通过命令行界面在交换机上配置基于MAC的身份验证

目标

802.1X是允许列出设备的管理工具，可确保不未经授权访问您的网络。本文档介绍如何使用命令行界面(CLI)在交换机上配置基于MAC的身份验证。

有关其他信息，请参阅词汇表。

RADIUS 如何工作？

802.1X身份验证有三个主要组件：请求方（客户端）、身份验证器(网络设备（如交换机）和身份验证服务器(RADIUS)。 远程身份验证拨入用户服务(RADIUS)是使用身份验证、授权和记帐(AAA)协议的接入服务器，帮助管理静态IP地址为192.168.1.100，身份验证器的静态IP地址为192.168.1.101。

适用设备

- SX350X系列
- SG350XG系列
- Sx550X 系列
- SG550XG系列

软件版本

- 2.4.0.94

在交换机上配置RADIUS服务器

步骤1.通过SSH连接到您的交换机，该交换机将成为RADIUS服务器。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。

注意： 要了解如何通过SSH或Telnet访问SMB交换机，请单击 这里。

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：

步骤3.使用radius server **enable命**令启用RADIUS服务器。

```
login as: cisco



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


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

步骤4.要创建密钥，请在全局配置**模式下使用radius server** nas secret key命令。参数定义为：

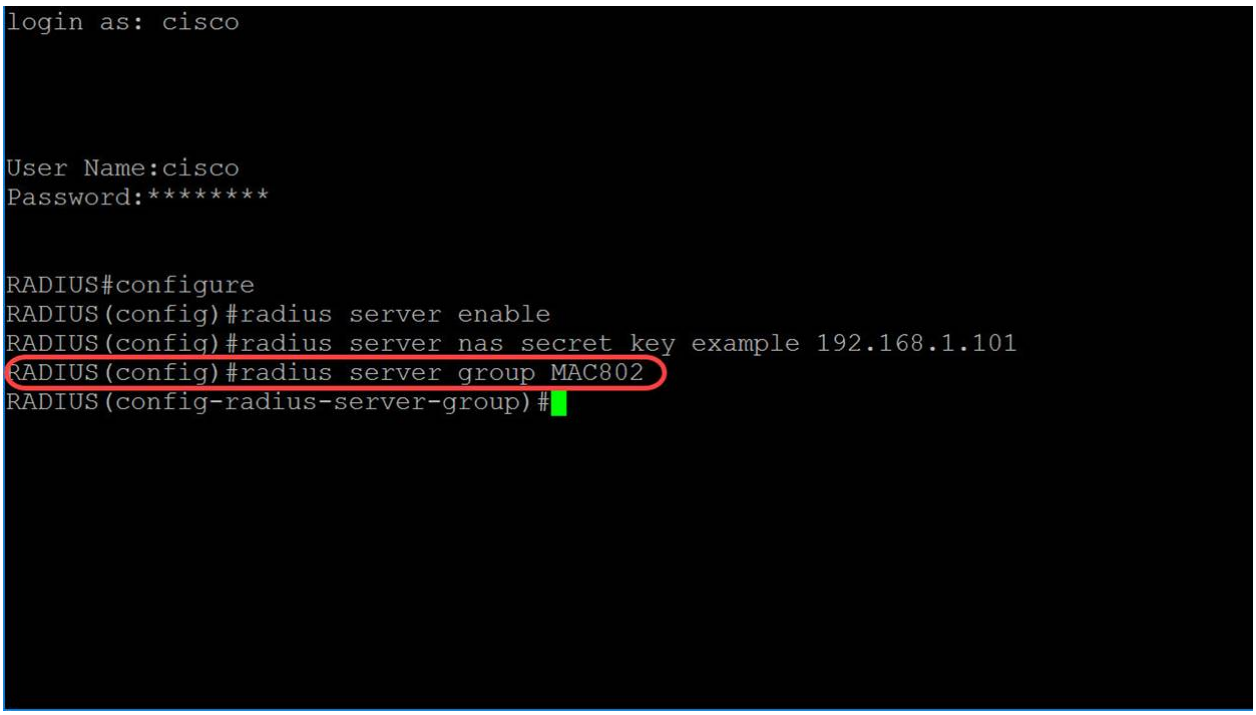
- key — 指定设备与给定组用户之间的通信的身份验证和加密密钥。此范围为0到128个字符。
- default — 指定将用于与没有私钥的NAS通信的默认密钥。
- ip-address — 指定RADIUS客户端主机IP地址。IP地址可以是IPv4、IPv6或IPv6z地址。

在本例中，我们将使用**example**作为密钥，**192.168.1.101**作为身份验证器的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)#
```

步骤5.要进入RADIUS服务器组配置模式并创建组（如果组不存在），请在全局配置模式下使用radius server group命令。

在本文中，我们将使用**MAC802**作为组名。



步骤6.要创建用户，请在全局配**置模式下**使用radius server user命令。参数定义为：

- user-name — 指定用户名。长度为1-32个字符。
- group-name — 指定用户组名称。组名称的长度为1到32个字符。
- unencrypted-password — 指定用户密码。长度可以是1到64个字符。

在本例中，我们将使用以太网端口的MAC地址作为用户名,**MAC802**作为*组名*,**未加密口令**作为示例。

注意： MAC地址中的某些二进制八位数已模糊。密码**示例**不是强密码。请使用更强的密码，因为这仅用作示例。另请注意，图中的命令过长，它自动封装了命令。

```
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)#
```

步骤7.（可选）要结束当前配置会话并返回特权EXEC模式，请使用**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#
```

步骤8.（可选）要将任何文件从源复制到目标，请在特权EXEC模式下使用**copy**命令。在本例中，我们将将运行配置保存到启动配置。

```
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] ?
```

步骤9.（可选）系统将显示一条消息，询问您是否要覆盖启动配置文件。键入**Y**表示是，键入N表示否。我们将键入**Y**以覆盖启动配置文件。

```
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#
```

配置身份验证器交换机

步骤1.对将要成为身份验证器的交换机执行SSH。默认用户名和密码为cisco/cisco。如果已配置新的用户名或密码，请输入这些凭证。

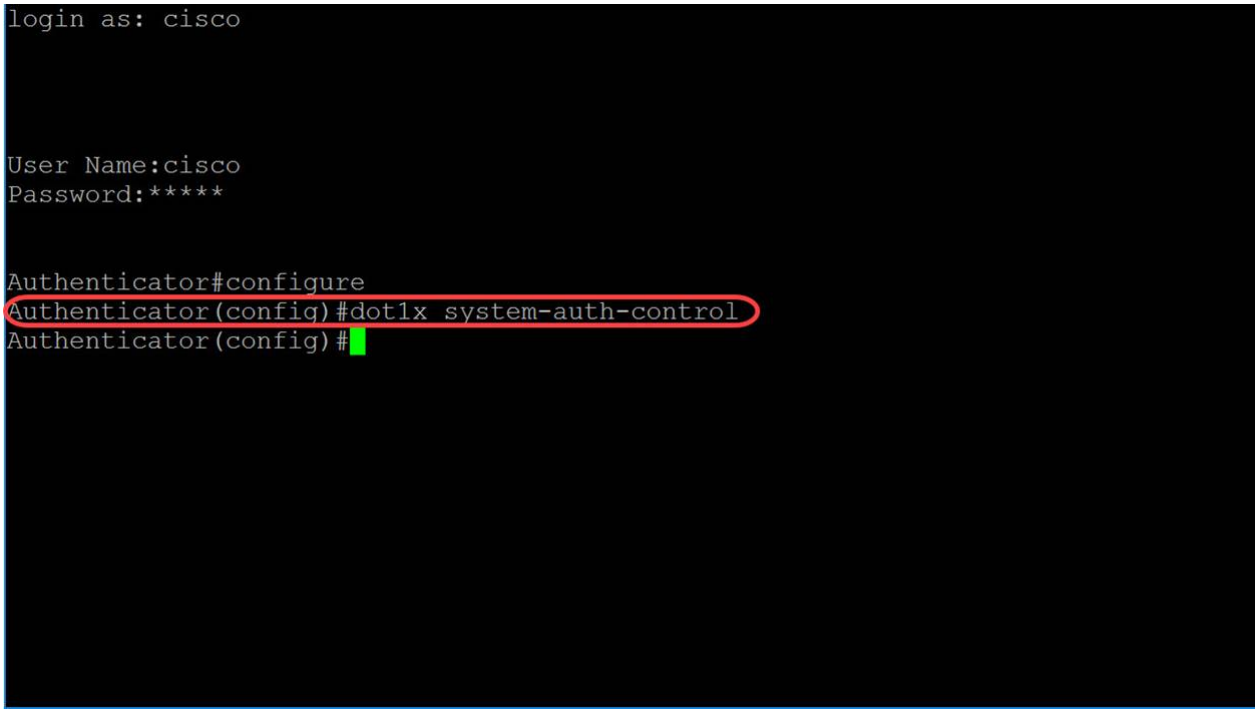
注意： 要了解如何通过SSH或Telnet访问SMB交换机，请单击 这里。

```
login as: cisco



User Name:cisco
Password:*****


Authenticator#
```

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：

```
login as: cisco



User Name:cisco
Password:*****


Authenticator#configure
```

步骤3.要全局启用802.1X，请在全局配置模式下使用dot1x system-auth-control命令。

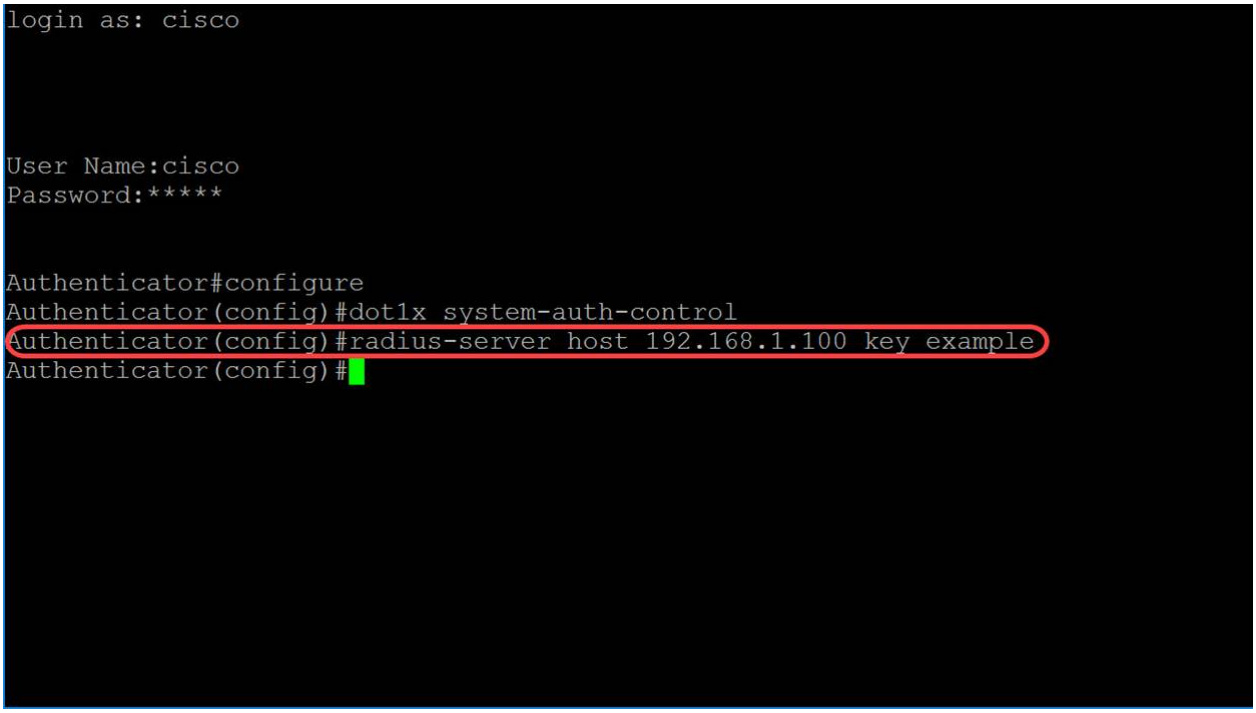


步骤4.使用radius-server **host全局配**置模式命令配置RADIUS服务器主机。参数定义为：

- ip-address — 指定RADIUS服务器主机IP地址。IP地址可以是IPv4、IPv6或IPv6z地址。
- hostname — 指定RADIUS服务器主机名。仅支持转换到IPv4地址。长度为1-158个字符，主机名各部分的最大标签长度为63个字符。
- auth-port *auth-port-number* — 指定身份验证请求的端口号。如果端口号设置为0，则主机不用于身份验证。范围为0-65535。
- Acc-port *acct-port-number* — 记帐请求的端口号。如果设置为0，则主机不用于记账。如果未指定，则端口号默认为1813。
- timeout *timeout* — 1-30
- retransmit *retries* — 指定重试重新传输的次数。范围为1-15。
- deadtime *deadtime* — 指定事务请求跳过RADIUS服务器的时间长度（以分钟为单位）。范围为0到2000。
- key *key-string* — 指定设备和RADIUS服务器之间所有RADIUS通信的身份验证和加密密钥。此密钥必须与RADIUS守护程序上使用的加密匹配。要指定空字符串，请输入“”。长度可以是0到128个字符。如果省略此参数，则使用全局配置的RADIUS密钥。
- key *encrypted-key-string* — 与key-string相同，但密钥采用加密格式。
- priority *priority* — 指定服务器的使用顺序，其中0具有最高优先级。优先级范围为0-65535。
- usage {login|dot1.x|all} — 指定RADIUS服务器使用类型。可能的值为：
  - login — 指定RADIUS服务器用于用户登录参数身份验证。
  - dot1.x — 指定RADIUS服务器用于802.1x端口身份验证。

- all — 指定RADIUS服务器用于用户登录身份验证和802.1x端口身份验证。

在本例中，仅使用主机和密钥参数。我们将使用IP地址**192.168.1.100**作为RADIUS服务器IP地址，**单词**example作为密钥字符串。

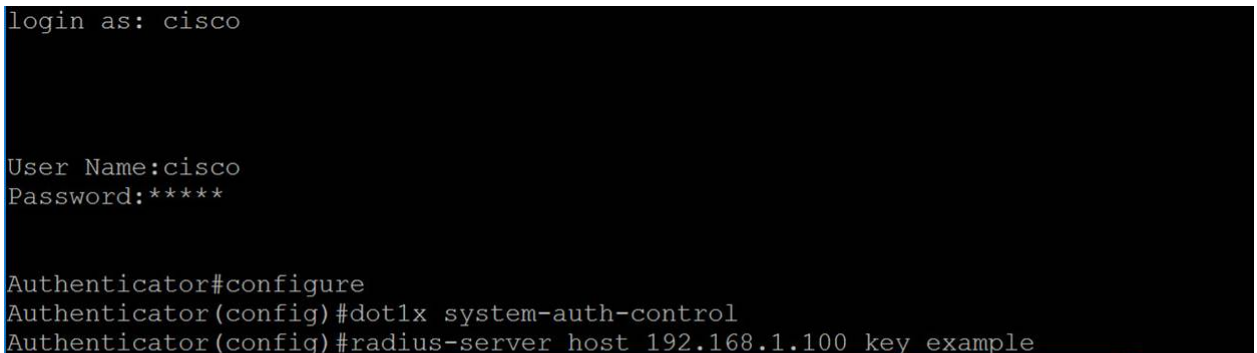


步骤5.在基于MAC的身份验证中，请求方的用户名基于请求方设备的MAC地址。以下内容定义了此基于MAC的用户名的格式，该用户名从交换机发送到RADIUS服务器，作为身份验证过程的一部分。以下字段定义为：

- mac-auth type — 选择MAC身份验证类型
  - eap — 对交换机（RADIUS客户端）和RADIUS服务器（对基于MAC的请求方进行身份验证）之间的流量使用RADIUS和EAP封装。
  - radius — 对交换机（RADIUS客户端）和RADIUS服务器（对基于MAC的请求方进行身份验证）之间的流量使用不带EAP封装的RADIUS。
- groupsize — 作为用户名发送的MAC地址的分隔符之间的ASCII字符数。选项是分隔符之间的1、2、4或12个ASCII字符。
- 分隔符 — 用作MAC地址中定义的字符组之间的分隔符的字符。选项是连字符、冒号或点作为分隔符。
- case — 以小写或大写发送用户名。选项为小写或大写。

dot1x mac-auth

在本示例中，我们将使用**eap**作为我们的mac-authentication类型，使用**2**的组大小、**冒号**作为分隔符，并以大写形式发送我们的用户**名**。



步骤6.使用以下命令定义交换机将用于基于MAC的身份验证而不是主机MAC地址的密码。我们将使用单词example作为密码。

```
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)#
```

步骤7.要进入接口配置模式以配置接口，请使用**interface** Global Configuration mode命令。我们将配置GigabitEthernet1/0/1，因为我们的终端主机已连接到它。

注意： 请勿配置连接到RADIUS服务器的端口。

```
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)#
```

注意： 如果要同时配置多个端口，请使用interface range命令。

请参阅以下示例，使用range命令配置端口1-4:

步骤8.要允许IEEE802.1X授权端口上的单个主机（客户端）或多个主机，请在接口配置模式下使用**dot1x host-mode**命令。参数定义为：

- 多主机 — 启用多主机模式
  - 如果至少有一个授权客户端，则端口会被授权。
  - 当端口未授权且启用访客VLAN时，无标记流量将重新映射到访客VLAN。除非标记流量属于访客VLAN或未经身份验证的VLAN，否则将丢弃该流量。如果端口上未启用访客VLAN，则只桥接属于未经身份验证的VLAN的标记流量。
  - 当端口被授权时，会根据静态VLAN成员端口配置桥接来自连接到端口的所有主机的无标记和有标记流量。
  - 您可以指定来自授权端口的无标记流量将重新映射到身份验证过程中由RADIUS服务器分配的VLAN。除非标记流量属于RADIUS分配的VLAN或未经身份验证的VLAN，否则将丢弃该流量。端口上的Radius VLAN分配在端口*身份验证页*中设置。
- 单主机 — 启用单主机模式
  - 如果有授权的客户端，则端口被授权。一个端口上只能有一台主机获得授权。
  - 当端口未授权且启用访客VLAN时，无标记流量将重新映射到访客VLAN。除非标记流量属于访客VLAN或未经身份验证的VLAN，否则将丢弃该流量。如果端口上未启用访客VLAN，则只桥接属于未经身份验证的VLAN的标记流量。
  - 当端口被授权时，来自授权主机的未标记和已标记流量会根据静态VLAN成员端口配置进行桥接。来自其他主机的流量将被丢弃。
  - 用户可以指定在身份验证过程中，来自授权主机的无标记流量将重新映射到由RADIUS服务器分配的VLAN。除非标记流量属于RADIUS分配的VLAN或未经身份验证的VLAN，否则将丢弃该流量。端口上的Radius VLAN分配在端口*身份验证页*中设置。
- 多会话 — 启用多会话模式
  - 与单主机和多主机模式不同，多会话模式中的端口没有身份验证状态。此状态分配给连接到端口的每个客户端。
  - 无论主机是否已授权，属于未经身份验证的VLAN的标记流量都始终会桥接。
  - 来自非未经身份验证的VLAN的未授权主机的已标记和未标记流量在VLAN上定义和启用时重新映射到访客VLAN，或在端口上未启用访客VLAN时丢弃。
  - 您可以指定来自授权端口的无标记流量将重新映射到身份验证过程中由RADIUS服务器分配的VLAN。除非标记流量属于RADIUS分配的VLAN或未经身份验证的VLAN，否则将丢弃该流量。端口上的Radius VLAN分配在端口*身份验证页*中设置。

在本例中，我们将主机模式配置为多会话。

```
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
```

步骤9.要在端口上配置身份验证方法，请使用以下命令启用基于MAC的身份验证。

```
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)#
```

步骤10.要在设备上启用基于端口的身份验证和授权，请使用**port-control** 命令配置端口控制值。我们将选择管理端口授权状态为**auto**。这将允许我们在设备上启用基于端口的身份验证和授权。接口根据设备和客户端之间的身份验证交换在授权或未授权状态之间移动。

```
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)#
```

步骤11.（可选）要结束当前配置会话并返回特权EXEC模式，请使用**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
```

步骤12.（可选）要将任何文件从源复制到目标，请在特权EXEC模式下使用**copy**命令。在本例中，我们将将运行配置保存到启动配置。

```
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] ?
```

步骤13.（可选）系统将显示一条消息，询问您是否要覆盖启动配置文件。键入**Y**表示是，**键**入N表示否。我们将键入**Y**以覆盖启动配置文件。

```
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#
```

结论

您现在应该已使用CLI在交换机上配置基于MAC的身份验证。按照以下步骤验证基于MAC的身份验证是否正常工作。

步骤1.要显示设备的活动802.1X授权用户，请在特权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
```

步骤2.要显示802.1X接口或指定的接口状态，请在特权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
```