通過CLI配置交換機上的全域性802.1x屬性

簡介

IEEE 802.1x標準便於客戶端和伺服器之間的訪問控制。在本地存取網路(LAN)或交換器可向使用者端提供服務之前，連線到交換器連線埠的使用者端必須透過執行遠端驗證撥入使用者服務(RADIUS)的驗證伺服器進行驗證。

802.1x身份驗證限制未經授權的客戶端通過可公開訪問的埠連線到LAN。802.1x身份驗證是客戶端 — 伺服器模型。在此模型中，網路裝置具有以下特定角色：

- 客戶端或請求方 — 客戶端或請求方是請求訪問LAN的網路裝置。客戶端連線到身份驗證器。
- 驗證器 — 驗證器是提供網路服務並將請求埠連線的網路裝置。支援以下身份驗證方法：

  — 基於802.1x — 所有身份驗證模式都支援。在基於802.1x的身份驗證中，身份驗證器從802.1x消息或EAP over LAN(EAPoL)資料包中提取可擴展身份驗證協定(EAP)消息，並使用RADIUS協定將其傳遞到身份驗證伺服器。

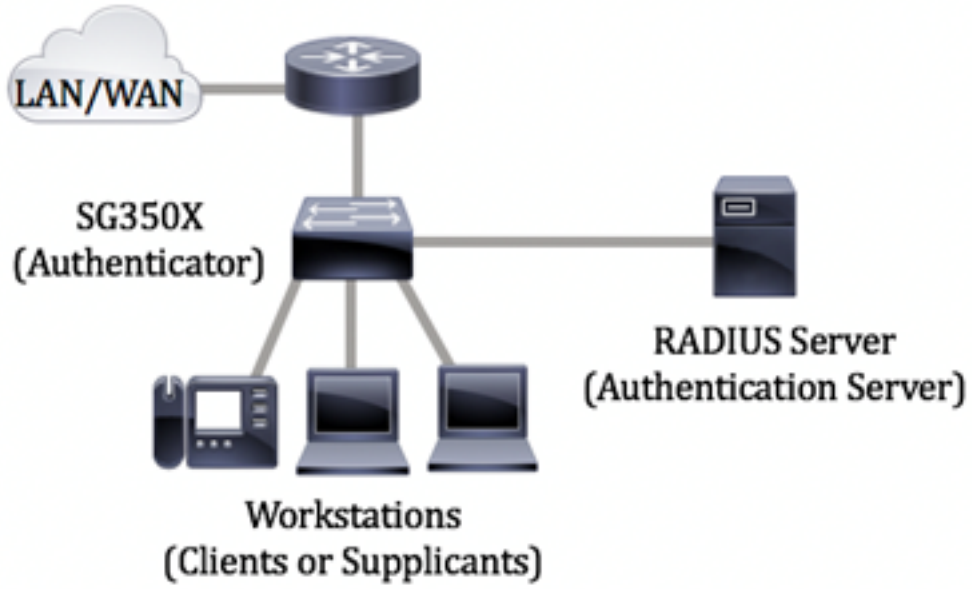
  — 基於MAC — 所有身份驗證模式都支援。基於媒體訪問控制(MAC)，驗證器本身代表尋求網路訪問的客戶端執行軟體的EAP客戶端部分。

  — 基於Web — 僅在多會話模式下支援。使用基於Web的身份驗證，身份驗證器本身代表尋求網路訪問的客戶端執行軟體的EAP客戶端部分。

- 身份驗證伺服器 — 身份驗證伺服器執行客戶端的實際身份驗證。裝置的身份驗證伺服器是具有EAP擴展的RADIUS身份驗證伺服器。

附註：網路裝置可以是客戶端，也可以是請求方、驗證方，或者每個埠都可以。

下圖顯示了根據特定角色配置裝置的網路。本示例使用SG350X交換機。



指南 在 配置802.1x:

1. 設定RADIUS伺服器。若要瞭解如何配置交換機上的RADIUS伺服器設定，請按一下此處。
2. 設定虛擬區域網路(VLAN)。 要使用交換機的基於Web的實用程式建立VLAN，請按一下此

處。有關基於CLI的說明，請按一下此處。
3. 在交換機上配置埠到VLAN設定。要使用基於Web的實用程式進行配置，請按一下此處。要使用CLI，請按一下此處。
4. 在交換機上配置全域性802.1x屬性。有關如何通過交換機的基於Web的實用程式配置全域性802.1x屬性的說明，請按一下此處。
5. （可選）在交換機上配置時間範圍。若要瞭解如何配置交換機上的時間範圍設定，請按一下此處。
6. 配置802.1x埠身份驗證。要使用交換機的基於Web的實用程式，請按一下此處。

目標

本文提供如何透過交換器的指令行介面(CLI)設定全域802.1x屬性的說明，其中包括驗證和訪客VLAN屬性。訪客VLAN提供對不需要通過802.1x、基於MAC或基於Web的身份驗證對訂閱裝置或埠進行身份驗證和授權的服務的訪問。

適用裝置

- Sx300系列
- Sx350系列
- SG350X系列
- Sx500系列
- Sx550X系列

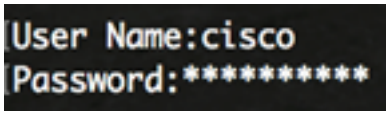
軟體版本

- 1.4.7.06 — Sx300、Sx500
- 2.2.8.04 — Sx350、SG350X、Sx550X

通過CLI配置交換機上的802.1x屬性

配置802.1x設定

步驟1.登入到交換機控制檯。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。



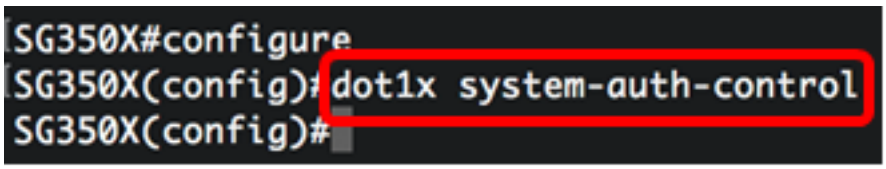
附註：這些命令可能會因交換機的確切型號而異。在本示例中，通過Telnet訪問SG350X交換機。

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：

```
SG350x#configure
```

步驟3.要在交換機上全域性啟用802.1x身份驗證，請在全域性配置模式下使用**dot1x system-auth-control**命令。

```
SG350x(config)#dotx1 system-auth-control
```



步驟4.（可選）要在交換機上全域性禁用802.1x身份驗證，請輸入以下命令：

```
SG350x(config)#no dotx1 system-auth-control
```

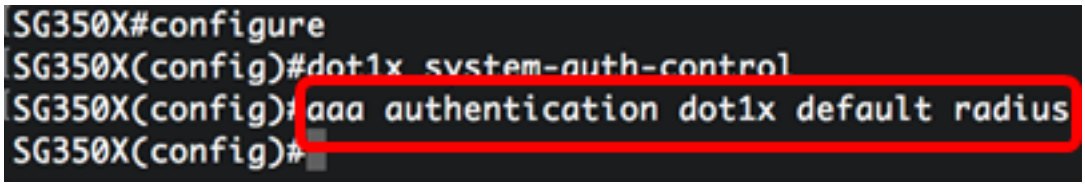
附註：如果禁用此功能，則會禁用802.1X、基於MAC的身份驗證和基於網路的身份驗證。

步驟5.要在啟用802.1x身份驗證時指定哪些伺服器用於身份驗證，請輸入以下內容：

```
SG350x(config)#aaa authentication dot1x default [radius none | radius |]
```

選項包括：

- radius none — 此操作將首先在RADIUS伺服器的幫助下執行埠身份驗證。如果沒有來自伺服器的響應（例如伺服器關閉時），則不執行身份驗證，並且允許會話。如果伺服器可用且使用者憑據不正確，則訪問將被拒絕，會話將結束。
- radius — 此操作會根據RADIUS伺服器執行連線埠驗證。如果未執行身份驗證，則會話將終止。這是預設身份驗證。
- none — 不對使用者進行身份驗證並允許會話。



附註：在本示例中，預設的802.1x身份驗證伺服器是RADIUS。

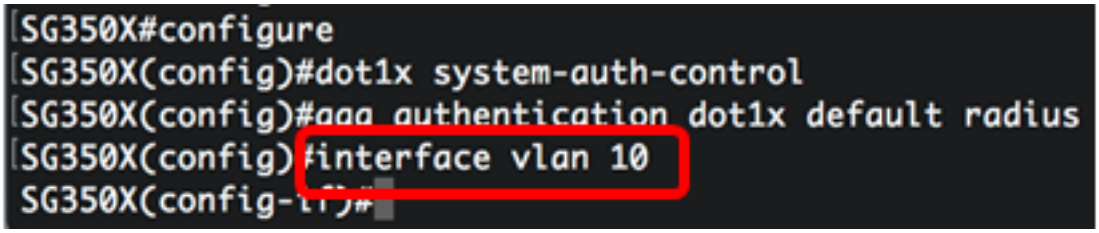
步驟6。（可選）要恢復預設身份驗證，請輸入以下內容：

```
SG350X(config)#no aaa authentication dot1x default
```

步驟7.在全域性配置模式下，通過輸入以下內容進入VLAN介面配置上下文：

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

- vlan-id — 指定要配置的VLAN ID。



步驟8.要對未經授權的埠啟用訪客VLAN，請輸入以下內容：

```
SG350X(config-if)#dot1x guest-vlan
```

附註：如果啟用訪客VLAN，所有未授權的埠將自動加入在訪客VLAN中選擇的VLAN。如果連線埠稍後獲得授權，則會將其從訪客VLAN中移除。

```
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)#
```

步驟9.要退出介面配置上下文，請輸入以下內容：

```
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)#
```

步驟10.要設定啟用802.1X（或埠啟動）和將埠新增到訪客VLAN之間的時間延遲，請輸入以下內容：

```
SG350X(config)#dot1x guest-vlan timeout [timeout]
```

- timeout — 指定啟用802.1X（或埠啟動）和將埠新增到訪客VLAN之間的時間延遲（以秒為單位）。範圍為30到180秒。

附註：連結後，如果軟體沒有偵測802.1x要求者或連線埠驗證失敗，則只有在訪客VLAN逾時期間到期後，才會將連線埠新增到訪客VLAN。如果連線埠從「已授權」變更為「未授權」，則只有在訪客VLAN逾時期間到期後，才會將連線埠新增到訪客VLAN。您可以從VLAN身份驗證啟用或禁用VLAN身份驗證。

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

附註：在本例中，使用的訪客VLAN超時為60秒。

步驟11.要啟用陷阱，請選中以下一個或多個選項：

```
SG350X(config)# dot1x traps authentication [failure | |] [802.1x | mac | web]
```

選項包括：

- 802.1x身份驗證失敗陷阱 — 如果802.1x身份驗證失敗，則傳送陷阱。
- 802.1x驗證成功陷阱 — 如果802.1x驗證成功，則傳送陷阱。
- mac authentication failure traps — 如果MAC身份驗證失敗，則傳送陷阱。
- mac authentication success traps — 如果MAC身份驗證成功，則傳送陷阱。
- web驗證失敗陷阱 — 如果Web驗證失敗，則傳送陷阱。
- web驗證成功陷阱 — 如果Web驗證成功，則傳送陷阱。
- web驗證安靜陷阱 — 如果開始進入安靜週期，則傳送陷阱。

附註：在此示例中，輸入了802.1x身份驗證失敗和成功陷阱。

```
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)#
```

步驟12.要退出介面配置上下文，請輸入以下內容：

```
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#
```

步驟13。（可選）要在交換機上顯示已配置的全域性802.1x屬性，請輸入以下內容：

```
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
```

現在，您應該在交換機上成功配置802.1x屬性。

設定VLAN驗證

啟用802.1x時，除非未經授權的埠或裝置是訪客VLAN或未經身份驗證VLAN的一部分，否則不允許這些埠或裝置訪問VLAN。需要將埠手動新增到VLAN。

要在VLAN上禁用身份驗證，請執行以下步驟：

步驟1.在交換機的特權EXEC模式下，輸入以下命令進入全域性配置模式：

```
SG350X#configure
```

步驟2.在全域性配置模式下，通過輸入以下內容進入VLAN介面配置上下文：

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

- vlan-id — 指定要配置的VLAN ID。

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#
```

附註：在本範例中，選擇VLAN 20。

步驟3.要在VLAN上禁用802.1x身份驗證，請輸入以下命令：

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

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#dot1x auth-not-req
SG350X(config-if)#
```

步驟4.（可選）要在VLAN上啟用802.1x身份驗證，請輸入以下內容：

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

步驟5.要退出介面配置上下文，請輸入以下內容：

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#dot1x auth-not-req
SG350X(config-if)#end
SG350X#
```

步驟6。（可選）要在交換機上顯示802.1x全域性身份驗證設定，請輸入以下內容：

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

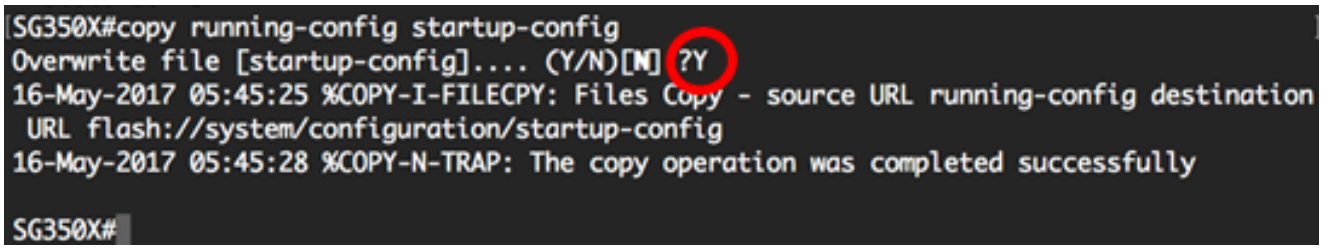
附註：在本範例中，VLAN 20顯示為未驗證的VLAN。

步驟7.（可選）在交換機的特權EXEC模式下，輸入以下命令，將配置的設定儲存到啟動配置檔案中：

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

```
SG350X#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?
```

步驟8.（可選）出現Overwrite file [startup-config]...提示後，在鍵盤上按**Y**選擇「Yes」，或按**N**選擇「No」。



現在，您應該已經成功地在交換機上的VLAN上配置了802.1x身份驗證設定。

重要事項：要繼續配置交換機上的802.1x埠身份驗證設定，請遵循上述准則。