Konfigurieren globaler 802.1x-Eigenschaften auf einem Switch über die CLI

Einleitung

IEEE 802.1x ist ein Standard, der die Zugriffskontrolle zwischen Client und Server vereinfacht. Bevor einem Client Services über ein Local Access Network (LAN) oder einen Switch bereitgestellt werden können, muss der mit dem Switch-Port verbundene Client vom Authentifizierungsserver authentifiziert werden, der den Remote Authentication Dial-In User Service (RADIUS) ausführt.

Die 802.1x-Authentifizierung hindert nicht autorisierte Clients daran, über öffentlich zugängliche Ports eine Verbindung mit einem LAN herzustellen. Die 802.1x-Authentifizierung ist ein Client-Server-Modell. Bei diesem Modell haben Netzwerkgeräte die folgenden spezifischen Rollen:

- Client oder Supplicant (Client oder Supplicant): Ein Client oder Supplicant ist ein Netzwerkgerät, das den Zugriff auf das LAN anfordert. Der Client ist mit einem Authentifizierer verbunden.
- Authentifizierer - Ein Authentifizierer ist ein Netzwerkgerät, das Netzwerkdienste bereitstellt und mit dem die Supplicant Ports verbunden sind. Folgende Authentifizierungsmethoden werden unterstützt:

  - 802.1x-basiert - Wird in allen Authentifizierungsmodi unterstützt. Bei der 802.1x-basierten Authentifizierung extrahiert der Authentifizierer die EAP-Nachrichten (Extensible Authentication Protocol) aus den 802.1x-Nachrichten oder EAP over LAN (EAPoL)-Paketen und leitet sie mithilfe des RADIUS-Protokolls an den Authentifizierungsserver weiter.

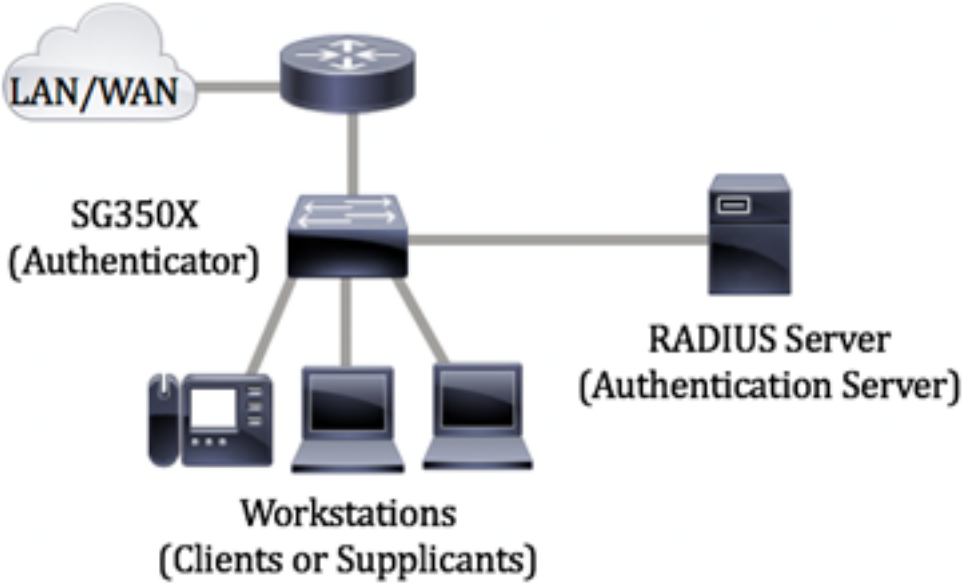
  - MAC-basiert - Wird in allen Authentifizierungsmodi unterstützt. Bei MAC-basierter (Media Access Control) Ausführung des EAP-Client-Teils der Software durch den Authentifizierer selbst im Auftrag der Clients, die Netzwerkzugriff anfordern.

  - Webbasiert - Wird nur in Multisitzungsmodi unterstützt. Bei webbasierter Authentifizierung führt der Authentifizierer selbst den EAP-Client-Teil der Software für die Clients aus, die Netzwerkzugriff anfordern.

- Authentifizierungsserver - Ein Authentifizierungsserver führt die eigentliche Authentifizierung des Clients durch. Der Authentifizierungsserver für das Gerät ist ein RADIUS-Authentifizierungsserver mit EAP-Erweiterungen.

  Anmerkung: Ein Netzwerkgerät kann entweder Client oder Komponente, Authentifizierer oder beide pro Port sein.

  Das nachfolgende Bild zeigt ein Netzwerk, das die Geräte entsprechend den spezifischen Rollen konfiguriert hat. In diesem Beispiel wird ein SG350X-Switch verwendet.



Richtlinien in 802.1x konfigurieren:

1. Konfigurieren Sie den RADIUS-Server. Um zu erfahren, wie Sie die RADIUS-Servereinstellungen auf Ihrem Switch konfigurieren, klicken Sie hier.
2. Konfigurieren von Virtual Local Area Networks (VLANs) Klicken Sie hier, um VLANs mithilfe des webbasierten Dienstprogramms Ihres Switches zu erstellen. Anweisungen für die Konfiguration über die Kommandozeilenschnittstelle finden Sie hier.
3. Konfigurieren der Port-VLAN-Einstellungen auf dem Switch Klicken Sie hier, um das webbasierte Dienstprogramm zu konfigurieren. Klicken Sie hier, um die CLI zu verwenden.
4. Konfigurieren Sie die globalen 802.1x-Eigenschaften auf dem Switch. Anweisungen zum Konfigurieren der globalen 802.1x-Eigenschaften über das webbasierte Dienstprogramm des Switches finden Sie hier.
5. (Optional) Konfigurieren Sie den Zeitbereich auf dem Switch. Um zu erfahren, wie Sie die Zeitbereichseinstellungen auf Ihrem Switch konfigurieren, klicken Sie hier.
6. 802.1x-Port-Authentifizierung konfigurieren Klicken Sie hier, um das webbasierte Dienstprogramm des Switches zu verwenden.

Ziel

Dieser Artikel enthält Anweisungen zum Konfigurieren globaler 802.1x-Eigenschaften über die Befehlszeilenschnittstelle (CLI) des Switches, einschließlich der Authentifizierungs- und Gast-VLAN-Eigenschaften. Das Gast-VLAN bietet Zugriff auf Services, für die die Abonnementgeräte oder -ports nicht authentifiziert und autorisiert werden müssen, und zwar über 802.1x, MAC-basierte oder webbasierte Authentifizierung.

Unterstützte Geräte

- Sx300-Serie
- Sx350-Serie
- SG350X-Serie
- Sx500-Serie

- Sx550X-Serie

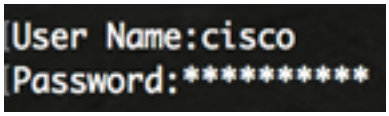
Software-Version

- 1.4.7.06: Sx300, Sx500
- 2.2.8.04: Sx350, SG350X, Sx550X

Konfigurieren von 802.1x-Eigenschaften auf einem Switch über die CLI

802.1x-Einstellungen konfigurieren

Schritt 1: Melden Sie sich bei der Switch-Konsole an. Der Standardbenutzername und das Standardkennwort lauten "cisco". Wenn Sie einen neuen Benutzernamen oder ein neues Kennwort konfiguriert haben, müssen Sie an dieser Stelle diese neuen Anmeldeinformationen eingeben.



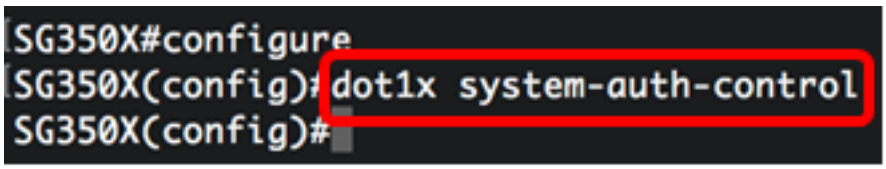
Anmerkung: Die Befehle können je nach genauem Switch-Modell variieren. In diesem Beispiel wird über Telnet auf einen SG350X-Switch zugegriffen.

Schritt 2: Geben Sie im privilegierten EXEC-Modus des Switch den nachfolgenden Befehl ein, um in den globalen Konfigurationsmodus zu wechseln.

```
SG350x#Konfiguration
```

Schritt 3: Um die 802.1x-Authentifizierung auf dem Switch global zu aktivieren, verwenden Sie den Befehl **dot1x system-auth-control** im globalen Konfigurationsmodus.

```
SG350x(config)#dotx1 Systemauth-Control
```



Schritt 4: (Optional) Geben Sie Folgendes ein, um die 802.1x-Authentifizierung auf dem Switch global zu deaktivieren:

```
SG350x(config)#no dotx1 System-Auth-Control
```

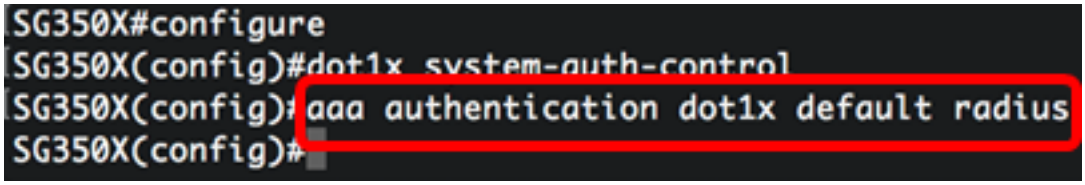
Anmerkung: Wenn diese Option deaktiviert ist, werden 802.1X-, MAC- und webbasierte Authentifizierungen deaktiviert.

Schritt 5: Geben Sie Folgendes ein, um festzulegen, welche Server bei aktivierter 802.1x-Authentifizierung für die Authentifizierung verwendet werden:

```
SG350x(config)#aa authentication dot1x default [radius none] | Radius | keine]
```

Folgende Optionen sind verfügbar:

- radius none: Führt zuerst mithilfe des RADIUS-Servers die Port-Authentifizierung durch. Wenn der Server nicht reagiert, z. B. wenn der Server ausgefallen ist, wird keine Authentifizierung durchgeführt, und die Sitzung ist zulässig. Wenn der Server verfügbar ist und die Anmeldeinformationen des Benutzers falsch sind, wird der Zugriff verweigert und die Sitzung beendet.
- radius - Führt die Port-Authentifizierung auf Basis des RADIUS-Servers aus. Wenn keine Authentifizierung durchgeführt wird, wird die Sitzung beendet. Dies ist die Standardauthentifizierung.
- none: authentifiziert den Benutzer nicht und lässt die Sitzung zu.



Anmerkung: In diesem Beispiel ist der standardmäßige 802.1x-Authentifizierungsserver RADIUS.

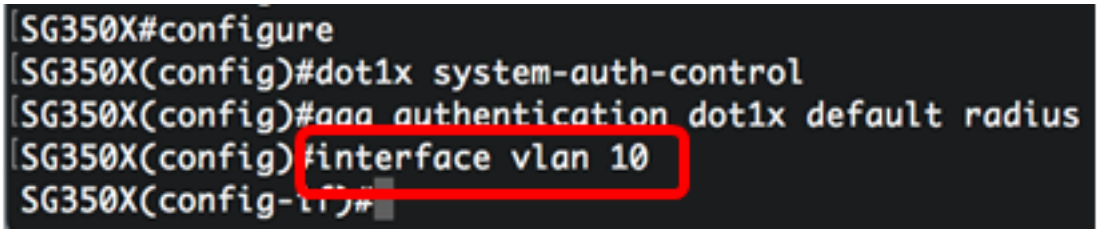
Schritt 6: (Optional) Geben Sie Folgendes ein, um die Standardauthentifizierung wiederherzustellen:

```
SG350X(config)#no aa authetication dot1x default
```

Schritt 7: Geben Sie im globalen Konfigurationsmodus den VLAN Interface Configuration-Kontext ein, indem Sie Folgendes eingeben:

```
SG350X(config)#interface vlan [vlan-id]
```

- vlan-id: Gibt eine zu konfigurierende VLAN-ID an.



Schritt 8: Um die Verwendung eines Gast-VLAN für nicht autorisierte Ports zu aktivieren, geben Sie Folgendes ein:

```
SG350X(config-if)#dot1x Gast-VLAN
```

Anmerkung: Wenn ein Gast-VLAN aktiviert ist, werden alle nicht autorisierten Ports automatisch dem im Gast-VLAN ausgewählten VLAN hinzugefügt. Wenn ein Port später autorisiert wird, wird er aus dem Gast-VLAN entfernt.

Schritt 9: Geben Sie den nachfolgenden Befehl ein, um den Kontext für die Schnittstellenkonfiguration zu verlassen.

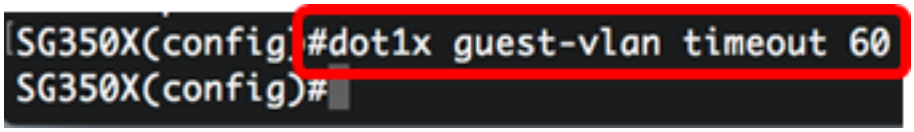
```
SG350X(config-if)#exit
```

Schritt 10: Geben Sie Folgendes ein, um die Zeitverzögerung zwischen der Aktivierung von 802.1X (oder der Aktivierung eines Ports) und dem Hinzufügen eines Ports zum Gast-VLAN festzulegen:

```
SG350X(config)#dot1x Gast-VLAN Timeout [timeout]
```

- timeout (Zeitüberschreitung): Gibt die Zeitverzögerung in Sekunden zwischen der Aktivierung von 802.1X (oder dem Anschluss nach oben) und dem Hinzufügen des Ports zum Gast-VLAN an. Der Bereich liegt zwischen 30 und 180 Sekunden.

Anmerkung: Wenn die Software nach dem Verbindungsaufbau keine 802.1x-Komponente erkennt oder die Port-Authentifizierung fehlgeschlagen ist, wird der Port dem Gast-VLAN erst nach Ablauf der Gast-VLAN-Zeitüberschreitungsfrist hinzugefügt. Wenn sich der Port von Authorized (Autorisiert) zu Not Authorized (Nicht autorisiert) ändert, wird der Port dem Gast-VLAN erst nach Ablauf der Timeout-Zeit für das Gast-VLAN hinzugefügt. Sie können die VLAN-Authentifizierung über die VLAN-Authentifizierung aktivieren oder deaktivieren.



Anmerkung: In diesem Beispiel wird ein Guest VLAN Timeout von 60 Sekunden verwendet.

Schritt 11: Aktivieren Sie zum Aktivieren von Traps eine oder mehrere der folgenden Optionen:

```
SG350X(config)# dot1x-Traps-Authentifizierung [Fehler | Erfolg | leise] [802.1x | Mac | Web]
```

Folgende Optionen sind verfügbar:

- 802.1x-Authentifizierungsfehler-Traps - Senden von Traps, wenn die 802.1x-Authentifizierung fehlschlägt.
- Erfolgsfallen für 802.1x-Authentifizierung: Senden Sie Traps, wenn die 802.1x-Authentifizierung erfolgreich ist.
- MAC Authentication Failure Traps (MAC-Authentifizierungsfehler): Senden von Traps, wenn MAC-Authentifizierung fehlschlägt.
- MAC Authentication Success Traps - Senden Sie Traps, wenn die MAC-Authentifizierung erfolgreich ist.

- web authentication failure traps - Senden von Traps, wenn die Webauthentifizierung fehlschlägt.
- Web Authentication Success Traps - Senden Sie Traps, wenn die Webauthentifizierung erfolgreich ist.
- web authentication still traps - Senden von Traps, wenn eine ruhige Periode beginnt.

Anmerkung: In diesem Beispiel werden 802.1x-Authentifizierungsfehler und Erfolgsfallen eingegeben.

```
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#dot1x traps authentication success 802.1x
SG350X(config)#dot1x traps authentication failure 802.1x
SG350X(config)#
```

Schritt 12: Geben Sie den nachfolgenden Befehl ein, um den Kontext für die Schnittstellenkonfiguration zu verlassen.

```
SG350X(config)#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)#dot1x guest-vlan timeout 60
SG350X(config)#dot1x traps authentication success 802.1x
SG350X(config)#dot1x traps authentication failure 802.1x
SG350X(config)#exit
SG350X#
```

Schritt 13: (Optional) Geben Sie Folgendes ein, um die konfigurierten globalen 802.1x-Eigenschaften auf dem Switch anzuzeigen:

```
SG350X#show dot1x
```

```
SG350X(config)#exit
SG350X#show dot1x

Authentication is enabled
Authenticating Servers: Radius
Unauthenticated VLANs: 20
Guest VLAN: VLAN 10, timeout 60 sec
Authentication failure traps are enabled for 802.1x
Authentication success traps are enabled for 802.1x
Authentication quiet traps are disabled
```

Sie sollten jetzt die 802.1x-Eigenschaften auf Ihrem Switch erfolgreich konfiguriert haben.

Konfigurieren der VLAN-Authentifizierung

Wenn 802.1x aktiviert ist, dürfen nicht autorisierte Ports oder Geräte nur dann auf das VLAN

zugreifen, wenn sie Teil des Gast-VLAN oder eines nicht authentifizierten VLAN sind. Die Ports müssen den VLANs manuell hinzugefügt werden.

Um die Authentifizierung in einem VLAN zu deaktivieren, gehen Sie wie folgt vor:

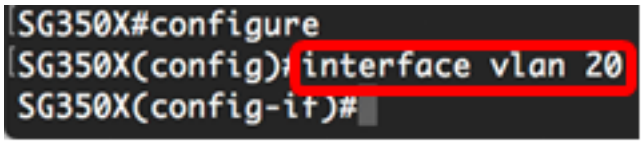
Schritt 1: Geben Sie im privilegierten EXEC-Modus des Switch den nachfolgenden Befehl ein, um in den globalen Konfigurationsmodus zu wechseln.

```
SG350X#Konfiguration
```

Schritt 2: Geben Sie im globalen Konfigurationsmodus den VLAN Interface Configuration-Kontext ein, indem Sie Folgendes eingeben:

```
KSG350x(config)# interface vlan [vlan-id]
```

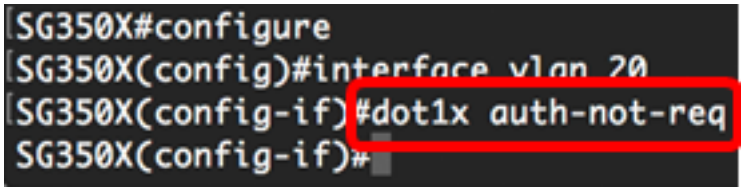
- vlan-id: Gibt eine zu konfigurierende VLAN-ID an.



Anmerkung: In diesem Beispiel wird VLAN 20 ausgewählt.

Schritt 3: Um die 802.1x-Authentifizierung im VLAN zu deaktivieren, geben Sie Folgendes ein:

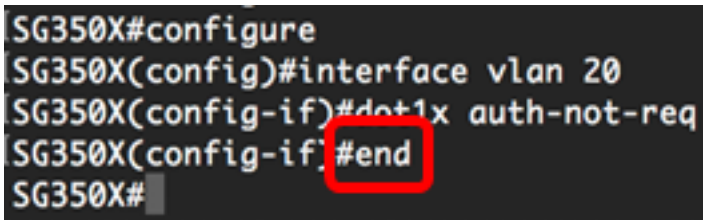
SG350X(config-if)#dot1x auth-not-req



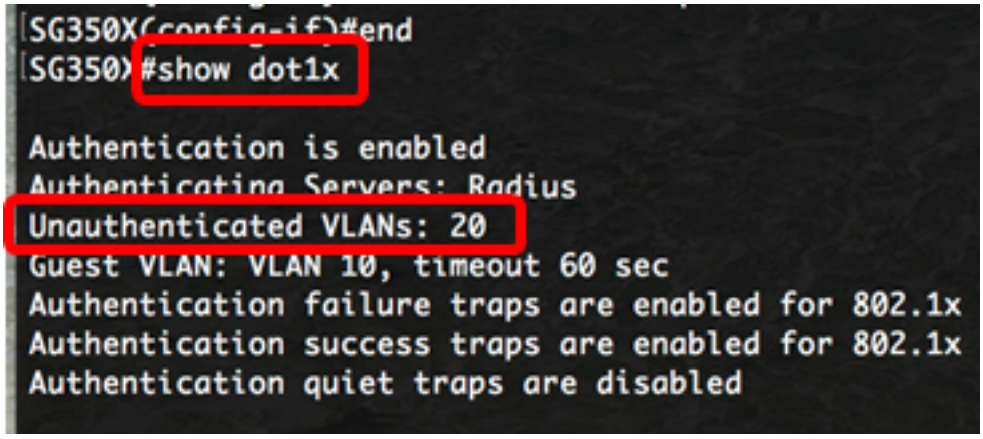
Schritt 4: (Optional) Geben Sie Folgendes ein, um die 802.1x-Authentifizierung im VLAN zu aktivieren:

SG350X(config-if)#no dot1x auth-not-req

Schritt 5: Geben Sie den nachfolgenden Befehl ein, um den Kontext für die Schnittstellenkonfiguration zu verlassen.



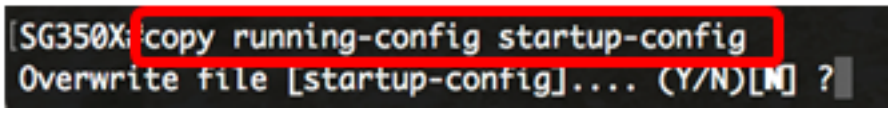
Schritt 6: (Optional) Geben Sie Folgendes ein, um die globalen 802.1x-Authentifizierungseinstellungen auf dem Switch anzuzeigen:



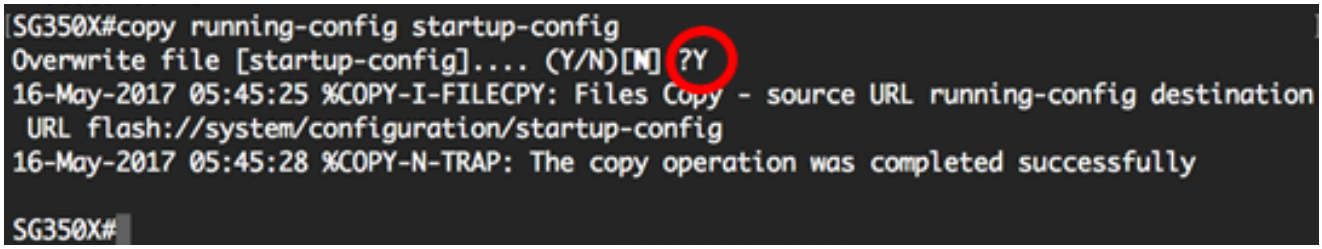
Anmerkung: In diesem Beispiel wird VLAN 20 als nicht authentifiziertes VLAN angezeigt.

Schritt 7: Geben Sie optional im privilegierten EXEC-Modus des Switch den nachfolgenden Befehl ein, um die konfigurierten Einstellungen in der Datei mit der Startkonfiguration zu speichern.

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



Schritt 8: Drücken Sie optional auf der Tastatur auf **Y für "Yes" oder N für "No", sobald die Aufforderung "Overwrite file [startup-config]...." angezeigt wird.**



Sie sollten jetzt die 802.1x-Authentifizierungseinstellungen auf den VLANs auf Ihrem Switch erfolgreich konfiguriert haben.

Wichtig: Um mit der Konfiguration der 802.1x-Port-Authentifizierungseinstellungen auf Ihrem Switch fortzufahren, befolgen Sie die Richtlinien oben.