Configurer les propriétés 802.1x globales sur un commutateur via l'interface de ligne de commande

Introduction

IEEE 802.1x est une norme qui facilite le contrôle d'accès entre un client et un serveur. Avant que les services puissent être fournis à un client par un réseau local (LAN) ou un commutateur, le client connecté au port du commutateur doit être authentifié par le serveur d'authentification qui exécute le service d'utilisateur RADIUS (Remote Authentication Dial-In User Service).

L'authentification 802.1x empêche les clients non autorisés de se connecter à un réseau local via des ports accessibles au public. L'authentification 802.1x est un modèle client-serveur. Dans ce modèle, les périphériques réseau ont les rôles spécifiques suivants :

- Client ou demandeur : un client ou demandeur est un périphérique réseau qui demande l'accès au réseau local. Le client est connecté à un authentificateur.
- Authentificateur : un authentificateur est un périphérique réseau qui fournit des services réseau et auquel les ports du demandeur sont connectés. Les méthodes d'authentification suivantes sont prises en charge :

  - Basé sur 802.1x — Pris en charge dans tous les modes d'authentification. Dans l'authentification basée sur 802.1x, l'authentificateur extrait les messages EAP (Extensible Authentication Protocol) des messages 802.1x ou des paquets EAPoL (EAPoL) et les transmet au serveur d'authentification, à l'aide du protocole RADIUS.

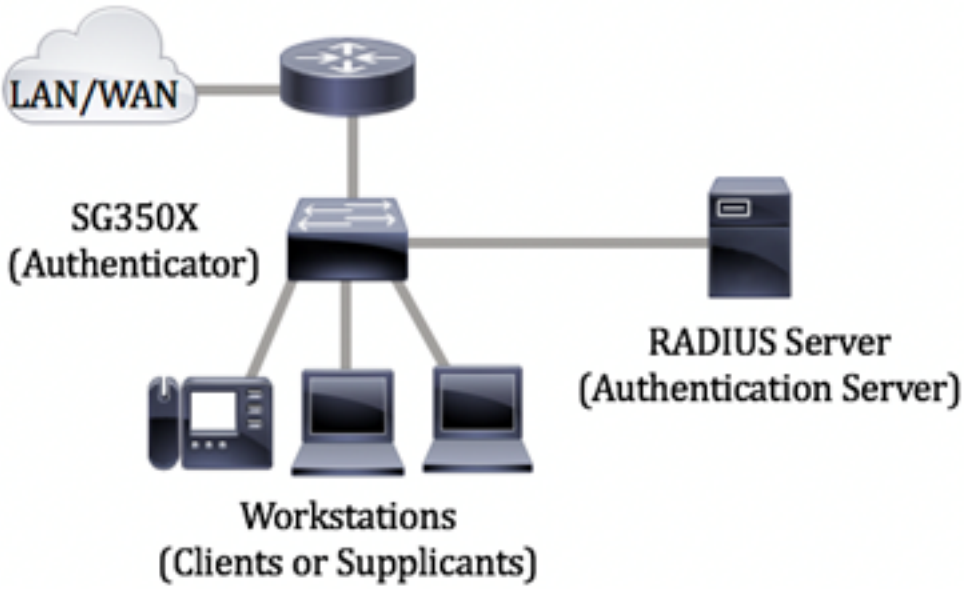
  - Basé sur MAC — Pris en charge dans tous les modes d'authentification. Avec le contrôle d'accès au support (MAC), l'authentificateur exécute lui-même la partie client EAP du logiciel au nom des clients qui cherchent à accéder au réseau.

  - Web : pris en charge uniquement en mode multisessions. Avec l'authentification basée sur le Web, l'authentificateur exécute lui-même la partie client EAP du logiciel au nom des clients qui cherchent à accéder au réseau.

- Serveur d'authentification : un serveur d'authentification effectue l'authentification réelle du client. Le serveur d'authentification du périphérique est un serveur d'authentification RADIUS avec des extensions EAP.

  Note: Un périphérique réseau peut être un client ou un demandeur, un authentificateur ou les deux par port.

  L'image ci-dessous affiche un réseau qui a configuré les périphériques en fonction des rôles spécifiques. Dans cet exemple, un commutateur SG350X est utilisé.



Directives dans configuration de 802.1x::

1. Configurez le serveur RADIUS. Pour savoir comment configurer les paramètres du serveur RADIUS sur votre commutateur, cliquez ici.
2. Configurez les réseaux locaux virtuels (VLAN). Pour créer des VLAN à l'aide de l'utilitaire Web de votre commutateur, cliquez ici. Pour obtenir des instructions basées sur l'interface de ligne de commande, cliquez ici.
3. Configurez les paramètres Port to VLAN sur votre commutateur. Pour configurer à l'aide de l'utilitaire Web, cliquez ici. Pour utiliser l'interface de ligne de commande, cliquez ici.
4. Configurez les propriétés globales 802.1x sur le commutateur. Pour obtenir des instructions sur la configuration des propriétés 802.1x globales via l'utilitaire Web du commutateur, cliquez ici.
5. (Facultatif) Configurez la plage de temps sur le commutateur. Pour savoir comment configurer les paramètres de plage de temps sur votre commutateur, cliquez ici.
6. Configurez l'authentification de port 802.1x. Pour utiliser l'utilitaire Web du commutateur, cliquez ici.

Objectif

Cet article explique comment configurer les propriétés 802.1x globales via l'interface de ligne de commande (CLI) du commutateur, qui incluent l'authentification et les propriétés VLAN invité. Le VLAN invité fournit un accès aux services qui ne nécessitent pas l'authentification et l'autorisation des périphériques ou des ports d'abonnement via l'authentification 802.1x, MAC ou Web.

Périphériques pertinents

- Série Sx300
- Gamme Sx350
- Gamme SG350X
- Série Sx500
- Gamme Sx550X

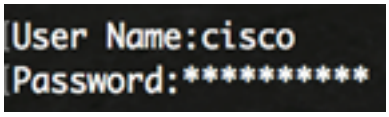
Version du logiciel

- 1.4.7.06 - Sx300, Sx500
- 2.2.8.04 - Sx350, SG350X, Sx550X

Configurer les propriétés 802.1x sur un commutateur via l'interface de ligne de commande

Configuration des paramètres 802.1x

Étape 1. Connectez-vous à la console du commutateur. Le nom d'utilisateur et le mot de passe par défaut sont cisco/cisco. Si vous avez configuré un nouveau nom d'utilisateur ou mot de passe, saisissez plutôt les informations d'identification.



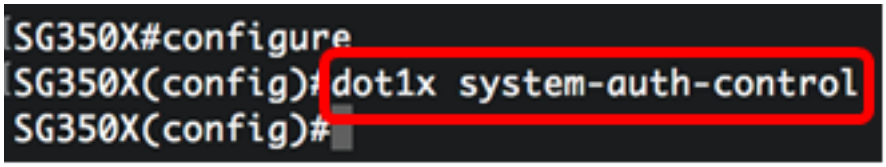
Note: Les commandes peuvent varier en fonction du modèle exact de votre commutateur. Dans cet exemple, le commutateur SG350X est accessible via Telnet.

Étape 2. À partir du mode d'exécution privilégié du commutateur, passez en mode de configuration globale en entrant ce qui suit :

```
SG350x#configure
```

Étape 3. Pour activer globalement l'authentification 802.1x sur le commutateur, utilisez la commande **dot1x system-auth-control** en mode Configuration globale.

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



Étape 4. (Facultatif) Pour désactiver globalement l'authentification 802.1x sur le commutateur, saisissez ce qui suit :

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

Note: Si cette option est désactivée, les authentifications 802.1X, MAC et Web sont désactivées.

Étape 5. Pour spécifier les serveurs utilisés pour l'authentification lorsque l'authentification 802.1x est activée, saisissez ce qui suit :

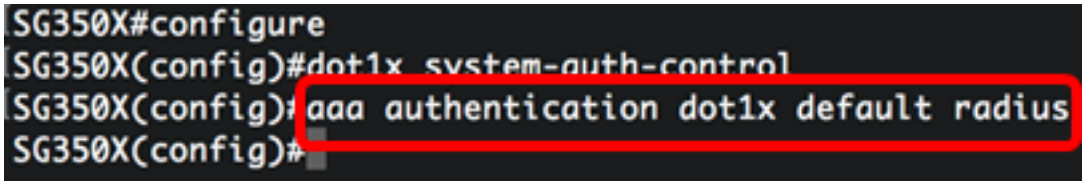
```
SG350x(config)#aaa authentication dot1x default [radius none | rayon | aucun]
```

Les options sont les suivantes :

- radius none : effectue d'abord l'authentification du port à l'aide du serveur RADIUS. Si le serveur ne répond pas, par exemple lorsque le serveur est en panne, aucune authentification

n'est effectuée et la session est autorisée. Si le serveur est disponible et que les informations d'identification de l'utilisateur sont incorrectes, l'accès est refusé et la session est terminée.

- radius : effectue l'authentification du port en fonction du serveur RADIUS. Si aucune authentification n'est effectuée, la session est interrompue. Il s'agit de l'authentification par défaut.
- none : n'authentifie pas l'utilisateur et autorise la session.



Note: Dans cet exemple, le serveur d'authentification 802.1x par défaut est RADIUS.

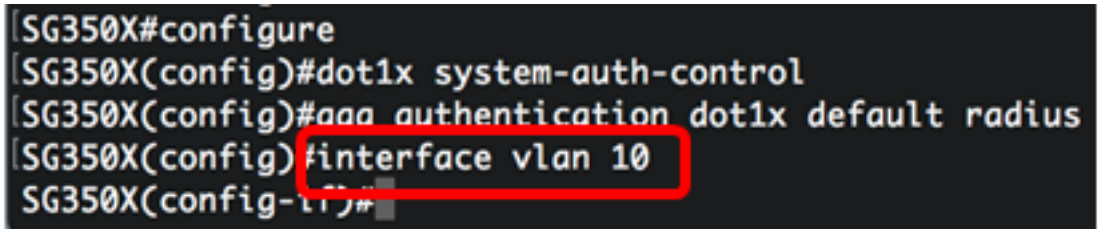
Étape 6. (Facultatif) Pour restaurer l'authentification par défaut, saisissez ce qui suit :

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

Étape 7. En mode de configuration globale, saisissez le contexte de configuration de l'interface VLAN en entrant les informations suivantes :

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

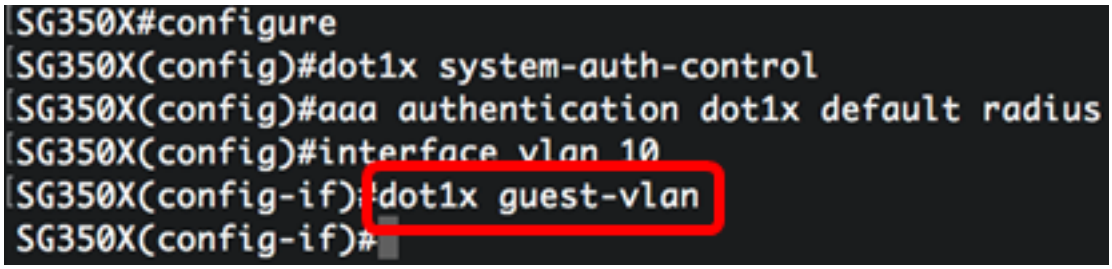
- vlan-id : spécifie un ID VLAN à configurer.



Étape 8. Pour activer l'utilisation d'un VLAN invité pour les ports non autorisés, saisissez ce qui suit :

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

Note: Si un VLAN invité est activé, tous les ports non autorisés rejoignent automatiquement le VLAN sélectionné dans le VLAN invité. Si un port est autorisé ultérieurement, il est supprimé du VLAN invité.



Étape 9. Pour quitter le contexte de configuration d'interface, saisissez ce qui suit :

```
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)#
```

Étape 10. Pour définir le délai entre l'activation de la norme 802.1X (ou le port actif) et l'ajout d'un port au VLAN invité, saisissez ce qui suit :

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

- timeout : spécifie le délai en secondes entre l'activation de la norme 802.1X (ou port up) et l'ajout du port au VLAN invité. La plage est comprise entre 30 et 180 secondes.

Note: Après la liaison, si le logiciel ne détecte pas de demandeur 802.1x ou si l'authentification du port a échoué, le port est ajouté au VLAN invité uniquement après l'expiration du délai d'expiration du VLAN invité. Si le port passe de Authorized à Not Authorized, le port est ajouté au VLAN invité uniquement après l'expiration du délai d'expiration du VLAN invité. Vous pouvez activer ou désactiver l'authentification VLAN à partir de l'authentification VLAN.

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

Note: Dans cet exemple, le délai d'attente du VLAN invité utilisé est de 60 secondes.

Étape 11. Pour activer les interruptions, sélectionnez une ou plusieurs des options suivantes :

```
SG350X(config)# dot1x piège l'authentification [échec | succès | tranquille] [802.1x | mac | Web]
```

Les options sont les suivantes :

- Interruptions d'échec d'authentification 802.1x — Envoyez des interruptions si l'authentification 802.1x échoue.
- Interruptions de réussite de l'authentification 802.1x — Envoyez des interruptions si l'authentification 802.1x réussit.
- pièges d'échec d'authentification mac : envoi de pièges en cas d'échec de l'authentification MAC.
- pièges de réussite de l'authentification mac : envoi de pièges si l'authentification MAC réussit.
- pièges d'échec d'authentification Web — Envoyez des pièges si l'authentification Web échoue.
- pièges de réussite de l'authentification Web — Envoyez des pièges si l'authentification Web réussit.
- pièges silencieux d'authentification Web — Envoyez des pièges si une période de silence commence.

Note: Dans cet exemple, l'échec de l'authentification 802.1x et les pièges de réussite sont

entrés.

```
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)#
```

Étape 12. Pour quitter le contexte de configuration d'interface, saisissez ce qui suit :

```
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#
```

Étape 13. (Facultatif) Pour afficher les propriétés 802.1x globales configurées sur le commutateur, saisissez ce qui suit :

```
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
```

Vous devez maintenant avoir correctement configuré les propriétés 802.1x sur votre commutateur.

Configurer l'authentification VLAN

Lorsque 802.1x est activé, les ports ou périphériques non autorisés ne sont pas autorisés à accéder au VLAN à moins qu'ils ne fassent partie du VLAN invité ou d'un VLAN non authentifié. Les ports doivent être ajoutés manuellement aux VLAN.

Pour désactiver l'authentification sur un VLAN, procédez comme suit :

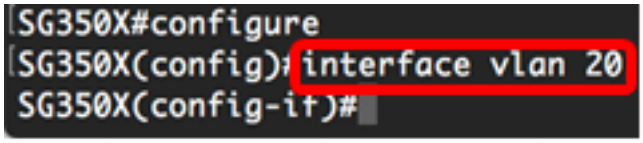
Étape 1. À partir du mode d’exécution privilégié du commutateur, passez en mode de configuration globale en entrant ce qui suit :

```
SG350X#configure
```

Étape 2. En mode de configuration globale, saisissez le contexte de configuration de l'interface VLAN en entrant les informations suivantes :

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

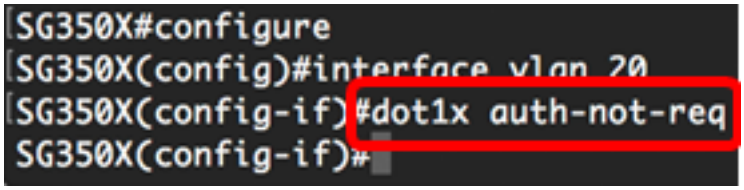
- vlan-id : spécifie un ID VLAN à configurer.



Note: Dans cet exemple, VLAN 20 est sélectionné.

Étape 3. Pour désactiver l'authentification 802.1x sur le VLAN, saisissez ce qui suit :

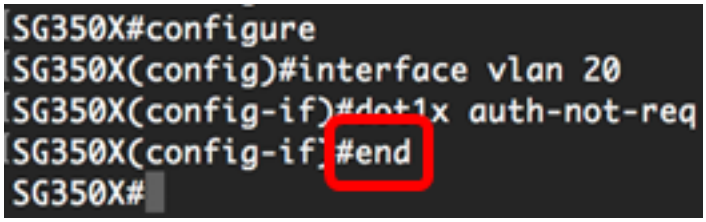
SG350X(config-if)#dot1x auth-not-req



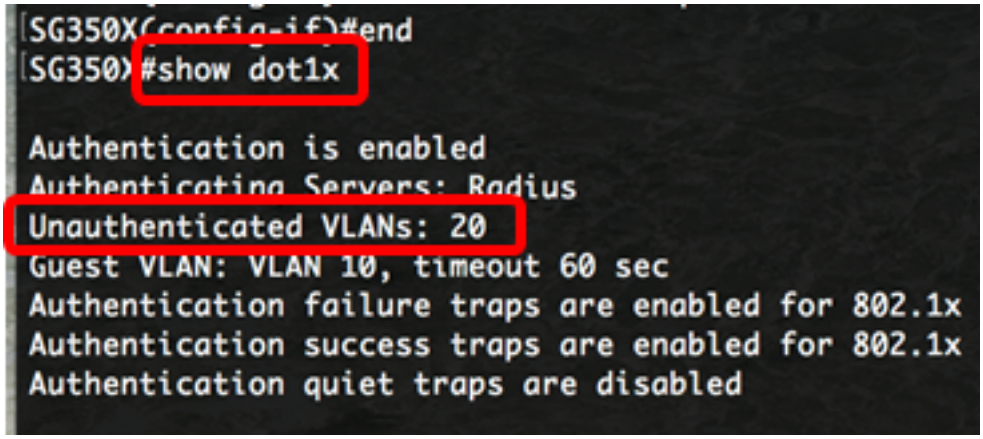
Étape 4. (Facultatif) Pour activer l'authentification 802.1x sur le VLAN, saisissez ce qui suit :

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

Étape 5. Pour quitter le contexte de configuration d'interface, saisissez ce qui suit :



Étape 6. (Facultatif) Pour afficher les paramètres d'authentification globale 802.1x sur le commutateur, saisissez ce qui suit :

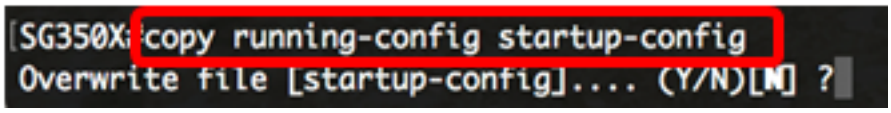


Note: Dans cet exemple, le VLAN 20 apparaît comme un VLAN non authentifié.

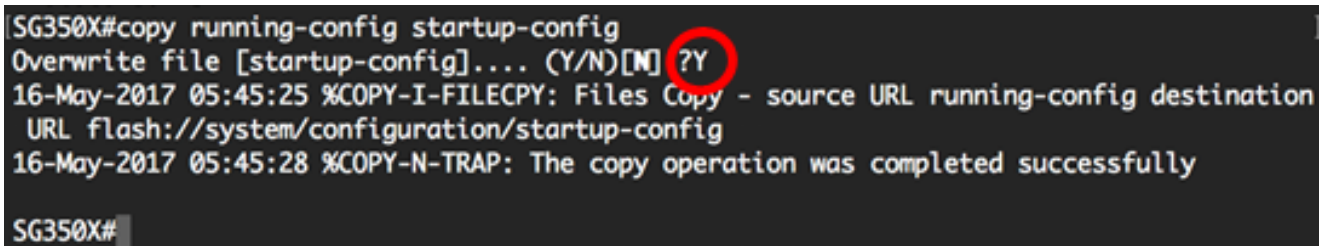
Étape 7. (Facultatif) Dans le mode d'exécution privilégié du commutateur, enregistrez les

paramètres configurés dans le fichier de configuration initiale, en saisissant ce qui suit :

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



Étape 8. (Facultatif) Appuyez sur **Y** pour Oui ou **N** pour Non sur votre clavier une fois que l'invite Overwrite file [startup-config]... s'affiche.



Vous devez maintenant avoir correctement configuré les paramètres d'authentification 802.1x sur les VLAN de votre commutateur.

Important : Pour continuer la configuration des paramètres d'authentification de port 802.1x sur votre commutateur, suivez les directives ci-dessus.