MAC Based Access Control List (ACL)- und Access Control Entry (ACE)-Konfiguration für Managed Switches der Serie 300

Ziel

Eine Zugriffskontrollliste (Access Control List, ACL) ist eine Sicherheitstechnologie, mit der der Datenfluss im Netzwerk zugelassen oder verweigert wird. MAC-basierte ACLs verwenden Layer-2-Informationen, um den Datenverkehr zuzulassen oder zu verweigern. Ein Access Control Entry (ACE) enthält die tatsächlichen Kriterien für Zugriffsregeln. Sobald der ACE erstellt wurde, wird er auf eine ACL angewendet. Die Managed Switches der Serie 300 unterstützen maximal 512 ACLs und 512 ACEs.

In diesem Artikel wird erläutert, wie MAC-basierte ACLs erstellt werden und wie ACEs auf die ACLs der Managed Switches der Serie 300 angewendet werden.

Anwendbare Geräte

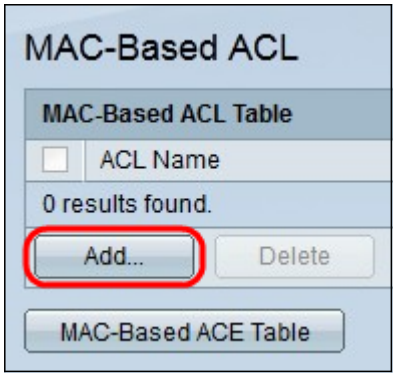
·SG300-10PP
· SG300-10MPP
· SG300-28PP-R
SG300-28SFP-R
SF302-08MPP
· SF302-08PP
· SF300-24PP-R
· SF300-48PP-R

Softwareversion

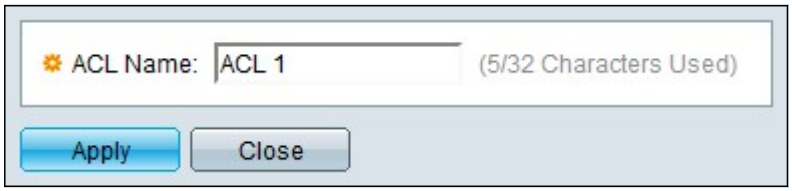
·1.4.0.00p3 [SG300-28SFP-R]
· 6.2.10.18 [Alle anderen zutreffenden Geräte]

MAC-basierte ACL

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

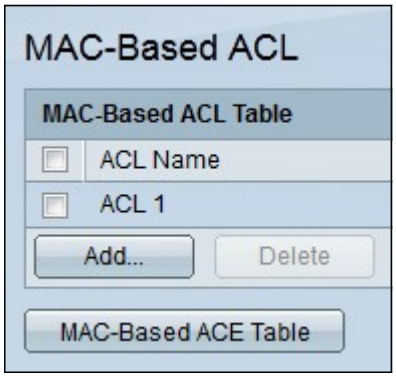


Schritt 2: Klicken Sie auf **Hinzufügen**. Das Fenster *MAC-basierte Zugriffskontrollliste hinzufügen* wird angezeigt.



Schritt 3: Geben Sie im Feld ACL Name (ACL-Name) einen Namen für die ACL ein.

Schritt 4: Klicken Sie auf **Übernehmen**. Die ACL wird erstellt.



MAC-basierter ACE

Wenn ein Frame an einem Port empfangen wird, verarbeitet der Switch den Frame über die erste ACL. Wenn der Frame mit einem ACE-Filter der ersten ACL übereinstimmt, wird die ACE-Aktion ausgeführt. Wenn der Frame mit keinem der ACE-Filter übereinstimmt, wird die nächste ACL verarbeitet. Wenn in allen relevanten ACLs keine Übereinstimmung mit einem ACE gefunden wird, wird der Frame standardmäßig verworfen.

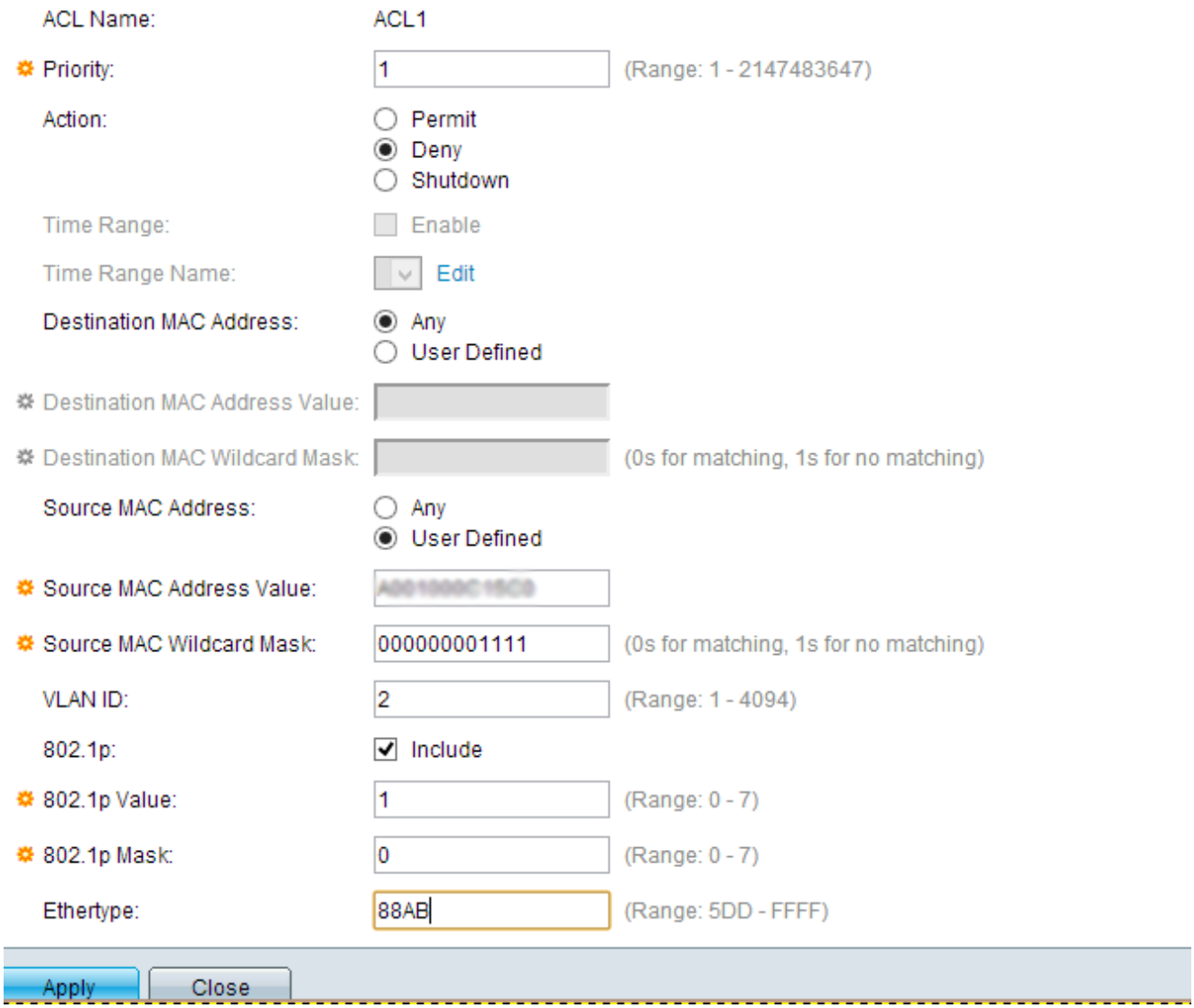
Hinweis: Diese Standardaktion kann vermieden werden, indem ein ACE mit niedriger Priorität erstellt wird, der den gesamten Datenverkehr zulässt.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Access Control > MAC Based ACE**. Die Seite *MAC Based ACE* wird geöffnet:

Schritt 2: Wählen Sie in der Dropdown-Liste ACL Name (ACL-Name) eine ACL aus, auf die eine Regel angewendet werden soll.

Schritt 3: Klicken Sie auf **Los**. Die bereits für die ACL konfigurierten ACEs werden angezeigt.

Schritt 4: Klicken Sie auf **Hinzufügen**, um der ACL eine neue Regel hinzuzufügen. Das Fenster *MAC-basierter ACE hinzufügen* wird angezeigt.



Im Feld ACL Name (ACL-Name) wird der Name der ACL angezeigt.

Schritt 5: Geben Sie den Prioritätswert für den ACE im Feld Priorität ein. ACEs mit einem höheren Prioritätswert werden zuerst verarbeitet. Der Wert 1 ist die höchste Priorität.

Schritt 6: Klicken Sie auf das Optionsfeld für die gewünschte Aktion, die ausgeführt wird,

wenn ein Frame die erforderlichen Kriterien des ACE erfüllt.

·Zulassen - Der Switch leitet Pakete weiter, die die erforderlichen Kriterien des ACEs erfüllen.

·Verweigern: Der Switch verwirft Pakete, die nicht die erforderlichen ACE-Kriterien erfüllen.

·Herunterfahren - Der Switch verwirft Pakete, die nicht die erforderlichen ACE-Kriterien erfüllen, und deaktiviert den Port, an dem die Pakete empfangen wurden.

Hinweis: Deaktivierte Ports können auf der Seite *Porteinstellungen* erneut aktiviert werden.

Schritt 7: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Zeitbereich, um die Konfiguration eines Zeitbereichs für den ACE zu ermöglichen. Zeitbereiche werden verwendet, um die Zeitspanne zu begrenzen, in der ein ACE aktiv ist.

Schritt 8: Wählen Sie aus der Dropdown-Liste "Time Range Name" (Zeitbereichsname) einen Zeitraum aus, der auf den ACE angewendet werden soll.

Hinweis: Klicken Sie auf **Bearbeiten**, um zu der *Zeitbereichsseite* zu navigieren und einen Zeitbereich zu erstellen.

Schritt 9: Klicken Sie auf das Optionsfeld, das den gewünschten Kriterien des ACE im Feld Ziel-MAC-Adresse entspricht.

·Any (Beliebig): Alle Ziel-MAC-Adressen gelten für den ACE.

·Benutzerdefiniert - Geben Sie eine MAC-Adresse und eine MAC-Platzhaltermaske ein, die auf den ACE in den Feldern Ziel-MAC-Adressenwert und Ziel-MAC-Wildcard-Maske angewendet werden soll. Platzhaltermasken werden verwendet, um einen Bereich von MAC-Adressen zu definieren.

Schritt 10: Klicken Sie auf das Optionsfeld, das den gewünschten Kriterien des ACE im Feld Quell-MAC-Adresse entspricht.

·Any (Beliebig): Alle Quell-MAC-Adressen gelten für den ACE.

·Benutzerdefiniert - Geben Sie eine MAC-Adresse und eine MAC-Platzhaltermaske ein, die auf den ACE in den Feldern Ziel-MAC-Adressenwert und Ziel-MAC-Wildcard-Maske angewendet werden soll. Platzhaltermasken werden verwendet, um einen Bereich von MAC-Adressen zu definieren.

Schritt 11: Geben Sie eine VLAN-ID ein, die dem VLAN-Tag des Frames zugeordnet wird.

Schritt 12: (Optional) Um 802.1p-Werte in die ACE-Kriterien aufzunehmen, aktivieren Sie **Include** in das 802.1p-Feld. 802.1p beinhaltet die Technologie Class of Service (CoS). CoS ist ein 3-Bit-Feld in einem Ethernet-Frame, das zur Unterscheidung des Datenverkehrs verwendet wird.

Schritt 13: Wenn 802.1p-Werte enthalten sind, geben Sie die folgenden Felder ein.

·802.1p-Wert: Geben Sie den 802.1p-Wert ein, der zugeordnet werden soll. 802.1p ist eine Spezifikation, die Layer-2-Switches die Möglichkeit gibt, Datenverkehr zu priorisieren und dynamische Multicast-Filterung durchzuführen.

·802.1p Mask (802.1p-Maske): Geben Sie die Platzhaltermaske der 802.1p-Werte ein.

Diese Platzhaltermaske wird verwendet, um den Bereich von 802.1p-Werten zu definieren.

Schritt 14: Geben Sie den Ethertype-Frames ein, der zugeordnet werden soll. Ethertype ist ein zwei Oktett-Feld in einem Ethernet-Frame, das verwendet wird, um anzugeben, welches Protokoll für die Nutzlast des Frames verwendet wird.

Schritt 15: Klicken Sie auf **Übernehmen**. Der ACE wird erstellt. In diesem Beispiel verweigert der erstellte ACE den Datenverkehr, der von den definierten Quell-MAC-Adressen an alle Zieladressen gesendet wird.