Comportamento de segurança de porta para switches CBS séries 250 e 350 com firmware 3.1

Objetivo

Este artigo fornece uma demonstração para mostrar as alterações com as configurações de segurança de porta padrão nos switches Cisco Business 250 e 350 a partir do firmware versão 3.1.

Dispositivos aplicáveis | Versão do firmware

- CBS250 (Folha de dados) | 3.1 (Download mais recente)
- CBS350 (Folha de dados) | 3.1 (Download mais recente)
- CBS350-2X (Folha de dados) | 3.1 (Download mais recente)
- CBS350-4X (Folha de dados) | 3.1 (Download mais recente)

Introdução

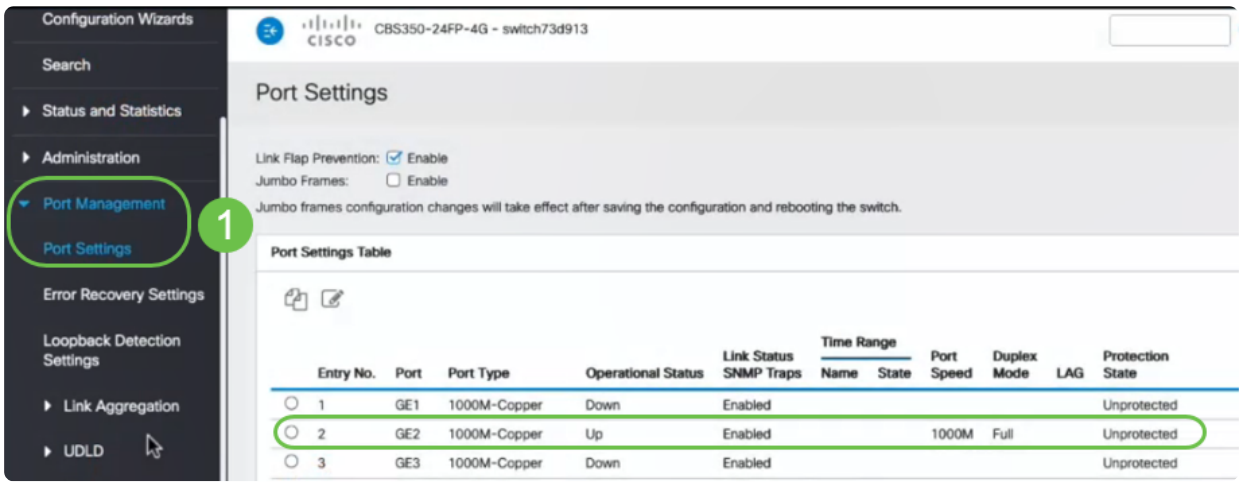
É importante executar a versão mais recente do firmware quando uma nova versão for lançada. Na primavera de 2021, a versão 3.1 do firmware para os switches CBS 250 e 350 foi lançada, alterando o comportamento padrão da segurança de porta. Essas alterações foram feitas para melhorar a segurança do endpoint. Confira a demonstração para saber mais.

Demonstração do comportamento padrão da segurança de porta (Firmware versão 3.1)

Nesta demonstração, a segurança de porta é ativada na interface GE2 de um switch Cisco Business 350 atualizado para a versão de firmware 3.1. Moveremos um PC conectado na porta 2 do switch (GE2) para a porta 4 do switch (GE4) e observaremos o comportamento padrão da segurança de porta.

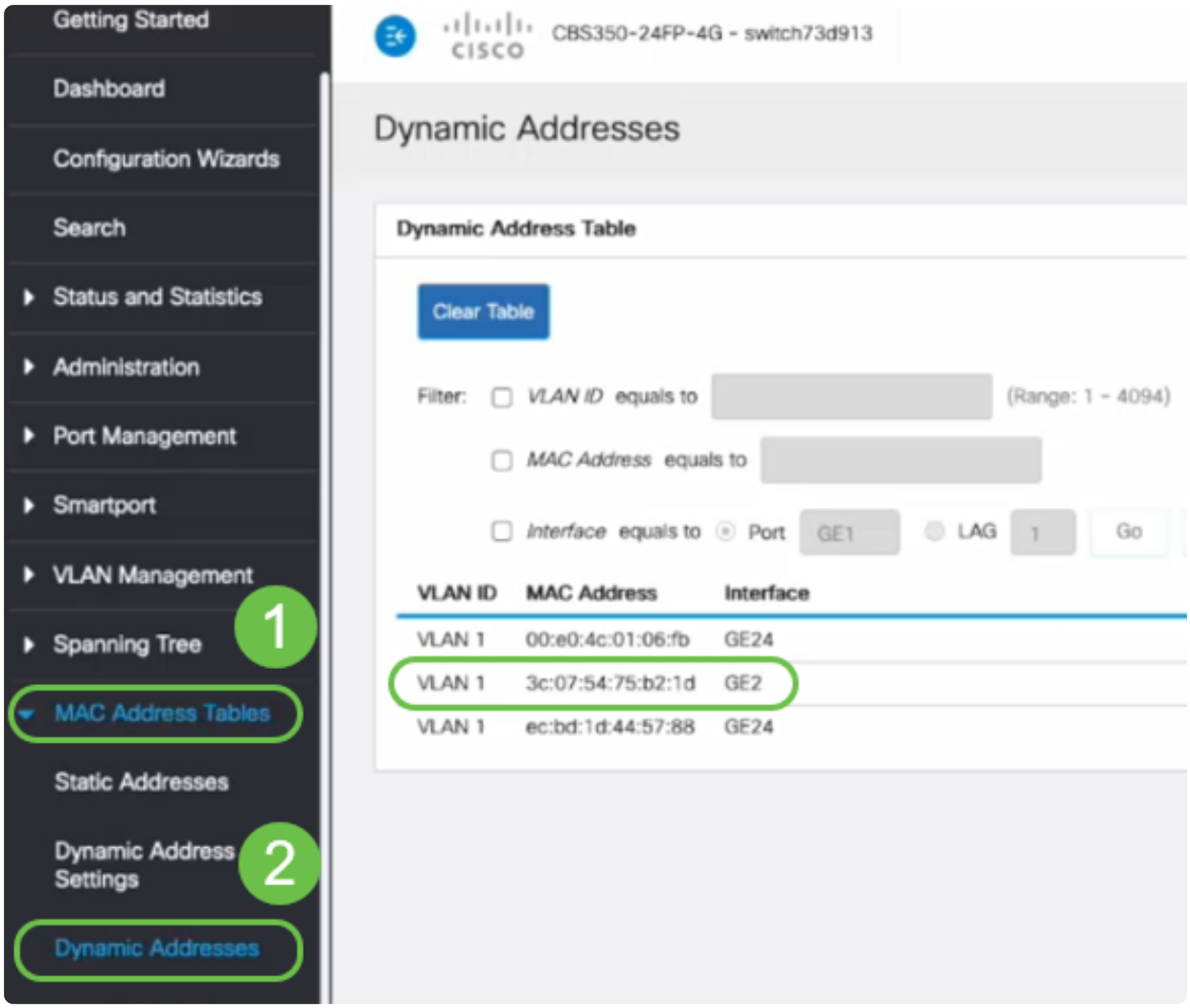
Passo 1

Primeiro, navegamos para Gerenciamento de porta > Configurações de porta e verificamos se o PC está conectado à porta 2 do switch (GE2) e o Status operacional da porta está mostrando Up.



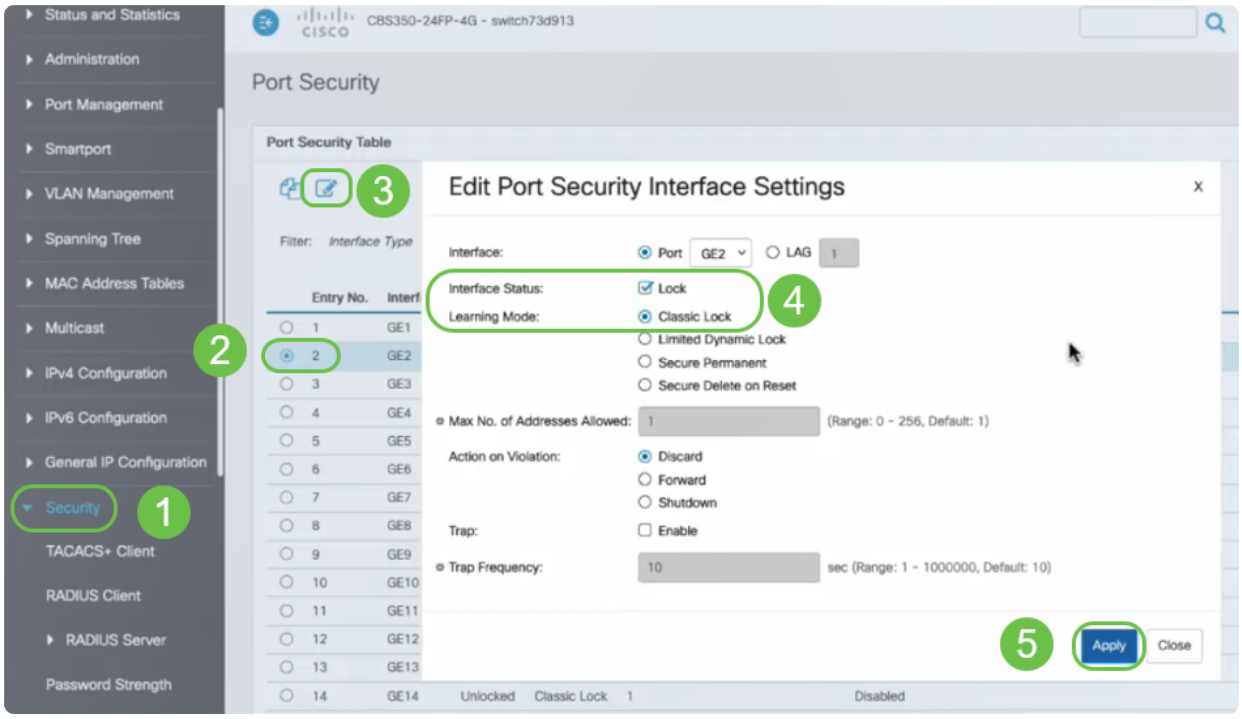
Passo 2

Em seguida, navegamos até MAC Address Tables > Dynamic Addresses e verificamos o endereço MAC do PC associado à porta 2 do switch (GE2).



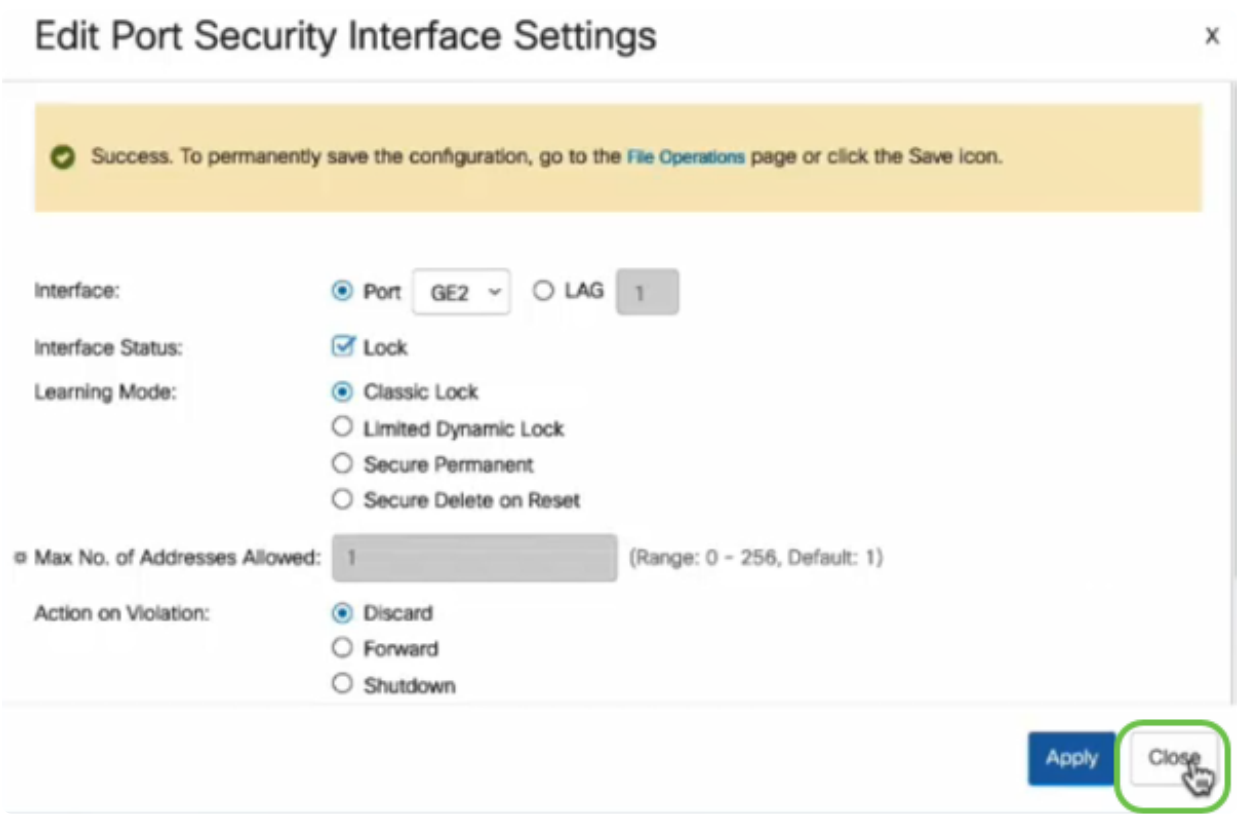
Etapa 3

Navegamos até o menu Security, selecionamos a porta 2 do switch (GE2) e clicamos no ícone de edição. Ativamos a opção Lock ao lado de Interface Status. O Modo de Aprendizado será mostrado como Bloqueio Clássico. Deixamos Action on Violation como Discard e clicamos em Apply.



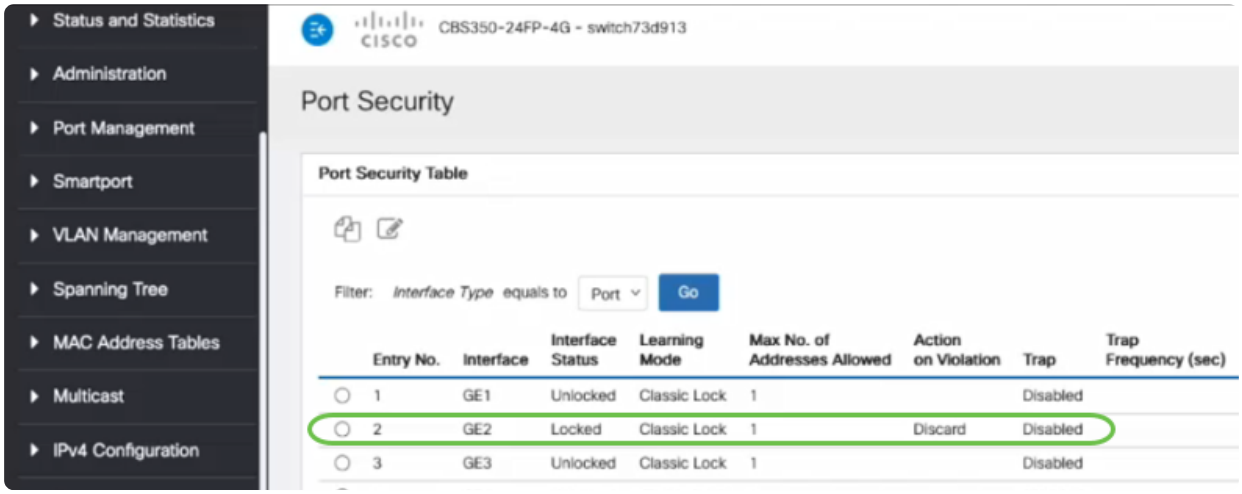
Passo 4

Uma notificação de êxito será exibida na tela, então clicamos em Fechar.



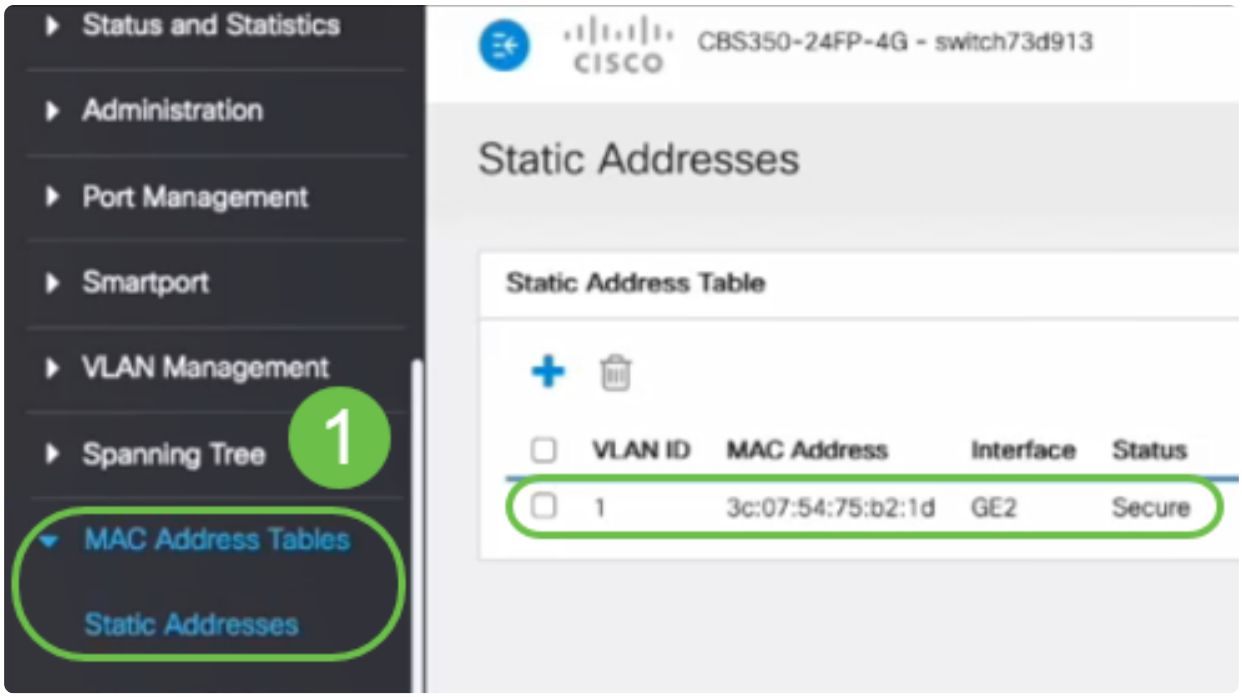
Etapa 5

O Status da interface GE2 será exibido como Bloqueado.



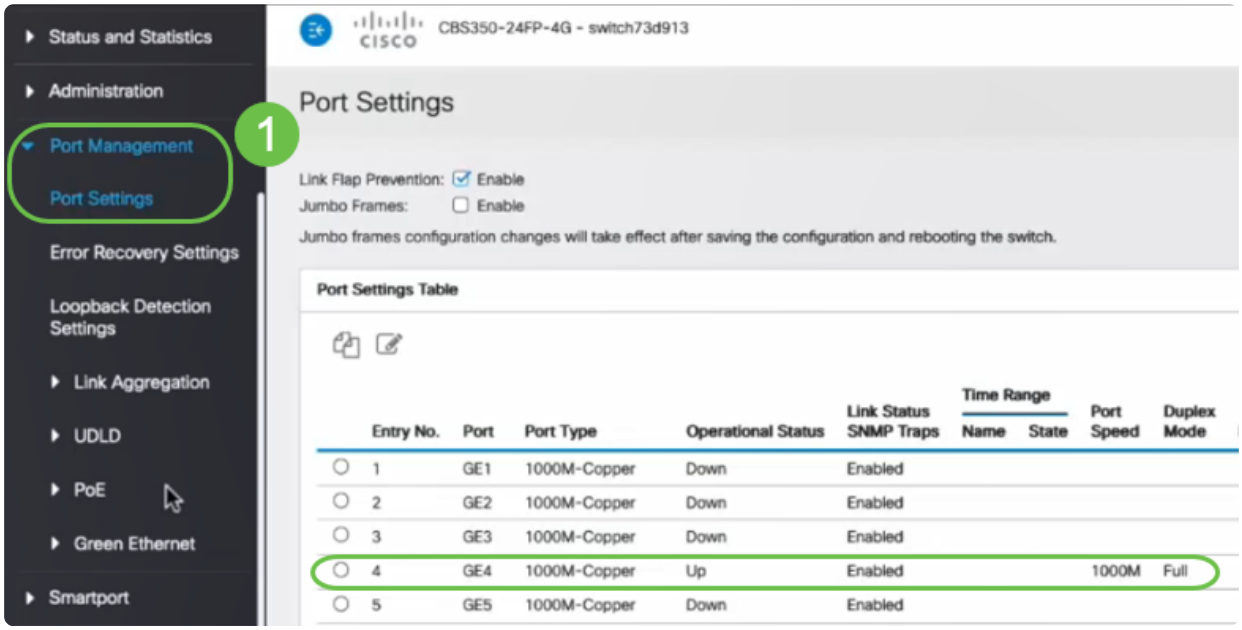
Etapa 6

Navegamos até MAC Address Tables > Static Addresses. O endereço MAC do PC associado à interface GE2 será refletido na tabela Static Addresses.



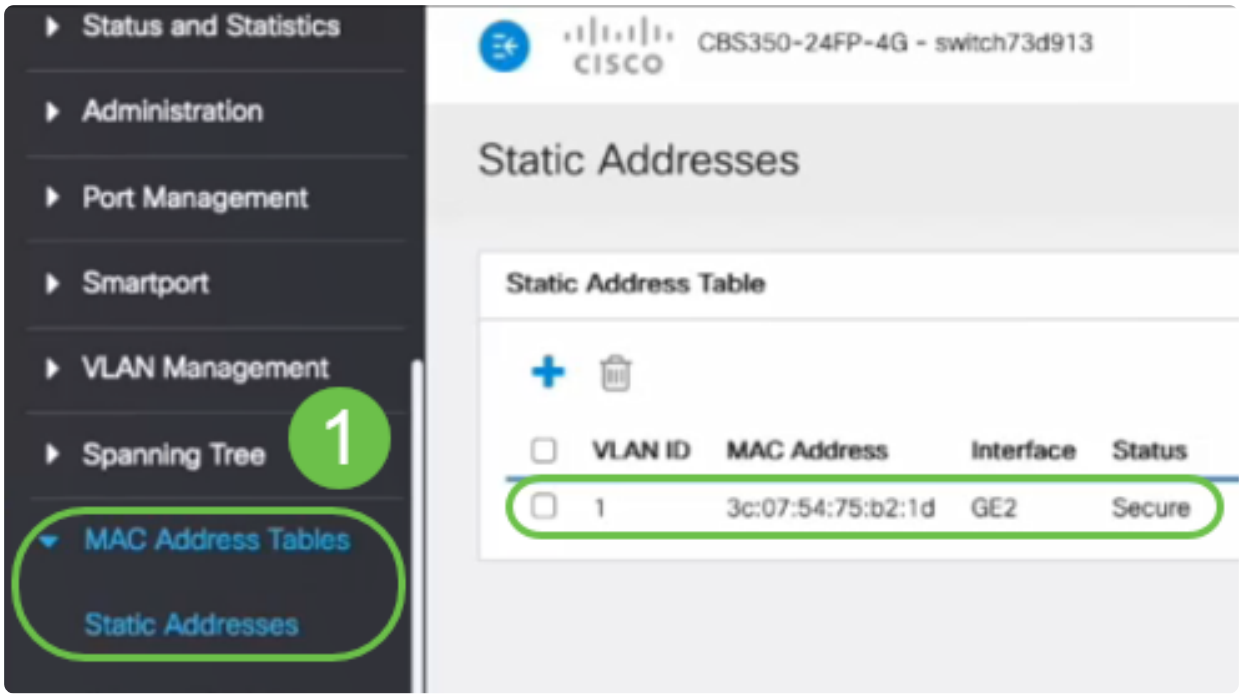
Etapa 7

Moveremos o PC da porta 2 do switch (GE2) para a porta 4 do switch (GE4) e garantiremos que o status operacional da interface GE4 mostre Up.



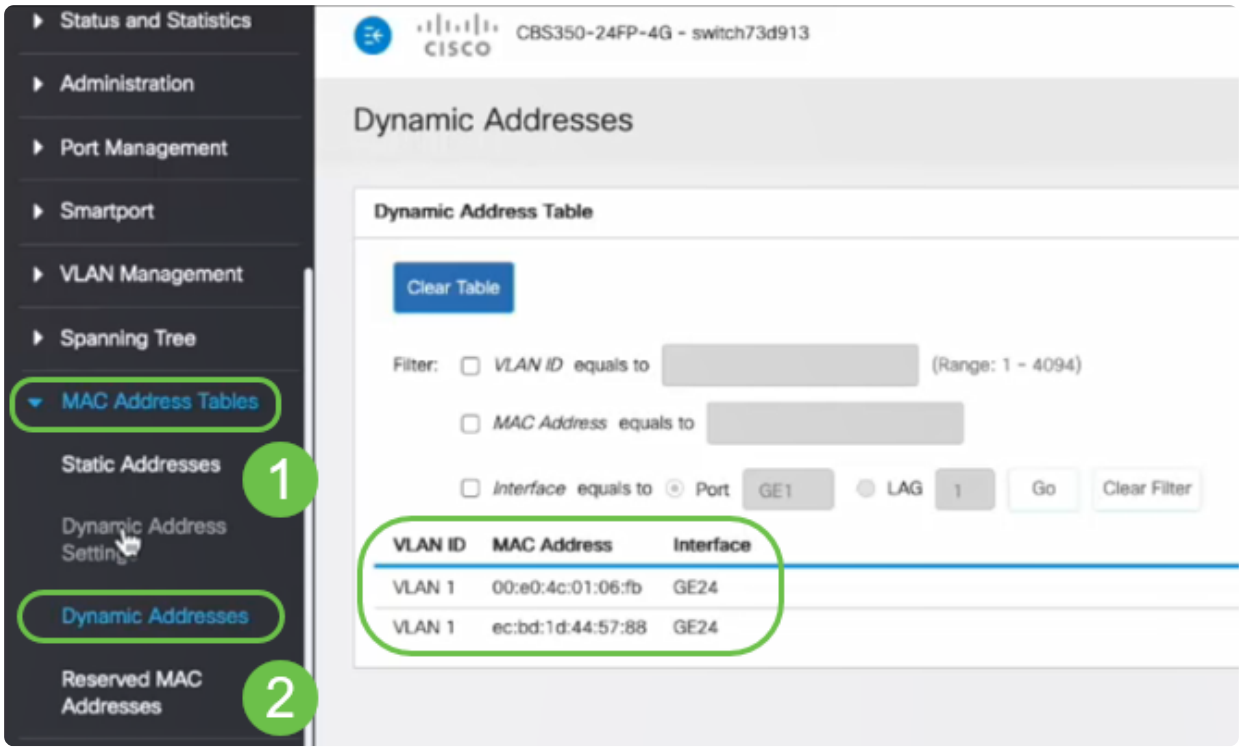
Passo 8

Navegamos até MAC Address Tables > Static Addresses. O endereço MAC do PC associado à interface GE2 ainda aparecerá na tabela Static Addresses.



Passo 9

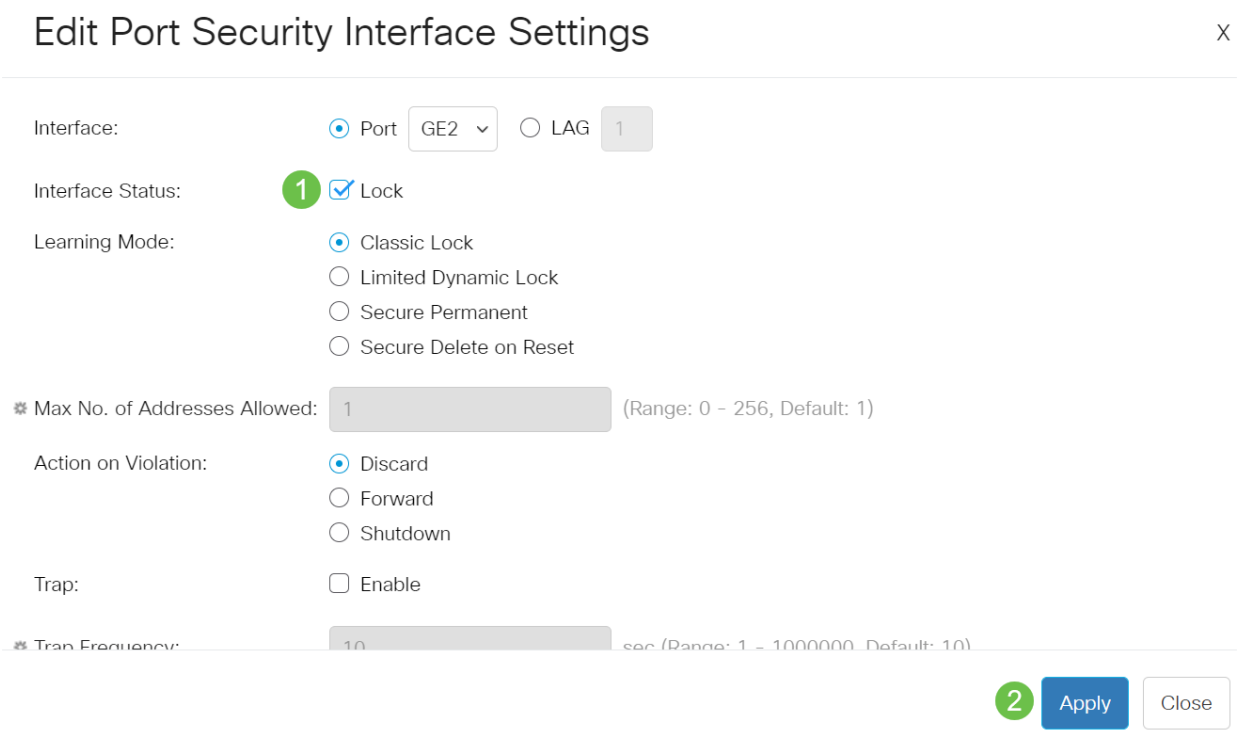
Navegamos até MAC Address Tables > Dynamic Addresses. O PC (endereço MAC 3c:07:54:75:b2:1d) está conectado à interface GE4. Mesmo que o Status Operacional da interface GE4 seja Ativo, o PC não poderá obter um endereço IP de DHCP (Dynamic Host Configuration Protocol). Na tabela de endereços dinâmicos, podemos verificar o mesmo.



> ⓘ Note:
>
> O PC (endereço MAC 3c:07:54:75:b2:1d) só obterá um endereço IP DHCP quando estiver conectado à interface GE2, pois a Tabela de Endereços Estáticos mostra que a ligação de endereços MAC com a interface GE2. Se quisermos remover o endereço MAC do PC da interface GE2 para que possamos usá-lo em outra porta, precisamos desbloquear a porta seguindo as etapas opcionais a seguir.

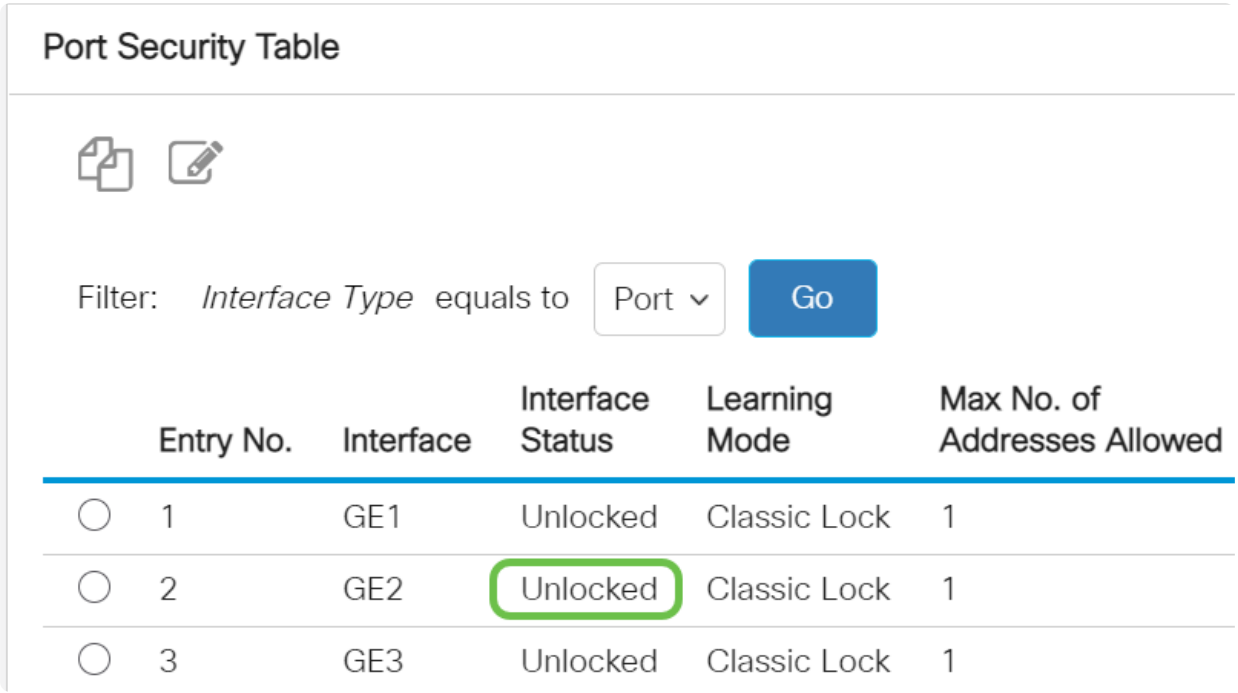
Etapa 10 (opcional)

Desmarque o botão de opção Lock e clique em Apply.



Etapa 11 (opcional)

O Status da interface será exibido agora como desbloqueado.



Etapa 12

Por fim, clicamos no ícone salvar para salvar permanentemente a configuração.

Conclusão

Pronto, agora você sabe o novo comportamento padrão de segurança de porta da versão de firmware 3.1 e posterior!

Procurando mais artigos sobre o switch CBS250 ou CBS350? Confira qualquer um dos links abaixo para obter mais informações.

Configurações de SNMP Visualizações de SNMP Grupos de SNMP Atualização de imagem de DHCP Intensidade da senha Configurações de TCP e UDP Configurações de tempo Atualizar firmware Melhores práticas de Smartport Solução de problemas: Sem endereço IP Solucionar problemas de Smartports Solucionar problemas de sincronização de link Criar VLANs

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.