIOS ermöglicht Anwendungen auf separaten Computern die Kommunikation, indem die Dienste bereitgestellt werden, die sie für die Kommunikation nutzen können.
- pppoe - Diese Option filtert Point-to-Point Protocol over Ethernet (PPPoE)-Pakete auf Basis der ACL-Anweisung. Es wird hauptsächlich in DSL-Diensten (Digital Subscriber Line) verwendet.

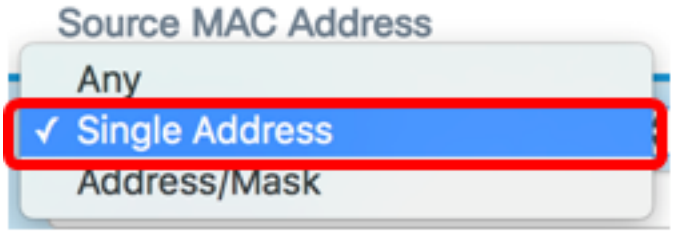


Hinweis: In diesem Beispiel wird ipv4 ausgewählt.

Schritt 13: Definieren Sie die Quell-MAC-Adresse aus der Dropdown-Liste "Quell-MAC-

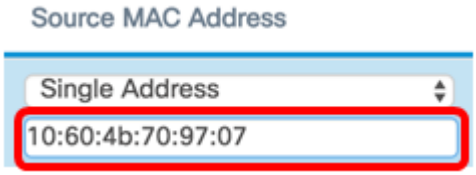
Adresse". Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Mit dieser Option kann der WAP den Filter auf Pakete aus einer beliebigen MAC-Adresse anwenden.
- Single Address (Einzeladresse): Mit dieser Option kann der WAP den Filter auf Pakete einer angegebenen MAC-Adresse anwenden.
- Address/Mask (Adresse/Maske): Mit dieser Option kann der WAP den Filter auf Pakete mit einer MAC-Adresse und der Maske des WAP anwenden.



Hinweis: In diesem Beispiel wird die Einzeladresse ausgewählt.

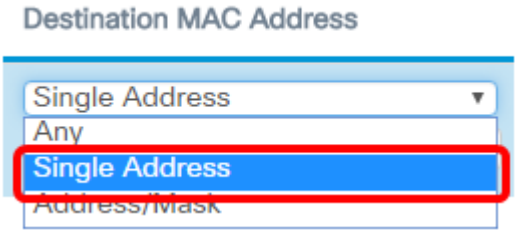
Schritt 14: Geben Sie die Quell-MAC-Adresse im Feld *Quell-MAC-Adresse ein*.



Hinweis: In diesem Beispiel wird 10:60:4b:70:97:07 eingegeben. Dies ist die MAC-Adresse von PC1.

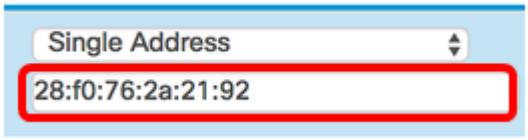
Schritt 15: Definieren Sie die MAC-Zieladresse aus der Dropdown-Liste "Ziel-MAC-Adresse". Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Mit dieser Option kann der WAP den Filter auf Pakete aus einer beliebigen MAC-Adresse anwenden.
- Single Address (Einzeladresse): Mit dieser Option kann der WAP den Filter auf Pakete einer angegebenen MAC-Adresse anwenden.
- Address/Mask (Adresse/Maske): Mit dieser Option kann der WAP den Filter auf Pakete mit einer MAC-Adresse und der Maske des WAP anwenden.



Hinweis: In diesem Beispiel wird die Einzeladresse ausgewählt.

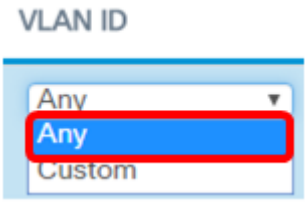
Schritt 16: Geben Sie die MAC-Zieladresse im Feld **Ziel-MAC-Adresse ein**.



Hinweis: In diesem Beispiel wird 28:f0:76:2a:21:92 eingegeben. Dies ist die MAC-Adresse von Laptop2.

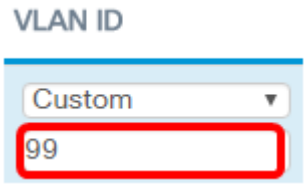
Schritt 17: Wählen Sie aus der Dropdown-Liste eine VLAN-ID aus.

- Any (Beliebig): Diese Option ermöglicht jede VLAN-ID, die das Netzwerk durchläuft.
- Benutzerdefiniert: Mit dieser Option können Sie eine bestimmte VLAN-ID eingeben. Wenn Sie diese Option auswählen, fahren Sie mit Schritt 18 fort.



Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt.

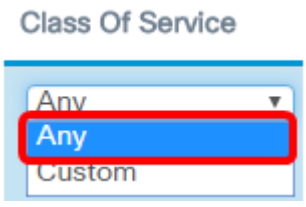
Schritt 18: (Optional) Wenn Sie Custom (Benutzerdefiniert) auswählen, geben Sie die VLAN-ID in das Feld *VLAN-ID ein*.



Hinweis: In diesem Beispiel wird 99 eingegeben.

Schritt 19: (Optional) Wählen Sie eine Class of Service aus der Dropdown-Liste aus. Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Mit dieser Option können Pakete mit beliebiger Priorität eine Verbindung mit dem Netzwerk herstellen.
- Benutzerdefiniert - Mit dieser Option können Sie Pakete auf einer bestimmten Prioritätsebene filtern.



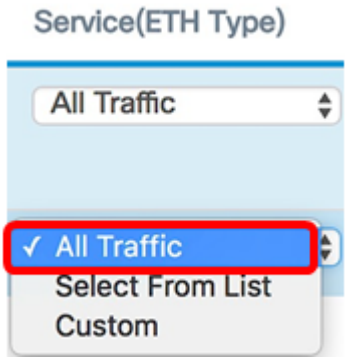
Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt. Wenn Sie Custom (Benutzerdefiniert) auswählen, geben Sie die Priorität im Feld *Class of Service (Serviceklasse) ein*.

Schritt 20: Klicken Sie erneut auf die + Schaltfläche, um eine Genehmigungsregel hinzuzufügen.

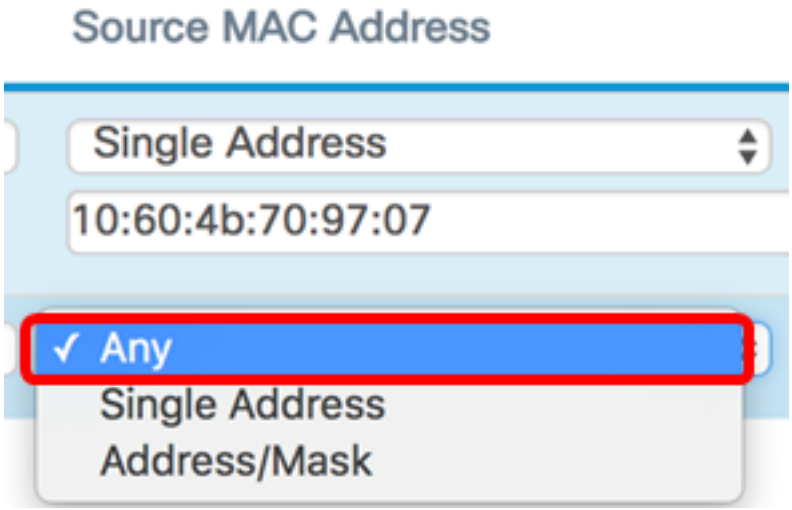
Hinweis: Da am Ende jeder erstellten Regel eine implizite Verweigerung vorliegt, wird dringend empfohlen, der ACL eine Genehmigungsregel hinzuzufügen, um den Datenverkehr von anderen Geräten im Netzwerk zuzulassen.

Schritt 21: Klicken Sie auf den Pfeil des Dropdown-Menüs Aktion, und wählen Sie **Zulassen aus**.

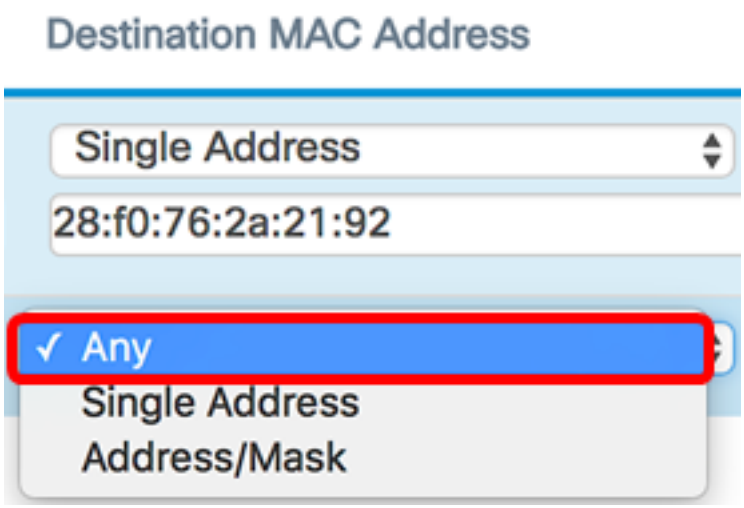
Schritt 22: Klicken Sie auf den Pfeil des Dropdown-Menüs Service (ETH-Typ), und wählen Sie **Alle Datenverkehr** aus.



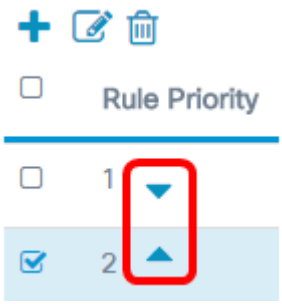
Schritt 23: Klicken Sie auf das Dropdown-Menü Quell-MAC-Adresse, und wählen Sie **Any (Beliebig)** aus. Dies würde Datenverkehr von anderen MAC-Adressen im Netzwerk mit Ausnahme der in der ersten Regel angegebenen PC1-MAC-Adresse zulassen.



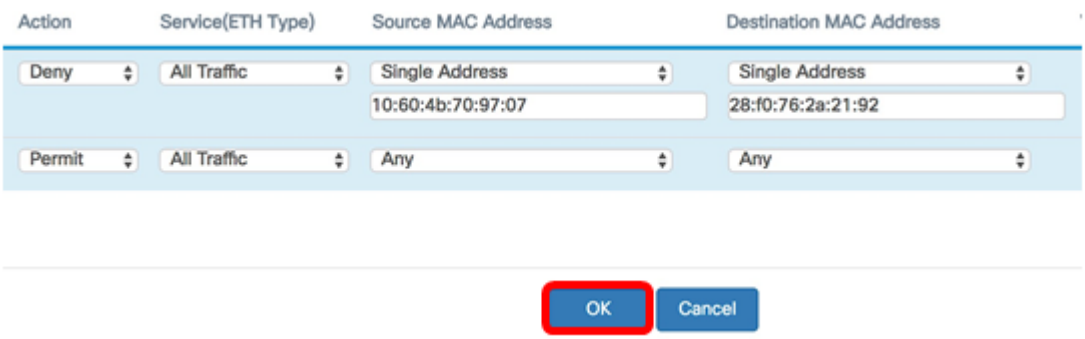
Schritt 24: Klicken Sie auf das Dropdown-Menü Ziel-MAC-Adresse, und wählen Sie **Any (Beliebig)** aus. Dies ermöglicht den Datenverkehr zu beliebigen MAC-Adressen im Netzwerk.



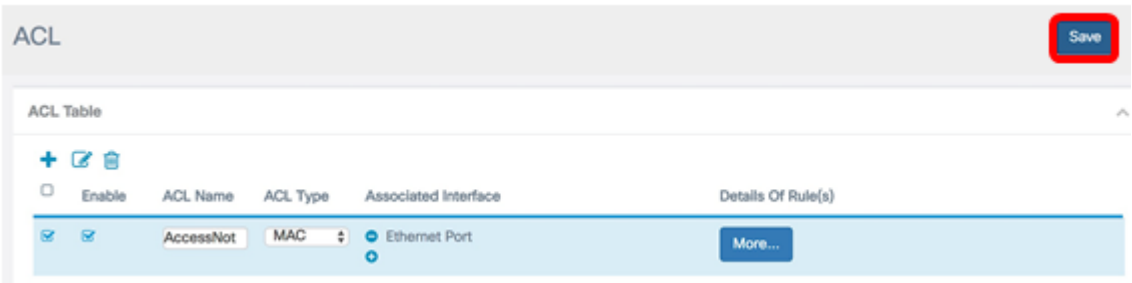
Schritt 25.(Optional) Ändern Sie die Priorität der Regel, indem Sie auf die Pfeile nach oben und unten klicken, bis die Regel in Kraft ist.



Schritt 26: Klicken Sie auf **OK**.



Schritt 27: Klicken Sie auf **Speichern**.



Sie sollten jetzt die MAC-ACL auf dem WAP125 oder WAP581 Access Point konfiguriert haben.

Sehen Sie sich ein Video zu diesem Artikel an..

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.