Configurar propriedades 802.1x globais em um switch através da CLI

Introduction

O IEEE 802.1x é um padrão que facilita o controle de acesso entre um cliente e um servidor. Antes que os serviços possam ser fornecidos a um cliente por uma LAN (Local Access Network, rede de acesso local) ou por um switch, o cliente conectado à porta do switch deve ser autenticado pelo servidor de autenticação que executa o RADIUS (Remote Authentication Dial-In User Service, serviço de usuário de discagem de autenticação remota).

A autenticação 802.1x restringe a conexão de clientes não autorizados a uma LAN através de portas acessíveis publicamente. A autenticação 802.1x é um modelo cliente-servidor. Neste modelo, os dispositivos de rede têm as seguintes funções específicas:

- Cliente ou requerente — Um cliente ou requerente é um dispositivo de rede que solicita acesso à LAN. O cliente está conectado a um autenticador.
- Autenticador — Um autenticador é um dispositivo de rede que fornece serviços de rede e ao qual as portas suplicantes estão conectadas. Os seguintes métodos de autenticação são suportados:

  - Baseado em 802.1x — Suportado em todos os modos de autenticação. Na autenticação baseada em 802.1x, o autenticador extrai as mensagens EAP (Extensible Authentication Protocol) das mensagens 802.1x ou dos pacotes EAP sobre LAN (EAPoL) e as passa para o servidor de autenticação, usando o protocolo RADIUS.

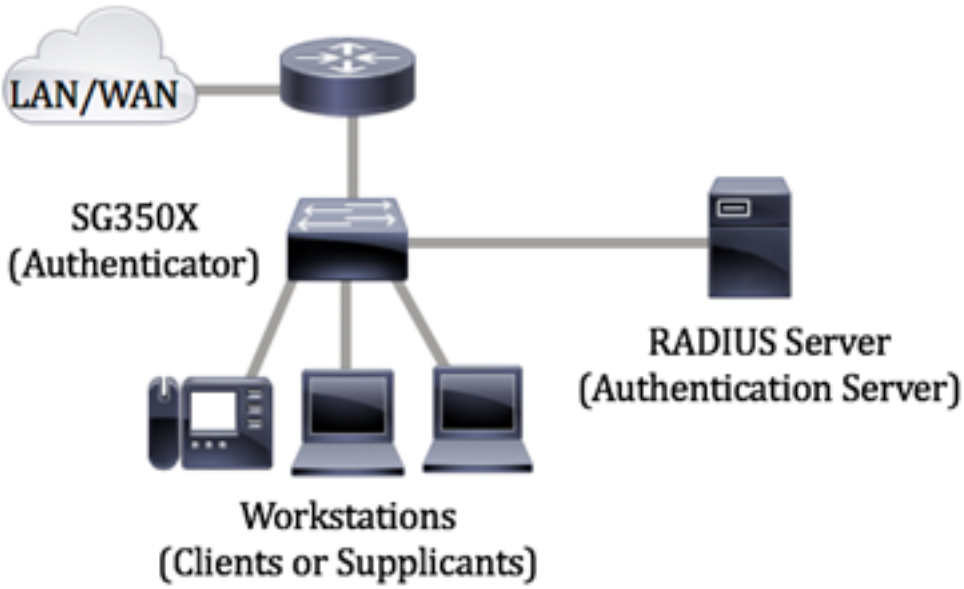
  - Baseado em MAC — Suportado em todos os modos de autenticação. Com base no Media Access Control (MAC), o próprio autenticador executa a parte do cliente EAP do software em nome dos clientes que buscam acesso à rede.

  - Baseado na Web — Suportado somente em modos multisessões. Com a autenticação baseada na Web, o próprio autenticador executa a parte do cliente EAP do software em nome dos clientes que procuram acesso à rede.

- Servidor de autenticação — Um servidor de autenticação executa a autenticação real do cliente. O servidor de autenticação do dispositivo é um servidor de autenticação RADIUS com extensões EAP.

  Note: Um dispositivo de rede pode ser um cliente ou um suplicante, um autenticador ou ambos por porta.

  A imagem abaixo exibe uma rede que configurou os dispositivos de acordo com as funções específicas. Neste exemplo, um switch SG350X é usado.



Diretrizes in configurando 802.1x:

1. Configure o servidor RADIUS. Para saber como configurar as definições do servidor RADIUS no comutador, clique aqui.
2. Configurar redes locais virtuais (VLANs). Para criar VLANs usando o utilitário baseado na Web do switch, clique aqui. Para obter instruções baseadas na CLI, clique aqui.
3. Defina as configurações de porta para VLAN no switch. Para configurar usando o utilitário baseado na Web, clique aqui. Para usar a CLI, clique aqui.
4. Configure as propriedades globais do 802.1x no switch. Para obter instruções sobre como configurar as propriedades globais do 802.1x através do utilitário baseado na Web do switch, clique aqui.
5. (Opcional) Configure o intervalo de tempo no switch. Para saber como configurar as definições de intervalo de tempo no comutador, clique aqui.
6. Configurar a autenticação de porta 802.1x. Para usar o utilitário baseado na Web do switch, clique aqui.

Objetivo

Este artigo fornece instruções sobre como configurar propriedades 802.1x globais através da CLI (Command Line Interface, interface de linha de comando) do switch, que incluem propriedades de autenticação e VLAN de convidado. A VLAN de convidado fornece acesso a serviços que não exigem que os dispositivos ou portas de assinatura sejam autenticados e autorizados por meio de autenticação 802.1x, baseada em MAC ou baseada na Web.

Dispositivos aplicáveis

- Sx300 Series
- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

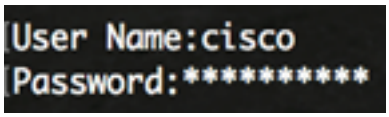
Versão de software

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

Configurar as propriedades 802.1x em um Switch através da CLI

Definir as configurações do 802.1x

Etapa 1. Log in to the switch console. O nome do usuário e a senha padrão são cisco/cisco. Se você configurou um novo nome do usuário ou senha, digite as credenciais.



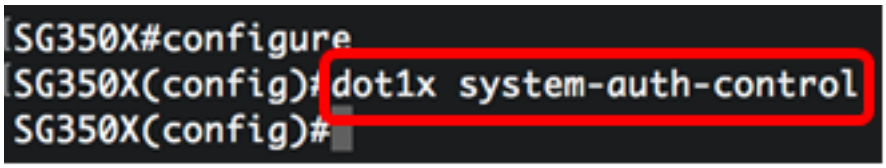
Note: Os comandos podem variar de acordo com o modelo exato do switch. Neste exemplo, o switch SG350X é acessado por meio do Telnet.

Etapa 2. No modo EXEC com privilégios do switch, insira o modo de configuração global digitando o seguinte:

```
SG350x#configurar
```

Etapa 3. Para habilitar globalmente a autenticação 802.1x no switch, use o comando **dot1x system-auth-control** no modo de Configuração Global.

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



Etapa 4. (Opcional) Para desabilitar globalmente a autenticação 802.1x no switch, insira o seguinte:

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

Note: Se isso estiver desativado, 802.1X, as autenticações baseadas em MAC e na Web serão desativadas.

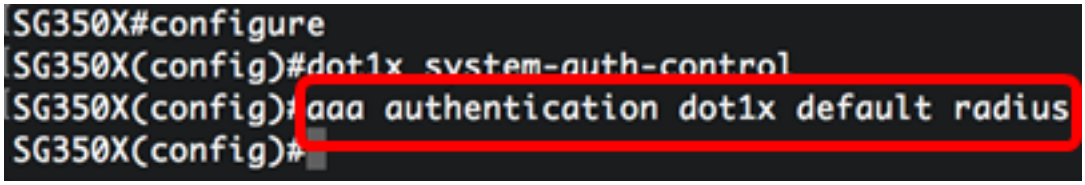
Etapa 5. Para especificar quais servidores são usados para autenticação quando a autenticação 802.1x está habilitada, insira o seguinte:

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

As opções são:

- radius none — Isso executa a autenticação de porta primeiro com a ajuda do servidor RADIUS. Se não houver resposta do servidor, como quando o servidor está inoperante, nenhuma autenticação será executada e a sessão será permitida. Se o servidor estiver disponível e as credenciais do usuário estiverem incorretas, o acesso será negado e a sessão será encerrada.

- radius — Isso executa a autenticação de porta com base no servidor RADIUS. Se não houver autenticação executada, a sessão será encerrada. Esta é a autenticação padrão.
- none — Não autentica o usuário e permite a sessão.



Note: Neste exemplo, o servidor de autenticação 802.1x padrão é RADIUS.

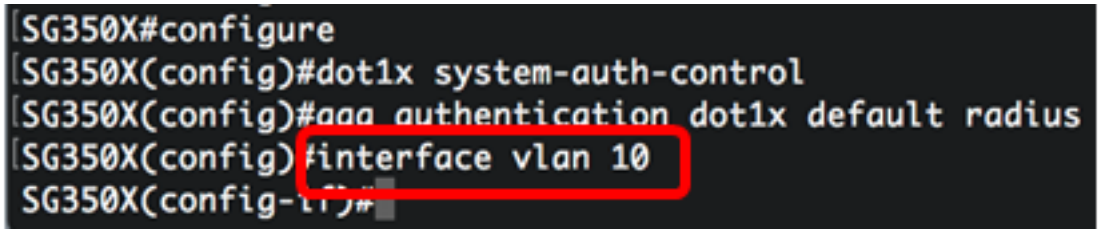
Etapa 6. (Opcional) Para restaurar a autenticação padrão, insira o seguinte:

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

Passo 7. No modo de Configuração global, insira o contexto de Configuração da Interface VLAN inserindo o seguinte:

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

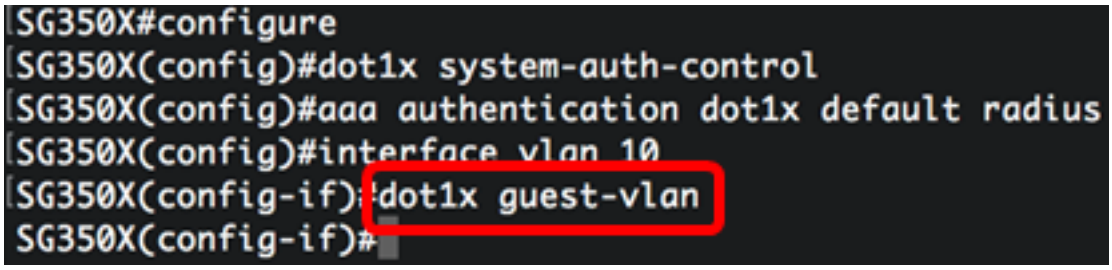
- vlan-id — Especifica um ID de VLAN a ser configurado.



Etapa 8. Para habilitar o uso de uma VLAN de convidado para portas não autorizadas, insira o seguinte:

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

Note: Se uma VLAN de convidado estiver habilitada, todas as portas não autorizadas automaticamente ingressarão na VLAN escolhida na VLAN de convidado. Se uma porta for autorizada posteriormente, ela será removida da VLAN de convidado.



Etapa 9. Para sair do contexto de configuração de interface, digite o seguinte:

```
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)#
```

Etapa 10. Para definir o intervalo de tempo entre a ativação do 802.1X (ou porta para cima) e a adição de uma porta à VLAN de convidado, insira o seguinte:

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

- timeout — Especifica o intervalo de tempo em segundos entre a ativação do 802.1X (ou port up) e a adição da porta à VLAN de convidado. O intervalo vai de 30 a 180 segundos.

Note: Após o linkup, se o software não detectar um suplicante 802.1x ou se a autenticação de porta tiver falhado, a porta será adicionada à VLAN de convidado somente após o período de tempo limite da VLAN de convidado expirar. Se a porta mudar de Autorizada para Não Autorizada, a porta será adicionada à VLAN Convidada somente após o período de tempo limite da VLAN Convidada expirar. Você pode habilitar ou desabilitar a autenticação de VLAN da autenticação de VLAN.

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

Note: Neste exemplo, o tempo limite da VLAN de convidado usado é de 60 segundos.

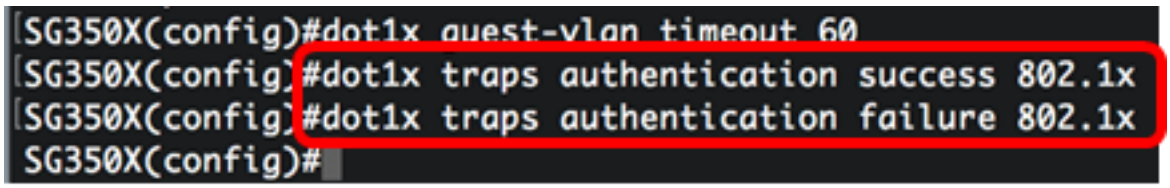
Etapa 11. Para ativar armadilhas, marque uma ou mais das seguintes opções:

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

As opções são:

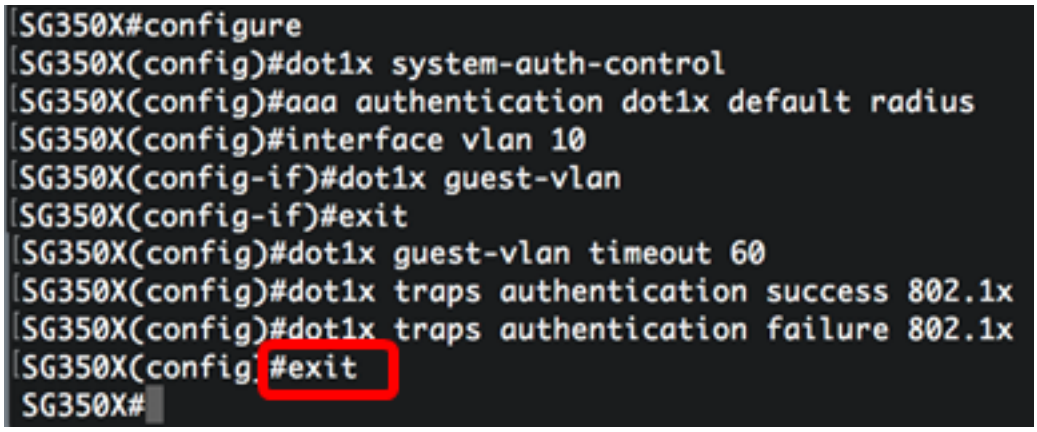
- Armadilhas de falha de autenticação 802.1x — Enviar armadilhas se a autenticação 802.1x falhar.
- Armadilhas de sucesso de autenticação 802.1x — envie armadilhas se a autenticação 802.1x for bem-sucedida.
- traps de falha de autenticação mac — Enviar traps se a autenticação MAC falhar.
- armadilhas de sucesso de autenticação mac — envie armadilhas se a autenticação MAC for bem-sucedida.
- traps de falha de autenticação da Web — Enviar traps se a autenticação da Web falhar.
- armadilhas de sucesso de autenticação da Web — envie armadilhas se a autenticação da Web for bem-sucedida.
- Armadilhas silenciosas de autenticação da Web — Enviar armadilhas se um período tranquilo começar.

Note: Neste exemplo, são inseridas falhas de autenticação 802.1x e armadilhas de sucesso.



Etapa 12. Para sair do contexto de configuração de interface, digite o seguinte:

```
SG350X(config)#exit
```



Etapa 13. (Opcional) Para exibir as propriedades 802.1x globais configuradas no switch, insira o seguinte:

```
SG350X#show dot1x
```

Agora você deve ter configurado com êxito as propriedades 802.1x em seu switch.

Configurar a autenticação de VLAN

Quando o 802.1x é ativado, portas ou dispositivos não autorizados não têm permissão para acessar a VLAN a menos que façam parte da VLAN de convidado ou de uma VLAN não autenticada. As portas precisam ser adicionadas manualmente às VLANs.

Para desativar a autenticação em uma VLAN, siga estas etapas:

Etapa 1. No modo EXEC com privilégios do switch, insira o modo de configuração global digitando o seguinte:

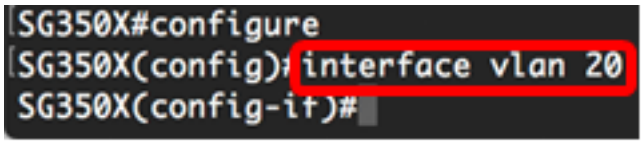
```
SG350X#configure
```

Etapa 2. No modo de Configuração global, insira o contexto de Configuração da Interface

VLAN inserindo o seguinte:

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

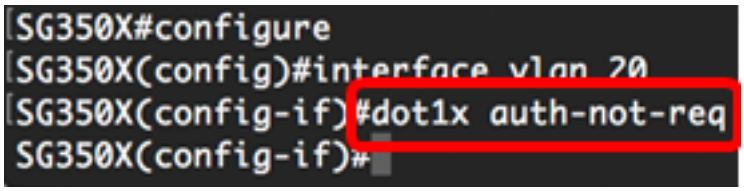
- vlan-id — Especifica um ID de VLAN a ser configurado.



Note: Neste exemplo, a VLAN 20 é escolhida.

Etapa 3. Para desativar a autenticação 802.1x na VLAN, digite o seguinte:

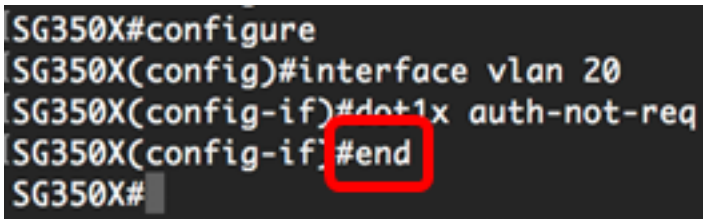
SG350X(config-if)#dot1x auth-not-req



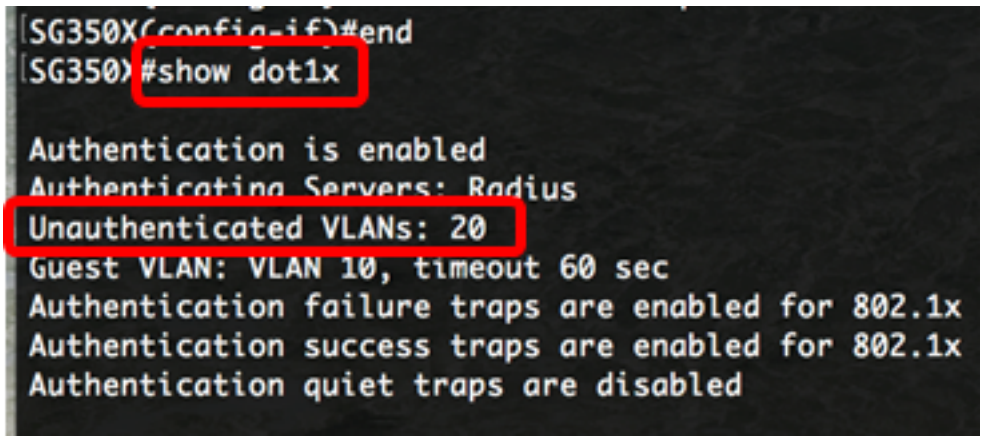
Etapa 4. (Opcional) Para habilitar a autenticação 802.1x na VLAN, insira o seguinte:

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

Etapa 5. Para sair do contexto de configuração de interface, digite o seguinte:



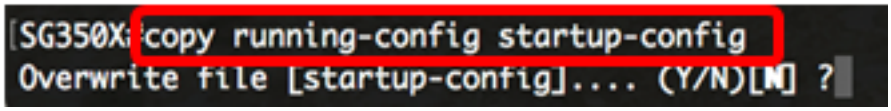
Etapa 6. (Opcional) Para exibir as configurações de autenticação global 802.1x no switch, insira o seguinte:



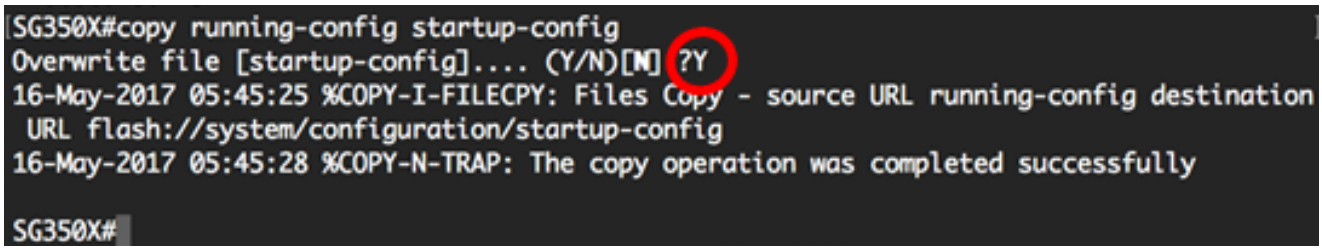
Note: Neste exemplo, a VLAN 20 é mostrada como uma VLAN não autenticada.

Passo 7. (Opcional) No modo EXEC com privilégios do switch, salve as configurações definidas no arquivo de configuração de inicialização, digitando o seguinte:

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



Etapa 8. (Opcional) Pressione Y para Sim ou N para Não no teclado quando o prompt Overwrite file (Substituir arquivo) [startup-config]… for exibido.



Agora você deve ter configurado com êxito as configurações de autenticação 802.1x nas VLANs do switch.

Importante: Para continuar a configuração das configurações de autenticação de porta 802.1x em seu switch, siga as diretrizes acima.