

MAC-gebaseerde Access Control List (ACL) en Access Control Entry (ACE) configuratie op 300 Series Managed-switches

Doel

Een toegangscontrolelijst (ACL) is een beveiligingstechnologie die wordt gebruikt om netwerkverkeersstroom toe te staan of te ontkennen. MAC-gebaseerde ACL's gebruiken Layer 2-informatie om toegang tot verkeer toe te staan of te ontkennen. Een Access Control Entry (ACE) bevat de eigenlijke toegangseisen. Zodra ACE wordt gecreëerd, wordt het toegepast op een ACL. De 300 Series Managed-switches ondersteunen een maximum van 512 ACL's en 512 ACE's.

Dit artikel legt uit hoe u MAC-gebaseerde ACL's kunt maken en hoe u ACE's op de ACL's kunt toepassen op de 300 Series Managed-switches.

Toepasselijke apparaten

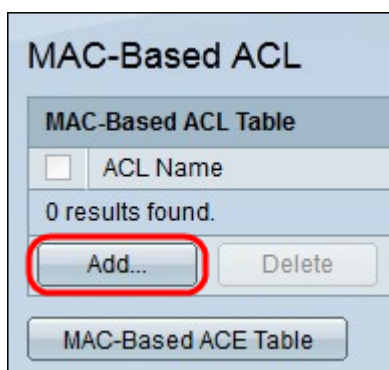
- SG300-10PP
- SG300-10MPP router
- SG300-28PP-R router
- SG300-28SFP-R switch
- SF302-08MPP router
- SF302-08PP
- SF300-24PP-R switch
- SF300-48PP-R switch

Softwareversie

- 1.4.0.00p3 [SG300-28SFP-R]
- 6.2.10.18 [Alle andere apparatuur]

MAC-gebaseerde ACL

Stap 1. Meld u aan bij het web configuratie hulpprogramma en kies **toegangscontrole > MAC-gebaseerde ACL**. De *MAC-gebaseerde ACL*-pagina wordt geopend:



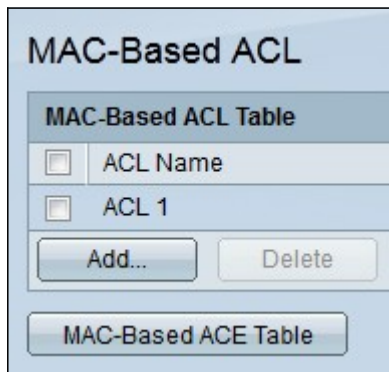
MAC-Based ACL	
MAC-Based ACL Table	
<input type="checkbox"/>	ACL Name
0 results found.	
<input type="button" value="Add..."/>	<input type="button" value="Delete"/>
MAC-Based ACE Table	

Stap 2. Klik op **Add**. Het *Add MAC-Based ACL*-venster verschijnt.



Stap 3. Voer een naam voor ACL in het veld Naam van ACL in.

Stap 4. Klik op **Toepassen**. ACL wordt gecreëerd.

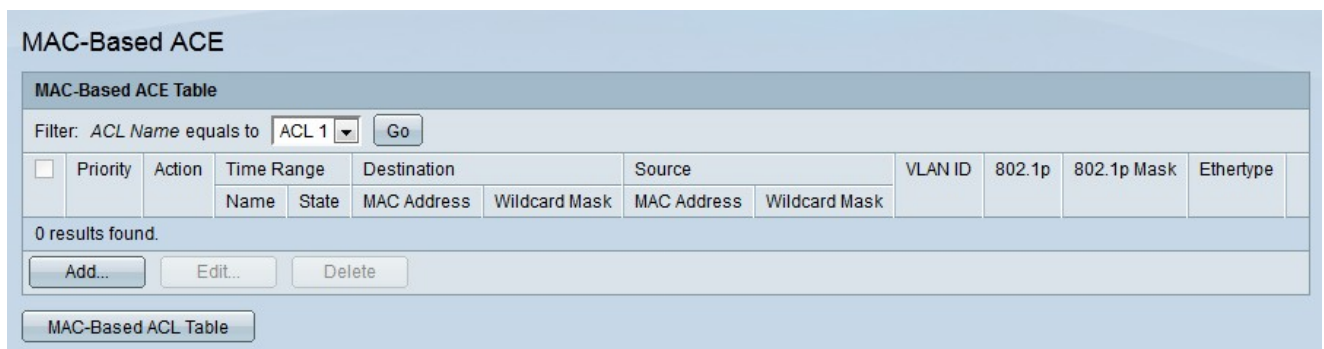


MAC-gebaseerde ACE

Wanneer een kader op een poort wordt ontvangen, verwerkt de schakelaar het kader door eerste ACL. Als het kader overeenkomt met een ACE-filter van de eerste ACL, wordt de ACE-actie uitgevoerd. Als het kader aan geen van de ACE filters voldoet, wordt volgende ACL verwerkt. Als geen overeenkomst in alle relevante ACL's op een ACE is gevonden, wordt het frame standaard verlaagd.

Opmerking: Deze standaardinstelling kan worden vermeden door de creatie van een ACE met lage prioriteit die al het verkeer mogelijk maakt.

Stap 1. Meld u aan bij het web configuratieprogramma en kies **toegangscontrole > MAC-gebaseerde ACE**. De *MAC-gebaseerde ACE*-pagina wordt geopend:



Stap 2. Kies een ACL-regel in de vervolgkeuzelijst ACL-naam om een regel op toe te passen.

Stap 3. Klik op **Ga**. De ACE's die reeds voor ACL zijn geconfigureerd worden weergegeven.

Stap 4. Klik op **Add** om een nieuwe regel aan de ACL toe te voegen. Het *Add MAC-Based ACE* venster verschijnt.

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	
Time Range:	<input type="checkbox"/> Enable	
Time Range Name:	<input type="button" value="v"/>	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="A001000C18C0"/>	
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)

Het veld ACL-naam geeft de naam van de ACL weer.

Stap 5. Voer de prioriteitswaarde van de ACE in het veld Prioriteit in. ACE's met een hogere prioriteit worden eerst verwerkt. De eerste waarde is de hoogste prioriteit.

Stap 6. Klik op de radioknop die correspondeert met de gewenste actie die wordt ondernomen wanneer een frame voldoet aan de vereiste criteria van de ACE.

- Vergunning — De schakelaar voorwaarts pakketten die aan de vereiste criteria van ACE voldoen.
- Deny — De schakelaar druppelt pakketten die niet aan de vereiste criteria van het ACE voldoen.
- Uitschakelen - De schakelaar druppelt pakketten in die niet aan de vereiste criteria van de ACE voldoen en schakelt de haven uit waar de pakketten werden ontvangen.

Opmerking: Uitgeschakelde poorten kunnen opnieuw worden geactiveerd op de pagina *Port Settings*.

Stap 7. Controleer het aanvinkvakje **Enable** in het veld Tijdbereik om een tijdbereik in de ACE-modus te laten instellen. De tijdbereiken worden gebruikt om de tijd te beperken die een ACE in werking is.

Stap 8. Kies in de vervolgkeuzelijst Naam tijdbereik een tijdbereik om op de ACE toe te

passen.

Opmerking: Klik op **Bewerken** om naar de pagina *Tijdbereik* te navigeren en een tijdbereik te maken.

Stap 9. Klik op de radioknop die aan de gewenste criteria van ACE in het veld MAC-adres van de bestemming voldoet.

- Any — Alle bestemming MAC-adressen zijn van toepassing op het ACE.
- Gebruiker gedefinieerd - Voer een MAC-adres en een MAC-jokermasker in dat op de ACE-toets moet worden toegepast in de velden MAC-adreswaarde en MAC-jokermasker van de bestemming. Wildcard maskers worden gebruikt om een bereik van MAC adressen te definiëren.

Stap 10. Klik op de radioknop die aan de gewenste criteria van ACE in het veld Bron-MAC-adres voldoet.

- Alle bron-MAC-adressen zijn van toepassing op ACE.
- Gebruiker gedefinieerd - Voer een MAC-adres en een MAC-jokermasker in dat op de ACE-toets moet worden toegepast in de velden MAC-adreswaarde en MAC-jokermasker van de bestemming. Wildcard maskers worden gebruikt om een bereik van MAC adressen te definiëren.

Stap 1. Voer een VLAN-id in dat met de VLAN-tag van het kader wordt aangepast.

Stap 12. (optioneel) Om 802.1p-waarden in ACE-criteria op te nemen, **neemt** de controle **ook** op in het veld 802.1p. 802.1p betreft de serviceklasse (CoS). CoS is een 3 bit veld in een Ethernet-frame dat wordt gebruikt om verkeer te differentiëren.

Stap 13. Als de waarden 802.1p zijn opgenomen, specificeert u de volgende velden.

- 802.1p Waarde — Voer de 802.1p waarde in die moet worden aangepast. 802.1p is een specificatie die Layer 2-switches de mogelijkheid geeft om prioriteit te geven aan verkeer en dynamische multicast filtering uit te voeren.
- Mash 802.1p — Voer het masker van de 802.1p-waarden in. Dit masker wordt gebruikt om de 802.1p-waarden te definiëren.

Stap 14. Voer het EtherType van het kader in dat moet worden aangepast. EtherType is een twee octetten veld in een Ethernet-frame dat wordt gebruikt om aan te geven welk protocol wordt gebruikt voor de lading van het frame.

Stap 15. Klik op **Toepassen**. De ACE is gemaakt. In dit voorbeeld, ontkent het gemaakte ACE verkeer dat van de bepaalde bron van MAC adressen naar alle bestemmingsadressen wordt verzonden.

MAC-Based ACE

MAC-Based ACE Table

Filter: ACL Name equals to

<input type="checkbox"/>	Priority	Action	Time Range		Destination		Source		VLAN ID	802.1p	802.1p Mask	EtherType	
			Name	State	MAC Address	Wildcard Mask	MAC Address	Wildcard Mask					
<input type="checkbox"/>	1	Deny			Any	Any	a0:01:00:0c:11:a0	00:00:00:00:11:11	2	1	0	804B	
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>													