

Konfigurieren von MAC-basierten Zugriffskontrolllisten (ACLs) und Zugriffskontrolllisten (ACEs) auf einem Managed Switch

Ziel

Eine Zugriffskontrollliste (Access Control List, ACL) ist eine Liste von Filtern für den Netzwerkverkehr und zugehörigen Aktionen zur Verbesserung der Sicherheit. Sie blockiert oder ermöglicht Benutzern den Zugriff auf bestimmte Ressourcen. Eine ACL enthält die Hosts, denen der Zugriff auf das Netzwerkgerät gestattet oder verweigert wird. Die MAC-basierte Zugriffskontrollliste (Media Access Control List, ACL) ist eine Liste der Quell-MAC-Adressen, die mithilfe von Layer-2-Informationen den Zugriff auf Datenverkehr zulassen oder verweigern. Wenn ein Paket von einem Wireless Access Point zu einem LAN-Port (Local Area Network) oder umgekehrt kommt, prüft dieses Gerät, ob die Quell-MAC-Adresse des Pakets mit einem Eintrag in dieser Liste übereinstimmt, und überprüft die ACL-Regeln auf den Inhalt des Frames. Anschließend werden die übereinstimmenden Ergebnisse verwendet, um dieses Paket zuzulassen oder zu verweigern. Pakete vom LAN zum LAN-Port werden jedoch nicht überprüft. Ein Access Control Entry (ACE) enthält die tatsächlichen Kriterien für Zugriffsregeln. Sobald der ACE erstellt wurde, wird er auf eine ACL angewendet. Sie sollten Zugriffslisten verwenden, um eine grundlegende Sicherheitsstufe für den Zugriff auf Ihr Netzwerk bereitzustellen. Wenn Sie keine Zugriffslisten für Ihre Netzwerkgeräte konfigurieren, können alle Pakete, die über den Switch oder Router übertragen werden, in alle Teile Ihres Netzwerks gelangen.

Dieser Artikel enthält Anweisungen zur Konfiguration von MAC-basierten ACLs und ACEs auf Ihrem Managed Switch.

Anwendbare Geräte | Softwareversion

- Serie Sx350 | 2.2.0.66 ([aktueller Download](#))
- SG350X-Serie | 2.2.0.66 ([aktueller Download](#))
- Serie Sx500 | 1.4.5.02 ([Download zuletzt](#))
- Serie Sx550X | 2.2.0.66 ([aktueller Download](#))

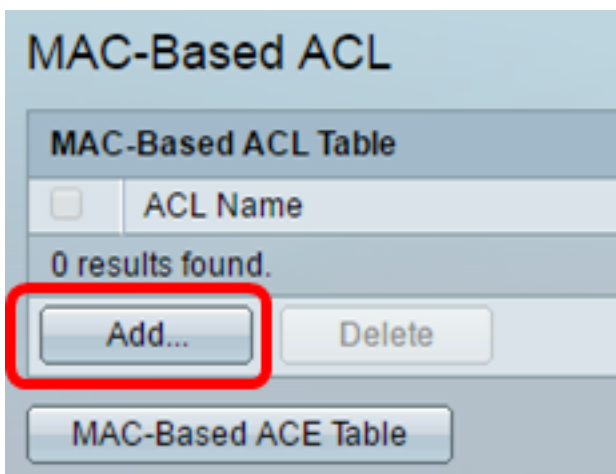
MAC-basierte ACL und ACE konfigurieren

MAC-basierte ACL konfigurieren

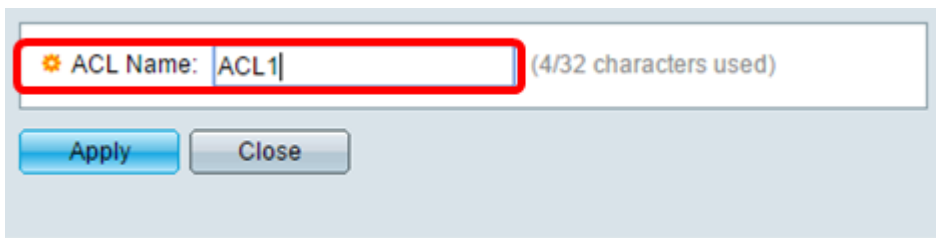
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und gehen Sie dann zu **Access Control > MAC-Based ACL**.



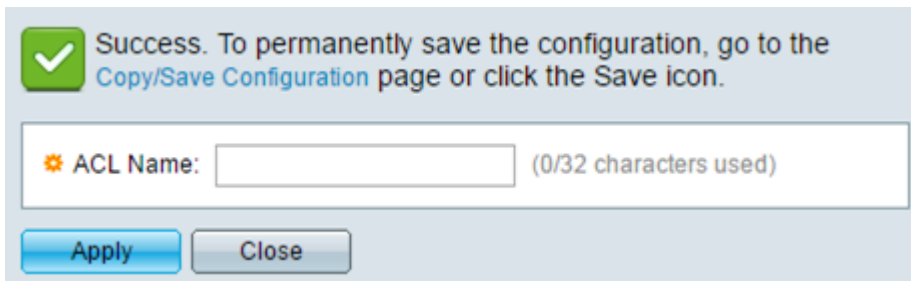
Schritt 2: Klicken Sie auf die Schaltfläche **Hinzufügen**.



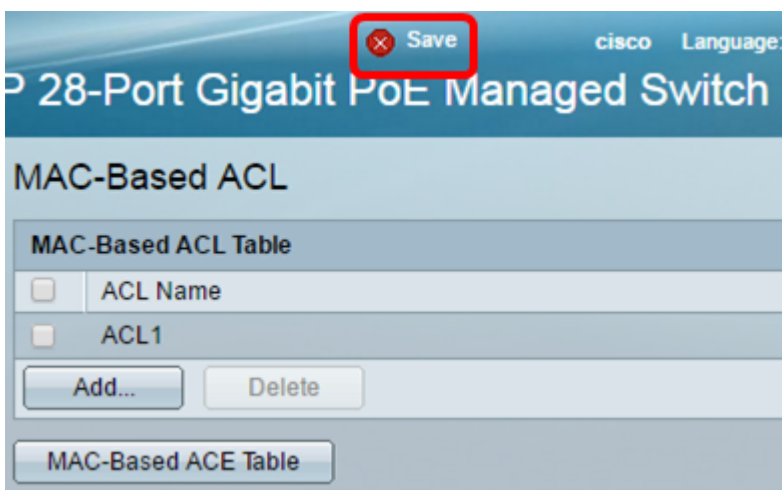
Schritt 3: Geben Sie im Feld ACL Name (ACL-Name) den Namen der neuen ACL ein.



Schritt 4: Klicken Sie auf **Übernehmen** und dann auf **Schließen**.



Schritt 5: (Optional) Klicken Sie auf **Speichern**, um die Einstellungen in der Startkonfigurationsdatei zu speichern.



Sie sollten jetzt eine MAC-basierte ACL auf Ihrem Switch konfiguriert haben.

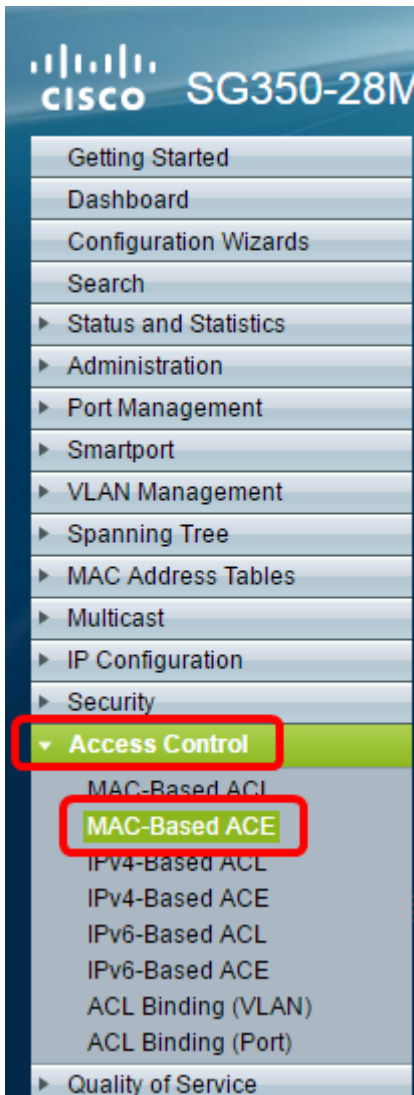
MAC-basierter ACE konfigurieren

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.

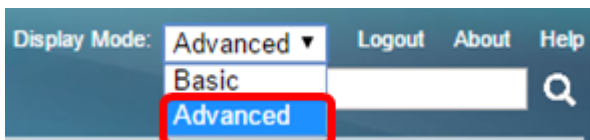
In diesem Szenario wird ein ACE erstellt, um Datenverkehr zu verweigern, der von einer bestimmten benutzerdefinierten Quell-MAC-Adresse an beliebige Zieladressen gesendet wird.

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

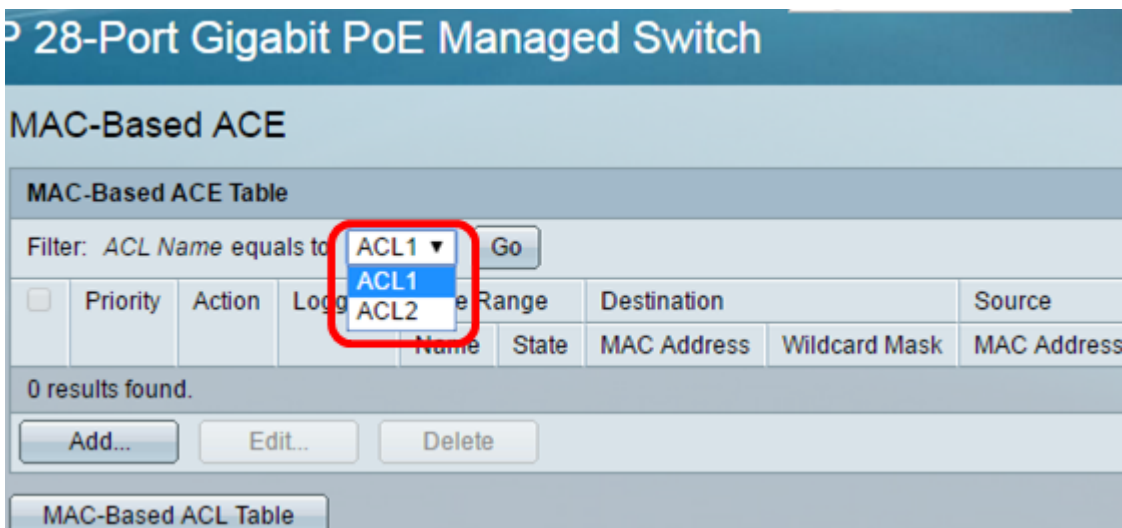
Schritt 1: Gehen Sie im webbasierten Dienstprogramm zu **Access Control > MAC-Based ACE**.



Wichtig: Um die verfügbaren Funktionen des Switches vollständig zu nutzen, wechseln Sie in den erweiterten Modus, indem Sie in der Dropdown-Liste Anzeigemodus oben rechts auf der Seite **Advanced (Erweitert)** auswählen.



Schritt 2: Wählen Sie eine ACL aus der Dropdown-Liste ACL Name (ACL-Name) aus, und klicken Sie dann auf **Go (Los)**.



Hinweis: Die bereits für die ACL konfigurierten ACEs werden in der Tabelle angezeigt.

Schritt 3: Klicken Sie auf die Schaltfläche **Hinzufügen**, um der ACL eine neue Regel hinzuzufügen.

Hinweis: Im Feld *ACL Name* wird der Name der ACL angezeigt.

Schritt 4: 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.

ACL Name:	ACL1
<input checked="" type="checkbox"/> Priority:	<input type="text" value="1"/> (Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
Logging:	<input checked="" type="checkbox"/> Enable

Schritt 5: (Optional) Aktivieren Sie das Kontrollkästchen **Enable Logging** (Protokollierung aktivieren), um die Protokollierung von ACL-Flüssen zu aktivieren, die der ACL-Regel entsprechen.

Schritt 6: Klicken Sie auf das Optionsfeld für die gewünschte Aktion, die ausgeführt wird, wenn ein Frame die erforderlichen Kriterien des ACE erfüllt.

Hinweis: In diesem Beispiel wird Verweigern ausgewählt.

<input checked="" type="checkbox"/> Priority:	<input type="text" value="1"/> (Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown

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

Deny (Verweigern): Der Switch verwirft Pakete, die die erforderlichen Kriterien des ACE 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: (Optional) Aktivieren Sie das Kontrollkästchen **Enable Time Range** (Zeitbereich aktivieren), um eine Konfiguration eines Zeitbereichs für den ACE zu ermöglichen. Zeitbereiche werden verwendet, um die Zeitspanne zu begrenzen, in der ein ACE aktiv ist.

Time Range:	<input checked="" type="checkbox"/> Enable
Time Range Name:	<input type="text" value="1"/> Edit

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

Time Range:	<input checked="" type="checkbox"/> Enable
Time Range Name:	<input type="text" value="1"/> Edit

Hinweis: Sie können auf **Bearbeiten** klicken, um zu der Seite "Time Range" zu navigieren und

einen Zeitbereich zu erstellen.

Time Range Name: 1 (1/32 characters used)

Absolute Starting Time: Immediate
 Date 2016 Jan 01 Time 00 00 HH:MM

Absolute Ending Time: Infinite
 Date 2017 Dec 01 Time 23 59 HH:MM

Apply Close

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

Destination MAC Address: Any
 User Defined

* Destination MAC Address Value:

* Destination MAC Wildcard Mask: (0s for matching, 1s for no matching)

Folgende Optionen stehen zur Verfügung:

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

User Defined (Benutzerdefiniert) - Geben Sie eine MAC-Adresse und eine MAC-Platzhaltermaske ein, die auf den ACE in den Feldern *Ziel-MAC-Adresswert* und *Ziel-MAC-Platzhaltermaske* angewendet werden sollen. Platzhaltermasken werden verwendet, um einen Bereich von MAC-Adressen zu definieren.

Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt. Wenn Sie diese Option wählen, bedeutet dies, dass der zu erstellende ACE den ACE-Verkehr blockiert.

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

ACL Name:	ACL1	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input checked="" type="checkbox"/> Enable	
Time Range:	<input checked="" type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="1"/> Edit	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text"/>	
Destination MAC Wildcard Mask:	<input type="text"/>	(0s for matching, 1s for no matching)
Source MAC Address:	<input type="radio"/> Any <input checked="" type="radio"/> User Defined	
Source MAC Address Value:	<input type="text" value="a2:b2:c2:d2:e2:f2"/>	
Source MAC Wildcard Mask:	<input type="text" value="000000001111"/>	(0s for matching, 1s for no matching)
VLAN ID:	<input type="text" value="2"/>	(Range: 1 - 4094)
802.1p:	<input checked="" type="checkbox"/> Include	
802.1p Value:	<input type="text" value="1"/>	(Range: 0 - 7)
802.1p Mask:	<input type="text" value="0"/>	(Range: 0 - 7)
Ethertype:	<input type="text" value="88AB"/>	(Range: 5DD - FFFF)

Apply Close

Folgende Optionen stehen zur Verfügung:

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

User Defined (Benutzerdefiniert) - Geben Sie eine MAC-Adresse und eine MAC-Platzhaltermaske ein, die auf den ACE in den Feldern *Source MAC Address Value* und *Source MAC Wildcard Mask* (*Quell-MAC-Adressenwert* und *Quell-MAC-Platzhaltermaske*) angewendet werden sollen. Platzhaltermasken werden verwendet, um einen Bereich von MAC-Adressen zu definieren.

Hinweis: In diesem Beispiel wird User Defined (Benutzerdefiniert) ausgewählt.

Schritt 11: (Optional) Geben Sie im Feld *VLAN ID* eine VLAN ID ein, die dem VLAN-Tag des Frames entspricht.

Schritt 12: (Optional) Um 802.1p-Werte in ACE-Kriterien einzubeziehen, aktivieren Sie das Kontrollkästchen **Include** in the 802.1p. 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. Die Werte lauten wie folgt:

- 0 — Hintergrund. Die Daten, die am wenigsten priorisiert werden, wie Massenübertragungen, Spiele usw.
- 1 — Bester Aufwand. Die Daten, die eine bestmögliche Bereitstellung für normale LAN-Prioritäten erfordern. Das Netzwerk bietet keine Garantie für die Zustellung, aber die Daten erhalten eine unbestimmte Bitrate und Lieferzeit, die auf dem Datenverkehr basieren.
- 2 — Hervorragender Aufwand. Die Daten, die für wichtige Benutzer die bestmögliche Bereitstellung erfordern.
- 3 - Critical Application like Linux Virtual Server (LVS) Phone Session Initiation Protocol (SIP)
- 4 - Video. Latenz und Jitter unter 100 ms.
- 5 - Voice Cisco IP-Telefon-Standard. Latenz und Jitter unter 10 ms.
- 6 - LVS-Telefon RTP (Inter-Network Control LVS).
- 7 - Netzwerkkontrolle Hohe Anforderung an die Wartung und Unterstützung der Netzwerkinfrastruktur.

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: (Optional) Geben Sie den Ethertype-Typ des zu vergleichenden Frames ein. Ethertype ist ein 2-Oktett-Feld in einem Ethernet-Frame, das verwendet wird, um anzugeben, welches Protokoll für die Nutzlast des Frames verwendet wird.

Schritt 14: Klicken Sie auf **Übernehmen** und anschließend auf **Schließen**. Der ACE wird erstellt und dem Namen der ACL zugeordnet.

Schritt 15: Klicken Sie auf **Speichern**, um die Einstellungen in der Startkonfigurationsdatei zu speichern.

28-Port Gigabit PoE Managed Switch

MAC-Based ACE

MAC-Based ACE Table

Filter: ACL Name equals to

<input type="checkbox"/>	Priority	Action	Logging	Time Range		Destination
				Name	State	MAC Address
<input type="checkbox"/>	1	Deny	Enabled	1	Active	Any
<input type="checkbox"/>	2	Permit	Enabled	1	Active	a1:b1:c1:d1:e1:f1

Sie sollten jetzt einen MAC-basierten ACE auf Ihrem Switch konfiguriert haben.

Weitere Links, die Sie vielleicht nützlich finden:

- [Produktseite für Switches der Serie 350](#)
- [Produktseite für Switches der Serie 350X](#)
- [Produktseite für Switches der Serie 550](#)
- [Produktseite für Switches der Serie 550X](#)

Sehen Sie sich ein Video zu diesem Artikel an..

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)