Konfigurieren der MAC-basierten Authentifizierung auf einem Switch über die Befehlszeilenschnittstelle

Ziel

802.1X ist ein Verwaltungstool, mit dem Sie Listengeräte zulassen können, um unautorisierten Zugriff auf Ihr Netzwerk zu verhindern. In diesem Dokument wird erläutert, wie Sie die MAC-basierte Authentifizierung auf einem Switch mithilfe der CLI (Command Line Interface) konfigurieren.

Weitere Informationen finden Sie im Glossar.

Wie funktioniert Radius?

Die 802.1X-Authentifizierung besteht aus drei Hauptkomponenten: einer Komponente (Client), einem Authentifizierer (Netzwerkgerät wie einem Switch) und einem Authentifizierungsserver (RADIUS). Der Remote Authentication Dial-In User Service (RADIUS) ist ein Zugriffsserver, der AAA-Protokoll (Authentication, Authorization, Accounting) verwendet, um die Verwaltung zu unterstützen. Er hat die statische IP-Adresse 192.168.1.100 und die statische IP-Adresse 192.168.1.101.

Anwendbare Geräte

- Serie Sx350X
- SG350XG-Serie
- Serie Sx550X
- SG550XG-Serie

Softwareversion

- 2.4,0,94

Konfigurieren eines RADIUS-Servers auf einem Switch

Schritt 1: SSH zu Ihrem Switch, der der RADIUS-Server sein wird. Der Standard-Benutzername und das Kennwort lautet cisco/cisco. Wenn Sie einen neuen Benutzernamen oder ein neues Kennwort konfiguriert haben, geben Sie stattdessen die Anmeldeinformationen ein.

Hinweis: Um zu erfahren, wie Sie über SSH oder Telnet auf einen SMB-Switch zugreifen können, klicken Sie auf hier.

```
login as: cisco



User Name:cisco
Password:********


RADIUS#
```

Schritt 2: Geben Sie im privilegierten EXEC-Modus des Switches Folgendes ein, um in den globalen Konfigurationsmodus zu wechseln:

```
login as: cisco



User Name:cisco
Password:********


RADIUS#configure
RADIUS(config)#
```

Schritt 3: Verwenden Sie den Befehl **radius server enable**, um den RADIUS-Server zu aktivieren.

```
login as: cisco



User Name:cisco
Password:********


RADIUS#configure
RADIUS(config)#radius server enable
RADIUS(config)#
```

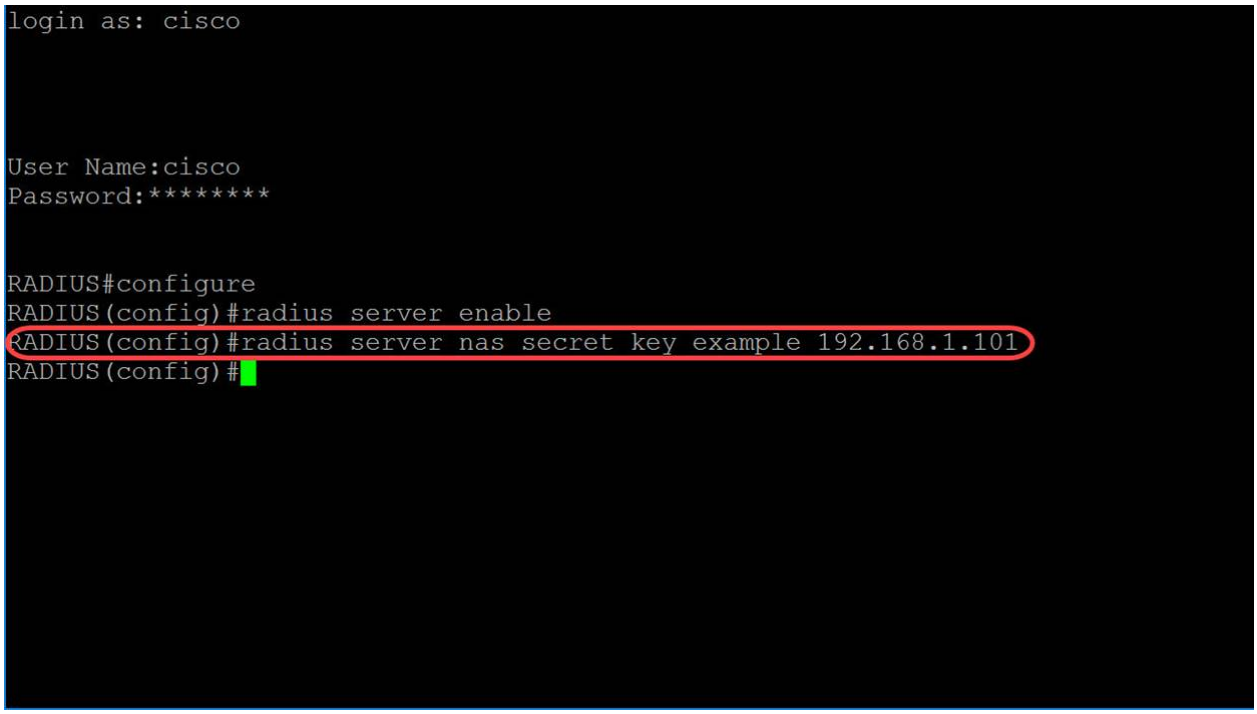
Schritt 4: Um einen geheimen Schlüssel zu erstellen, verwenden Sie den Befehl **radius server nas secret key** im globalen Konfigurationsmodus. Die Parameter sind wie folgt definiert:

- key - Gibt den Authentifizierungs- und Verschlüsselungsschlüssel für die Kommunikation zwischen dem Gerät und den Benutzern der angegebenen Gruppe an. Dieser Bereich umfasst 0 bis 128 Zeichen.

- default - Gibt den standardmäßigen geheimen Schlüssel an, der für die Kommunikation mit NAS ohne privaten Schlüssel angewendet wird.

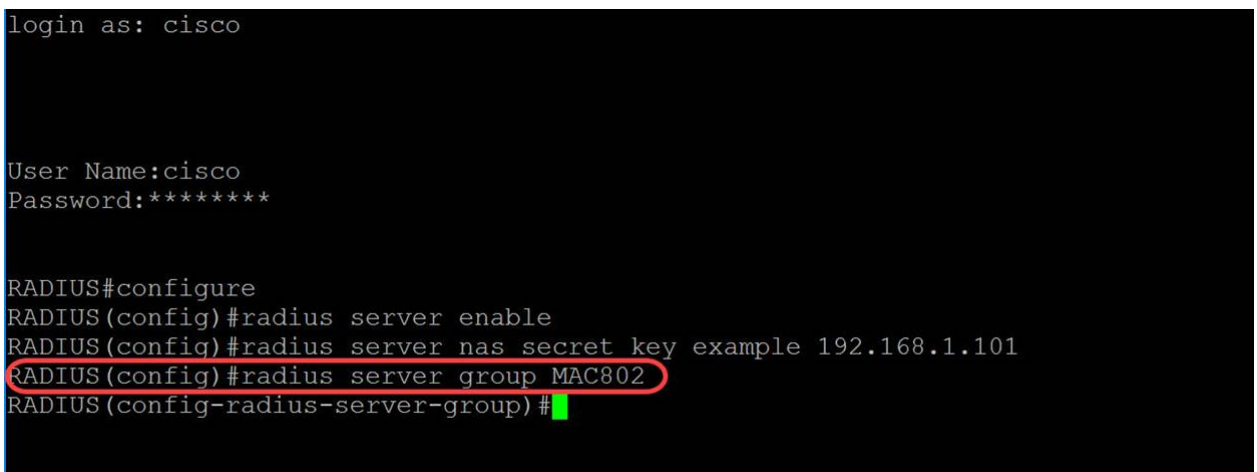
- ip-address - Gibt die IP-Adresse des RADIUS-Client-Hosts an. Bei der IP-Adresse kann es sich um eine IPv4-, IPv6- oder IPv6z-Adresse handeln.

In diesem Beispiel wird **example** als Schlüssel und **192.168.1.101** als IP-Adresse unseres Authentifizierers verwendet.



Schritt 5: Um in den RADIUS Server Group Configuration-Modus zu wechseln und eine Gruppe zu erstellen, falls diese nicht vorhanden ist, verwenden Sie den Befehl radius server group im Global Configuration-Modus.

In diesem Artikel wird **MAC802** als unser Gruppenname verwendet.

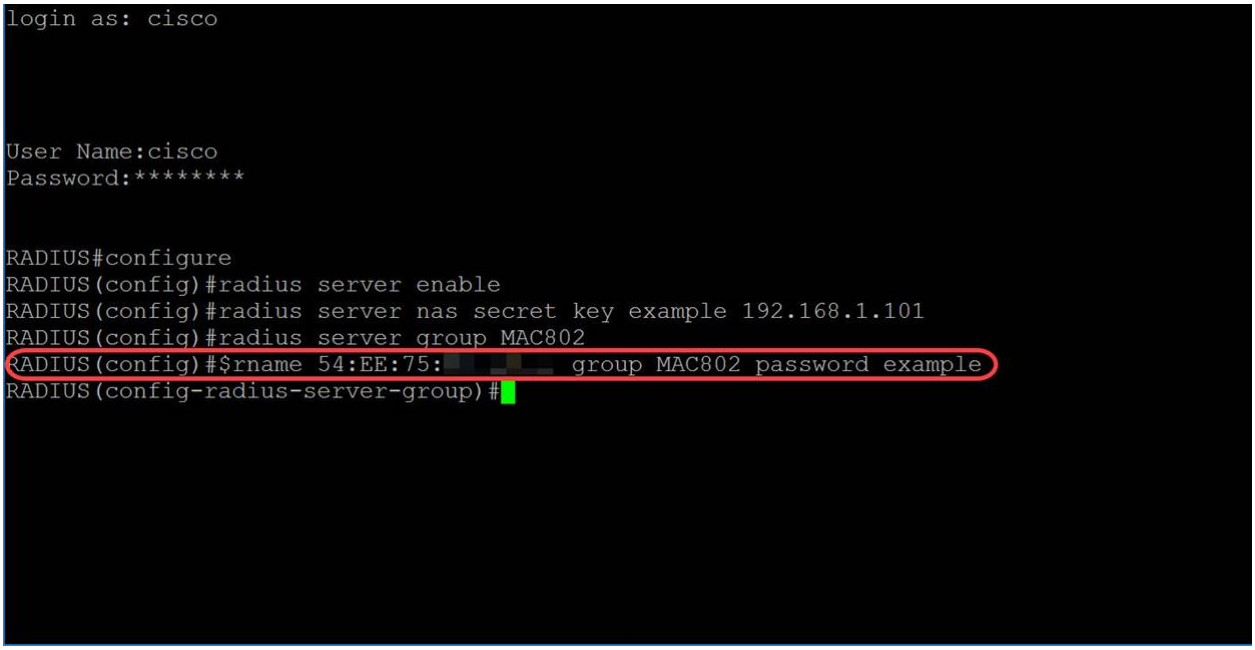


Schritt 6: Um einen Benutzer zu erstellen, verwenden Sie den Befehl **radius server user** im globalen Konfigurationsmodus. Die Parameter sind wie folgt definiert:

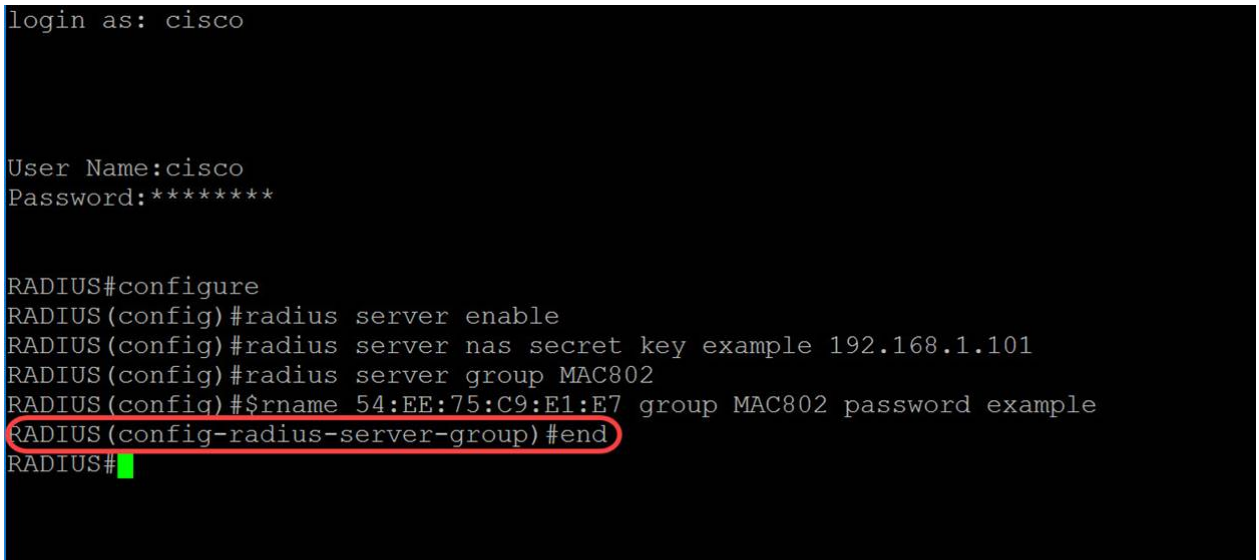
- user-name (Benutzername): Gibt den Benutzernamen an. Die Länge ist 1-32 Zeichen.
- group-name: Gibt den Namen der Benutzergruppe an. Die Länge des Gruppennamen beträgt 1-32 Zeichen.
- uncrypted-password - Gibt das Benutzerkennwort an. Die Länge kann zwischen 1 und 64 Zeichen betragen.

In diesem Beispiel verwenden wir die MAC-Adresse unseres Ethernet-Ports als *Benutzernamen*, **MAC802** als *Gruppennamen* und das *unverschlüsselte Kennwort* als **Beispiel.**

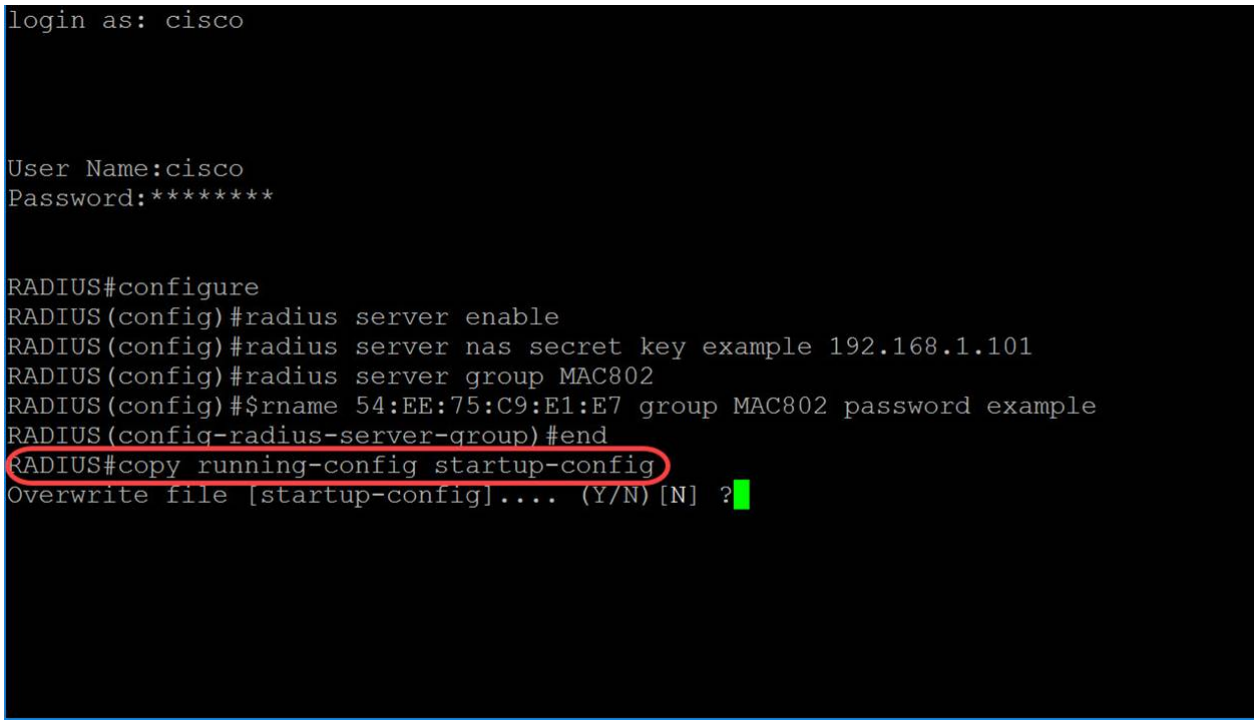
Hinweis: Einige der Oktette in der MAC-Adresse sind verschwommen. Das **Beispiel für** ein Kennwort ist kein sicheres Kennwort. Verwenden Sie ein sichereres Kennwort, da dieses nur als Beispiel verwendet wurde. Beachten Sie auch, dass der Befehl im Bild zu lang war, dass er automatisch den Befehl eingeschlossen hat.



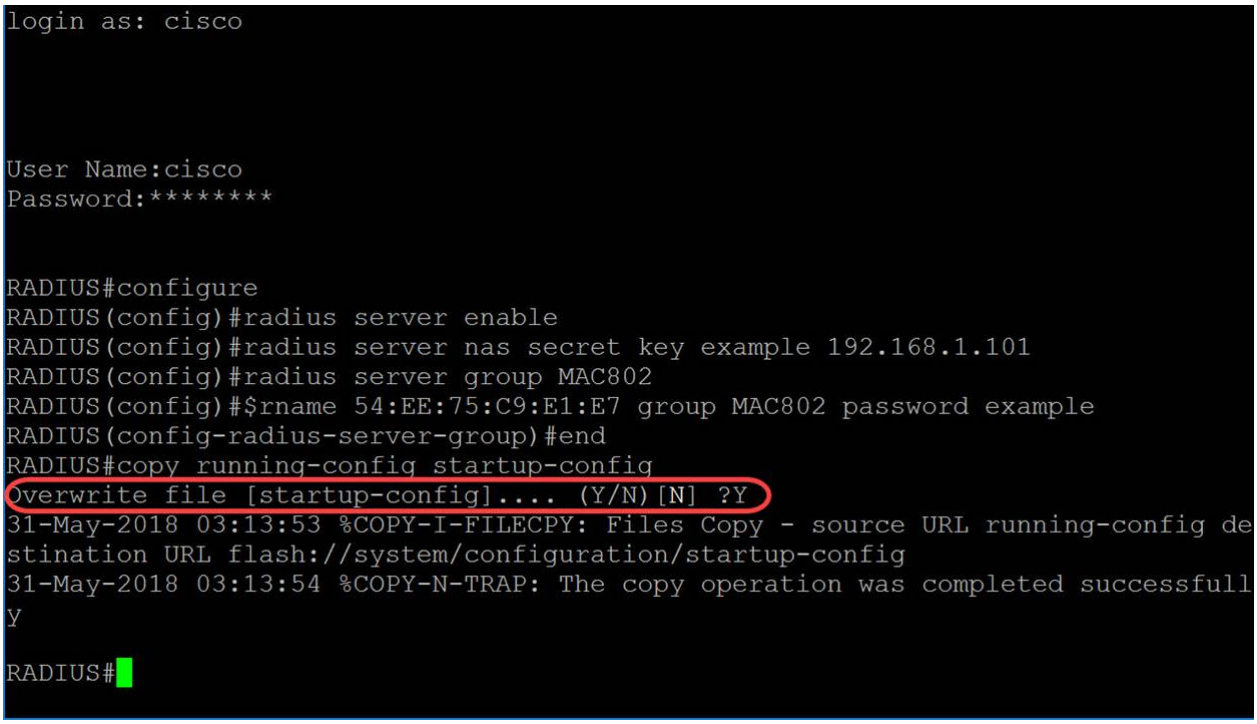
Schritt 7: (Optional) Um die aktuelle Konfigurationssitzung zu beenden und zum privilegierten EXEC-Modus zurückzukehren, verwenden Sie den **Befehl end**.



Schritt 8: (Optional) Um eine beliebige Datei von einer Quelle in ein Ziel zu kopieren, verwenden Sie den Befehl **copy** im privilegierten EXEC-Modus. In diesem Beispiel speichern wir unsere aktuelle Konfiguration als startup-config.



Schritt 9: (Optional) Es wird eine Meldung angezeigt, in der Sie gefragt werden, ob Sie die Startkonfigurationsdatei überschreiben möchten. Geben Sie **Y** für Ja oder **N** für Nein ein. Wir werden **Y** eingeben, um unsere startup-config-Datei zu überschreiben.



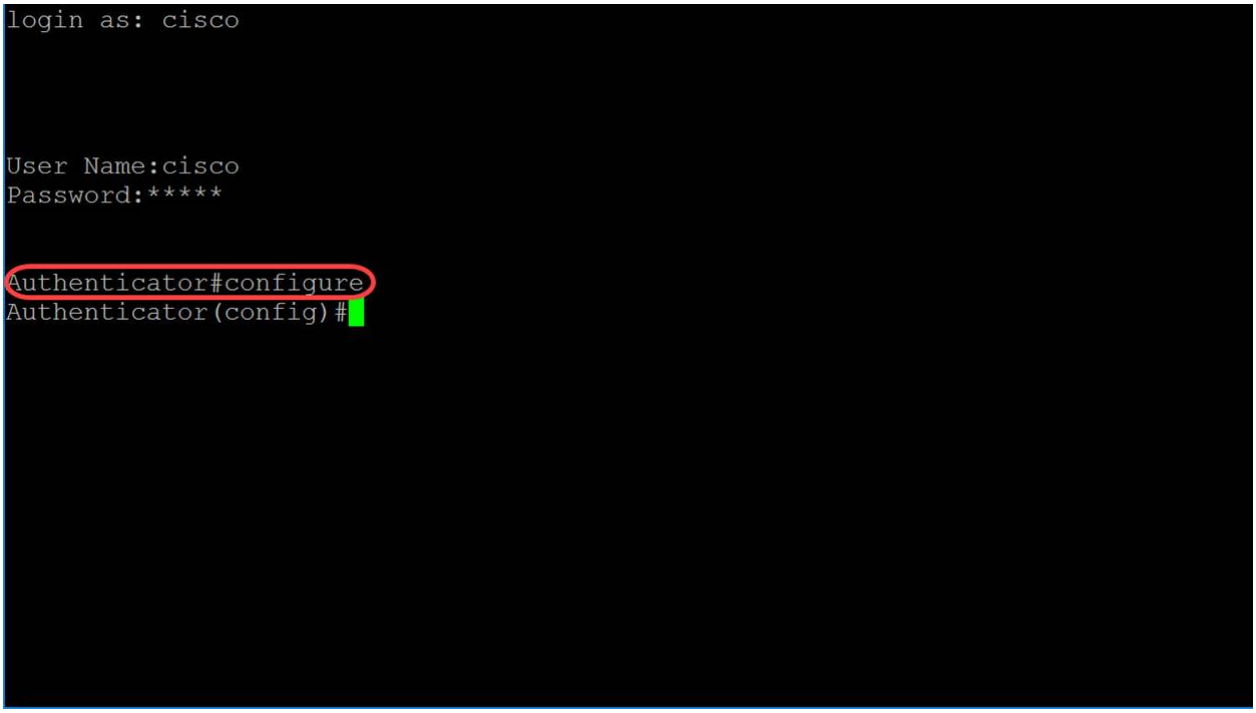
Konfigurieren des Authentifizierer-Switches

Schritt 1: SSH an den Switch, der als Authentifizierer fungieren soll. Der Standard-Benutzername und das Kennwort lautet cisco/cisco. Wenn Sie einen neuen Benutzernamen oder ein neues Kennwort konfiguriert haben, geben Sie diese stattdessen ein.

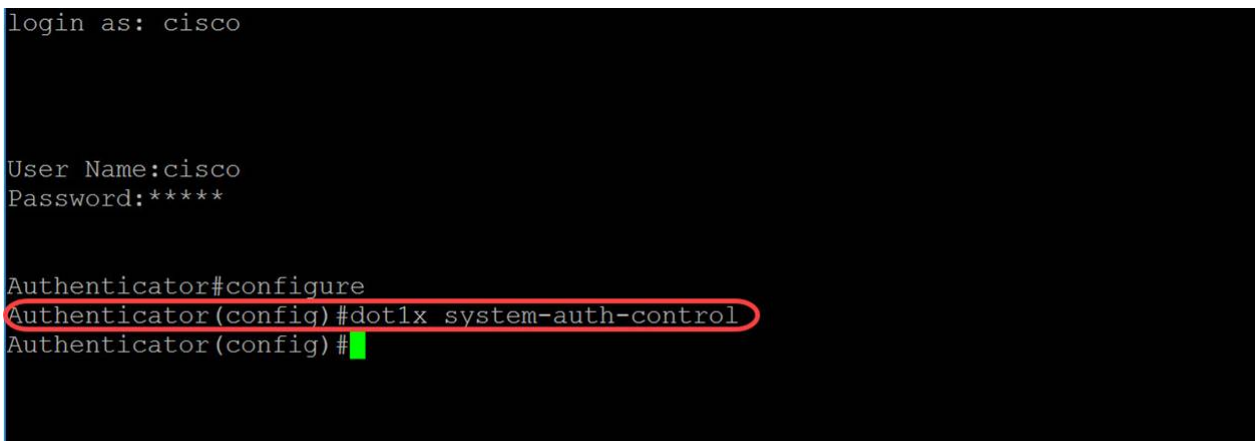
Hinweis: Um zu erfahren, wie Sie über SSH oder Telnet auf einen SMB-Switch zugreifen

können, klicken Sie auf hier.

Schritt 2: Geben Sie im privilegierten EXEC-Modus des Switches Folgendes ein, um in den globalen Konfigurationsmodus zu wechseln:



Schritt 3: Um 802.1X global zu aktivieren, verwenden Sie den Befehl dot1x system-auth-control im globalen Konfigurationsmodus.



Schritt 4: Verwenden Sie den Befehl **RADIUS-Server-Host** Global Configuration Mode, um einen RADIUS-Server-Host zu konfigurieren. Die Parameter sind wie folgt definiert:

- ip-address - Gibt die IP-Adresse des RADIUS-Server-Hosts an. Bei der IP-Adresse kann es sich um eine IPv4-, IPv6- oder IPv6z-Adresse handeln.

- hostname: Gibt den Hostnamen des RADIUS-Servers an. Die Übersetzung nur in IPv4-Adressen wird unterstützt. Die Länge des Hostnamens liegt zwischen 1 und 158 Zeichen, und die maximale Länge des Labels beträgt 63 Zeichen.

- auth-port *auth-port-number* - Gibt die Portnummer für Authentifizierungsanforderungen an. Wenn die Portnummer auf 0 festgelegt ist, wird der Host nicht für die Authentifizierung verwendet. Der Bereich liegt zwischen 0 und 65.535.

- ACC-Port *ACT-Port-Nummer* - Portnummer für Buchhaltungsanfragen. Der Host wird nicht für die Abrechnung verwendet, wenn er auf 0 festgelegt ist. Wenn nicht angegeben, lautet die Standardeinstellung für die Portnummer 1813.

- timeout *timeout* - Gibt den Timeoutwert in Sekunden an. Der Bereich liegt zwischen 1 und 30.

- reÜbertragen *von Versuchen* - Gibt die Anzahl der erneuten Übertragungen an. Der Bereich liegt zwischen 1 und 15.

- Deadtime *Deadtime* - Gibt die Zeitdauer in Minuten an, während der ein RADIUS-Server von Transaktionsanforderungen übersprungen wird. Sie reicht von 0 bis 2000.

- key *key-Zeichenfolge*: Gibt den Authentifizierungs- und Verschlüsselungsschlüssel für alle RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Server an. Dieser Schlüssel muss mit der im RADIUS-Daemon verwendeten Verschlüsselung übereinstimmen. Um eine leere Zeichenfolge anzugeben, geben Sie "" ein. Die Länge kann zwischen 0 und 128 Zeichen betragen. Wird dieser Parameter ausgelassen, wird der global konfigurierte Radius-Schlüssel verwendet.

- key *encrypted-key-string* - Wie eine Schlüsselzeichenfolge, aber der Schlüssel ist im verschlüsselten Format.

- priority *priority (Prioritätspriorität*) - Gibt die Reihenfolge an, in der Server verwendet werden, wobei 0 die höchste Priorität hat. Der Prioritätsbereich liegt zwischen 0 und 65.535.

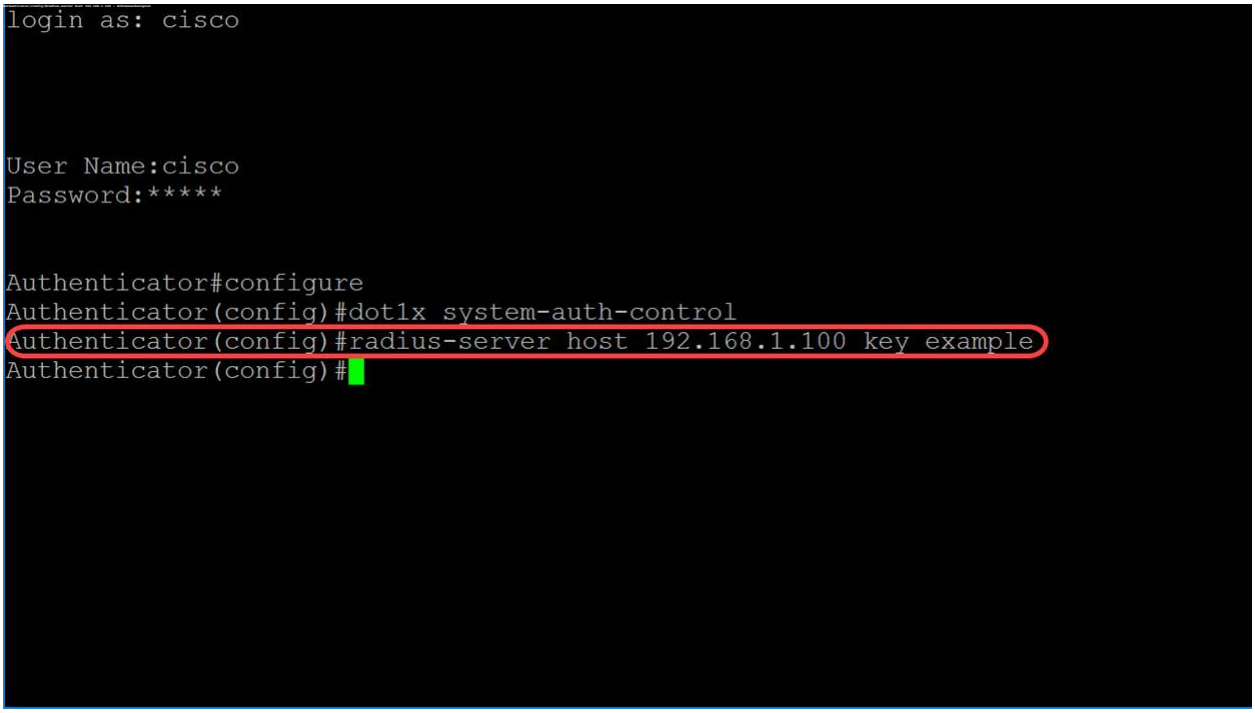
- use {login|dot1.x|all} — gibt den RADIUS-Serververwendungstyp an. Mögliche Werte sind:

    - login - Gibt an, dass der RADIUS-Server für die Authentifizierung von Benutzeranmeldeinformationen verwendet wird.

    - dot1.x - Gibt an, dass der RADIUS-Server für die 802.1x-Portauthentifizierung verwendet wird.

    - all - Gibt an, dass der RADIUS-Server für die Benutzeranmeldeauthentifizierung und die 802.1x-Portauthentifizierung verwendet wird.

In diesem Beispiel werden nur der Host und die Schlüsselparameter verwendet. Wir verwenden die IP-Adresse **192.168.1.100** als IP-Adresse des RADIUS-Servers und das Wort **example** als Schlüsselzeichenfolge.

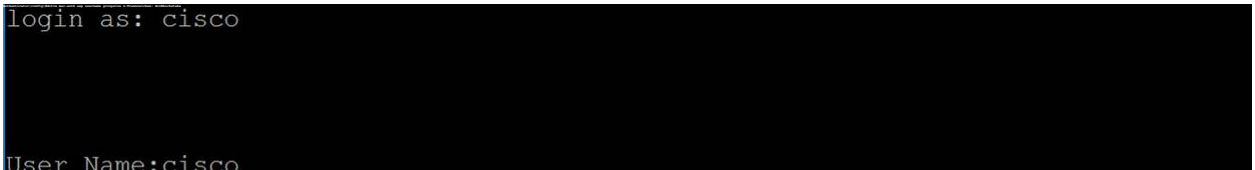


Schritt 5: Bei der MAC-basierten Authentifizierung basiert der Benutzername des Supplicant auf der MAC-Adresse des jeweiligen Geräts. Im Folgenden wird das Format dieses MAC-basierten Benutzernamen definiert, der vom Switch im Rahmen des Authentifizierungsprozesses an den RADIUS-Server gesendet wird. Die folgenden Felder sind definiert als:

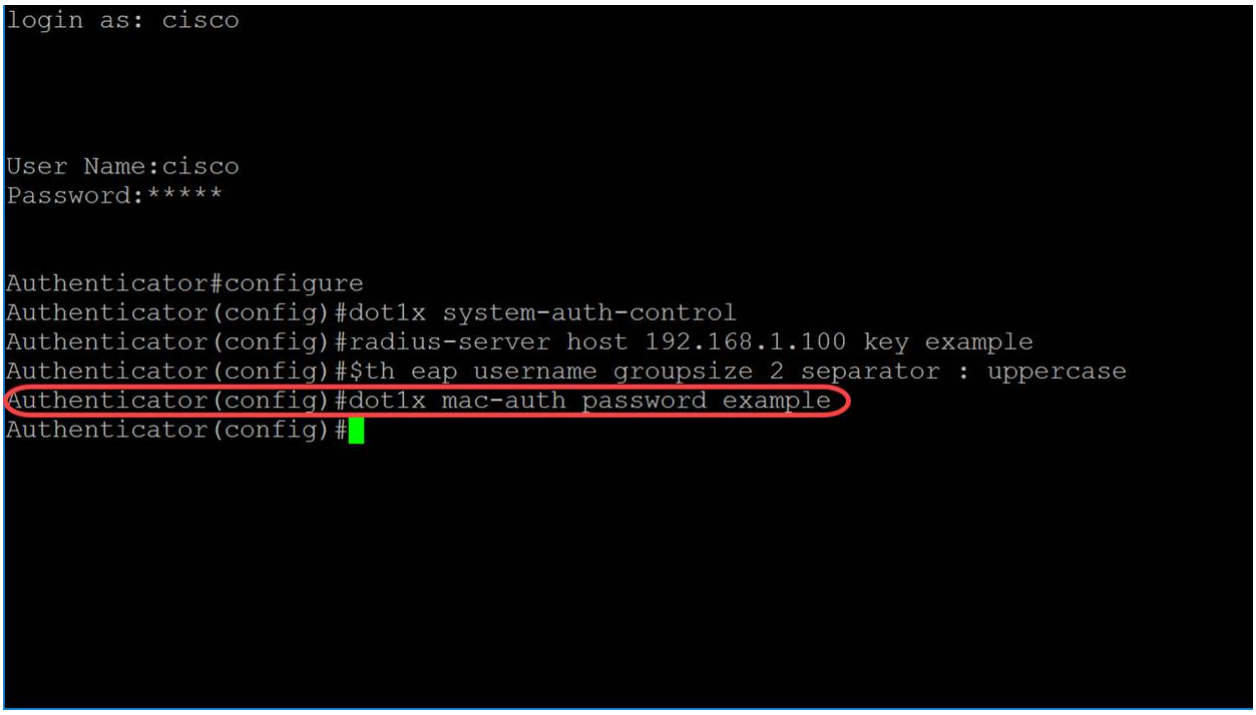
- MAC-Authentifizierungstyp - Wählen Sie einen MAC-Authentifizierungstyp aus.
    - eap - Verwenden Sie RADIUS mit EAP-Kapselung für den Datenverkehr zwischen dem Switch (RADIUS-Client) und dem RADIUS-Server, der eine MAC-basierte Komponente authentifiziert.
    - radius - Verwenden Sie für den Datenverkehr zwischen dem Switch (RADIUS-Client) und dem RADIUS-Server, der eine MAC-basierte Komponente authentifiziert, RADIUS ohne EAP-Kapselung.
- groupsize - Anzahl der ASCII-Zeichen zwischen Trennzeichen der als Benutzername gesendeten MAC-Adresse. Sie können 1, 2, 4 oder 12 ASCII-Zeichen zwischen Trennzeichen verwenden.
- Trennzeichen: Zeichen, das als Trennzeichen zwischen den definierten Zeichengruppen in der MAC-Adresse verwendet wird. Als Trennzeichen können Bindestrich, Doppelpunkt oder Punkt verwendet werden.
- case - Senden Sie den Benutzernamen in Groß- oder Kleinschreibung. Die Optionen sind Groß- oder Kleinschreibung.

dot1x mac-auth

In diesem Beispiel verwenden wir **eap** als MAC-Authentifizierungstyp, eine Gruppengröße von **2**, den **Doppelpunkt** als Trennzeichen und senden unseren Benutzernamen in **Großbuchstaben**.

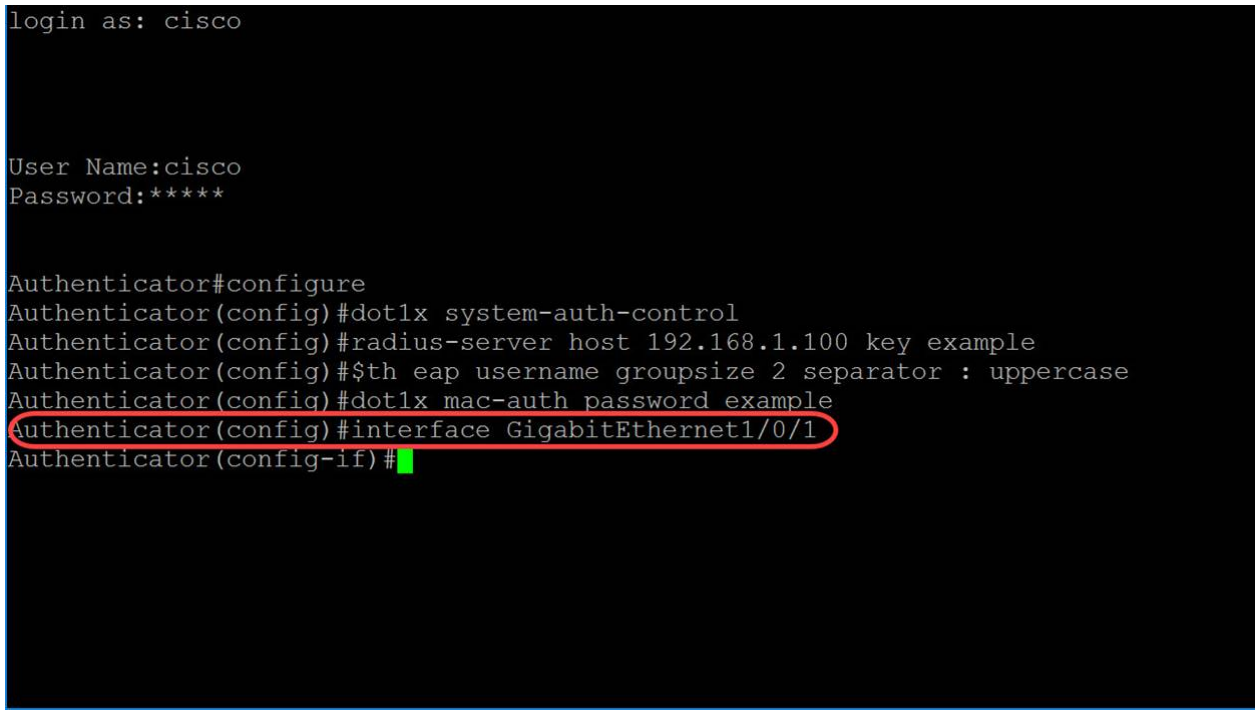


Schritt 6: Verwenden Sie den folgenden Befehl, um das Kennwort festzulegen, das der Switch für die MAC-basierte Authentifizierung anstelle der MAC-Adresse des Hosts verwendet. Wir verwenden das Wort **example** als unser Kennwort.



Schritt 7: Um in den Schnittstellenkonfigurationsmodus zu wechseln, um eine Schnittstelle zu konfigurieren, verwenden Sie den Befehl **interface** Global Configuration Mode. Wir werden GigabitEthernet1/0/1 konfigurieren, da unser End-Host mit ihm verbunden ist.

Hinweis: Konfigurieren Sie den Port, der mit dem RADIUS-Server verbunden ist, nicht.



Hinweis: Wenn Sie mehrere Ports gleichzeitig konfigurieren möchten, verwenden Sie den Befehl interface range (Schnittstellenbereich).

Das nachfolgende Beispiel zeigt die Konfiguration der Ports 1-4 mithilfe des Range-Befehls:

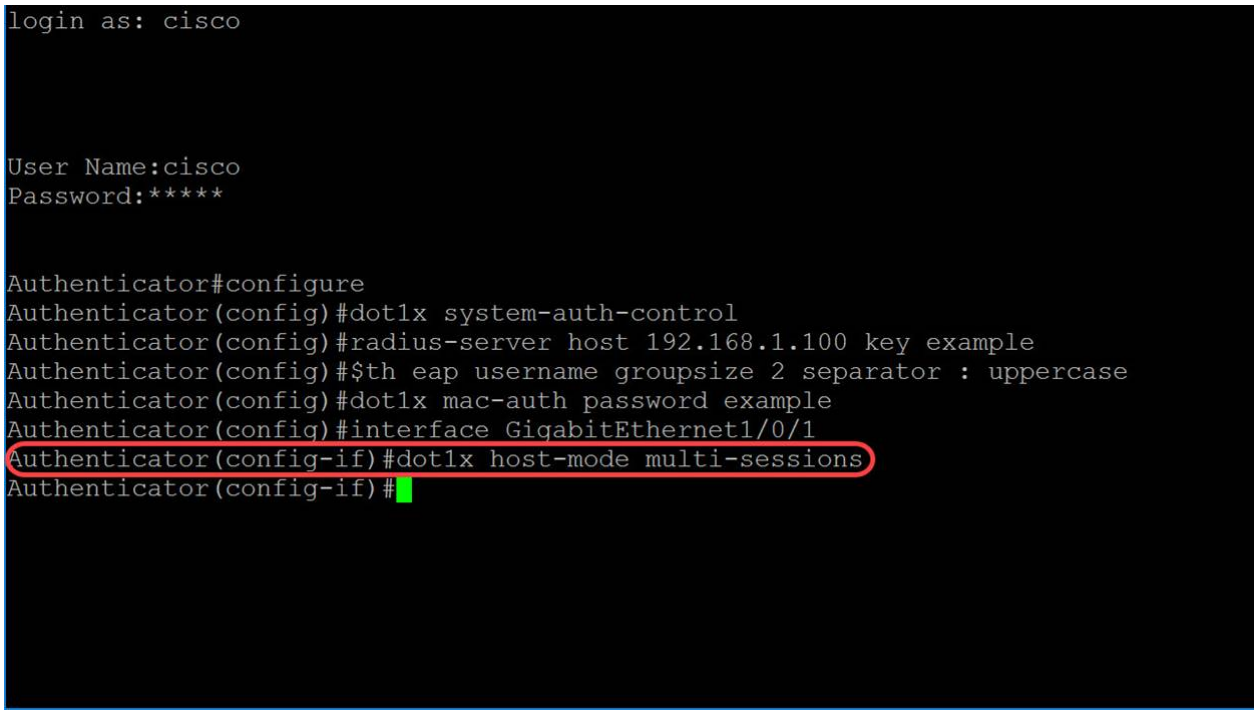
Schritt 8: Um einen einzelnen Host (Client) oder mehrere Hosts an einem IEEE802.1X-autorisierten Port zuzulassen, verwenden Sie den Befehl **dot1x im Host-Modus** im Schnittstellenkonfigurationsmodus. Die Parameter sind wie folgt definiert:

- Multi-Host - Mehrere Hosts aktivieren
    - Ein Port ist autorisiert, wenn mindestens ein autorisierter Client vorhanden ist.
    - Wenn ein Port nicht autorisiert ist und ein Gast-VLAN aktiviert ist, wird nicht markierter Datenverkehr dem Gast-VLAN neu zugeordnet. Tagged Datenverkehr wird verworfen, es sei denn, er gehört zum Gast-VLAN oder zu einem nicht authentifizierten VLAN. Wenn das Gast-VLAN auf einem Port nicht aktiviert ist, wird nur markierter Datenverkehr überbrückt, der zu nicht authentifizierten VLANs gehört.
    - Wenn ein Port autorisiert ist, wird der nicht getaggte und getaggte Datenverkehr aller Hosts, die mit dem Port verbunden sind, je nach der Konfiguration des statischen Ports für die VLAN-Mitgliedschaft überbrückt.
    - Sie können festlegen, dass nicht markierter Datenverkehr vom autorisierten Port einem VLAN zugewiesen wird, das während des Authentifizierungsprozesses von einem RADIUS-Server zugewiesen wird. Der getaggte Datenverkehr wird verworfen, es sei denn, er gehört zum RADIUS-zugewiesenen VLAN oder zu den nicht authentifizierten VLANs. Die RADIUS-VLAN-Zuweisung für einen Port wird auf der Seite *Port Authentication (Portauthentifizierung)* festgelegt.
- Single-Host - Einzelhost-Modus aktivieren
    - Ein Port ist autorisiert, wenn ein autorisierter Client vorhanden ist. Auf einem Port kann nur ein Host autorisiert werden.
    - Wenn ein Port nicht autorisiert ist und das Gast-VLAN aktiviert ist, wird nicht markierter Datenverkehr dem Gast-VLAN neu zugeordnet. Tagged Datenverkehr wird verworfen, es sei denn, er gehört zum Gast-VLAN oder zu einem nicht authentifizierten VLAN. Wenn ein Gast-VLAN auf dem Port nicht aktiviert ist, wird nur markierter Datenverkehr überbrückt, der zu den nicht authentifizierten VLANs gehört.
    - Wenn ein Port autorisiert ist, wird der nicht getaggte und getaggte Datenverkehr vom autorisierten Host basierend auf der Konfiguration des statischen Ports für die VLAN-Mitgliedschaft überbrückt. Datenverkehr von anderen Hosts wird verworfen.
    - Ein Benutzer kann festlegen, dass nicht markierter Datenverkehr vom autorisierten Host einem VLAN zugeordnet wird, das während des Authentifizierungsprozesses von einem RADIUS-Server zugewiesen wird. Der getaggte Datenverkehr wird verworfen, es sei denn, er gehört zum RADIUS-zugewiesenen VLAN oder zu den nicht authentifizierten VLANs. Die RADIUS-VLAN-Zuweisung für einen Port wird auf der *Port*-Authentifizierungsseite festgelegt.
- Multisitzungen - Multisitzungsmodus aktivieren
    - Im Gegensatz zum Single-Host- und Multi-Host-Modus besitzt ein Port im Multi-Session-Modus keinen Authentifizierungsstatus. Dieser Status wird jedem Client zugewiesen, der mit dem Port verbunden ist.
    - Tagged-Datenverkehr, der zu einem nicht authentifizierten VLAN gehört, wird immer überbrückt, unabhängig davon, ob der Host autorisiert ist oder nicht.

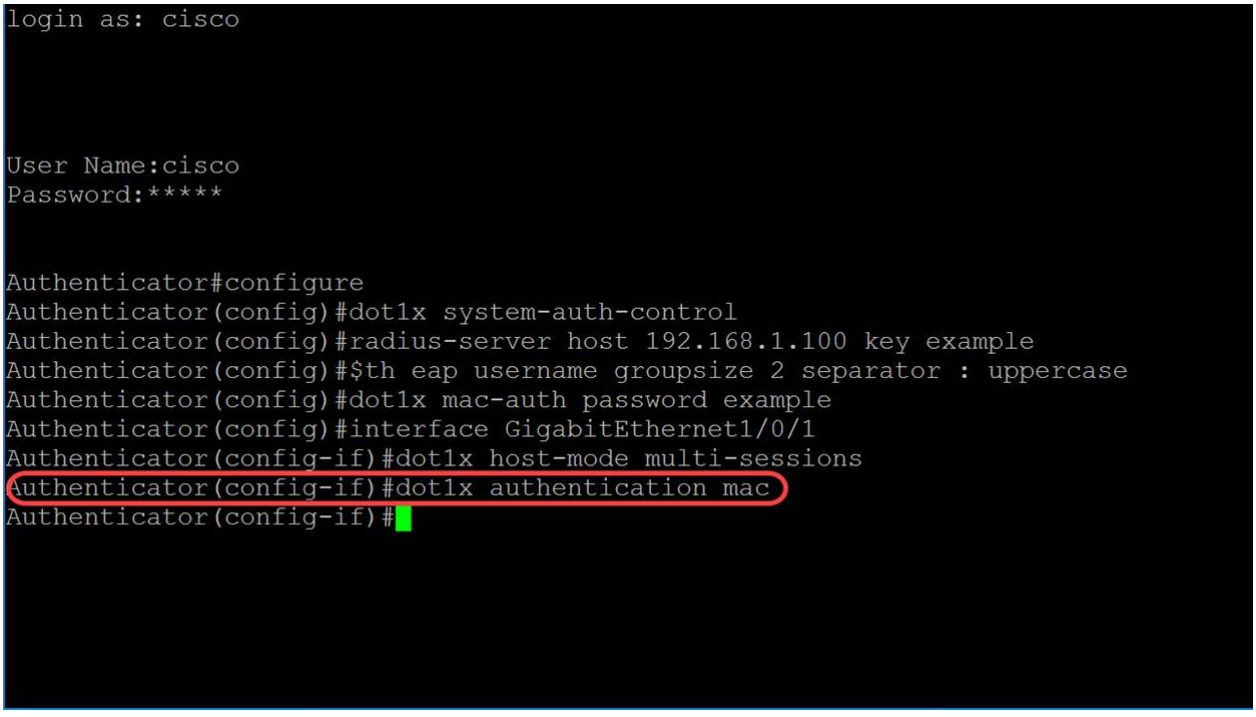
- Getaggte und nicht getaggte Zugriffe von nicht autorisierten Hosts, die nicht zu einem nicht authentifizierten VLAN gehören, werden dem Gast-VLAN neu zugeordnet, wenn sie im VLAN definiert und aktiviert sind, oder verworfen, wenn das Gast-VLAN auf dem Port nicht aktiviert ist.

- Sie können festlegen, dass nicht markierter Datenverkehr vom autorisierten Port einem VLAN zugewiesen wird, das während des Authentifizierungsprozesses von einem RADIUS-Server zugewiesen wird. Der getaggte Datenverkehr wird verworfen, es sei denn, er gehört zum RADIUS-zugewiesenen VLAN oder zu den nicht authentifizierten VLANs. Die RADIUS-VLAN-Zuweisung für einen Port wird auf der Seite *Port Authentication* festgelegt.

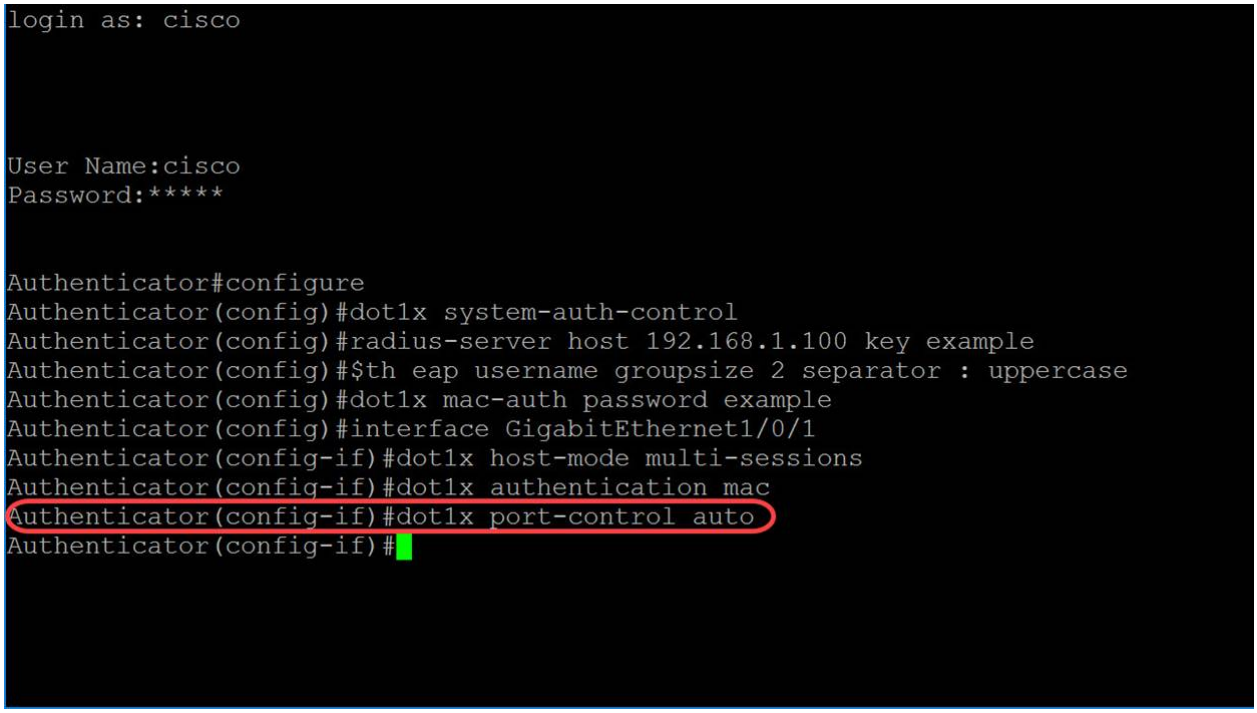
In diesem Beispiel wird der Host-Modus so konfiguriert, dass er mehrere Sitzungen umfasst.



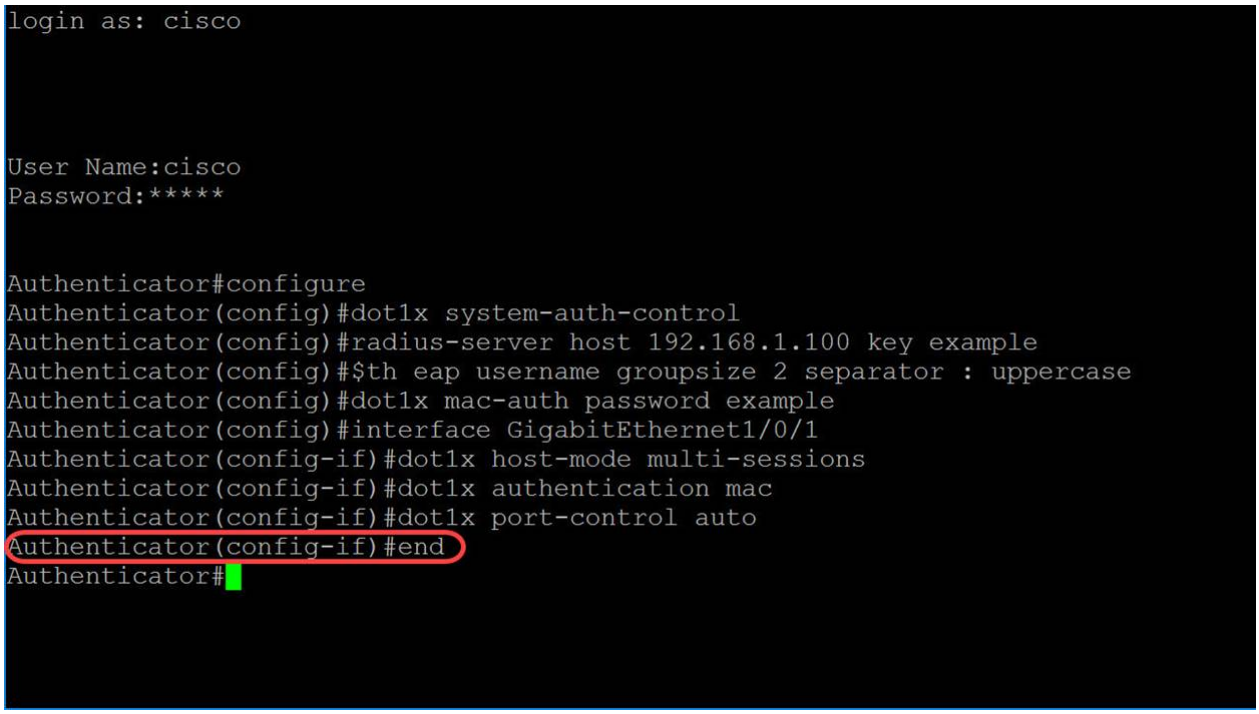
Schritt 9: Um die Authentifizierungsmethode auf einem Port zu konfigurieren, verwenden Sie den folgenden Befehl, um die MAC-basierte Authentifizierung zu aktivieren.



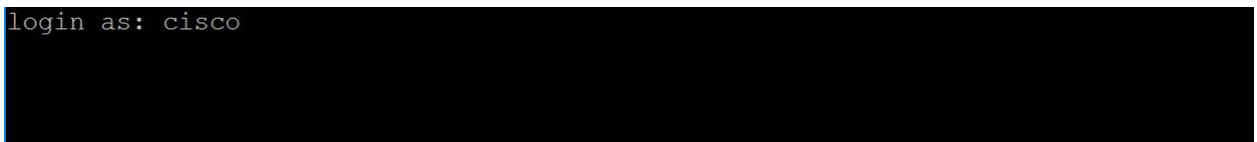
Schritt 10: Um die Port-basierte Authentifizierung und Autorisierung auf dem Gerät zu aktivieren, verwenden Sie den Befehl **port-control**, um den Port-Kontrollwert zu konfigurieren. Der Autorisierungsstatus des Verwaltungsports wird als **Auto** ausgewählt. Dadurch können wir die Port-basierte Authentifizierung und Autorisierung auf dem Gerät aktivieren. Die Schnittstelle wechselt zwischen einem autorisierten oder einem nicht autorisierten Zustand, der auf dem Authentifizierungsaustausch zwischen Gerät und Client basiert.



Schritt 11: (Optional) Um die aktuelle Konfigurationssitzung zu beenden und zum privilegierten EXEC-Modus zurückzukehren, verwenden Sie den **Befehl end**.



Schritt 12: (Optional) Um eine beliebige Datei von einer Quelle in ein Ziel zu kopieren, verwenden Sie den Befehl **copy** im privilegierten EXEC-Modus. In diesem Beispiel speichern wir unsere aktuelle Konfiguration als startup-config.



Schritt 13: (Optional) Es erscheint eine Meldung, in der Sie gefragt werden, ob Sie die Startkonfigurationsdatei überschreiben möchten. Geben Sie **Y** für Ja oder **N** für Nein ein. Wir werden **Y** eingeben, um unsere startup-config-Datei zu überschreiben.

```
User Name:cisco
Password:*****

Authenticator#configure
Authenticator(config)#dot1x system-auth-control
Authenticator(config)#radius-server host 192.168.1.100 key example
Authenticator(config)#$th eap username groupsize 2 separator : uppercase
Authenticator(config)#dot1x mac-auth password example
Authenticator(config)#interface GigabitEthernet1/0/1
Authenticator(config-if)#dot1x host-mode multi-sessions
Authenticator(config-if)#dot1x authentication mac
Authenticator(config-if)#dot1x port-control auto
Authenticator(config-if)#end
Authenticator#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
31-May-2018 03:35:43 %COPY-I-FILECPY: Files Copy - source URL running-config des
tination URL flash://system/configuration/startup-config
31-May-2018 03:35:45 %COPY-N-TRAP: The copy operation was completed successfully

Authenticator#
```

Schlussfolgerung

Sie sollten jetzt die MAC-basierte Authentifizierung auf Ihrem Switch über die CLI konfiguriert haben. Führen Sie die folgenden Schritte aus, um zu überprüfen, ob die MAC-basierte Authentifizierung funktioniert.

Schritt 1: Um aktive 802.1X-autorisierte Benutzer für das Gerät anzuzeigen, verwenden Sie den Befehl **show dot1x users** im privilegierten EXEC-Modus.

```
Authenticator#configure
Authenticator(config)#dot1x system-auth-control
Authenticator(config)#radius-server host 192.168.1.100 key example
Authenticator(config)#$th eap username groupsize 2 separator : uppercase
Authenticator(config)#dot1x mac-auth password example
Authenticator(config)#interface GigabitEthernet1/0/1
Authenticator(config-if)#dot1x host-mode multi-sessions
Authenticator(config-if)#dot1x authentication mac
Authenticator(config-if)#dot1x port-control auto
Authenticator(config-if)#end
Authenticator#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
31-May-2018 03:35:43 %COPY-I-FILECPY: Files Copy - source URL running-config des
tination URL flash://system/configuration/startup-config
31-May-2018 03:35:45 %COPY-N-TRAP: The copy operation was completed successfully

Authenticator#show dot1x users

                          MAC               Auth   Auth   Session        VLAN
Port     Username         Address           Method Server Time
-------- ---------------- ----------------- ------ ------ -------------- ----
gi1/0/1  54:EE:75:[redacted] 54:ee:75:[redacted] MAC    Remote 00:01:45

Authenticator#
```

Schritt 2: Um die 802.1X-Schnittstellen oder den angegebenen Schnittstellenstatus anzuzeigen, verwenden Sie den Befehl **show dot1x** im privilegierten EXEC-Modus.

```
Authenticator#show dot1x interface GigabitEthernet1/0/1

Authentication is enabled
Authenticator Global Configuration:
```