Configureer de MAC-gebaseerde toegangscontrolelijst (ACL) en toegangscontrolelijst (ACE) op een beheerde switch

Doel

Een toegangscontrolelijst (ACL) is een lijst van netwerkverkeersfilters en bijbehorende acties die worden gebruikt om de beveiliging te verbeteren. Het blokkeert of maakt gebruikers toegang tot specifieke bronnen. Een ACL bevat de hosts die toegang tot het netwerkapparaat is toegestaan of geweigerd. Media Access Control List (MAC) op basis van Access Control List (ACL) is een lijst van bron-MAC-adressen die Layer 2-informatie gebruiken om toegang tot verkeer te toestaan of te weigeren. Als een pakket afkomstig is van een draadloos access point naar een LAN-poort (Local Area Network) of omgekeerd, controleert dit apparaat of het bron-MAC-adres van het pakket overeenkomt met een willekeurige ingang in deze lijst en controleert u de ACL-regels tegen de inhoud van het kader. Het gebruikt vervolgens de gecompenseerde resultaten om dit pakje toe te staan of te ontkennen. Er wordt echter niet gecontroleerd of pakketten van LAN naar LAN poort zijn. Een Access Control Entry (ACE) bevat de eigenlijke toegangseisen. Zodra ACE wordt gecreëerd, wordt het toegepast op een ACL. U dient toegangslijsten te gebruiken om een basisniveau van beveiliging te bieden voor de toegang tot uw netwerk. Als u geen toegangslijsten op uw netwerkapparaten vormt, kunnen alle pakketten die door de schakelaar of router worden verzonden, op alle delen van uw netwerk worden toegestaan.

Dit artikel bevat instructies hoe u MAC-gebaseerde ACL en ACE op uw beheerde switch kunt configureren.

Toepasselijke apparaten | Software versie

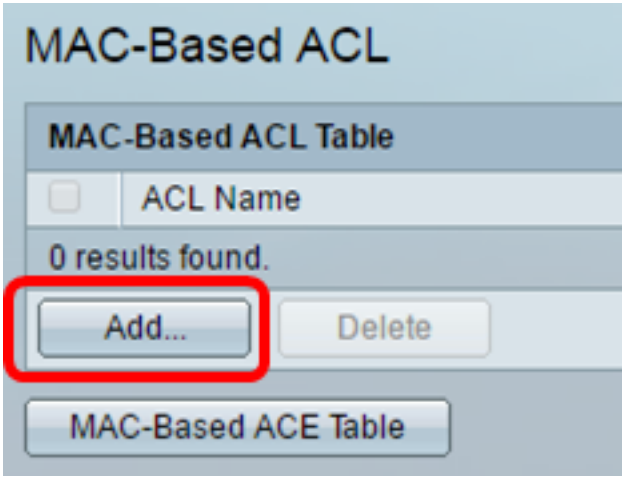
- Sx350 Series | 2.2.0.66 (laatste download)
- SG350X Series | 2.2.0.66 (laatste download)
- Sx500 Series | 1.4.5.02 (laatste download)
- Sx550X Series | 2.2.0.66 (laatste download)

MAC-gebaseerde ACL en ACE configureren

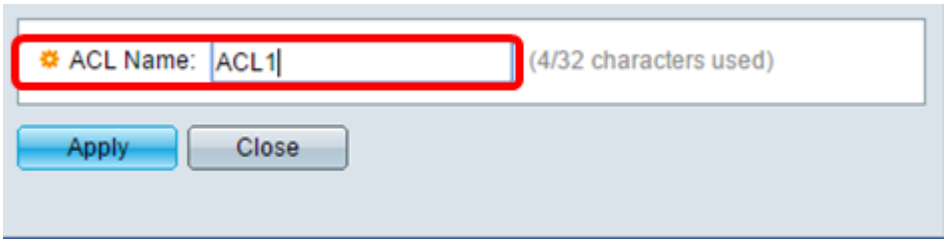
MAC-gebaseerde ACL-indeling

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma en gaat vervolgens naar **toegangscontrole > MAC-gebaseerde ACL**.

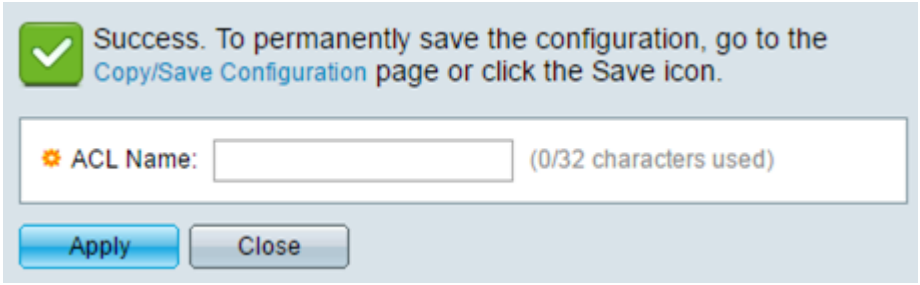
Stap 2. Klik op de knop **Add**.



Stap 3. Voer de naam van de nieuwe ACL in het veld Naam van ACL in.



Stap 4. Klik op **Toepassen** en vervolgens op **Sluiten**.



Stap 5. (Optioneel) Klik op **Opslaan** om instellingen in het opstartconfiguratiebestand op te slaan.

U zou nu een op MAC-gebaseerde ACL op uw schakelaar moeten hebben ingesteld.

MAC-gebaseerde ACE configureren

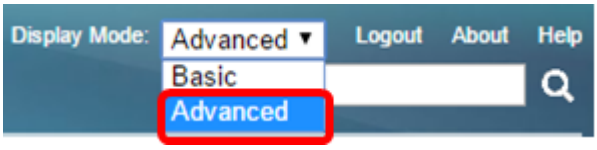
Wanneer een kader op een poort wordt ontvangen, verwerkt de schakelaar het kader door eerste ACL. Als het kader overeenkomt met een ACE-filter van de eerste ACL, wordt de ACE-actie uitgevoerd. Als het kader aan geen van de ACE filters voldoet, wordt volgende ACL verwerkt. Als geen overeenkomst in alle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

In dit scenario, zal een ACE worden gecreëerd om verkeer te ontkennen dat van een specifiek gebruiker-bepaald bron MAC adres naar om het even welke bestemmingsadressen wordt verzonden.

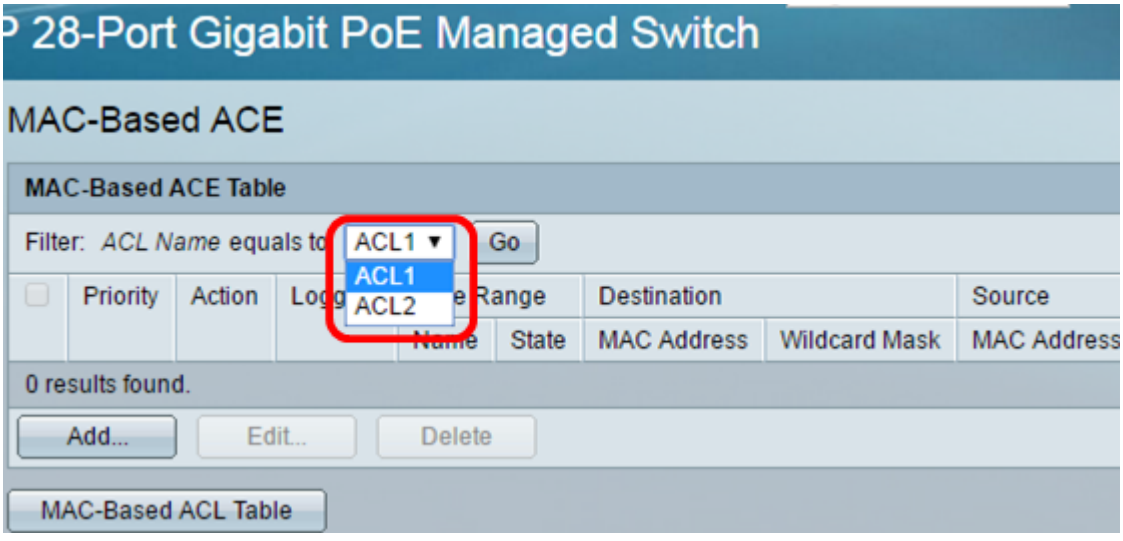
Opmerking: Deze standaardactie kan worden vermeden door de creatie van een ACE met lage prioriteit die al het verkeer toestaat.

Stap 1. Ga naar **toegangscontrole > MAC-gebaseerde ACE** op het web-gebaseerde **hulpprogramma**.

Belangrijk: Als u de beschikbare functies en functies van de switch volledig wilt gebruiken, verandert u deze naar de geavanceerde modus door **Geavanceerd** te kiezen in de vervolgkeuzelijst Weergave-modus in de rechterbovenhoek van de pagina.



Stap 2. Kies een ACL uit de vervolgkeuzelijst ACL-naam en klik vervolgens op **Ga**.

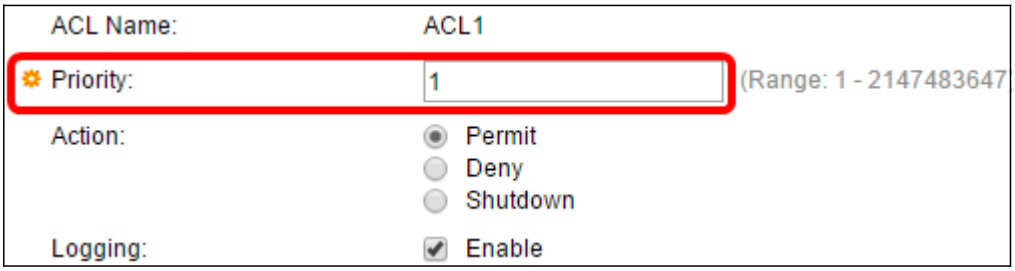


Opmerking: ACE's die al voor ACL zijn ingesteld, worden in de tabel weergegeven.

Stap 3. Klik op de knop **Add** om een nieuwe regel aan de ACL toe te voegen.

Opmerking: Het veld *ACL-naam* geeft de naam van de ACL weer.

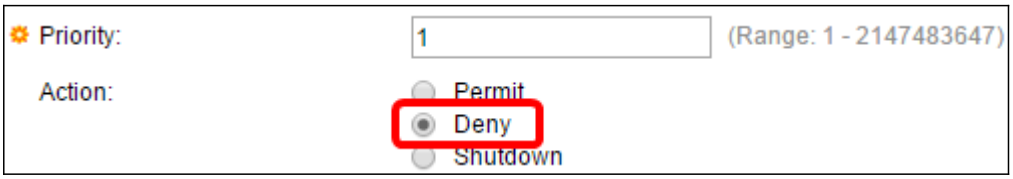
Stap 4. Voer de prioriteitswaarde van de ACE in het veld *Prioriteit in*. ACE's met een hogere prioriteit worden eerst verwerkt. De eerste waarde is de hoogste prioriteit.



Stap 5. (Optioneel) Controleer het vakje Vastlegging inschakelen om ACL-stromen toe te voegen die overeenkomen met de ACL-regel.

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.

Opmerking: In dit voorbeeld wordt Deny geselecteerd.



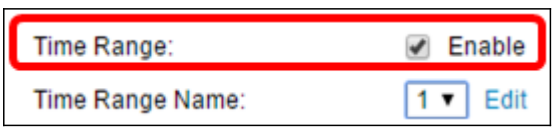
Toestemming — De schakelaar voorwaarts pakketten die aan de vereiste criteria van ACE voldoen.

Jeans: de schakelaar druppelt pakketten die aan de vereiste criteria van de ACE voldoen.

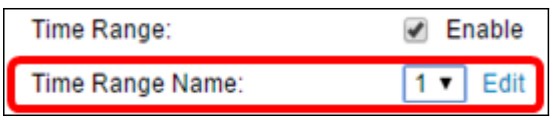
Shutdown - De schakelaar druppelt pakketten die niet aan de vereiste criteria van de ACE voldoen en schakelt de haven uit waar de pakketten werden ontvangen.

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

Stap 7. (Optioneel) Controleer het aankruisvakje Tijdbereik **inschakelen** om een tijdbereik in de ACE-modus te kunnen instellen. De tijdbereiken worden gebruikt om de tijd te beperken die een ACE in werking is.

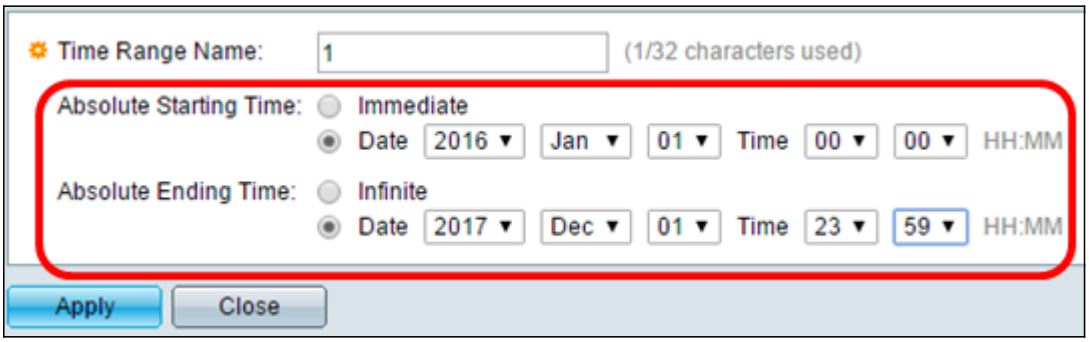


Stap 8. (Optioneel) Kies in de vervolgkeuzelijst Naam tijdbereik een tijdbereik om op de ACE toe te passen.

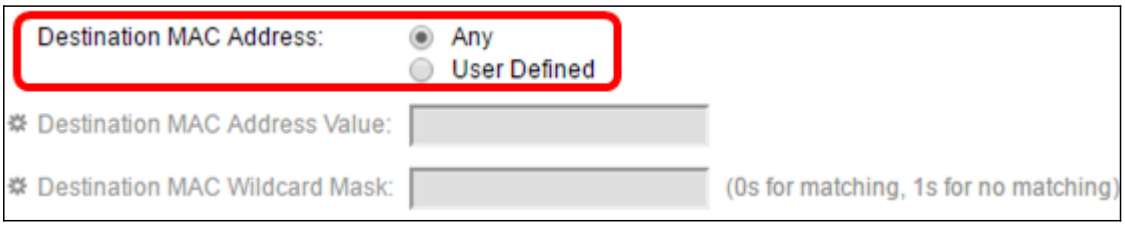


Opmerking: U kunt op **Bewerken** klikken om naar te navigeren en een tijdbereik te maken op de

pagina Tijdbereik.



Stap 9. Klik op de radioknop die aan de gewenste criteria van de ACE in het MAC-adresgebied van de bestemming beantwoordt.



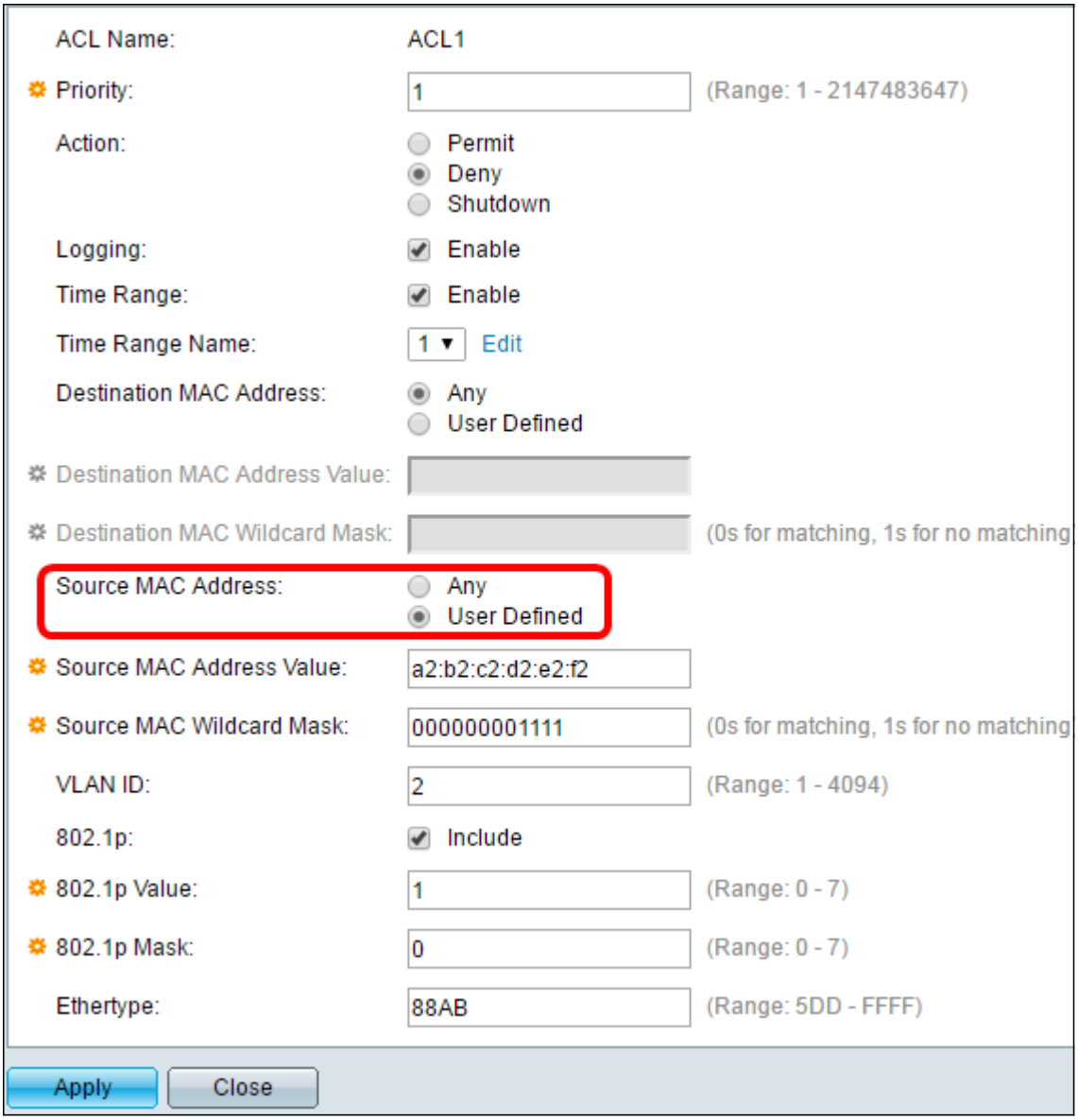
De opties zijn:

Alle — Alle MAC-adressen van het bestemming zijn van toepassing op de ACE.

Gebruiker gedefinieerd - Voer een MAC-adres en een MAC-jokermasker in dat op de ACE-kaart 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.

Opmerking: In dit voorbeeld wordt AnyRes gekozen. Voor deze optie betekent de ACE-optie dat het ACE-verkeer wordt geblokkeerd.

Stap 10. Klik op de radioknop die aan de gewenste criteria van ACE in het Bron MAC-adresgebied beantwoordt.



De opties zijn:

Alle bron-MAC-adressen zijn van toepassing op de ACE-band.

Gebruiker gedefinieerd - Voer een MAC-adres en een MAC-jokermasker in dat op de ACE-toets moet worden toegepast in de velden *Source MAC-adres* en *Source MAC-jokermasker*. Wildcard maskers worden gebruikt om een bereik van MAC adressen te definiëren.

Opmerking: In dit voorbeeld wordt de gebruikersdefinitie gekozen.

Stap 1. (Optioneel) In het veld *VLAN-ID* voert u een VLAN-ID in die met de VLAN-tag van het kader wordt aangepast.

Stap 12. (optioneel) Om 802.1p-waarden in ACE-criteria op te nemen, **controleer** in het aankruisvakje 802.1p. De 802.1p betreft de technologie-serviceklasse (CoS). CoS is een 3-bits veld in een Ethernet-kader dat wordt gebruikt om verkeer te differentiëren.

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

Waarde van 802.1p — Voer de waarde van 802.1p in die moet worden aangepast. De 802.1p

is een specificatie die Layer 2-switches de mogelijkheid geeft om prioriteit te geven aan verkeer en om dynamische multicast filtering uit te voeren. De waarden zijn als volgt:

- 0 — Achtergrond. De gegevens die het minst geprioriteerd zijn, zoals bulkoverdrachten, games, enzovoort.

- 1 — Best Fort. De gegevens die op basis van de normale LAN-prioriteit met de best mogelijke moeite moeten worden geleverd. Het netwerk biedt geen garantie bij levering, maar de gegevens krijgen ongespecificeerde bitsnelheid en levertijd gebaseerd op het verkeer.

- 2 — Uitstekende inspanning. De gegevens waarvoor de best mogelijke levering van verbindingen voor belangrijke gebruikers nodig is.

- 3 — Kritieke toepassing zoals Linux Virtual Server (LVS) telefoonSession Initiation Protocol (SIP).

- 4 — Video. Latency en Jitter, minder dan 100 ms.

- 5 — Standaard Cisco IP-telefoon. Latentie en Jitter minder dan 10 ms.

- 6 — Inter-network Control LVS phone Real-time Transport Protocol (RTP).

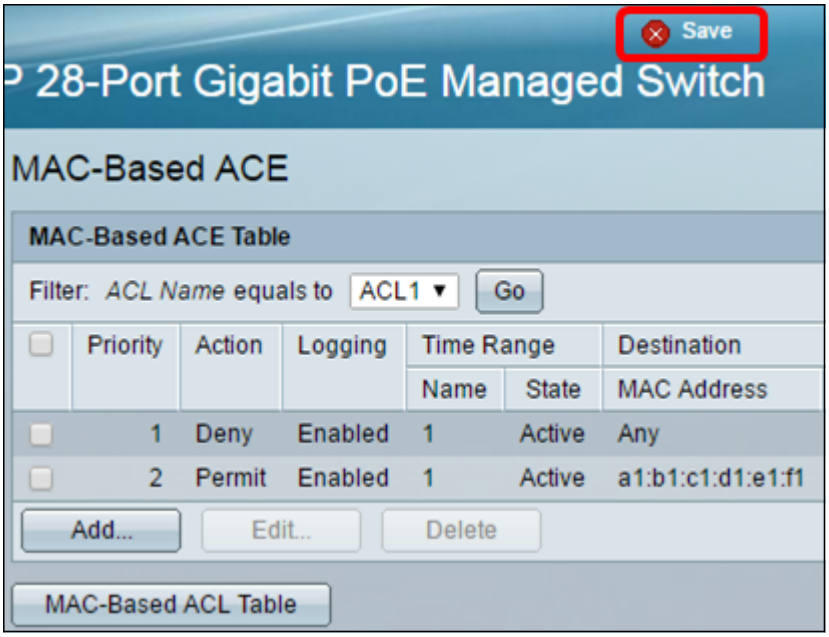
- 7 — Netwerkcontrole. Hoge behoefte om door te komen om de netwerkinfrastructuur te onderhouden en te ondersteunen.

802.1p masker — Voer het masker van de 802.1p-waarden in. Dit masker wordt gebruikt om de 802.1p-waarden te definiëren.

Stap 14. (Optioneel) Voer het EtherType in van het kader dat moet worden aangepast. EtherType is een gebied van 2 octetten in een Ethernet kader dat wordt gebruikt om aan te geven welk protocol voor de lading van het kader wordt gebruikt.

Stap 14. Klik op **Toepassen** dan op **Sluiten**. ACE wordt gecreëerd en geassocieerd met de ACL naam.

Stap 15. Klik op **Opslaan** om instellingen op te slaan in het opstartconfiguratiebestand.



U zou nu een MAC-Based ACE op uw switch moeten hebben ingesteld.

Andere mogelijk interessante links:

- Productpagina 350 Series switches
- Productpagina 350X Series-switches
- Productpagina 550 Series switches
- Productpagina 550X Series-switches

Bekijk een video gerelateerd aan dit artikel...

Klik hier om andere Tech Talks uit Cisco te bekijken