Configure 802.1x Supplicant Credentials on a Switch through the CLI

Introduction

IEEE 802.1x is a standard which facilitates access control between a client and a server. Before services can be provided to a client by a Local Area Network (LAN) or switch, the client connected to the switch port has to be authenticated by the authentication server which runs Remote Authentication Dial-In User Service (RADIUS).

The 802.1x authentication restricts unauthorized clients from connecting to a LAN through publicly-accessible ports. The 802.1x authentication is a client-server model. In this model, network devices have the following specific roles:

- Client or supplicant — A client or supplicant is a network device that requests access to the LAN. The client is connected to an authenticator.
- Authenticator — An authenticator is a network device that provides network services and to which supplicant ports are connected. The following authentication methods are supported:

  - 802.1x-based — Supported in all authentication modes. In 802.1x-based authentication, the authenticator extracts the Extensible Authentication Protocol (EAP) messages from the 802.1x messages or EAP over LAN (EAPoL) packets, and passes them to the authentication server, using the RADIUS protocol.

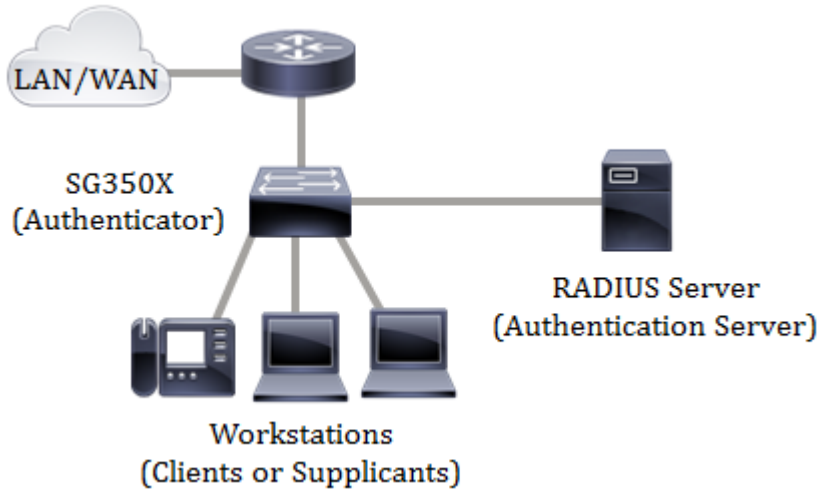
  - MAC-based — Supported in all authentication modes. With Media Access Control (MAC)-based, the authenticator itself executes the EAP client part of the software on behalf of the clients seeking network access.

  - Web-based — Supported only in multi-sessions modes. With web-based authentication, the authenticator itself executes the EAP client part of the software on behalf of the clients seeking network access.

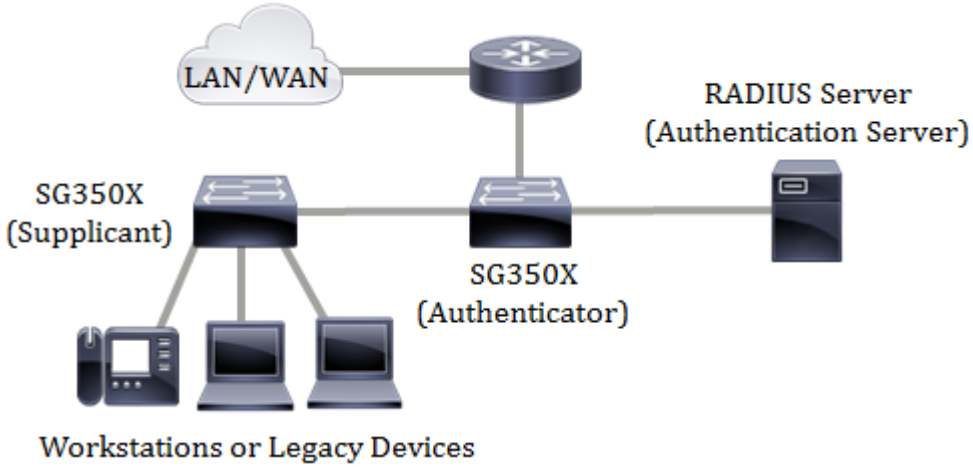
- Authentication server — An authentication server performs the actual authentication of the client. The authentication server for the device is a RADIUS authentication server with EAP extensions.

Note: A network device can be either a client or supplicant, authenticator, or both per port.

The image below displays a network that have configured the devices according to the specific roles. In this example, an SG350X switch is used.



However, you can also configure some ports on your switch as supplicants. Once the supplicant credentials are configured on a specific port on your switch, you can directly connect the devices that are not 802.1x-capable so the devices would be able to access the secured network. The image below shows a scenario of a network that has configured a switch as a supplicant.



Guidelines in configuring 802.1x:

1. Configure the RADIUS server. To learn how to configure the RADIUS server settings on your switch, click here.
2. Create a Virtual Local Area Network (VLAN). To create VLANs using the web-based utility of your switch, click here. For Command Line Interface (CLI)-based instructions, click here.
3. Configure Port to VLAN settings on your switch. To configure using the web-based utility, click here. To use the CLI, click here.
4. Configure the global 802.1x properties on the switch. For instructions on how to configure the global 802.1x properties through the web-based utility of the switch, click here. For CLI-based instructions, click here.
5. (Optional) Configure Time Range on the switch. To learn how to configure time range settings on your switch, click here. To use the CLI, click here.
6. Configure 802.1x supplicant credentials on the switch. To learn how to configure through the web-based utility, click here.The CLI-based instructions are provided in this article.
7. Configure 802.1x Port Authentication. To use the web-based utility of the switch, click here. To use the CLI, click here.

Objective

You can configure the switch as an 802.1x supplicant (client) on the wired network. An encrypted user name and password can be configured to allow the switch to authenticate using 802.1x.

On the networks that use IEEE 802.1x port-based network access control, a supplicant cannot gain access to the network until the 802.1x authenticator grants access. If your network uses 802.1x, you must configure 802.1x authentication information on the switch so that it can supply the information to the authenticator.

This article provides instructions on how to configure 802.1x supplicant credentials on your switch through the CLI.

Applicable Devices

- Sx350X Series
- SG350X Series
- SG550X Series

Software Version

- 2.3.0.130

Configure 802.1x Supplicant Credentials

Create 802.1x Supplicant Credentials

Step 1. Log in to the switch console. The default username and password is cisco/cisco. If you have configured a new username or password, enter the credentials instead.

Note: To learn how to access an SMB switch CLI through SSH or Telnet, click here.

Note: The commands may vary depending on the exact model of your switch. In this example, the SG350X switch is accessed through Telnet.

Step 2. From the Privileged EXEC mode of the switch, enter the Global Configuration mode by entering the following:

```
SG350X#configure
```

Step 3. To define the name of an 802.1x credential structure and enter the dot1x credentials configuration mode, enter the following:

```
SG350X(config)#dot1x credentials [name]
```

- name — The credential structure name is up to 32 characters.

```
SG350X#configure
SG350X(config)#dot1x credentials cisco
SG350X(config-dot1x-cred)#
```

Note: The switch supports up to 24 credentials. In this example, cisco is used.

Step 4. (Optional) To remove the credential structure, enter the following:

```
SG350X(config)#no dot1x credentials [name]
```

Note: A used credential cannot be removed.

Step 5. To specify a username for an 802.1x credential structure, enter the following:

```
SG350X(config-dot1x-cred)#username [username]
```

- username—The user name is up to 32 characters.

```
SG350X#configure
SG350X(config)#dot1x credentials cisco
SG350X(config-dot1x-cred)#username switchuser
SG350X(config-dot1x-cred)#
```

Note: In this example, switchuser is the specified username.

Step 6. (Optional) To remove the username, enter the following:

```
SG350X(config-dot1x-cred)#no username
```

Step 7. To specify a password for an 802.1x credential structure, enter either of the following:

```
SG350X(config-dot1x-cred)#password [password]
```

```
SG350X(config-dot1x-cred)#encrypted password [encryptedpassword]
```

- encrypted password — The password is in encrypted format.
- password — You can enter a plaintext password of up to 64 characters.

```
SG350X#configure
SG350X(config)#dot1x credentials cisco
SG350X(config-dot1x-cred)#username switchuser
SG350X(config-dot1x-cred)#password C!$C0123456
SG350X(config-dot1x-cred)#
```

Note: In this example, the plaintext password C!$C0123456 is entered.

Step 8. (Optional) To remove the password, enter the following:

```
SG350X(config-dot1x-cred)#no password
```

Step 9. (Optional) To add a description for the 802.1x credential structure, enter the following:

```
SG350X(config-dot1x-cred)#description [description]
```

Note: In this example, the description used is sg350x-supplicant.

Step 10. (Optional) To remove the description, enter the following:

```
SG350X(config-dot1x-cred)#no description
```

Step 11. Enter the **end** command to go back to the Privileged EXEC mode:

```
SG350X#end
```

```
SG350X#configure
SG350X(config)#dot1x credentials cisco
SG350X(config-dot1x-cred)#username switchuser
SG350X(config-dot1x-cred)#password C!$C0123456
SG350X(config-dot1x-cred)#description sg350x-supplicant
SG350X(config-dot1x-cred)#end
SG350X#
```

Step 12. (Optional) To display the configured 802.1x credentials, enter the following:

```
SG350X#show dot1x credentials
```

```
SG350X#show dot1x credentials
cisco
 description: sg350x-supplicant
 username: switchuser
 password's MD5: 6385a9e24338d1428ccd55cd27714779
SG350X#
```

Step 13. (Optional) In the Privileged EXEC mode of the switch, save the configured settings to the startup configuration file by entering the following:

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

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

Step 14. (Optional) Press **Y** for Yes or **N** for No on your keyboard once the Overwrite file [startup-config]… prompt appears.

```
SG350X#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
11-Aug-2017 05:21:59 %COPY-I-FILECPY: Files Copy - source URL running-config
 destination URL flash://system/configuration/startup-config
11-Aug-2017 05:22:02 %COPY-N-TRAP: The copy operation was completed successf
ully

SG350X#
```

You should now have successfully configured an 802.1x credential on your switch through the CLI.

Configure an 802.1x Supplicant Interface

To apply the configured 802.1x supplicant credentials, you must configure 802.1x authentication information on the switch so that it can supply the information to the authenticator. Follow these steps to configure an 802.1x supplicant interface:

Step 1. From the Privileged EXEC mode of the switch, enter the Global Configuration mode by entering the following:

```
SG350X#configure
```

Step 2. In the Global Configuration mode, enter the Interface Configuration context by entering the following:

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

- interface-id — Specifies an interface ID to be configured.

```
SG350X#configure
SG350X(config)#interface ge1/0/19
SG350X(config-if)#
```

Note: When the supplicant is enabled on an interface, the interface becomes an unauthorized. In this example, interface ge1/0/19 is being configured.

Step 3. To enable the dot1x supplicant role for the interface, enter the following:

```
SG350X(config-if)#dot1x supplicant [name]
```

- name — The name of the credential structure applied on the interface.

```
SG350X#configure
SG350X(config)#interface ge1/0/19
SG350X(config-if)#dot1x supplicant cisco
SG350X(config-if)#
```

Note: In this example, the previously created credential name is used which is cisco.

Step 4. Enter the **end** command to go back to the Privileged EXEC mode:

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

```
SG350X#configure
SG350X(config)#interface ge1/0/19
SG350X(config-if)#dot1x supplicant cisco
SG350X(config-if)#end
SG350X#
```

Step 5. To display the 802.1x status for the configured interface, use the **show dot1x** command in Privileged EXEC mode:

```
SG350X#show dot1x interface [interface-id]
```

- interface-id — Specifies the Ethernet port.

```
SG350X#show dot1x interface ge1/0/19

Authentication is enabled
Authenticator Global Configuration:
Authenticating Servers: Radius
Unauthenticated VLANs:
Guest VLAN: VLAN 60, timeout: immediately
Authentication failure traps are enabled for 802.1x, mac, web
Authentication success traps are enabled for 802.1x, mac, web
Authentication quiet traps are enabled
Supplicant Global Configuration:
Supplicant Authentication success traps are enabled
Supplicant Authentication failure traps are enabled

gi1/0/19
 Authenticator is disabled
 Supplicant is enabled
 Authenticator Configuration:
 Host mode: multi-host
 Authentication methods: 802.1X
 Port Administrated Status: force-authorized
 Guest VLAN: enabled
 VLAN Radius Attribute: enabled, static
 Open access: enabled
 Time-range name: Dayshift (Active now)
 Server timeout: 30 sec
 Port Operational Status: authorized
 Reauthentication is enabled
 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: 0
 Authentication fails: 0
 Supplicant Configuration:
 retry-max: 2
 EAP time period: 30
 Supplicant Held Period: 60
 Credentials Name: cisco
 Supplicant Operational status: unauthorized

SG350X#
```

Note: In this example, the 802.1x information for interface ge1/0/19 is displayed.

You should now have successfully configured an 802.1x supplicant on an interface on your switch through the CLI.