Global 802.1x Properties op een Switch configureren via de CLI

Inleiding

IEEE 802.1x is een standaard die toegangscontrole tussen een client en een server vergemakkelijkt. Voordat services aan een client kunnen worden geleverd door een LAN (Local Access Network) of switch, moet de client die is aangesloten op de switch-poort worden geauthentiseerd door de verificatieserver die Remote Authentication Dial-User Service (RADIUS) uitvoert.

802.1x-verificatie beperkt niet-geautoriseerde klanten tot het aansluiten op een netwerk via publiekelijk toegankelijke poorten. 802.1x-verificatie is een client-server-model. In dit model hebben netwerkapparaten de volgende specifieke rollen:

- Een client of leverancier — Een client of leverancier is een netwerkapparaat dat toegang tot het LAN vraagt. De client is verbonden met een authenticator.
- Authenticator - Een authenticator is een netwerkapparaat dat netwerkservices aanbiedt en waarmee aanvoerpoorten worden aangesloten. De volgende authenticatiemethoden worden ondersteund:

  - 802.1x-gebaseerd — Ondersteund in alle verificatiemodi. In 802.1x-gebaseerde verificatie haalt de authenticator de MAP-berichten uit de 802.1x-berichten of EAP-over-LAN-pakketten (EAPoL) van het Extensible Authentication Protocol (EAP), en geeft ze door aan de verificatieserver, met behulp van het RADIUS-protocol.

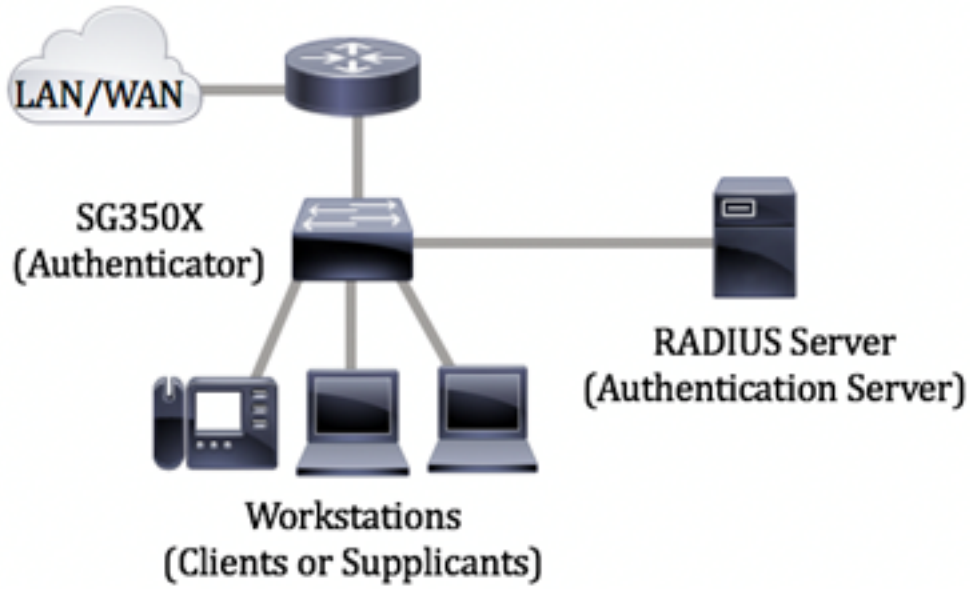
  - MAC-gebaseerd — Ondersteund in alle verificatiemodi. Met Media Access Control (MAC)-gebaseerde, voert de authenticator zelf het MAP-clientgedeelte van de software uit namens de klanten die netwerktoegang zoeken.

  - Web-gebaseerd — alleen ondersteund in multi-sessiemodi. Met webgebaseerde authenticatie voert de authenticator zelf het MAP-clientgedeelte van de software uit namens de klanten die netwerktoegang zoeken.

- Verificatieserver - Een verificatieserver voert de eigenlijke authenticatie van de client uit. De authenticatieserver voor het apparaat is een RADIUS-verificatieserver met EAP-extensies.

  Opmerking: Een netwerkapparaat kan een client of applicator zijn, authenticator of beide poorten.

  Het beeld hieronder toont een netwerk dat de apparaten volgens de specifieke rollen heeft gevormd. In dit voorbeeld wordt een SG350X switch gebruikt.



Richtsnoeren in configureren 802.1x:

1. Configuratie van de RADIUS-server. Klik hier voor informatie over het configureren van de RADIUS-serverinstellingen op uw switch.
2. Configuratie van Virtual Local Area Networks (VLAN's). Om VLAN's te maken die het web-based hulpprogramma van uw switch gebruiken, klik hier. Klik hier voor instructies met de opdrachtregel.
3. Configureer poort naar VLAN-instellingen op uw switch. Klik hier om te configureren met behulp van het webgebaseerde hulpprogramma. Klik hier om de CLI te gebruiken.
4. Configureer de algemene eigenschappen van de switch 802.1x. Voor instructies hoe u de wereldwijde 802.1x-eigenschappen kunt configureren via het webgebaseerde hulpprogramma van de switch, klik hier.
5. (Optioneel) Het instellen van tijdbereik op de switch. Klik hier om te leren hoe u de instellingen voor het tijdbereik op uw switch wilt configureren.
6. Configureer 802.1x poortverificatie. Om het web-based hulpprogramma van de switch te gebruiken, klik hier.

Doel

Dit artikel bevat instructies hoe u wereldwijde 802.1x-eigenschappen kunt configureren via de Opdrachtlijn Interface (CLI) van de switch, inclusief verificatie en eigenschappen van gast-VLAN. Gast VLAN verleent toegang tot services die niet vereisen dat de abonneeapparaten of -poorten worden geauthentiseerd en geautoriseerd via 802.1x, MAC-gebaseerde of web-gebaseerde verificatie.

Toepasselijke apparaten

- Sx300 Series
- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

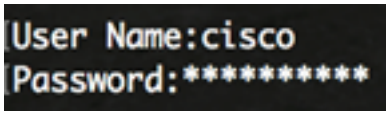
Softwareversie

- 1.4.7.06 — SX300, SX500
- 2.2.8.04 — SX350, SG350X, SX550X

Eigenschappen op een Switch via de CLI configureren

Instellingen 802.1x configureren

Stap 1. Meld u aan bij de switch-console. De standaardwaarden voor gebruikersnaam en wachtwoord zijn cisco/cisco. Als u een nieuwe gebruikersnaam of wachtwoord heeft geconfigureerd, moet u deze inloggegevens gebruiken.



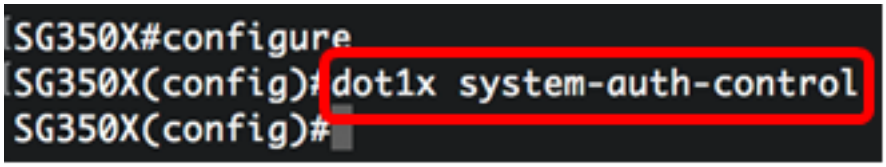
Opmerking: Afhankelijk van het exacte model van de switch kunnen de opdrachten variëren. In dit voorbeeld wordt de SG350X-switch benaderd via Telnet.

Stap 2. Voer in de modus Geprivigeerde EXEC van de switch de modus Global Configuration in door het volgende in te voeren:

```
SG350x#configuratie
```

Stap 3. Om 802.1x-verificatie op de switch mondiaal mogelijk te maken, gebruikt u de opdracht **dot1x systeem-auth-control** in de modus Global Configuration.

```
SG350x (configuratie)#dotx1 systeem-auth-control
```



Stap 4. (optioneel) Om 802.1x-verificatie wereldwijd uit te schakelen op de switch, voert u het volgende in:

```
SG350x (configuratie)#no dotx1 systeem-auth-control
```

Opmerking: Als dit wordt uitgeschakeld, worden 802.1X, MAC-gebaseerde en web-gebaseerde authenticaties uitgeschakeld.

Stap 5. Om aan te geven welke servers worden gebruikt voor verificatie wanneer 802.1x-verificatie is ingeschakeld, voert u het volgende in:

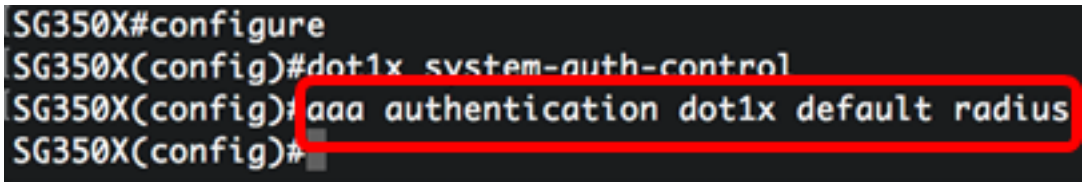
```
SG350x (configuratie)#aaa authenticatiedot1x standaard [straal geen | straal | geen]
```

De opties zijn:

- Straal geen - Dit voert eerst de poortverificatie uit met behulp van de RADIUS-server. Als er geen reactie is van de server zoals wanneer de server is ingedrukt, wordt er geen verificatie uitgevoerd en wordt de sessie toegestaan. Als de server beschikbaar is en de gebruikersreferenties niet correct zijn, wordt de toegang geweigerd en wordt de sessie

beëindigd.

- Straal — Dit voert de poortverificatie uit op basis van de RADIUS-server. Als er geen verificatie wordt uitgevoerd, wordt de sessie beëindigd. Dit is de standaardauthenticatie.
- geen — hiermee wordt de gebruiker niet geauthentiseerd en wordt de sessie toegestaan.



Opmerking: In dit voorbeeld is de standaard 802.1x-authenticatieserver RADIUS.

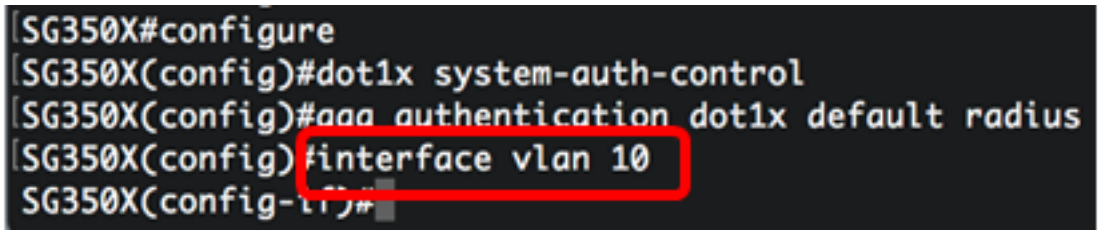
Stap 6. (Optioneel) Om de standaardverificatie te herstellen, voert u het volgende in:

```
SG350X (configuratie)#geen aA authetication dot1x standaard
```

Stap 7. In de modus Global Configuration voert u de VLAN-interfaceconfiguratie in door het volgende in te voeren:

```
SG350X (configuratie)#interface-VLAN [VLAN-id]
```

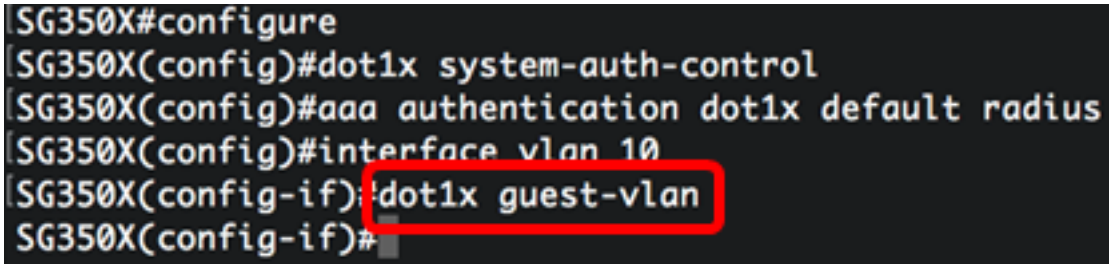
- VLAN-id - Specificeert een VLAN-id dat u wilt configureren.



Stap 8. Voer het volgende in om het gebruik van een gast VLAN voor onbevoegde poorten mogelijk te maken:

```
SG350X (configuratie-eventuele)#dot1x gastland-VLAN
```

Opmerking: Als een VLAN van de Gast wordt toegelaten, zullen alle onbevoegde havens automatisch zich bij het VLAN aansluiten dat in het VLAN van de Gast wordt geselecteerd. Als een poort later is geautoriseerd, wordt deze verwijderd uit het VLAN van de Gast.



Stap 9. Voer de volgende handelingen uit om de context van de interfaceconfiguratie te verlaten:

```
SG350X(config-if)#exit
```

```
SG350X#configure
SG350X(config)#dot1x system-auth-control
SG350X(config)#aaa authentication dot1x default radius
SG350X(config)#interface vlan 10
SG350X(config-if)#dot1x guest-vlan
SG350X(config-if)#exit
SG350X(config)#
```

Stap 10. Om de tijdvertraging in te stellen tussen het inschakelen van 802.1X (of het inschakelen van een poort) en het toevoegen van een poort aan het gastVLAN, specificeert u het volgende:

```
SG350X (configuratie)#dot1x gast-VLAN tijdelijke versie [timeout]
```

- timeout — Specificeert de tijdvertraging in seconden tussen het inschakelen van 802.1X (of poort omhoog) en het toevoegen van de poort aan de gast VLAN. Het bereik loopt van 30 tot 180 seconden.

Opmerking: Na verbinding, als de software geen 802.1x smeekbede detecteert of als de poortverificatie heeft gefaald, wordt de poort alleen aan de gast VLAN toegevoegd na de time-out van het Guest VLAN. Als de poort van Authorized om niet geautoriseerd verandert, wordt de haven aan het VLAN van de Gast toegevoegd slechts nadat de de time-out van West VLAN verstrijkt. U kunt VLAN-verificatie uit de VLAN-verificatie inschakelen of uitschakelen.

```
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#
```

Opmerking: In dit voorbeeld is de Time-out voor Guest VLAN gebruikt 60 seconden.

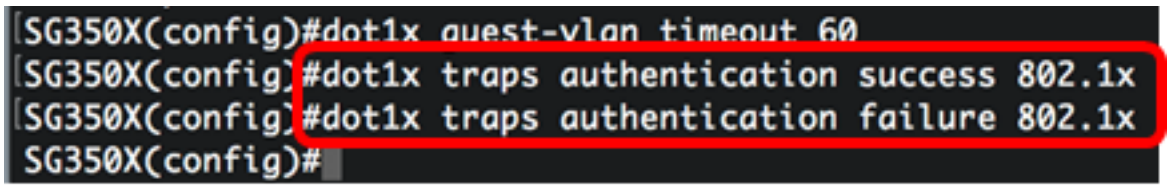
Stap 1. Controleer een of meer van de volgende opties om vallen in te schakelen:

```
SG350X (configuratie)# dot1x-gevangen verificatie [mislukking] | succes | stilte] [802.1x | mac | web]
```

De opties zijn:

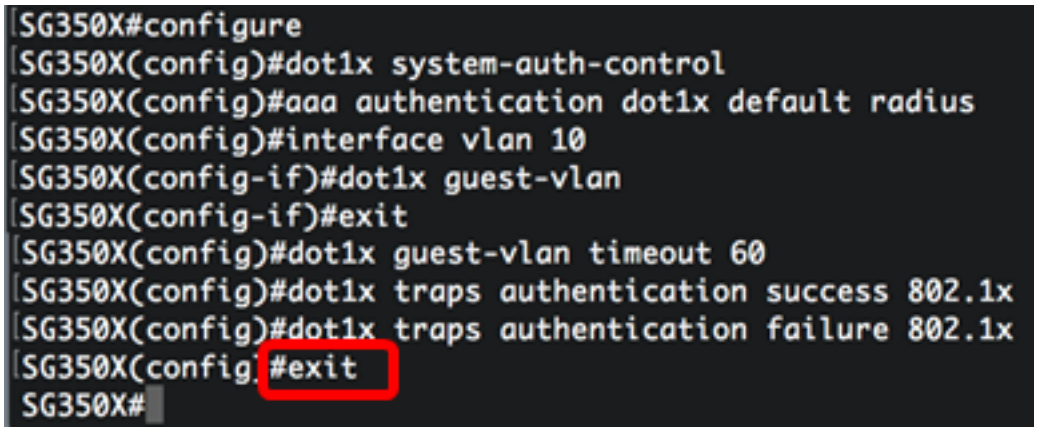
- Vangen voor 802.1x-echtheidscontrole — Verzend vallen als 802.1x-verificatie faalt.
- 802.1x authenticatie succesvolle vallen — Verzend vallen als 802.1x authenticatie slaagt.
- MAC-foutherkenningsklem - Verzend vallen als MAC-verificatie faalt.
- MAC-authenticatie succesklemmen — Vangen sturen als MAC-verificatie slaagt.
- Vallen van de mislukking van web authenticatie - Verzend vallen als Web authenticatie faalt.
- Vallen van de succes van web authenticatie - Verzend vallen als Web authenticatie succes heeft.
- Webex-detectiesleutels - Verzend vallen als een rustige periode begint.

Opmerking: In dit voorbeeld worden 802.1x authenticatiefout en succesvallen ingevoerd.



Stap 12. Voer de volgende informatie in om de interfaceconfiguratie te verlaten:

```
SG350X (configuratie)#exit
```



Stap 13. (Optioneel) Voer het volgende in om de geconfigureerde mondiale 802.1x-eigenschappen op de switch weer te geven:

```
SG350X#show dot1x
```

U dient nu de 802.1x-eigenschappen op uw switch te hebben ingesteld.

VLAN-verificatie configureren

Wanneer 802.1x wordt geactiveerd, mogen niet-geautoriseerde poorten of apparaten geen toegang tot het VLAN hebben, tenzij ze deel uitmaken van het Gast VLAN of een niet-echt gemaakt VLAN. De poorten moeten handmatig aan VLAN's worden toegevoegd.

Om verificatie op een VLAN uit te schakelen, volgt u deze stappen:

Stap 1. Voer in de modus Geprivigeerde EXEC van de switch de modus Global Configuration in door het volgende in te voeren:

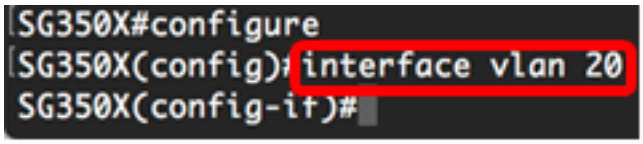
```
SG350X#configuratie
```

Stap 2. In de modus Global Configuration voert u de VLAN-interfaceconfiguratie in door het

volgende in te voeren:

```
KSG350x (configuratie)# interface-VLAN [VLAN-id]
```

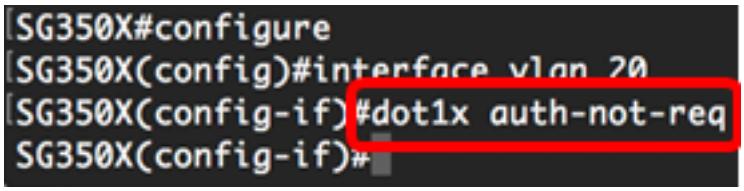
- VLAN-id - Specificeert een VLAN-id dat u wilt configureren.



Opmerking: In dit voorbeeld wordt VLAN 20 geselecteerd.

Stap 3. Voer de volgende handelingen in om 802.1x-verificatie op het VLAN uit te schakelen:

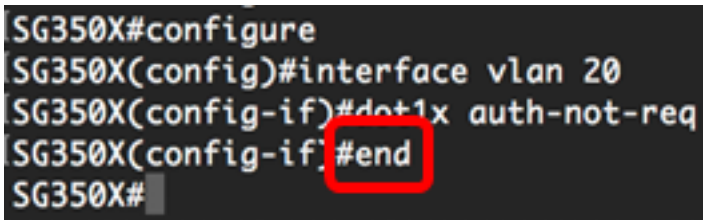
SG350X (Config-als)#dot1x auth-not-req



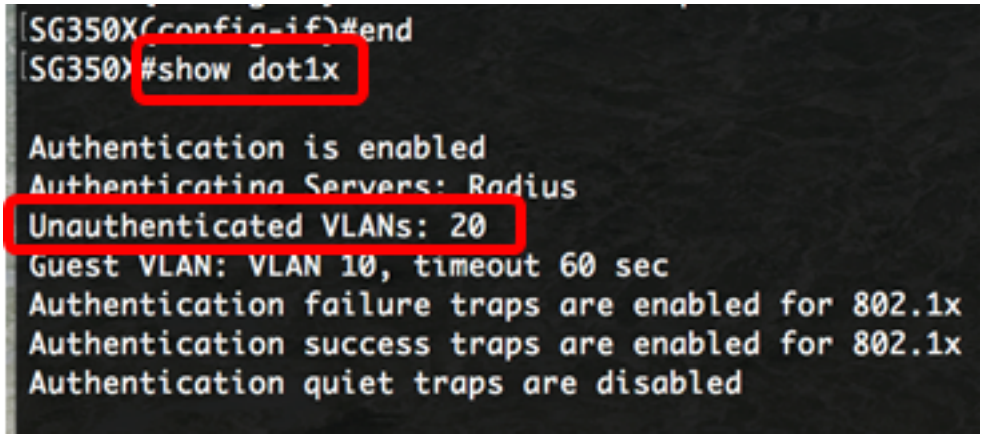
Stap 4. (Optioneel) Om 802.1x-verificatie op het VLAN mogelijk te maken, voert u het volgende in:

SG350X (configuratie-indien)#no dot1x auth-not-req

Stap 5. Voer de volgende handelingen uit om de interfaceconfiguratie te sluiten:



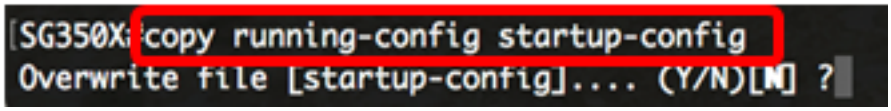
Stap 6. (Optioneel) Om de 802.1x mondiale authenticatie-instellingen op de switch weer te geven, voert u het volgende in:



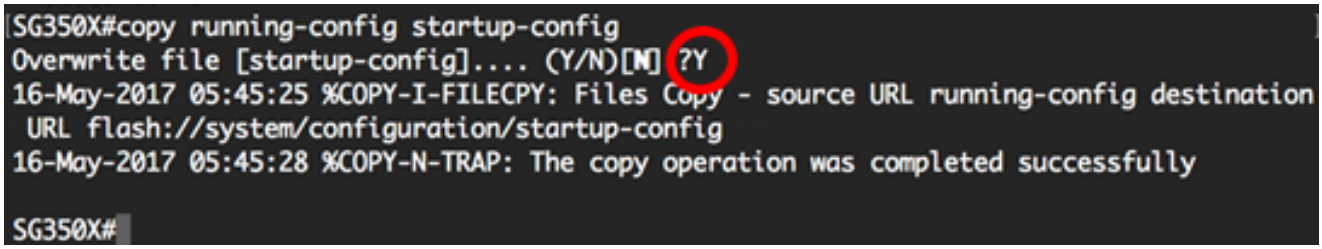
Opmerking: In dit voorbeeld, toont VLAN 20 als niet-echt gemaakt VLAN.

Stap 7. (Optioneel) In de bevoorrechte EXEC-modus van de switch, slaat u de geconfigureerde instellingen op in het opstartconfiguratiebestand, door het volgende in te voeren:

```
SG350X#copy running-config startup-config
```



Stap 8. (Optioneel) Druk op **Y** for Yes of **N** for No op uw toetsenbord zodra het Overschrijvingsbestand [opstartconfiguratie]... prompt verschijnt.



U hebt nu de 802.1x-verificatie-instellingen op de VLAN's op uw switch ingesteld.

Belangrijk: Om de 802.1x-instellingen voor poortverificatie op uw switch te configureren volgt u de bovenstaande richtlijnen.