Erstellen einer MAC-basierten ACL auf dem SG350XG und SG550XG

Ziel

Eine Zugriffskontrollliste (ACL) ist ein Regelsatz, der zum Bearbeiten von Paketen erstellt werden kann, je nachdem, ob sie bestimmte Kriterien erfüllen. Diese Kriterien können Quell- oder Zieladressen, Headerfelder und andere Komponenten eines Pakets sein. Wenn ein Paket den angegebenen Kriterien einer ACL entspricht, wird es entweder verworfen oder zum Fortfahren zugelassen. Eine MAC-basierte ACL verwendet Regeln, die den Layer-2-Header eines Pakets für diese Kriterien analysieren, z. B. MAC-Adressen, VLAN-IDs und Ethertype-Werte. Durch die Implementierung einer MAC-basierten Zugriffskontrollliste können Pakete, die über den Switch übertragen werden, auf Layer-2-Ebene gesteuert werden.

In diesem Dokument wird erläutert, wie Sie eine MAC-basierte Zugriffskontrollliste auf den SG350XG- und SG550XG-Switches erstellen und konfigurieren.

Unterstützte Geräte

- SG350XG
- SG550XG

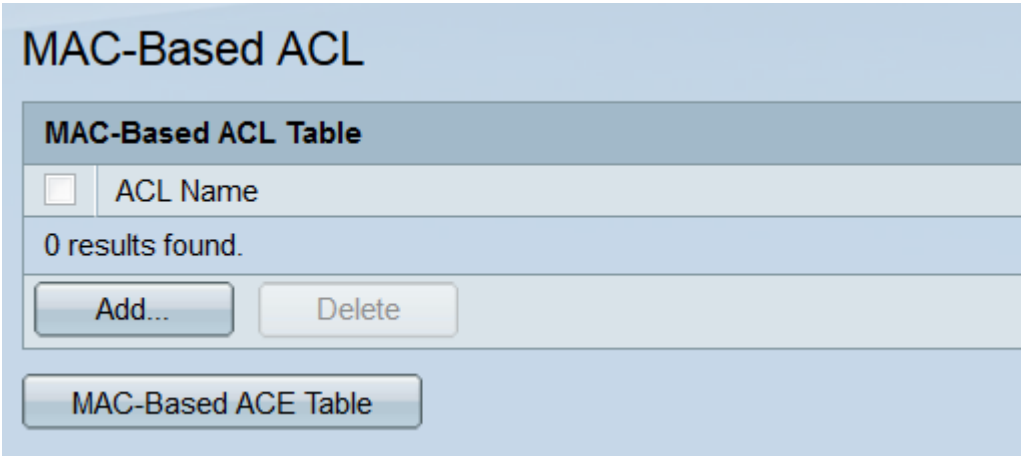
Software-Version

- V2.0.0.73

Konfigurieren MAC-basierte ACLs

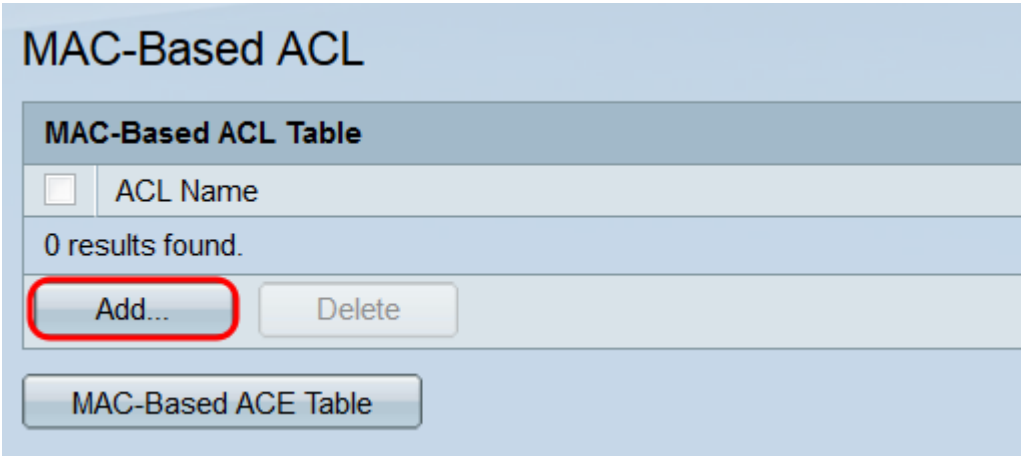
Erstellen eine ACL und Regeln

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Zugriffskontrolle > MAC-basierte Zugriffskontrollliste aus**. Die Seite *MAC-basierte ACL* wird geöffnet.

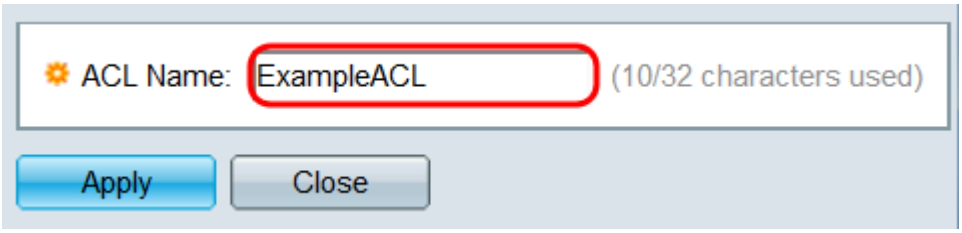


Schritt 2: In der *MAC-basierten ACL-Tabelle* werden alle MAC-basierten ACLs angezeigt,

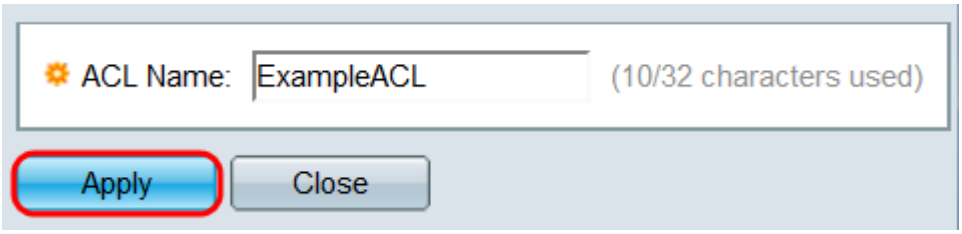
die sich derzeit auf dem Switch befinden. Um eine neue ACL zu erstellen, klicken Sie auf die Schaltfläche **Add...**. Das Fenster *MAC-basierte ACL hinzufügen* wird geöffnet.



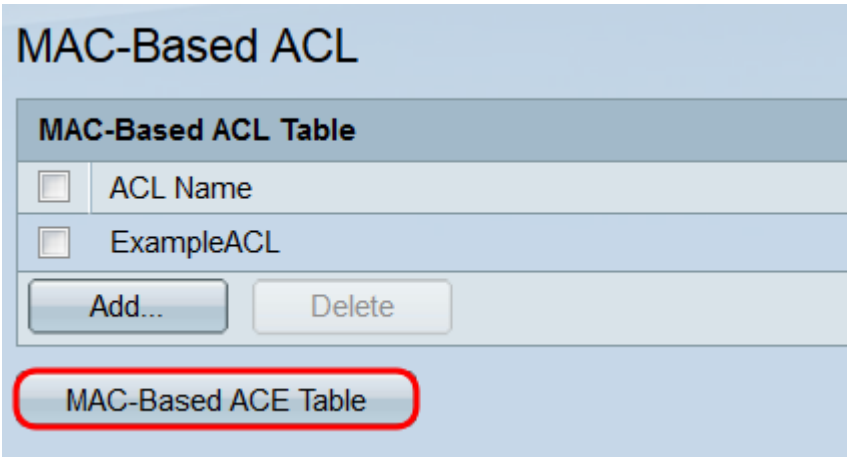
Schritt 3: Geben Sie im Feld *ACL Name* (ACL-Name*)* den Namen für die neue ACL ein. Dieser Name hat keine Auswirkungen auf die Funktion der Zugriffskontrollliste und dient nur zur Identifizierung.



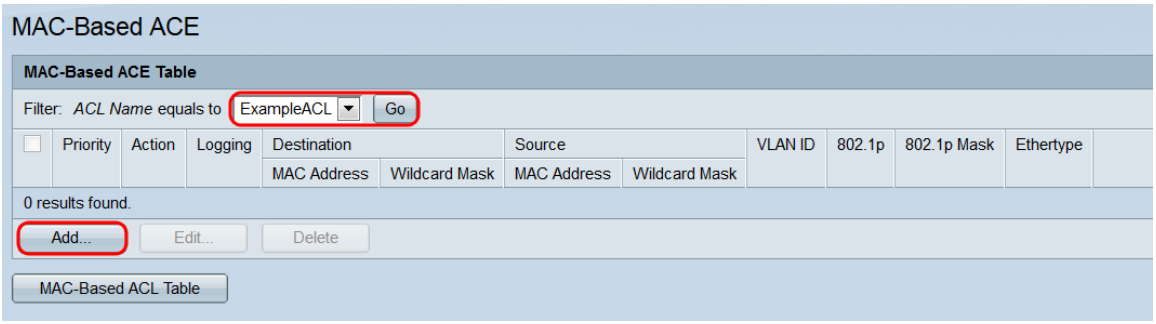
Schritt 4: Klicken Sie auf **Apply** (Anwenden). Die neue ACL wird der *MAC-basierten ACL-Tabelle* hinzugefügt. Klicken Sie auf **Schließen**, um zur *MAC-basierten ACL*-Seite zurückzukehren, oder erstellen Sie eine weitere ACL, indem Sie den vorherigen Schritt wiederholen.



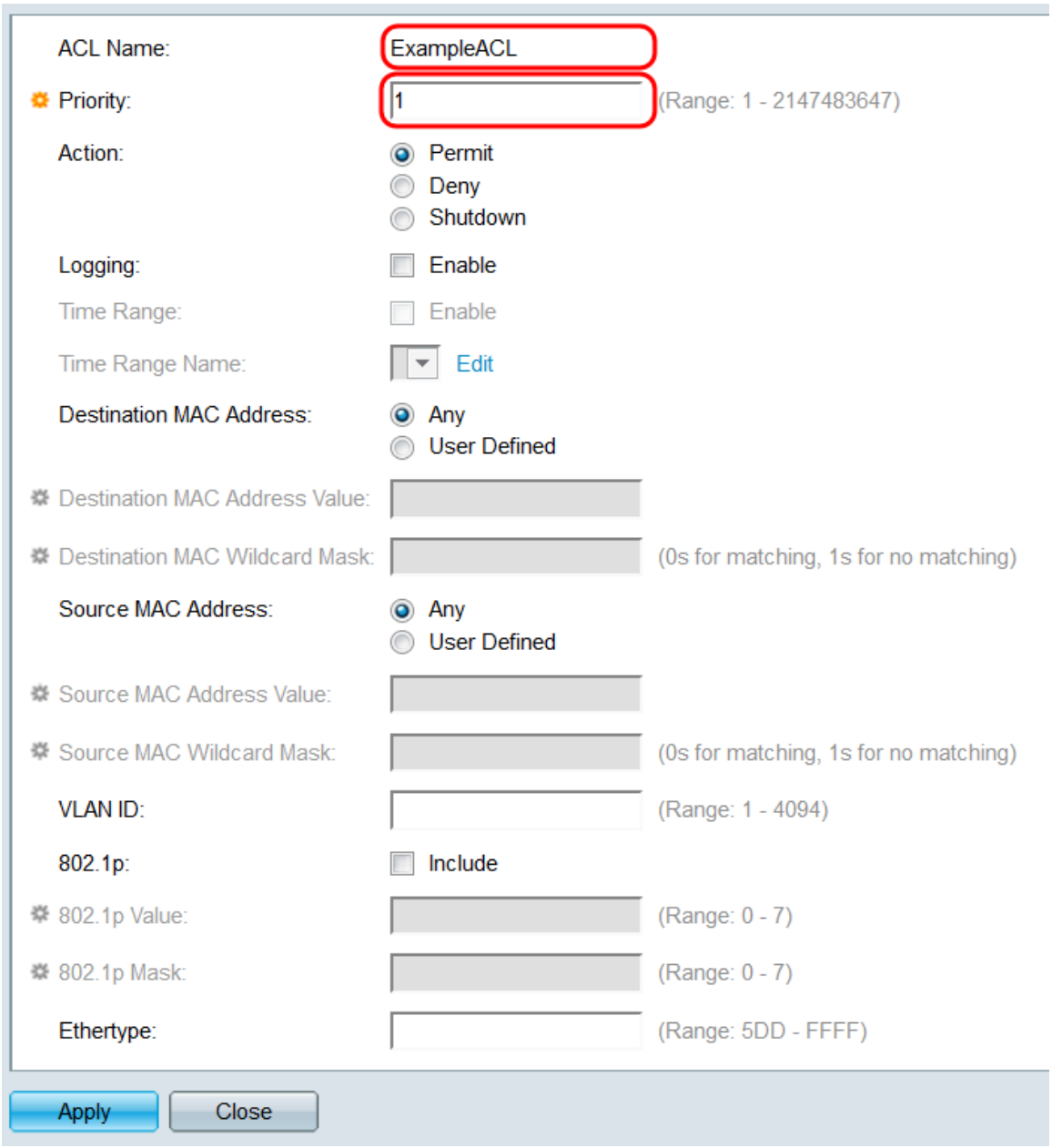
Schritt 5: Alle neu erstellten Zugriffskontrolllisten sind leer. d. h. es enthält keine Regeln, um Pakete basierend auf MAC-Adressen zu blockieren oder zuzulassen. Um diese Regeln zu erstellen, muss der ACL ein Zugriffskontrolleintrag (ACE) hinzugefügt werden. Klicken Sie dazu auf die Schaltfläche **MAC-Based ACE Table**, um zur *MAC-Based ACE*-Seite zu gelangen.



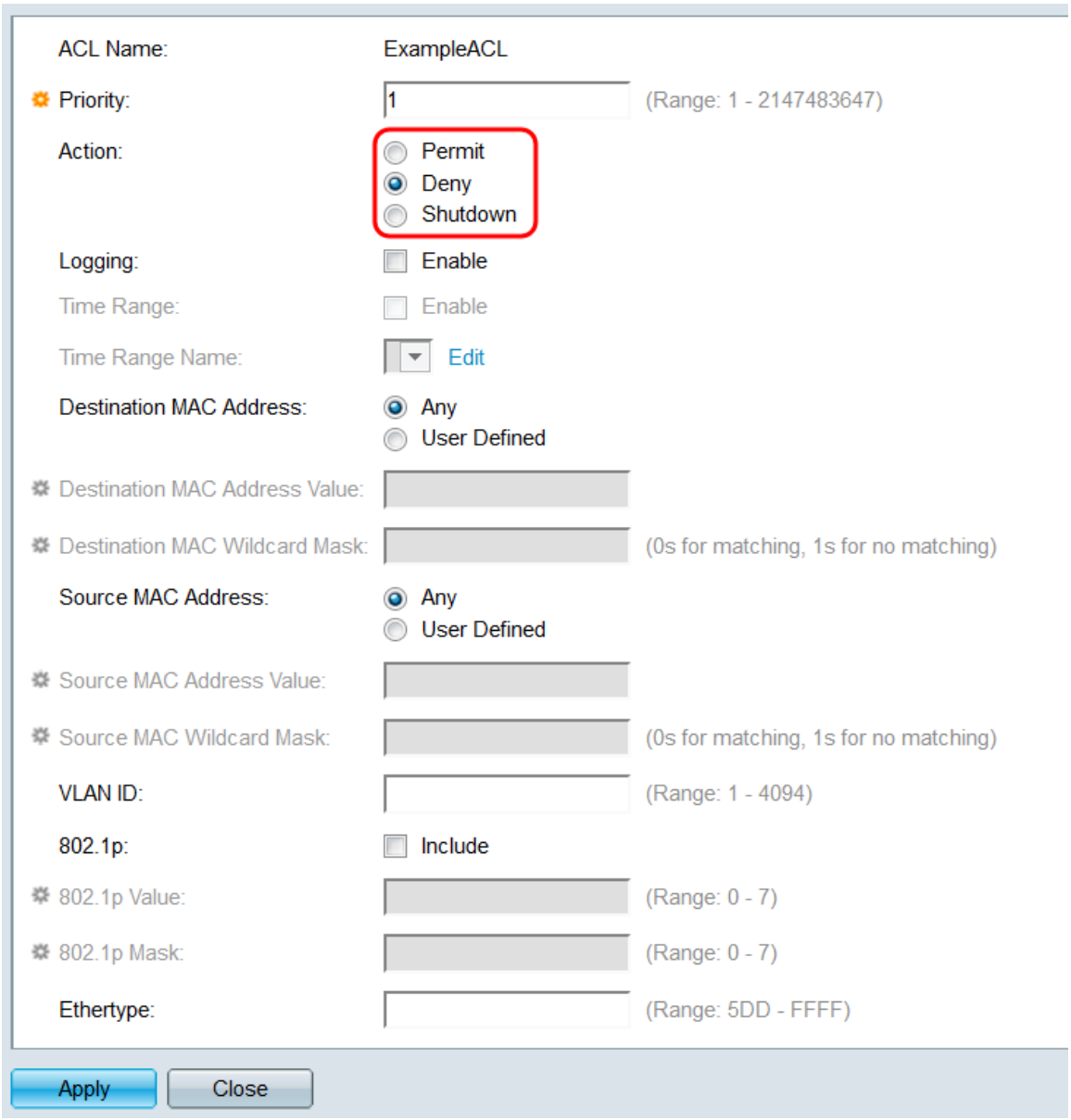
Schritt 6: Wählen Sie auf der Seite *MAC-Based ACE* (MAC-basierter ACE) die ACL aus, der Sie einen ACE hinzufügen möchten. Wählen Sie dazu in der Dropdown-Liste am oberen Rand der *MAC-basierten ACE-Tabelle aus,* und klicken Sie auf **Go (Los)**. In der Tabelle werden alle ACEs angezeigt, die aktuell der ausgewählten ACL zugeordnet sind. Um einen ACE hinzuzufügen, klicken Sie auf die Schaltfläche **Add...**. Das Fenster *MAC-basierter ACE hinzufügen* wird geöffnet.



Schritt 7: Das Feld *ACL Name* (ACL-Name) zeigt den Namen der ACL an, der ein ACE hinzugefügt wird. Geben Sie im Feld *Priorität* eine Prioritätsnummer für den ACE ein. Je höher die Priorität eines ACE ist, desto schneller wird er verarbeitet. Der Bereich liegt zwischen 1 und 2147483647, wobei 1 die höchste Priorität darstellt.



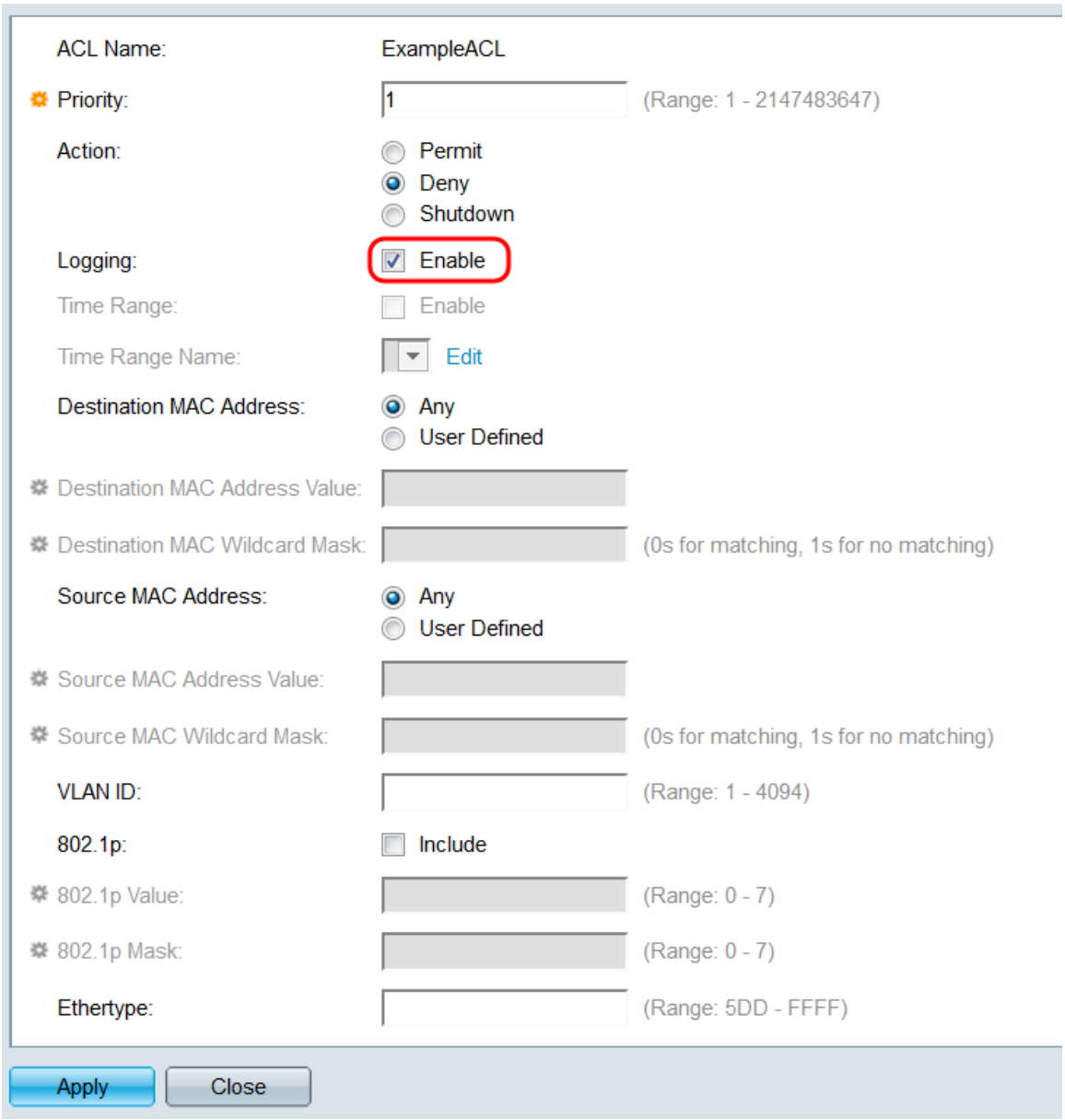
Schritt 8: Im Feld *Aktion* aktivieren Sie ein Optionsfeld, um zu bestimmen, was geschieht, wenn die ACE-Kriterien erfüllt sind.



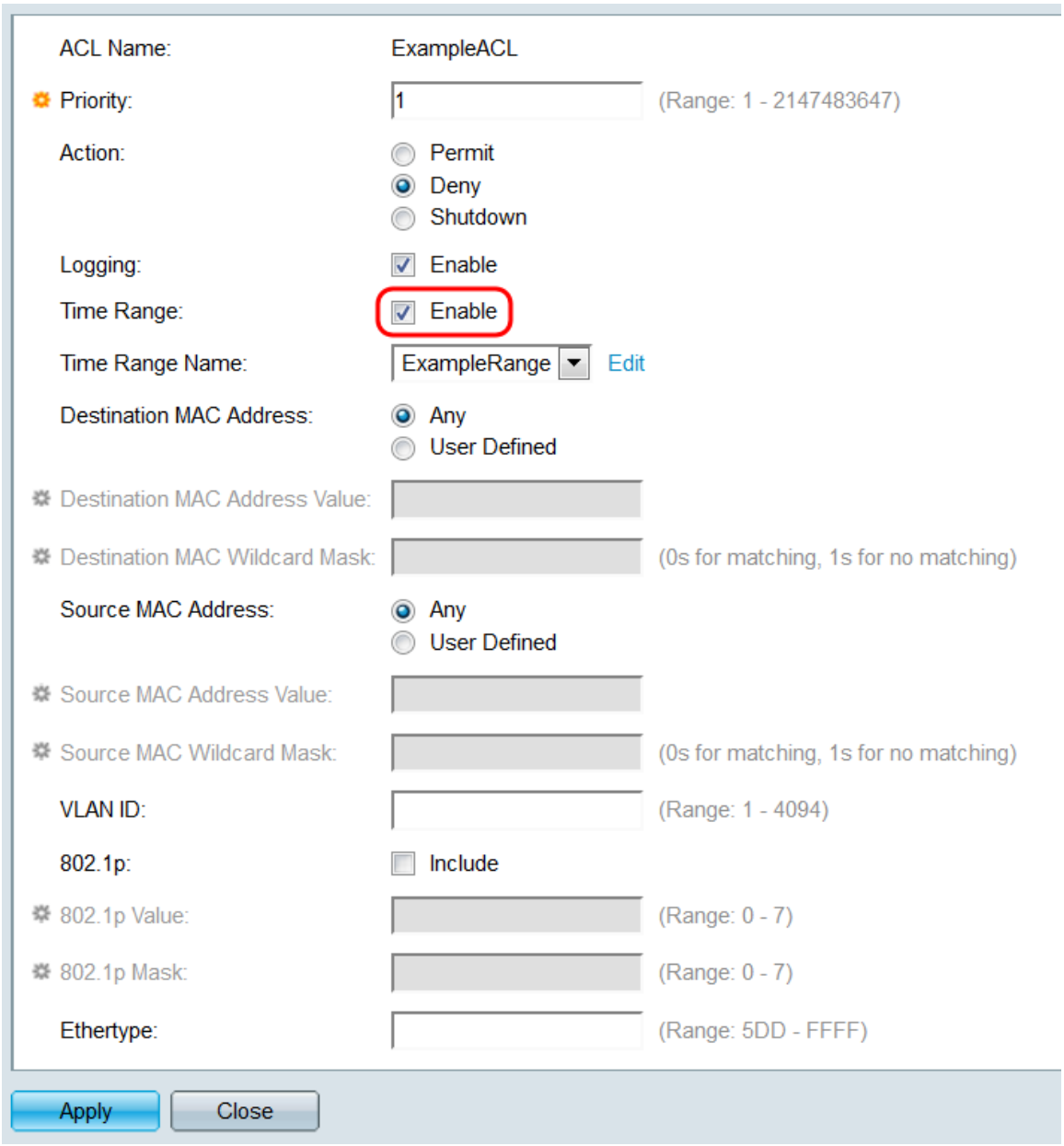
Folgende Optionen sind verfügbar:

- Zulassen - Leiten Sie Pakete weiter, die die Kriterien erfüllen.
- Verweigern - Verwerfen Sie Pakete, die die Kriterien erfüllen.
- Herunterfahren: Verwerfen Sie Pakete, die die Kriterien erfüllen, und deaktivieren Sie dann den Port.

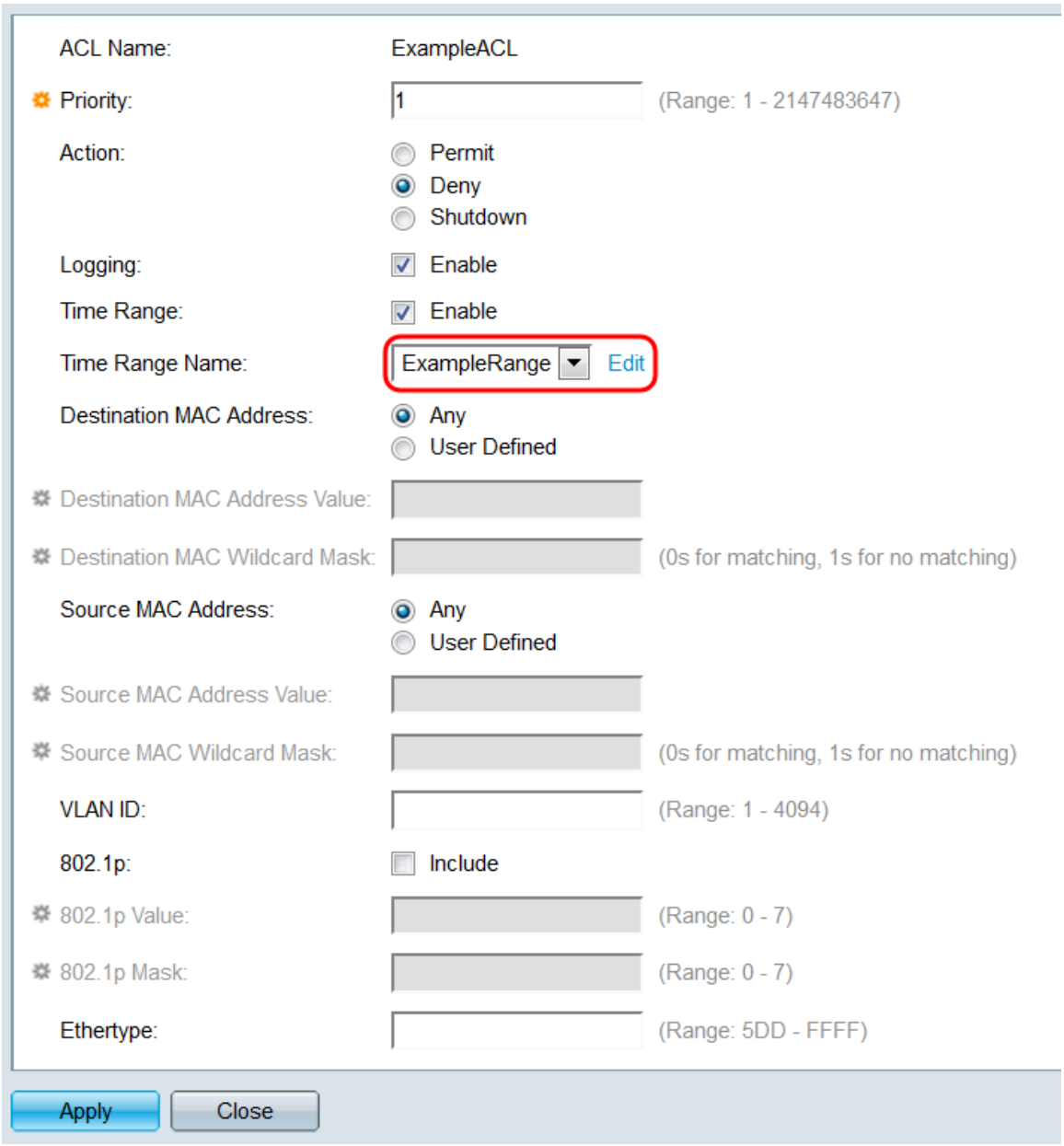
Schritt 9: Aktivieren Sie im Feld *Protokollierung* das **Kontrollkästchen Aktivieren**, um die Protokollierung von ACL-Flüssen zu aktivieren, die der ACE-Regel entsprechen. Wenn Sie den Standardanzeigemodus verwenden, fahren Sie mit Schritt 12 fort. Der Anzeigemodus kann über die Dropdown-Liste oben rechts im Webdienstprogramm geändert werden.



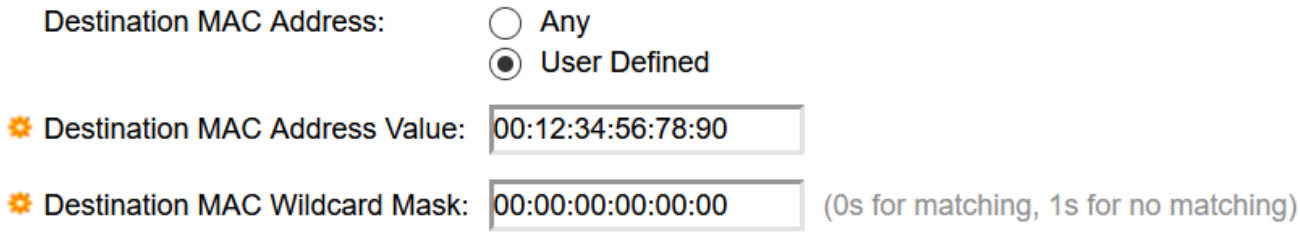
Schritt 10: Aktivieren Sie im Feld *Zeitbereich das* **Kontrollkästchen Enable (Aktivieren)**, damit der ACE nur für einen bestimmten Zeitraum aktiv ist. Wenn auf dem Switch keine vorhandenen Zeitbereiche konfiguriert sind, ist dieses Feld nicht verfügbar.



Schritt 11: Wenn Sie einen Zeitbereich für diesen ACE aktiviert haben, steht das Feld *Time Range Name* (*Zeitbereichsname*) zur Verfügung. Verwenden Sie die Dropdown-Liste, um einen Zeitraum auszuwählen, der bereits auf dem Switch konfiguriert ist und auf den ACE angewendet werden soll. Wenn auf dem Switch keine Zeitbereiche vorhanden sind, ist dieses Feld nicht verfügbar. Klicken Sie auf den Link **Bearbeiten**, um zur Seite *Zeitbereich zu* wechseln, um Zeitbereiche zu erstellen oder zu ändern. Weitere Informationen finden Sie im Artikel *Einrichten eines Zeitbereichs auf dem SG350XG und SG550XG*.



Schritt 12: Wählen Sie im Feld *Ziel-MAC-Adresse* ein Optionsfeld aus, um festzulegen, welche MAC-Zieladressen eine Übereinstimmung darstellen sollen. Wählen Sie **Any (Beliebig)** aus, damit jede Zieladresse einer Übereinstimmung entspricht, oder **User Defined (Benutzerdefiniert)**, um eine Adresse oder einen Adressbereich anzugeben.



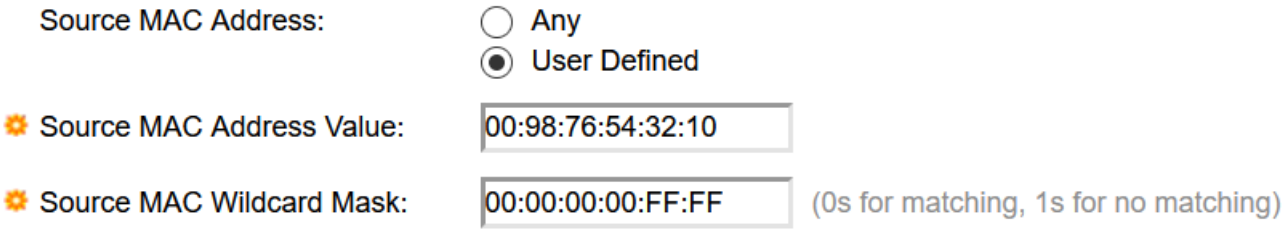
Wenn Sie **Benutzerdefiniert** ausgewählt haben, füllen Sie die folgenden Felder aus:

- Ziel-MAC-Adressenwert - Geben Sie die MAC-Zieladresse ein. Wenn ein Paket diese Zieladresse enthält, betrachtet der ACE diese als Übereinstimmung.
- Ziel-MAC-Platzhaltermaske - Geben Sie eine Maske ein, um einen Adressbereich zu definieren. Wenn Sie ein Bit auf 1 setzen, wird das entsprechende Bit in der MAC-Adresse

ignoriert, und die 0 wird den Bits entsprechen.

Hinweis: Bei einer Maske von 0000 000 000 000 000 000 000 000 000 000 000 000 000 111 11111 (d. h., dass Sie auf den Bits übereinstimmen, die es gibt s 0 und stimmen Sie nicht mit den Bits überein, bei denen es 1 s gibt). Sie müssen die 1s in einen Hexadezimalwert übersetzen und Sie schreiben 0 für jeweils vier Nullen. In diesem Beispiel wird die Maske seit 1111 111 = FF geschrieben: als 00:00:00:00:00:FF.

Schritt 13: Wählen Sie im Feld *Quell-MAC-Adresse* ein Optionsfeld aus, um zu bestimmen, welche Quell-MAC-Adressen eine Übereinstimmung darstellen. Wählen Sie **Any (Beliebig)**, damit die Quelladresse einer Übereinstimmung entspricht, oder **User Defined (Benutzerdefiniert)**, um eine Adresse oder einen Adressbereich anzugeben.



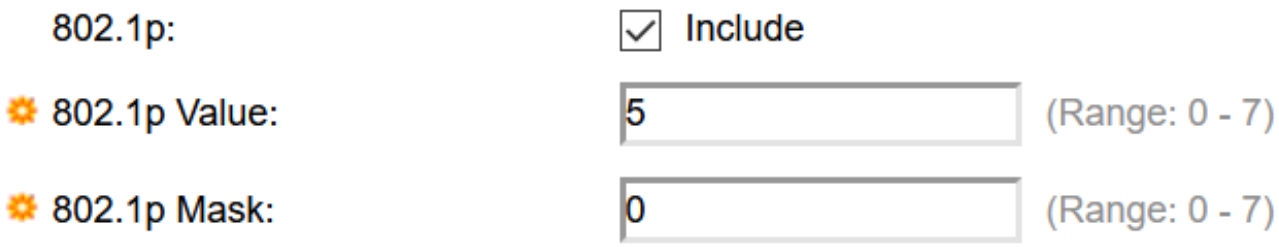
Wenn Sie **Benutzerdefiniert** ausgewählt haben, füllen Sie die folgenden Felder aus:

- Quell-MAC-Adressenwert - Geben Sie die Quell-MAC-Adresse ein. Wenn ein Paket diese Quelladresse enthält, betrachtet der ACE diese als Übereinstimmung.
- MAC-Platzhaltermaske - Geben Sie eine Maske ein, um einen Adressbereich festzulegen. Wenn Sie ein Bit auf 1 setzen, wird das entsprechende Bit in der MAC-Adresse ignoriert, und die 0-Bit-Einstellung entspricht den Bits (z. B. 00:00:00:00:00:11).

Hinweis: Bei einer Maske von 0000 000 000 000 000 000 000 000 000 000 000 000 000 111 11111 (d. h., dass Sie auf den Bits übereinstimmen, die es gibt s 0 und stimmen Sie nicht mit den Bits überein, bei denen es 1 s gibt). Sie müssen die 1s in einen Hexadezimalwert übersetzen und Sie schreiben 0 für jeweils vier Nullen. In diesem Beispiel wird die Maske seit 1111 111 = FF geschrieben: als 00:00:00:00:00:FF.

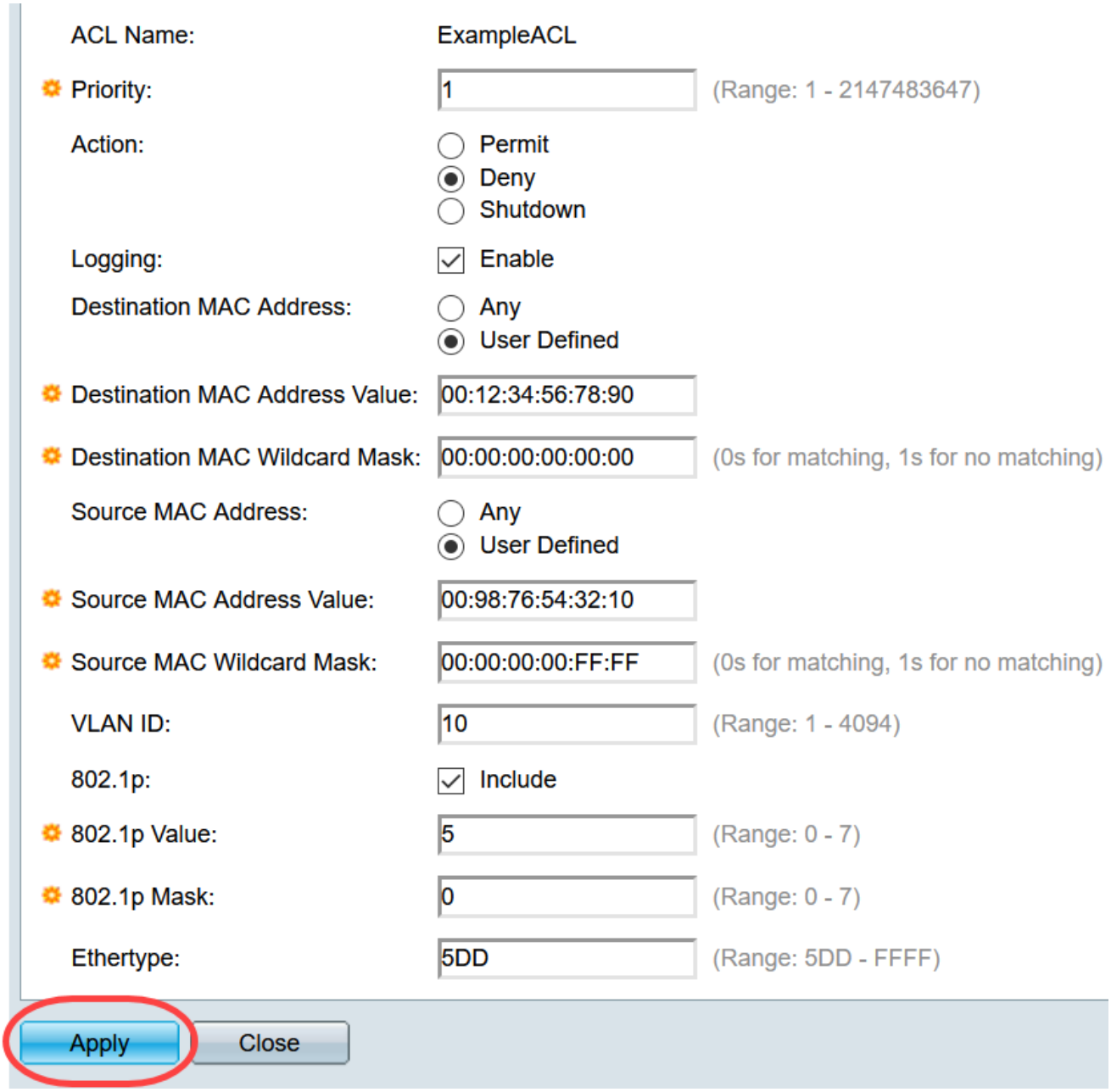
Schritt 14: Geben Sie im Feld "*VLAN ID*" eine VLAN-ID zwischen 1 und 4094 ein. Wenn ein Paket diese VLAN-ID enthält, betrachtet der ACE diese als Übereinstimmung. Dieses Feld ist nicht erforderlich. Wenn sie leer gelassen wird, berücksichtigt der ACE beim Überprüfen von Paketen keine VLAN-IDs.

Schritt 15: Aktivieren Sie im Feld *802.1p* das **Kontrollkästchen Include** (Einschließen), damit die Kriterien ACE include 802.1p festgelegt werden. Wenn Sie 802.1p-Kriterien eingeschlossen haben, geben Sie einen 802.1p-Wert und eine 802.1p-Maske in die Felder *802.1p Value* und *802.1p Mask ein*. Der Bereich für beide Felder liegt zwischen 0 und 7. Wenn ein Paket den entsprechenden 802.1p-Wert enthält und für die Maske passt, wird es vom ACE als Übereinstimmung betrachtet.



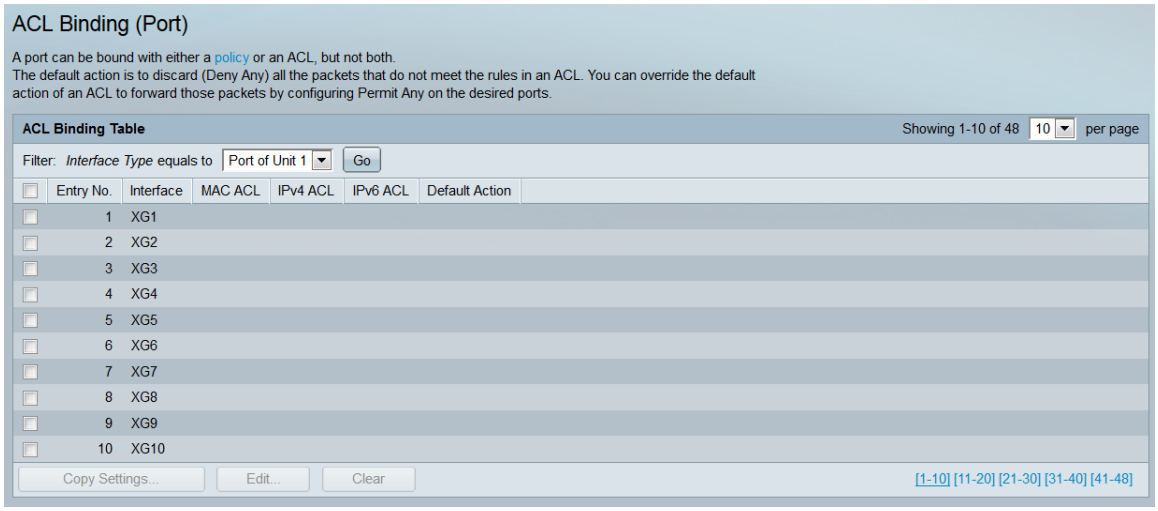
Schritt 16: Geben Sie im Feld *Ethertype* einen Ethertype-Wert ein, der mit eingehenden Paketen verglichen wird. Ethertype ist ein Zwei-Oktett-Feld in einem Frame, das angibt, welches Protokoll im Paket gekapselt ist. Der Bereich ist 5DD-FFFF. Wenn ein Paket den angegebenen Ethertype-Wert enthält, betrachtet der ACE diesen als Übereinstimmung. Eine Liste der Ethertype-Werte finden Sie auf dieser IEEE-Standardseite.

Schritt 17: Klicken Sie auf **Apply** (Anwenden). Der ACE wird der angegebenen ACL hinzugefügt. Klicken Sie auf **Schließen**, um zur *MAC-basierten ACE*-Seite zurückzukehren.

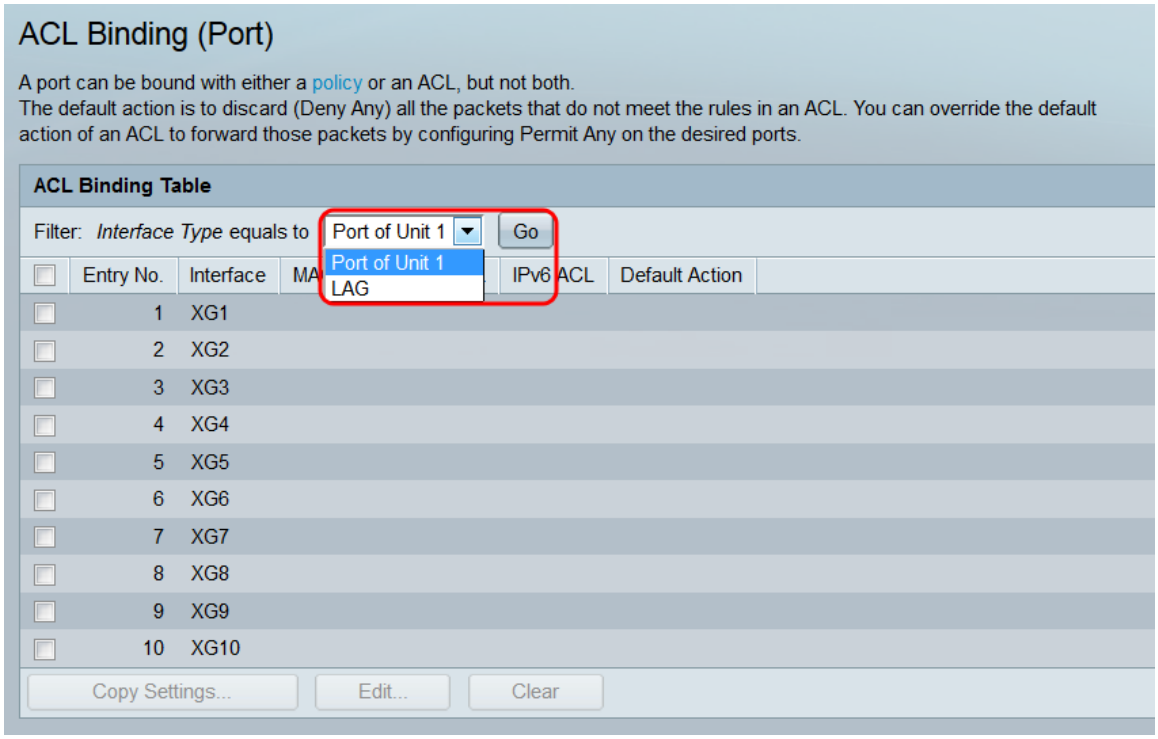


Zuordnung einer MAC-basierten ACL zu Ports

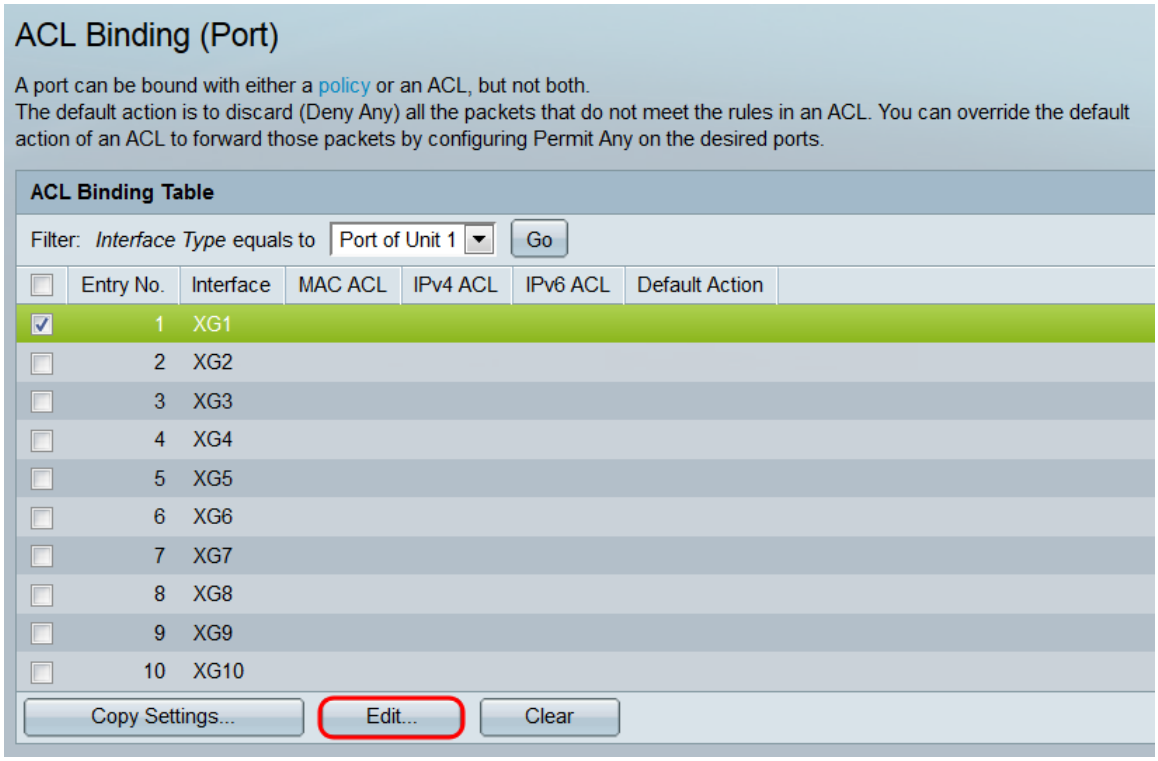
Schritt 1: Eine ACL kann entweder Ports oder VLANs zugeordnet werden. Um eine MAC-basierte ACL einem oder mehreren Ports zuzuordnen, navigieren Sie zu **Access Control > ACL Binding (Port)**. Die Seite *ACL Binding (Port)* wird geöffnet.



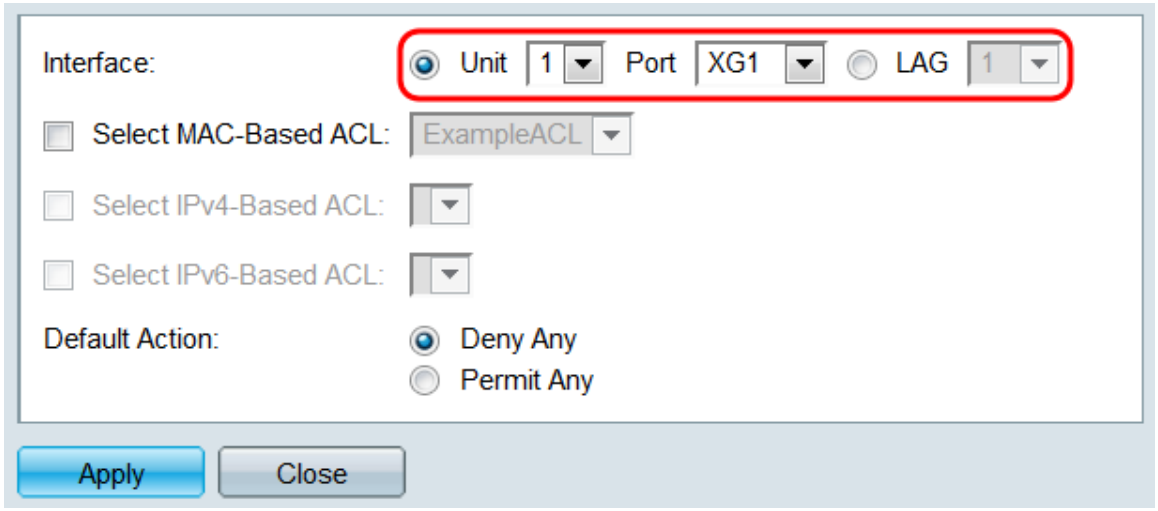
Schritt 2: Wählen Sie in der Dropdown-Liste am oberen Rand der *ACL Binding Table* entweder Ports oder LAG (Link Aggregation Group) als Schnittstellentyp aus. Wenn der Switch Teil eines Stacks ist, können Ports von anderen Einheiten ausgewählt werden. Klicken Sie auf **Go**, um eine Liste des angegebenen Schnittstellentyps anzuzeigen.



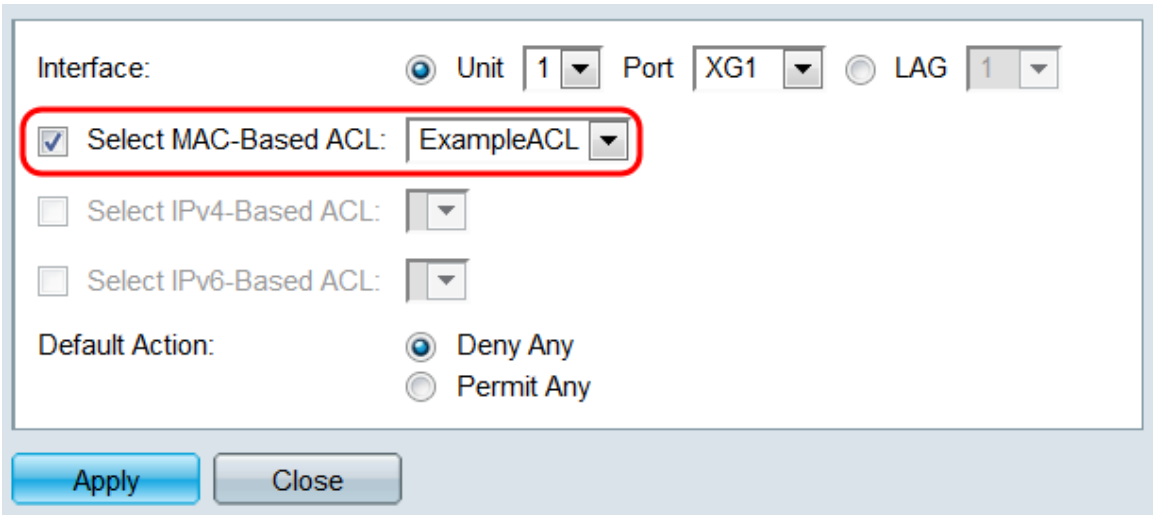
Schritt 3: Aktivieren Sie das Kontrollkästchen einer Schnittstelle, und klicken Sie dann auf die Schaltfläche **Bearbeiten...**. Das Fenster *ACL-Bindung bearbeiten* wird geöffnet.



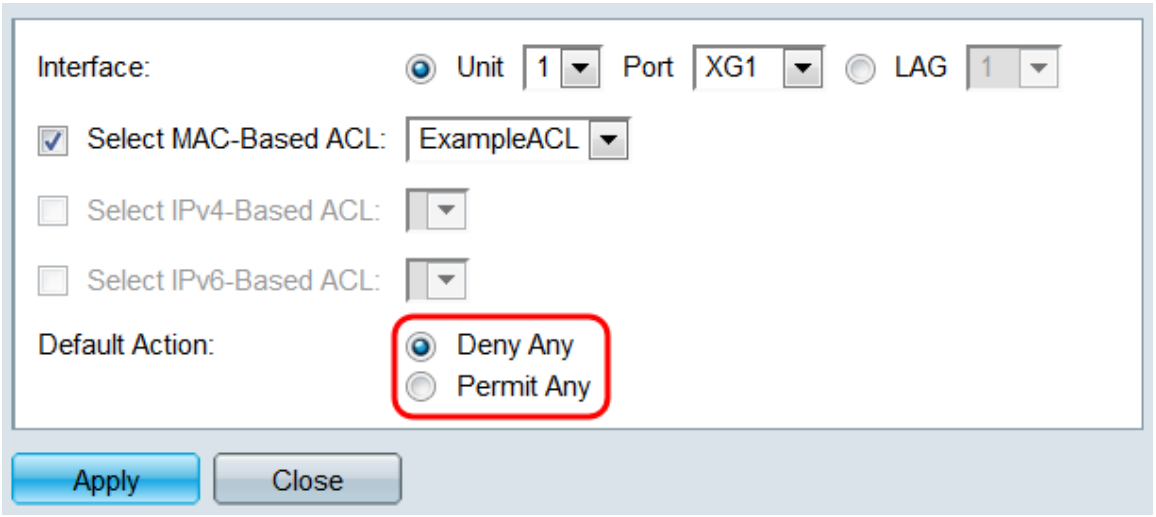
Schritt 4: Das Feld "*Schnittstelle*" zeigt den Port oder die LAG an, die gerade konfiguriert wird. Die in der *ACL-Bindungstabelle* ausgewählte Schnittstelle wird automatisch angezeigt. Dieses Feld kann verwendet werden, um schnell zwischen verschiedenen Schnittstellen zu wechseln, ohne zur Seite *ACL Binding (Port)* zurückzukehren.



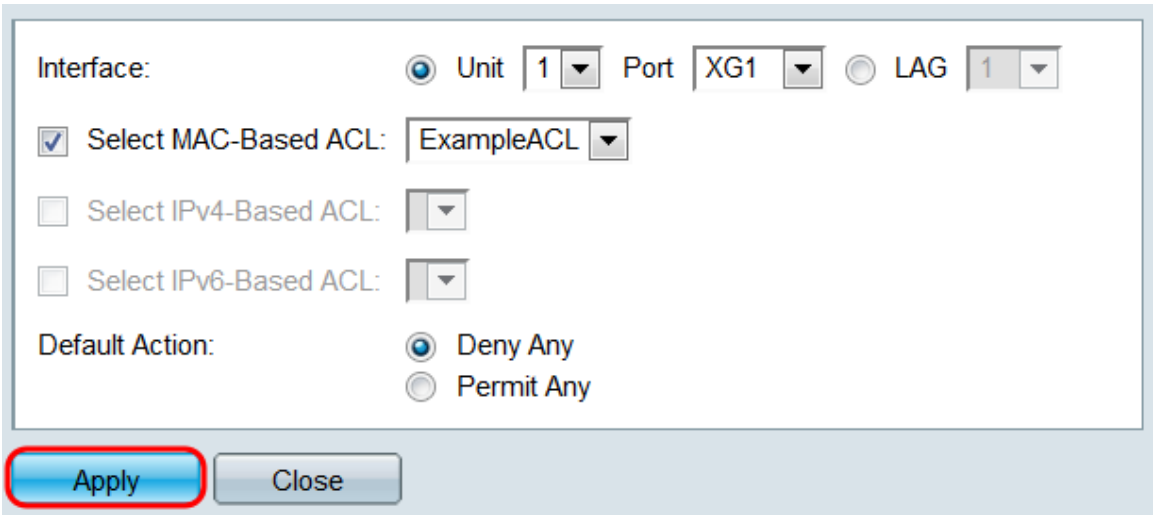
Schritt 5: Aktivieren Sie das Kontrollkästchen **MAC-basierte Zugriffskontrollliste auswählen**, und wählen Sie mithilfe der Dropdown-Liste eine ACL aus, die der angegebenen Schnittstelle zugeordnet werden soll.



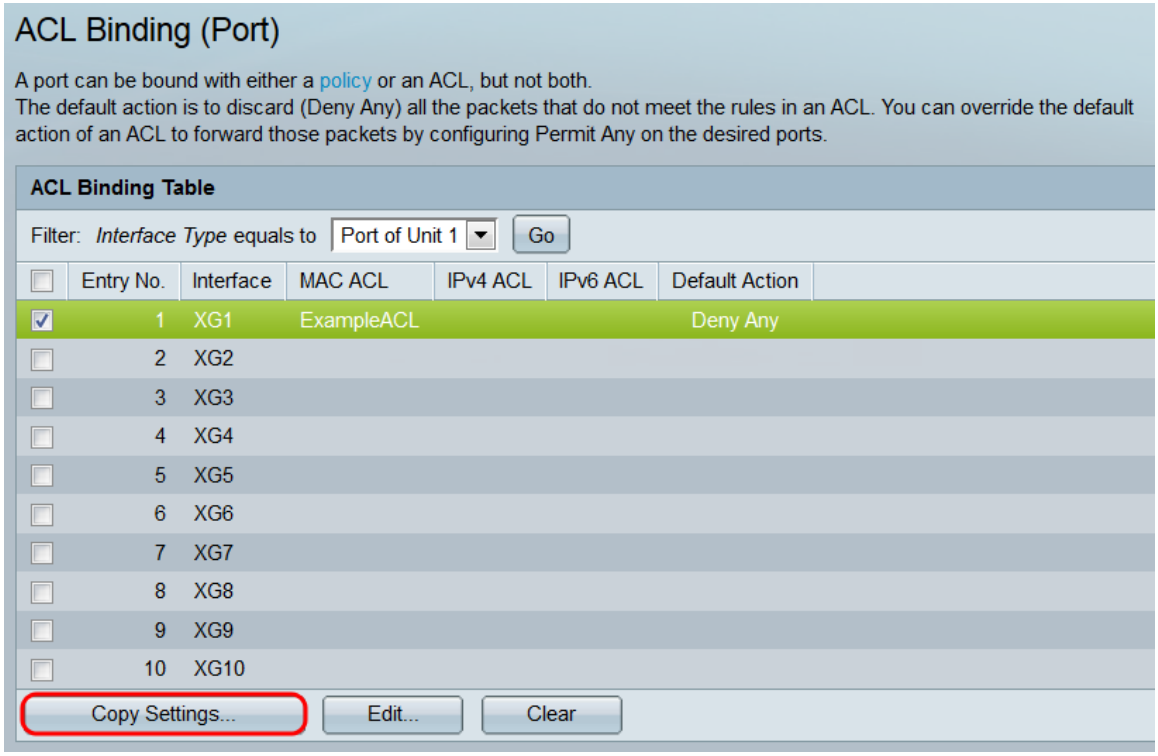
Schritt 6: Wählen Sie im Feld *Default Action* (Standardaktion) ein Optionsfeld aus, um festzulegen, wie Pakete behandelt werden, die nicht den Kriterien der ACL entsprechen. Der Standardwert ist **Deny Any (Any verweigern)**. Dadurch werden alle Pakete verworfen, die nicht den Kriterien der ACL entsprechen. Stattdessen leitet **"Permit Any"** nicht übereinstimmende Pakete weiter.



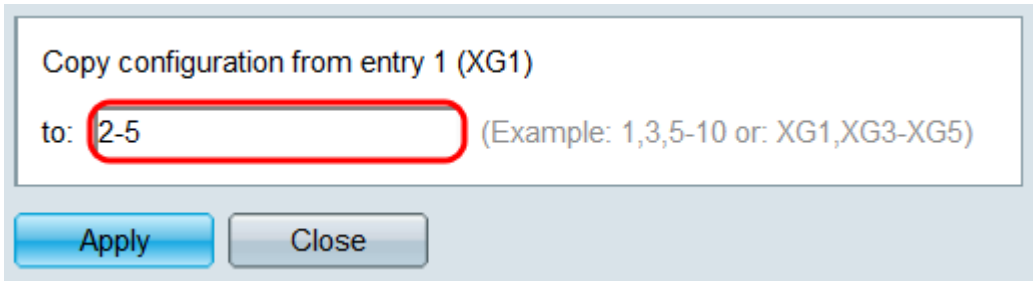
Schritt 7: Klicken Sie auf **Apply** (Anwenden). Die ACL ist der angegebenen Schnittstelle zugeordnet. Sie können das Feld *Schnittstelle* verwenden, um eine andere zu konfigurierende Schnittstelle auszuwählen, oder auf **Schließen** klicken, um zur Seite *ACL Binding (Port)* zurückzukehren.



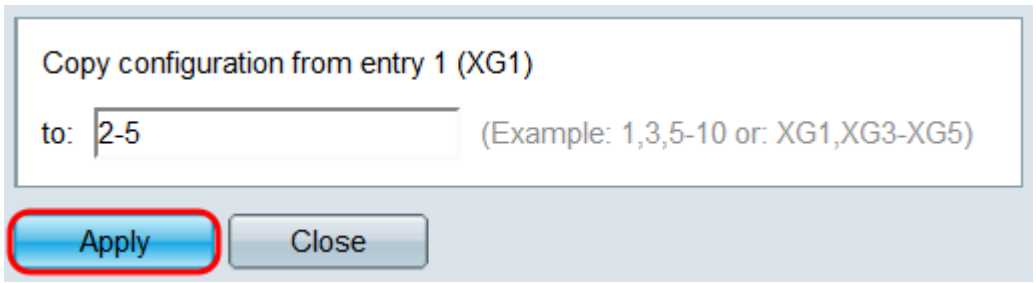
Schritt 8: Um die Einstellungen einer Schnittstelle schnell in andere Schnittstellen zu kopieren, aktivieren Sie das Kontrollkästchen der zu kopierenden Schnittstelle, und klicken Sie dann auf die Schaltfläche **Copy Settings...**. Das Fenster *Kopiereinstellungen* wird geöffnet.



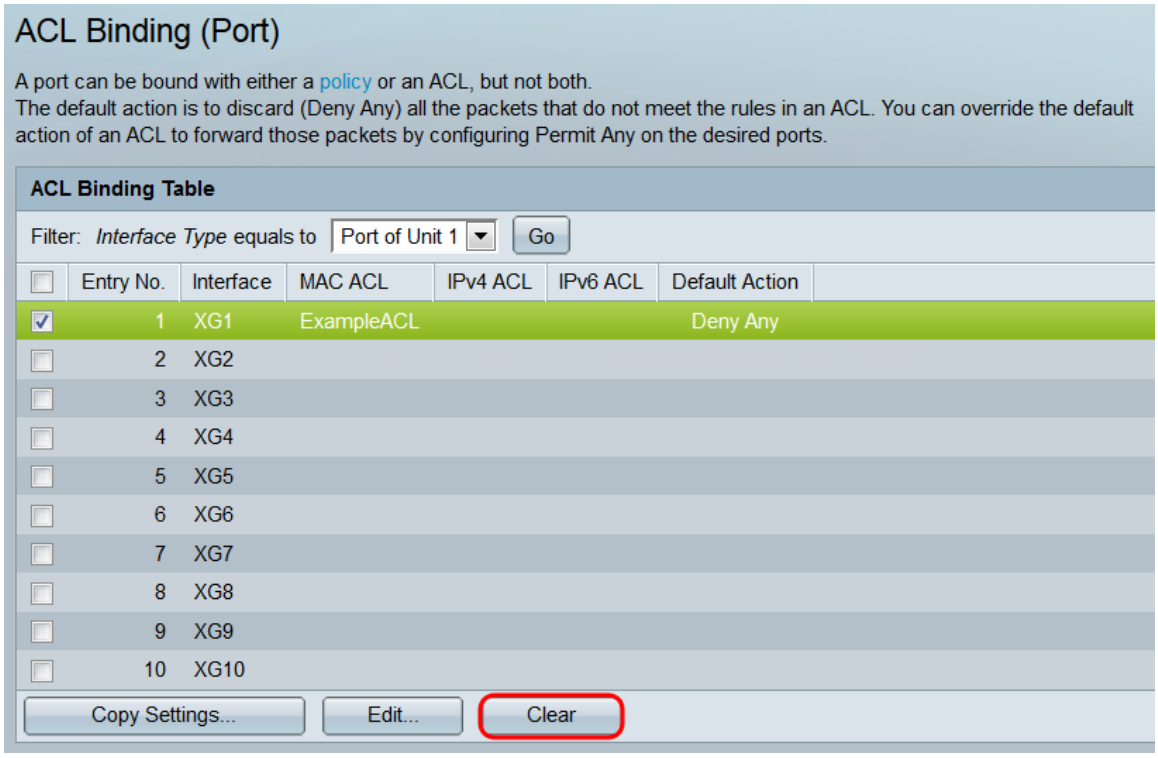
Schritt 9: Geben Sie im Textfeld die Schnittstelle oder Schnittstellen ein, in die Sie die Einstellungen kopieren möchten. Die Schnittstellen können durch Kommas getrennt oder ein Bereich angegeben werden.



Schritt 10: Klicken Sie auf **Apply** (Anwenden). Die Einstellungen werden kopiert.

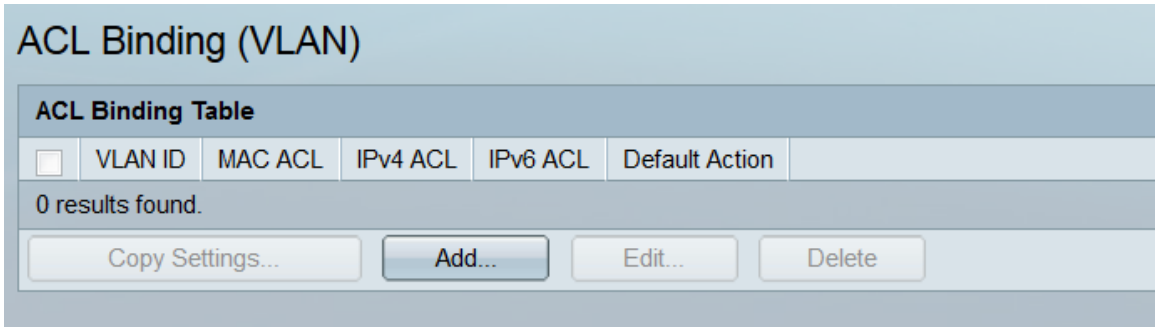


Schritt 11: Wenn Sie die Einstellungen einer Schnittstelle löschen möchten, aktivieren Sie das entsprechende Kontrollkästchen, und klicken Sie auf **Löschen**. Beachten Sie, dass mehrere Schnittstellen gleichzeitig ausgewählt und gelöscht werden können.

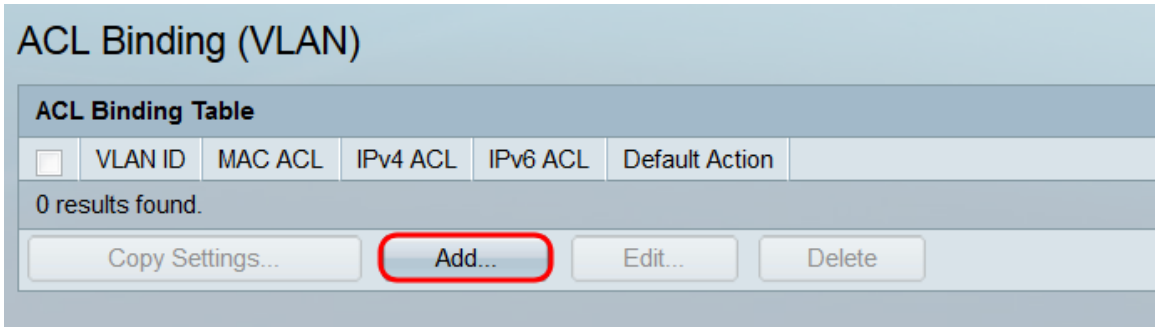


Zuordnung einer MAC-basierten ACL zu VLANs

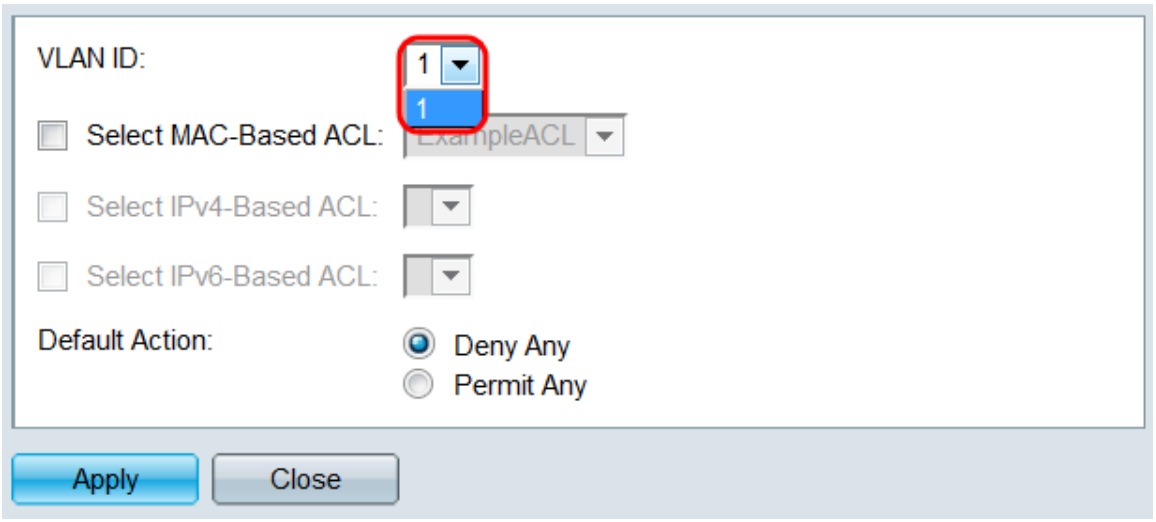
Schritt 1: Eine ACL kann entweder Ports oder VLANs zugeordnet werden. Um eine MAC-basierte ACL einem VLAN zuzuordnen, navigieren Sie zu **Access Control > ACL Binding (VLAN)**. Die Seite *ACL Binding (VLAN)* wird geöffnet.



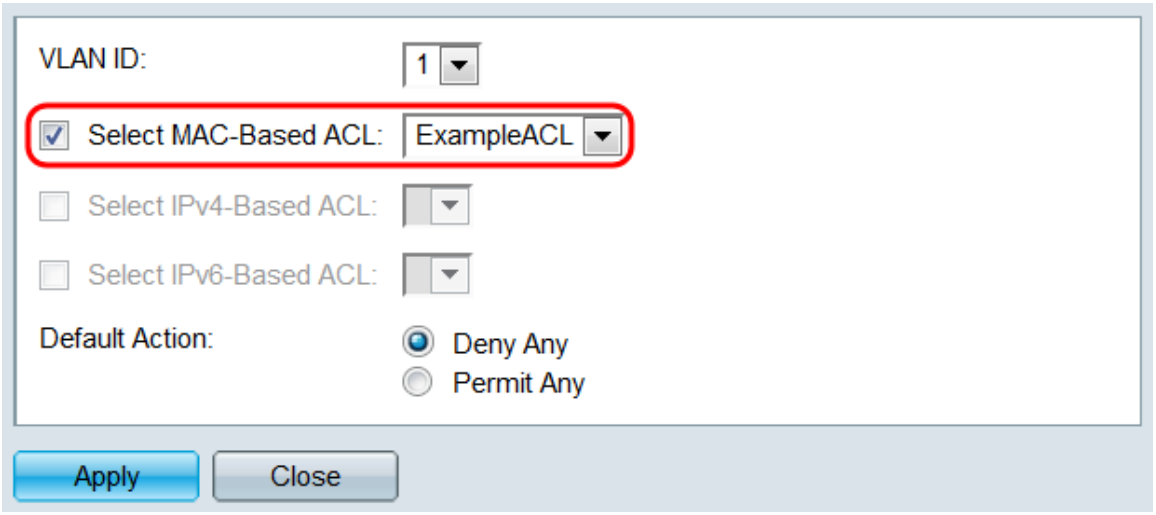
Schritt 2: Die *ACL-Bindungstabelle* zeigt alle ACLs an, die derzeit VLANs zugeordnet sind. Wenn keine Zugriffskontrolllisten zugeordnet wurden, ist die Tabelle leer. Um eine ACL einem VLAN zuzuordnen, klicken Sie auf die Schaltfläche **Hinzufügen...**. Das Fenster *ACL-Bindung hinzufügen* wird geöffnet.



Schritt 3: Wählen Sie ein VLAN aus, um mithilfe der Dropdown-Liste im Feld *VLAN ID* eine ACL zuzuordnen. Dieses Feld kann auch verwendet werden, um schnell zwischen verschiedenen VLANs zu wechseln, ohne zur Seite *ACL Binding (VLAN)* zurückzukehren.

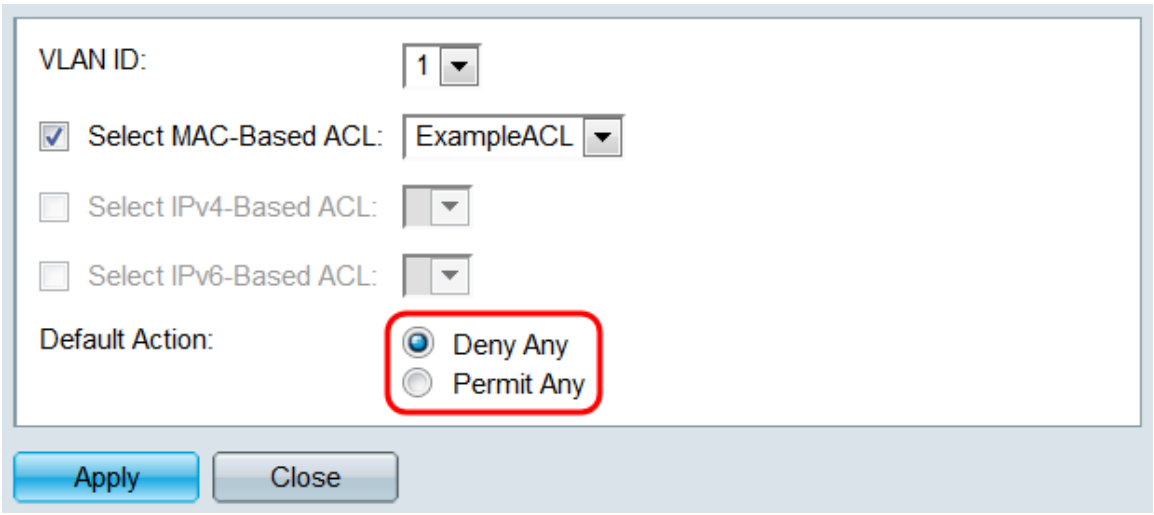


Schritt 4: Aktivieren Sie das Kontrollkästchen **MAC-basierte Zugriffskontrollliste auswählen**, und wählen Sie mithilfe der Dropdown-Liste eine Zugriffskontrollliste aus, die dem angegebenen VLAN zugeordnet werden soll.

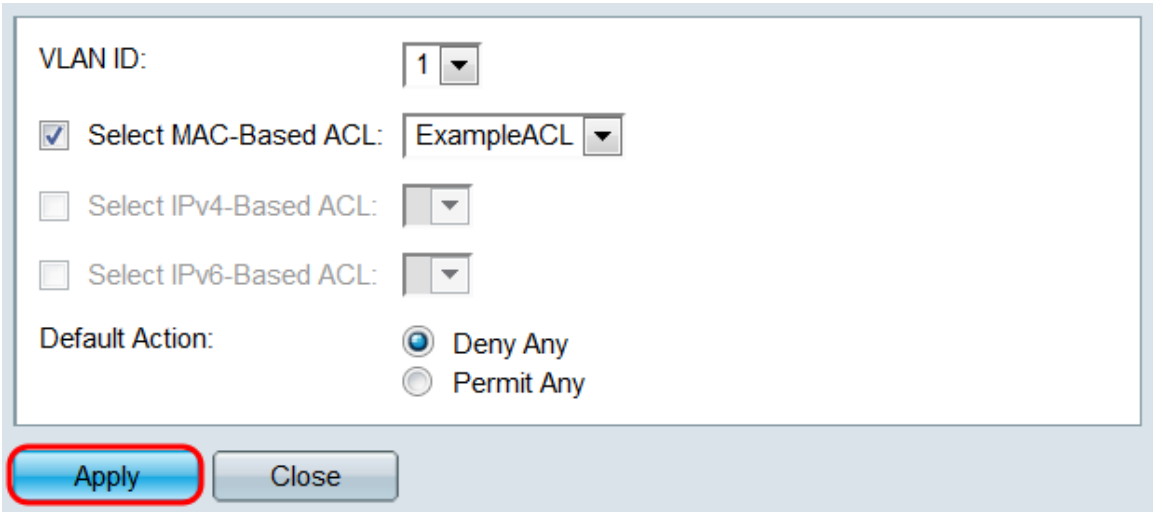


Hinweis: Eine MAC-basierte ACL, die eine VLAN-ID als Teil der Kriterien verwendet, kann nicht an ein VLAN gebunden werden. Darüber hinaus kann eine ACL mit einem Zeitbereich nicht an ein VLAN gebunden werden.

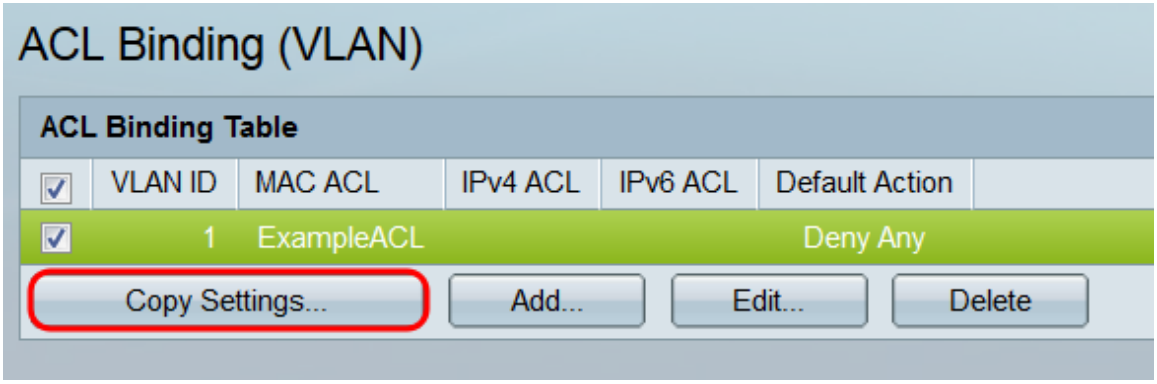
Schritt 5: Wählen Sie im Feld *Default Action* (Standardaktion) ein Optionsfeld aus, um festzulegen, wie Pakete behandelt werden, die nicht den Kriterien der ACL entsprechen. Der Standardwert ist **Deny Any (Any verweigern)**. Dadurch werden alle Pakete verworfen, die nicht den Kriterien der ACL entsprechen. Stattdessen leitet **"Permit Any"** nicht übereinstimmende Pakete weiter.



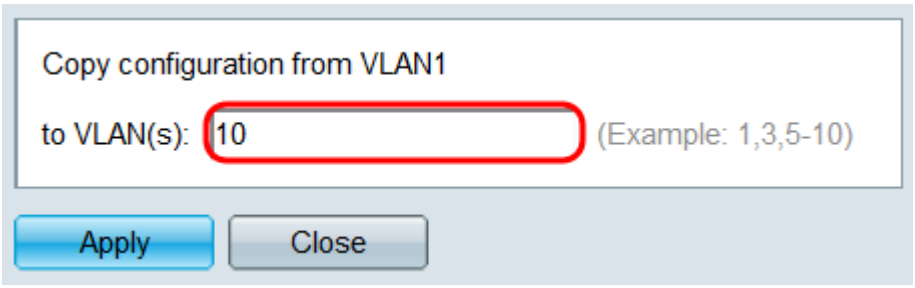
Schritt 6: Klicken Sie auf **Apply** (Anwenden). Die ACL ist dem angegebenen VLAN zugeordnet. Sie können das Feld *VLAN-ID* verwenden, um ein anderes zu konfigurierendes VLAN auszuwählen, oder auf **Schließen** klicken, um zur Seite *ACL Binding (VLAN)* zurückzukehren.



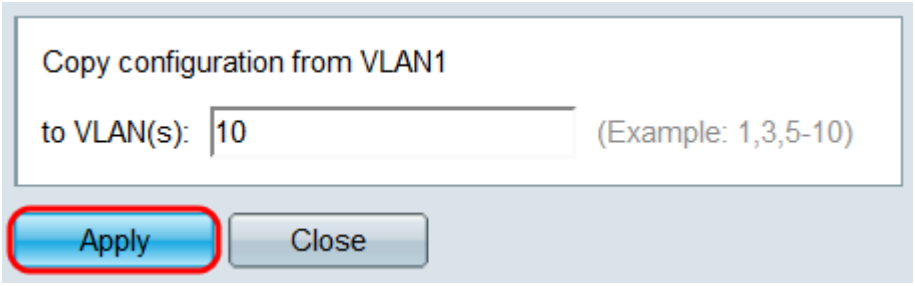
Schritt 7: Um schnell die VLAN-Einstellungen in andere VLANs zu kopieren, aktivieren Sie das Kontrollkästchen der VLAN-Konfiguration, die kopiert werden soll, und klicken Sie dann auf die Schaltfläche **Copy Settings...**. Das Fenster *Kopiereinstellungen* wird geöffnet.



Schritt 8: Geben Sie im Textfeld die VLAN-ID oder die VLAN-IDs ein, in die Sie die Einstellungen kopieren möchten. Die IDs können durch Kommas getrennt oder ein Bereich angegeben werden.



Schritt 9: Klicken Sie auf **Apply** (Anwenden). Die Einstellungen werden kopiert.



Schritt 10: Wenn Sie die Einstellungen eines VLAN löschen möchten, aktivieren Sie das entsprechende Kontrollkästchen, und klicken Sie auf **Löschen**. Beachten Sie, dass mehrere VLANs gleichzeitig ausgewählt und gelöscht werden können.