通過命令列介面在交換機上配置基於MAC的身份驗證

目標

802.1X是一種管理工具，允許列出裝置，確保不對您的網路進行未經授權的訪問。本文顯示如何使用命令列介面(CLI)在交換機上配置基於MAC的身份驗證。

請參閱辭彙表以瞭解其他資訊。

RADIUS 如何運作？

802.1X驗證有三個主要元件：請求方（使用者端）、驗證者(網路裝置（例如交換器）和驗證伺服器(RADIUS)。 遠端身份驗證撥入使用者服務(RADIUS)是一種使用身份驗證、授權和記帳(AAA)協定的訪問伺服器，可幫助管理靜態IP地址為192.168.1.100，而身份驗證器的靜態IP地址為192.168.1.101。

適用裝置

- Sx350X系列
- SG350XG系列
- Sx550X系列
- SG550XG系列

軟體版本

- 2.4.0.94

在交換機上配置RADIUS伺服器

步驟1.使用SSH連線到將成為RADIUS伺服器的交換機。預設使用者名稱和密碼為cisco/cisco。如果您已配置新的使用者名稱或密碼，請改為輸入憑據。

附註： 要瞭解如何通過SSH或Telnet訪問SMB交換機，請按一下 此處.

步驟2.在交換機的特權執行模式下，輸入以下命令進入全域性配置模式：

步驟3.使用**radius server enable**命令啟用RADIUS伺服器。

```
login as: cisco



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


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

步驟4.要建立金鑰，請在全域性配置模式下使用**radius server nas secret key**命令。引數定義為：

- key — 指定用於裝置與給定組的使用者之間通訊的身份驗證和加密金鑰。其範圍從0到128個字元。
- default — 指定將應用於與沒有私鑰的NAS通訊的預設金鑰。
- ip-address — 指定RADIUS客戶端主機IP地址。IP地址可以是IPv4、IPv6或IPv6z地址。

在本例中，我們將使用**example**作為金鑰，**192.168.1.101**作為身份驗證器的IP地址。

```
login as: cisco



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


RADIUS#configure
RADIUS(config)#radius server enable
RADIUS(config)#radius server nas secret key example 192.168.1.101
RADIUS(config)#
```

步驟5.要進入RADIUS伺服器組配置模式並在組不存在的情況下建立組，請在全域性配置模式下使用radius server group命令。

在本文中，我們將使用**MAC802作**為我們的組名。

```
login as: cisco



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


RADIUS#configure
RADIUS(config)#radius server enable
RADIUS(config)#radius server nas secret key example 192.168.1.101
RADIUS(config)#radius server group MAC802
RADIUS(config-radius-server-group)#
```

步驟6.要建立使用者，請在全域性配置模式下使用**radius server user**命令。引數定義為：

- user-name — 指定使用者名稱。長度為1-32個字元。
- group-name — 指定使用者組名稱。組名的長度為1到32個字元。
- unencrypted-password — 指定使用者密碼。長度可以是1到64個字元。

在本例中，我們將使用乙太網埠的MAC地址作為使用者名稱,**MAC802**作為*group-name*，並將*unencrypted-password*作為**example**。

附註： MAC位址中的某些八位元已模糊不清。密碼**範例**不是強密碼。請使用較強密碼，因為這只是一個示例。另請注意，命令在圖片中太長，因此會自動包裝命令。

```
login as: cisco



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


RADIUS#configure
RADIUS(config)#radius server enable
RADIUS(config)#radius server nas secret key example 192.168.1.101
RADIUS(config)#radius server group MAC802
RADIUS(config)#$rname 54:EE:75:      group MAC802 password example
RADIUS(config-radius-server-group)#
```

步驟7。（可選）要結束當前配置會話並返回特權執行模式，請使用**end**命令。

```
login as: cisco



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


RADIUS#configure
RADIUS(config)#radius server enable
RADIUS(config)#radius server nas secret key example 192.168.1.101
RADIUS(config)#radius server group MAC802
RADIUS(config)#$rname 54:EE:75:C9:E1:E7 group MAC802 password example
RADIUS(config-radius-server-group)#end
RADIUS#
```

步驟8.（可選）要將任何檔案從源複製到目標，請在特權EXEC模式下使用**copy**命令。在本例中，我們將運行配置儲存到啟動配置。

```
login as: cisco



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


RADIUS#configure
RADIUS(config)#radius server enable
RADIUS(config)#radius server nas secret key example 192.168.1.101
RADIUS(config)#radius server group MAC802
RADIUS(config)#$rname 54:EE:75:C9:E1:E7 group MAC802 password example
RADIUS(config-radius-server-group)#end
RADIUS#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?
```

步驟9.（可選）系統會顯示訊息，詢問您是否要覆寫啟動組態檔。輸入**Y**表示yes，輸入**N**表示no。我們將鍵入**Y**覆蓋啟動配置檔案。

```
login as: cisco



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


RADIUS#configure
RADIUS(config)#radius server enable
RADIUS(config)#radius server nas secret key example 192.168.1.101
RADIUS(config)#radius server group MAC802
RADIUS(config)#$rname 54:EE:75:C9:E1:E7 group MAC802 password example
RADIUS(config-radius-server-group)#end
RADIUS#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
31-May-2018 03:13:53 %COPY-I-FILECPY: Files Copy - source URL running-config de
stination URL flash://system/configuration/startup-config
31-May-2018 03:13:54 %COPY-N-TRAP: The copy operation was completed successfull
y

RADIUS#
```

配置身份驗證器交換機

步驟1.使用SSH連線到要成為身份驗證器的交換機。預設使用者名稱和密碼為cisco/cisco。如果已配置新的使用者名稱或密碼，請輸入這些憑據。

附註： 要瞭解如何通過SSH或Telnet訪問SMB交換機，請按一下 此處.

```
login as: cisco



User Name:cisco
Password:*****


Authenticator#
```

步驟2.在交換機的特權執行模式下，輸入以下命令進入全域性配置模式：

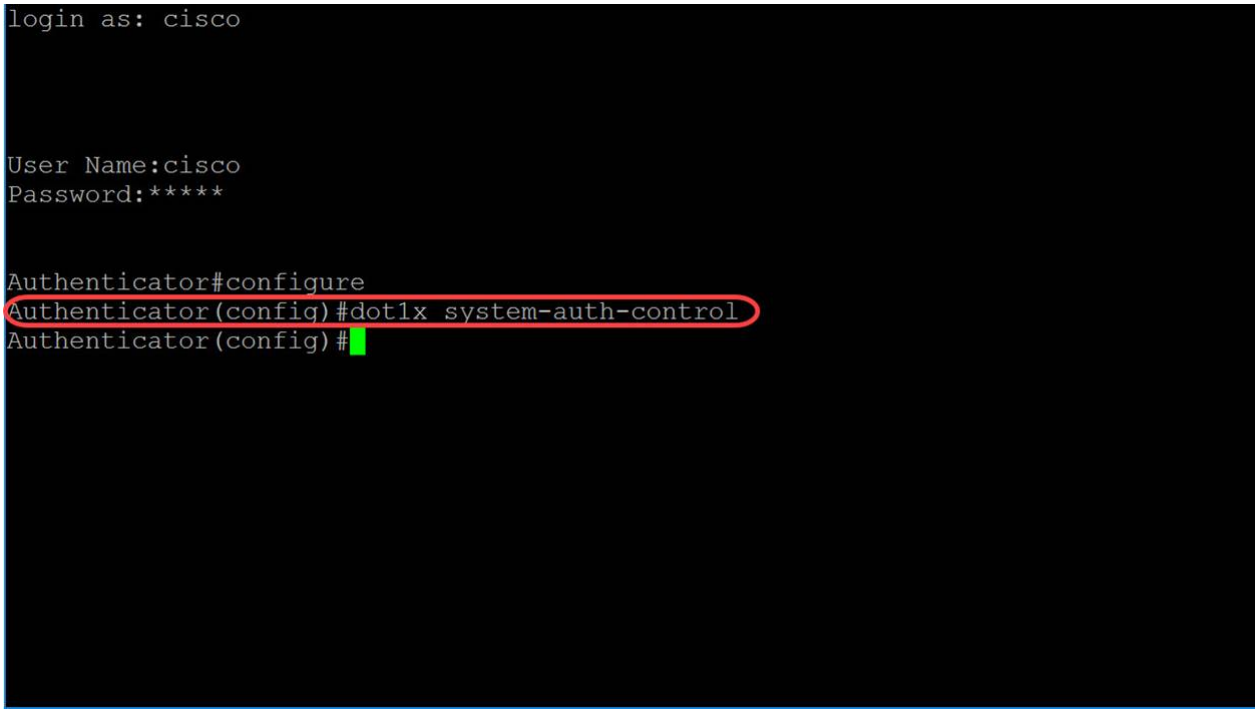
```
login as: cisco



User Name:cisco
Password:*****


Authenticator#configure
```

步驟3.要全域性啟用802.1X，請在全域性配置模式下使用dot1x system-auth-control命令。

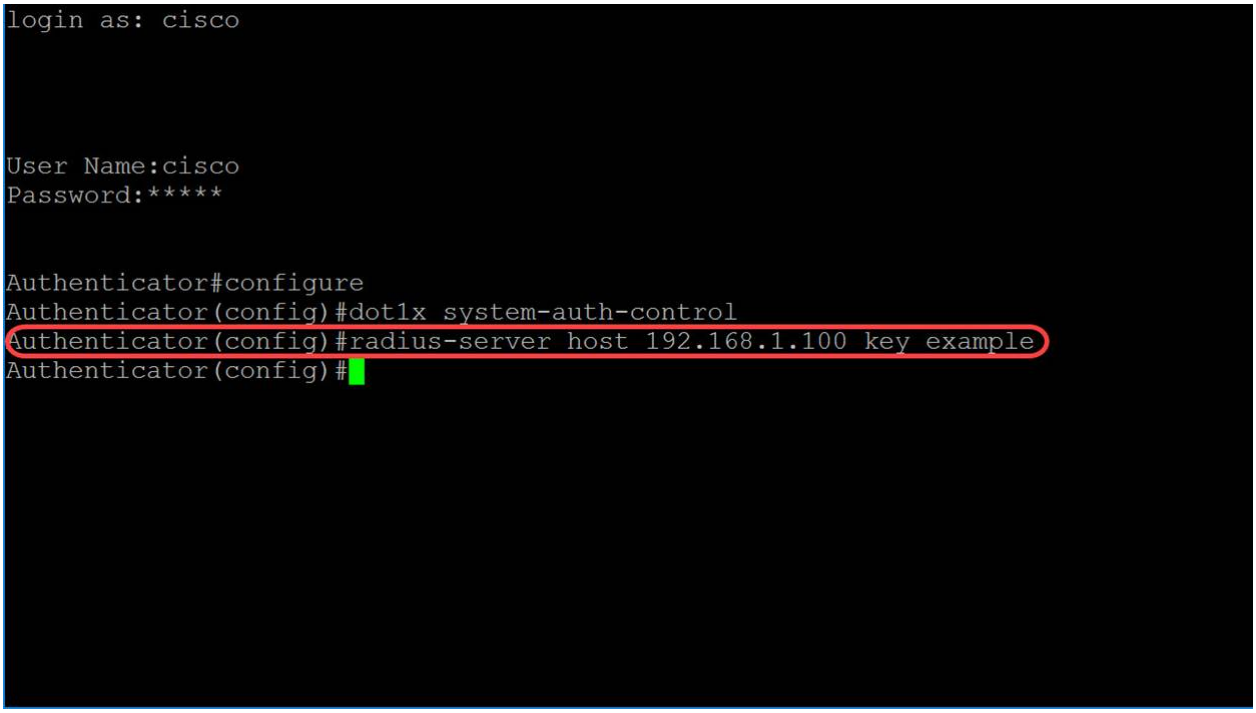


步驟4.使用**radius-server host**全域性配置模式命令配置RADIUS伺服器主機。引數定義為：

- ip-address — 指定RADIUS伺服器主機IP地址。IP地址可以是IPv4、IPv6或IPv6z地址。
- hostname — 指定RADIUS伺服器主機名。僅支援轉換為IPv4地址。主機名的長度介於1到158個字元之間，並且主機名各部分的最大標籤長度為63個字元。
- auth-port *auth-port-number* — 指定驗證要求的連線埠號碼。如果埠號設定為0，則不會使用主機進行身份驗證。範圍為0到65535。
- Acc-port *acct-port-number* — *計*算請求的埠號。如果設定為0，則不使用該主機進行記帳。如果未指定，則埠號預設為1813。
- timeout *timeout* — 130
- retransmit *retries* — 指定重試重新傳輸的次數。範圍為1-15。
- deadtime *deadtime* — 指定事務請求跳過RADIUS伺服器的時間長度（以分鐘為單位）。範圍從0到2000。
- key *key-string* — 為裝置和RADIUS伺服器之間的所有RADIUS通訊指定身份驗證和加密金鑰。此金鑰必須與RADIUS守護程式上使用的加密匹配。要指定空字串，請輸入「」。長度可以是0到128個字元。如果省略此引數，將使用全域性配置的radius金鑰。
- key *encrypted-key-string* — 與key-string相同，但金鑰是加密格式。
- priority *priority* — 指定伺服器的使用順序，其中0具有最高的優先順序。優先順序範圍為0到65535。
- 用法{login|dot1.x|all} — 指定RADIUS伺服器用法型別。可能的值為：
    - login — 指定RADIUS伺服器用於使用者登入引數身份驗證。
    - dot1.x — 指定RADIUS伺服器用於802.1x埠身份驗證。

- all — 指定RADIUS伺服器用於使用者登入身份驗證和802.1x埠身份驗證。

在此示例中，僅使用host和key引數。我們將使用IP地址**192.168.1.100**作為RADIUS伺服器IP地址，使用**example**作為key-string。

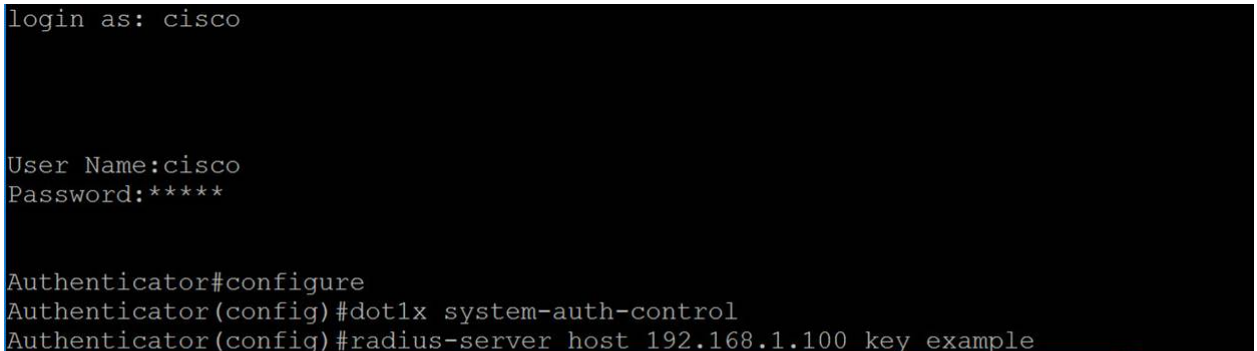


步驟5.在基於MAC的身份驗證中，請求方的使用者名稱基於請求方裝置MAC地址。以下內容定義身份驗證過程中從交換機傳送到RADIUS伺服器的基於MAC的使用者名稱的格式。以下欄位定義為：

- mac-auth type — 選擇MAC身份驗證型別
  - eap — 對交換機（RADIUS客戶端）和RADIUS伺服器（驗證基於MAC的請求方）之間的流量使用RADIUS和EAP封裝。
  - radius — 對交換器（RADIUS使用者端）和RADIUS伺服器之間的流量使用不含EAP封裝的RADIUS，RADIUS伺服器會驗證基於MAC的要求者。
- groupsize — 以使用者名稱傳送的MAC地址分隔符之間的ASCII字元數。選項是分隔符之間的1、2、4或12個ASCII字元。
- 分隔符 — 在MAC地址中定義的字元組之間用作分隔符的字元。選項包括連字元、冒號或點作為分隔符。
- case — 以大寫或小寫形式傳送使用者名稱。選項為小寫或大寫。

dot1x mac-auth

在本例中，我們將使用**eap**作為mac身份驗證型別，使用**2**的groupsize和**冒號**作為分隔符，並以大寫形式傳送使用者**名**。



步驟6.使用以下命令定義交換機將用於基於MAC的身份驗證的密碼，而不是主機MAC地址。我們將使用**example**一詞作為密碼。

```
login as: cisco



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)#
```

步驟7.要進入介面配置模式以配置介面，請使用**interface** Global Configuration mode命令。我們將配置GigabitEthernet1/0/1，因為我們的終端主機已連線到它。

附註： 請勿設定連線到RADIUS伺服器的連線埠。

```
login as: cisco



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)#
```

附註： 如果要同時配置多個埠，請使用interface range命令。

請參閱以下示例，使用range命令配置埠1-4:

步驟8.要在IEEE802.1X授權埠上允許一台主機（客戶端）或多個主機，請在介面配置模式下使用**dot1x host-mode**命令。引數定義為：

- 多主機 — 啟用多主機模式

  - 如果至少有一個授權客戶端，則埠是授權的。

  - 當連線埠未授權且訪客VLAN啟用時，未標籤的流量會重新對映到訪客VLAN。除非標籤的流量屬於訪客VLAN或屬於未經驗證的VLAN，否則會將其捨棄。如果在連線埠上未啟用訪客VLAN，則只會橋接屬於未經驗證VLAN的已標籤流量。

  - 當連線埠獲得授權時，會根據靜態VLAN成員身分連線埠組態，橋接來自連線到連線埠的所有主機的未標籤且已標籤的流量。

  - 您可以指定來自授權連線埠的未標籤流量會在驗證過程中重新對映到RADIUS伺服器指派的VLAN。除非標籤的流量屬於RADIUS指定的VLAN或未經驗證的VLAN，否則該流量會遭到捨棄。連線埠上的RADIUS VLAN分配在「*Port Authentication*」頁面中設定。

- 單主機 — 啟用單主機模式

  - 如果存在經授權的客戶端，則埠是經授權的。一個埠上只能授權一台主機。

  - 當連線埠未授權且訪客VLAN啟用時，未標籤的流量會重新對映到訪客VLAN。除非標籤的流量屬於訪客VLAN或屬於未經驗證的VLAN，否則會將其捨棄。如果在連線埠上未啟用訪客VLAN，則只會橋接屬於未經驗證VLAN的已標籤流量。

  - 當連線埠獲得授權時，來自授權主機的未標籤和已標籤流量會根據靜態VLAN成員身分連線埠組態橋接。來自其他主機的流量將被丟棄。

  - 使用者可以指定來自授權主機的未標籤流量在身份驗證過程中重新對映到RADIUS伺服器分配的VLAN。除非標籤的流量屬於RADIUS指派的VLAN或未經驗證的VLAN，否則會將其捨棄。連線埠上的RADIUS VLAN分配在「*Port Authentication*」頁面中設定。

- multi-sessions — 啟用多會話模式

  - 與單主機和多主機模式不同，多會話模式下的埠沒有身份驗證狀態。此狀態會指派給連線到連線埠的每個使用者端。

  - 無論主機是否獲得授權，都會橋接屬於未經驗證的VLAN的已標籤流量。

  - 來自非屬於未驗證VLAN的未授權主機的已標籤和未標籤流量如果已在VLAN上定義並啟用，則會重新對映到訪客VLAN；如果訪客VLAN未在埠上啟用，則會丟棄該流量。

  - 您可以指定來自授權連線埠的未標籤流量會在驗證過程中重新對映到RADIUS伺服器指派的VLAN。除非標籤的流量屬於RADIUS指定的VLAN或未經驗證的VLAN，否則該流量會遭到捨棄。在*Port Authentication*頁面中設定了埠上的RADIUS VLAN分配。

在本例中，我們將主機模式配置為多會話。

```
login as: cisco




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
```

步驟9.要在埠上配置身份驗證方法，請使用以下命令啟用基於MAC的身份驗證。

```
login as: cisco



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)#
```

步驟10.要在裝置上啟用基於埠的身份驗證和授權，請使用**port-control**命令配置埠控制值。我們將選擇管理埠授權狀態為**自動**。這將允許我們在裝置上啟用基於埠的身份驗證和授權。介面根據裝置與客戶端之間的身份驗證交換在授權或未經授權的狀態之間移動。

```
login as: cisco



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)#
```

步驟11。（可選）要結束當前配置會話並返回特權執行模式，請使用**end**命令。

```
login as: cisco



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
```

步驟12.（可選）要將任何檔案從源複製到目標，請在特權EXEC模式下使用**copy**命令。在本例中，我們將運行配置儲存到啟動配置。

```
login as: cisco



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] ?
```

步驟13.（可選）系統會顯示訊息，並詢問您是否要覆寫啟動組態檔。輸入**Y**表示yes，輸入**N**表示no。我們將鍵入**Y**覆蓋啟動配置檔案。

```


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#
```

結論

現在，您應該已經使用CLI在交換機上配置了基於MAC的身份驗證。按照以下步驟驗證基於MAC的身份驗證是否正常工作。

步驟1。要顯示裝置的活動802.1X授權使用者，請在特權EXEC模式下使用**show dot1x users**命令。

```
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
```

步驟2.要顯示802.1X介面或指定的介面狀態，請在特權EXEC模式下使用**show dot1x**命令。

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

Authentication is enabled
Authenticator Global Configuration:
Authenticating Servers: Radius
MAC-Based Authentication:
  Type: Eap
  Username Groupsize: 2
  Username Separator: :
  Username case: Uppercase
  Password: MD5 checksum 1a79a4d60de6718e8e5b326e338ae533
Unauthenticated VLANs:
Authentication failure traps are disabled
Authentication success traps are disabled
Authentication quiet traps are disabled
Supplicant Global Configuration:
Supplicant Authentication success traps are disabled
Supplicant Authentication failure traps are disabled

gi1/0/1
 Authenticator is enabled
 Supplicant is disabled
 Authenticator Configuration:
 Host mode: multi-sessions
 Authentication methods: mac
 Port Administrated Status: auto
 Guest VLAN: disabled
 VLAN Radius Attribute: disabled
 Open access: disabled
 Server timeout: 30 sec
 Maximum Hosts: unlimited
 Maximum Login Attempts: 0
 Reauthentication is disabled
 Reauthentication period: 3600 sec
 Silence period: 0 sec
 Quiet period: 60 sec
 Interfaces 802.1X-Based Parameters
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  Max req: 2
 Authentication success: 1
 Authentication fails: 0
 Number of Authorized Hosts: 1
```