通过CLI在交换机上配置全局802.1x属性

简介

IEEE 802.1x是一种标准，可促进客户端和服务器之间的访问控制。在通过本地接入网络(LAN)或交换机向客户端提供服务之前，连接到交换机端口的客户端必须由运行远程身份验证拨入用户服务(RADIUS)的身份验证服务器进行身份验证。

802.1x身份验证限制未授权客户端通过可公开访问的端口连接到LAN。802.1x身份验证是客户端 — 服务器模型。在此模型中，网络设备具有以下特定角色：

- 客户端或请求方 — 客户端或请求方是请求访问LAN的网络设备。客户端已连接到身份验证器。
- 身份验证器 — 身份验证器是提供网络服务并连接了请求方端口的网络设备。支持以下身份验证方法：

  — 基于802.1x — 在所有身份验证模式下均受支持。在基于802.1x的身份验证中，身份验证器从802.1x消息或LAN上EAP(EAPoL)数据包中提取可扩展身份验证协议(EAP)消息，然后使用RADIUS协议将其传递到身份验证服务器。

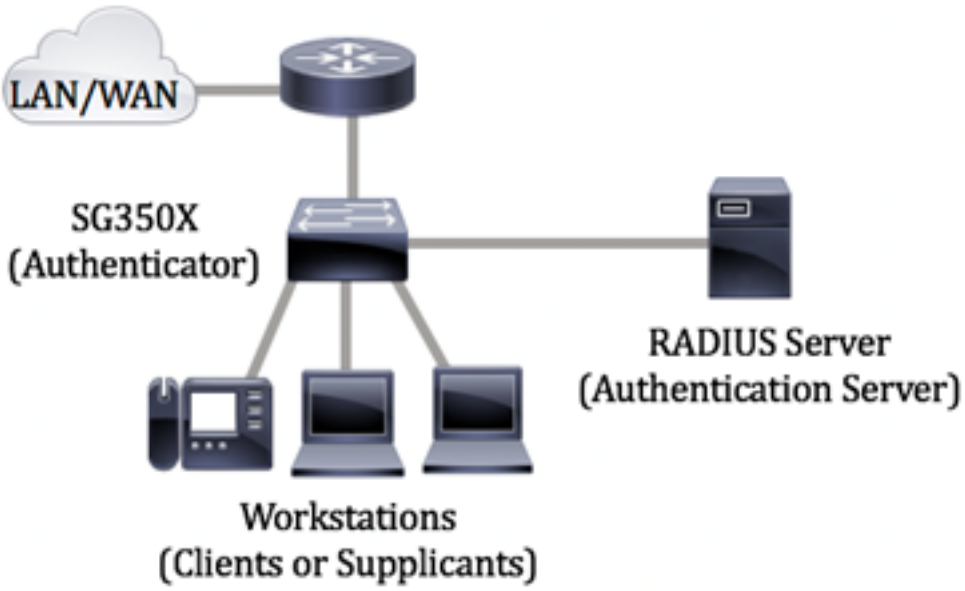
  — 基于MAC — 在所有身份验证模式中均受支持。使用基于媒体访问控制(MAC)的身份验证器，身份验证器本身代表寻求网络访问的客户端执行软件的EAP客户端部分。

  — 基于Web — 仅在多会话模式下受支持。使用基于Web的身份验证，身份验证器本身代表寻求网络访问的客户端执行软件的EAP客户端部分。

- 身份验证服务器 — 身份验证服务器执行客户端的实际身份验证。设备的身份验证服务器是具有EAP扩展的RADIUS身份验证服务器。

注意：网络设备可以是客户端或请求方、身份验证器，也可以是每个端口的两者。

下图显示根据特定角色配置设备的网络。在本例中，使用SG350X交换机。



准则 在 配置802.1x:

1. 配置 RADIUS 服务器。要了解如何在交换机上配置RADIUS服务器设置，请单击此处。

2. 配置虚拟局域网(VLAN)。 要使用交换机的基于Web的实用程序创建VLAN，请单击此处。有关基于CLI的说明，请单击此处。
3. 在交换机上配置端口到VLAN设置。要使用基于Web的实用程序进行配置，请单击此处。要使用CLI，请单击此处。
4. 在交换机上配置全局802.1x属性。有关如何通过交换机的基于Web的实用程序配置全局802.1x属性的说明，请单击此处。
5. （可选）在交换机上配置时间范围。要了解如何在交换机上配置时间范围设置，请单击此处。
6. 配置802.1x端口身份验证。要使用交换机的基于Web的实用程序，请单击此处。

目标

本文提供有关如何通过交换机的命令行界面(CLI)配置全局802.1x属性的说明，包括身份验证和访客VLAN属性。访客VLAN提供对服务的访问，这些服务不需要通过802.1x、基于MAC或基于Web的身份验证对订阅设备或端口进行身份验证和授权。

适用设备

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

软件版本

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

通过CLI在交换机上配置802.1x属性

配置802.1x设置

步骤1.登录交换机控制台。默认用户名和密码为cisco/cisco。如果已配置新的用户名或密码，请改为输入凭证。

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

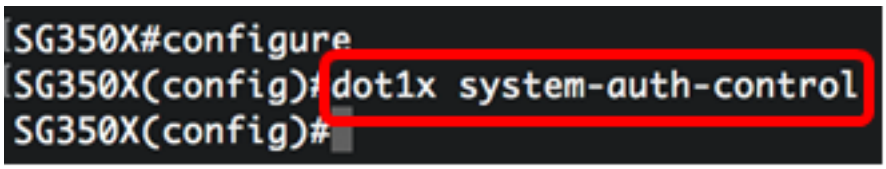
注意：命令可能因交换机的确切型号而异。在本例中，SG350X交换机通过Telnet访问。

步骤2.在交换机的特权执行模式下，输入以下命令进入全局配置模式：

```
SG350x#
```

步骤3.要在交换机上全局启用802.1x身份验证，请在全局配置模式下使用**dot1x system-auth-control**命令。

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



步骤4.（可选）要在交换机上全局禁用802.1x身份验证，请输入以下命令：

```
SG350x#no dotx1 –  –
```

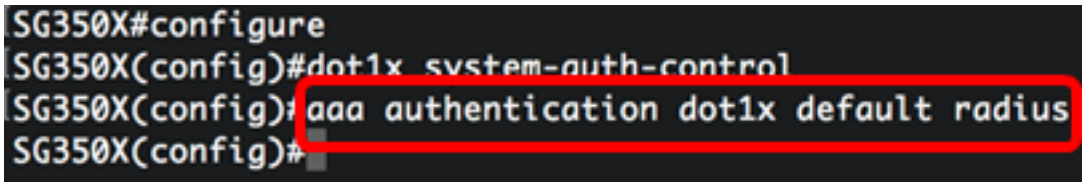
注意：如果禁用此功能，则禁用802.1X、基于MAC和基于Web的身份验证。

步骤5.要指定启用802.1x身份验证时用于身份验证的服务器，请输入以下命令：

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

选项有：

- radius none — 这首先在RADIUS服务器的帮助下执行端口身份验证。如果服务器没有响应，例如服务器关闭时，则不执行身份验证，并允许会话。如果服务器可用且用户凭证不正确，则会拒绝访问并结束会话。
- radius — 根据RADIUS服务器执行端口身份验证。如果未执行身份验证，则会终止会话。这是默认身份验证。
- none — 不对用户进行身份验证并允许会话。



注意：在本例中，默认802.1x身份验证服务器是RADIUS。

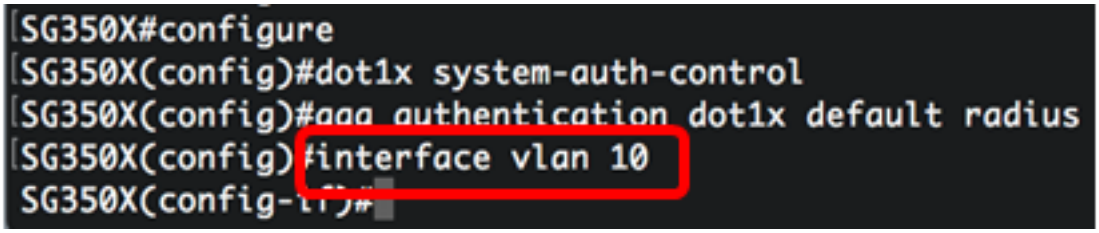
步骤6.（可选）要恢复默认身份验证，请输入以下命令：

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

步骤7.在全局配置模式下，输入以下命令进入VLAN接口配置情景：

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

- vlan-id — 指定要配置的VLAN ID。



步骤8.要启用对未授权端口的访客VLAN，请输入以下命令：

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

注意：如果启用了访客VLAN，所有未授权端口将自动加入访客VLAN中选择的VLAN。如果端口稍后获得授权，则会从访客VLAN中删除该端口。

```
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)#
```

步骤9.要退出接口配置上下文，请输入以下命令：

```
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)#
```

步骤10.要设置启用802.1X（或端口打开）和将端口添加到访客VLAN之间的时间延迟，请输入以下命令：

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

- timeout — 指定启用802.1X（或端口打开）和将端口添加到访客VLAN之间的时间延迟（以秒为单位）。范围为30到180秒。

注意：链路建立后，如果软件未检测到802.1x请求方，或者如果端口身份验证失败，则仅在访客VLAN超时期限到期后，才将端口添加到访客VLAN。如果端口从“已授权”(Authorized)更改为“未授权”(Not Authorized)，则只有在访客VLAN超时期限到期后，端口才会添加到访客VLAN。您可以从VLAN身份验证启用或禁用VLAN身份验证。

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

注意：在本例中，使用的访客VLAN超时为60秒。

步骤11.要启用陷阱，请选中以下一个或多个选项：

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

选项有：

- 802.1x身份验证失败陷阱 — 如果802.1x身份验证失败，则发送陷阱。
- 802.1x身份验证成功陷阱 — 如果802.1x身份验证成功，则发送陷阱。
- mac authentication failure traps — 如果MAC身份验证失败，则发送陷阱。
- mac authentication success traps — 如果MAC身份验证成功，则发送陷阱。
- Web身份验证失败陷阱 — 如果Web身份验证失败，则发送陷阱。
- Web身份验证成功陷阱 — 如果Web身份验证成功，则发送陷阱。
- Web身份验证静默陷阱 — 如果静默期开始，则发送陷阱。

注意：在本例中，输入802.1x身份验证失败和成功陷阱。

```
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)#
```

步骤12.要退出接口配置上下文，请输入以下命令：

```
SG350X#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#
```

步骤13.（可选）要显示交换机上已配置的全局802.1x属性，请输入以下命令：

```
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
```

现在，您应该已成功配置交换机上的802.1x属性。

配置VLAN身份验证

启用802.1x后，除非未授权端口或设备是访客VLAN或未经身份验证的VLAN的一部分，否则不允许它们访问VLAN。需要手动将端口添加到VLAN。

要在VLAN上禁用身份验证，请执行以下步骤：

步骤1.在交换机的特权执行模式下，输入以下命令进入全局配置模式：

```
SG350X#configure
```

步骤2.在全局配置模式下，输入以下命令进入VLAN接口配置情景：

```
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)#
```

注意：在本例中，选择VLAN 20。

步骤3.要在VLAN上禁用802.1x身份验证，请输入以下命令：

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

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

步骤4.（可选）要在VLAN上启用802.1x身份验证，请输入以下命令：

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

步骤5.要退出接口配置上下文，请输入以下命令：

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

步骤6.（可选）要显示交换机上的802.1x全局身份验证设置，请输入以下命令：

```
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
```

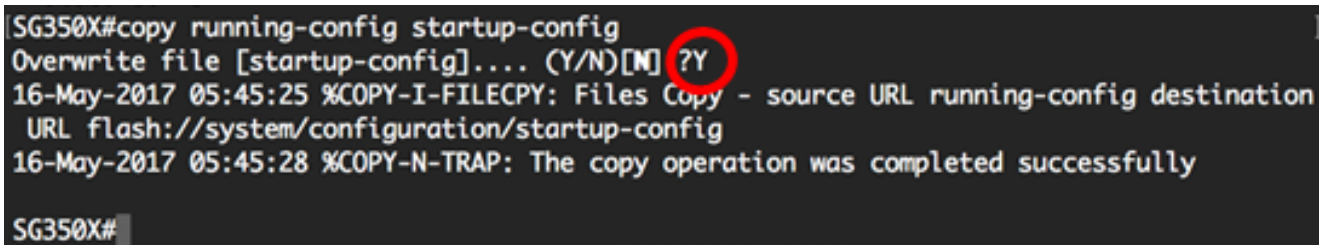
注意：在本例中，VLAN 20显示为未经身份验证的VLAN。

步骤7.（可选）在交换机的特权执行模式下，输入以下命令，将配置的设置保存到启动配置文件：

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

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

第8步。（可选）出现“Overwrite file [startup-config].....”提示**后，**在键盘上按Y表示“Yes”或**N表示**“No”。



现在，您应该已在交换机的VLAN上成功配置了802.1x身份验证设置。

重要信息：要继续在交换机上配置802.1x端口身份验证设置，请遵循上述指南。