Solucione problemas de alerta de falha recente do 802.1X no dispositivo Meraki

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Problema](#)
[Qual é o teste RADIUS em dispositivos Meraki?](#)
[Configurar](#)
[Diagrama de Rede](#)
[Verificar e solucionar problemas](#)
[Configuração 802.1X](#)
[Teste de verificação de configuração 802.1X](#)
[Informações Relacionadas](#)
[Nota](#)

Introduction

Este documento descreve como resolver o recente alerta de falha 802.1X no dispositivo Meraki.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Entender a solução básica de rede de longa distância definida por software (SDWAN) da Meraki
- Entender a política de acesso básica e a autenticação Radius

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

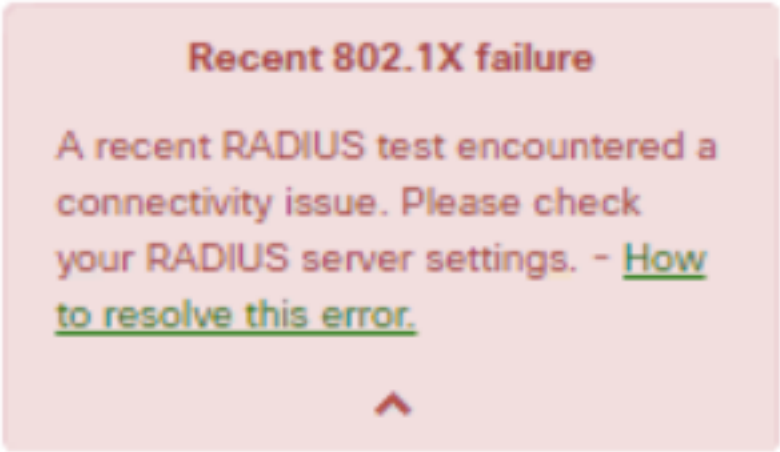
Problema

Os dispositivos Meraki usam a configuração de política do servidor AAA radius para autenticar o usuário final.

Qual é o teste RADIUS em dispositivos Meraki?

O alerta de falha recente do 802.1X exibiu que, se as mensagens periódicas de solicitação de acesso enviadas aos servidores RADIUS configurados estiverem inacessíveis, você deverá usar um período de tempo limite de 10 segundos.

Os dispositivos Meraki enviam periodicamente mensagens de solicitação de acesso aos servidores RADIUS configurados que usam a identidade **meraki_8021x_test** para garantir que os servidores RADIUS estejam acessíveis. Essas solicitações de acesso têm um tempo limite de 10 segundos e, se o servidor RADIUS não responder, ele considera que os servidores radius estão inalcançáveis e solicita a mensagem de alerta "Falha recente 802.1X". Consulte a captura de tela do alerta visto no dispositivo:



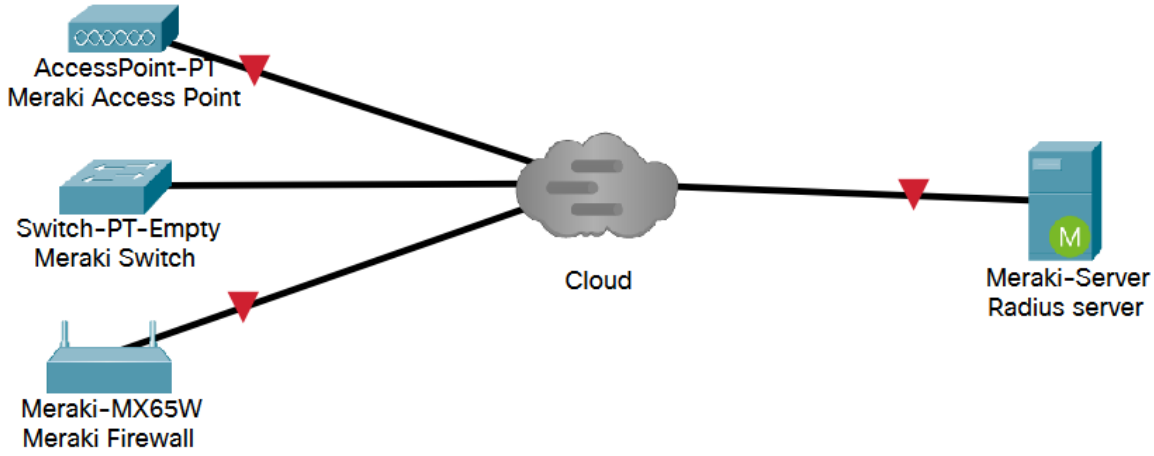
Um teste é considerado bem-sucedido se o dispositivo Meraki receber qualquer resposta RADIUS legítima (Access-Accept/Reject/Challenge) do servidor.

Com o teste RADIUS ativado, todos os servidores RADIUS são mantidos em execução de teste em cada nó pelo menos uma vez por 24 horas, independentemente do resultado do teste. Se um teste RADIUS falhar para um determinado nó, ele testa novamente a cada hora até que ocorra um resultado que passe. Uma aprovação subsequente marca o servidor alcançável, limpa o alerta e retorna ao ciclo de teste de 24 horas.

Configurar

Diagrama de Rede

Este é um diagrama simples de topologia que descreve a configuração:



Verificar e solucionar problemas

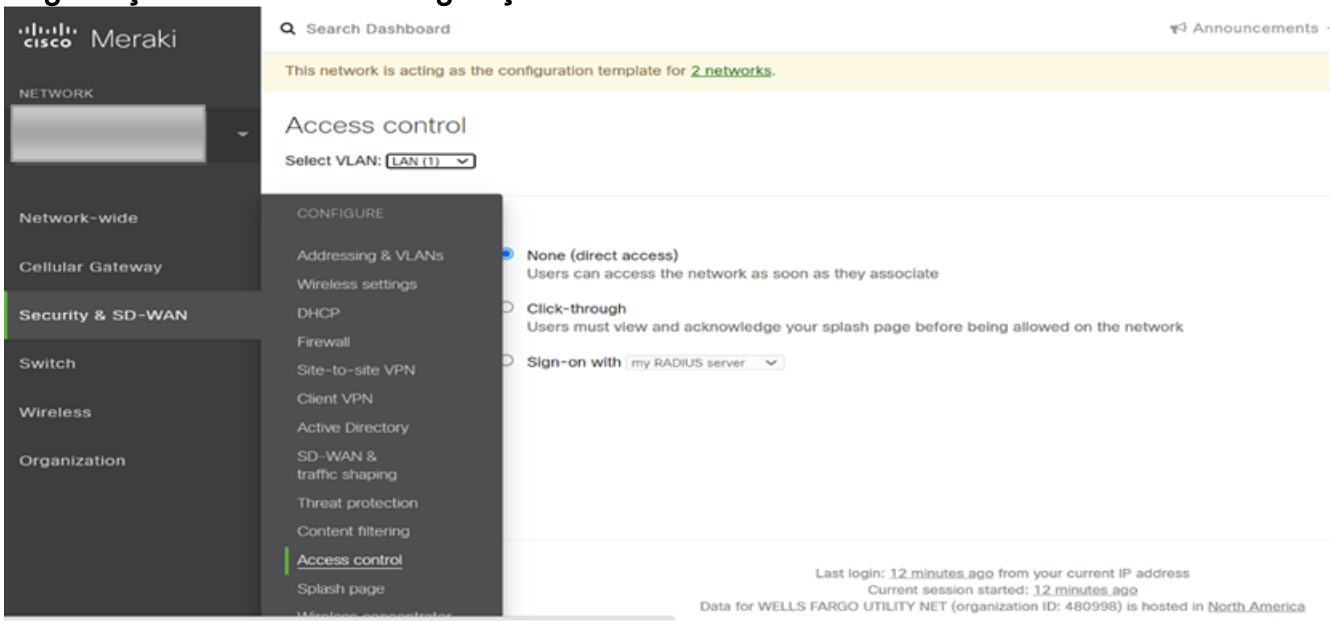
Configuração 802.1X

A configuração RADIUS 802.1X pode ser encontrada no caminho mostrado, dependendo do modelo do produto Meraki.

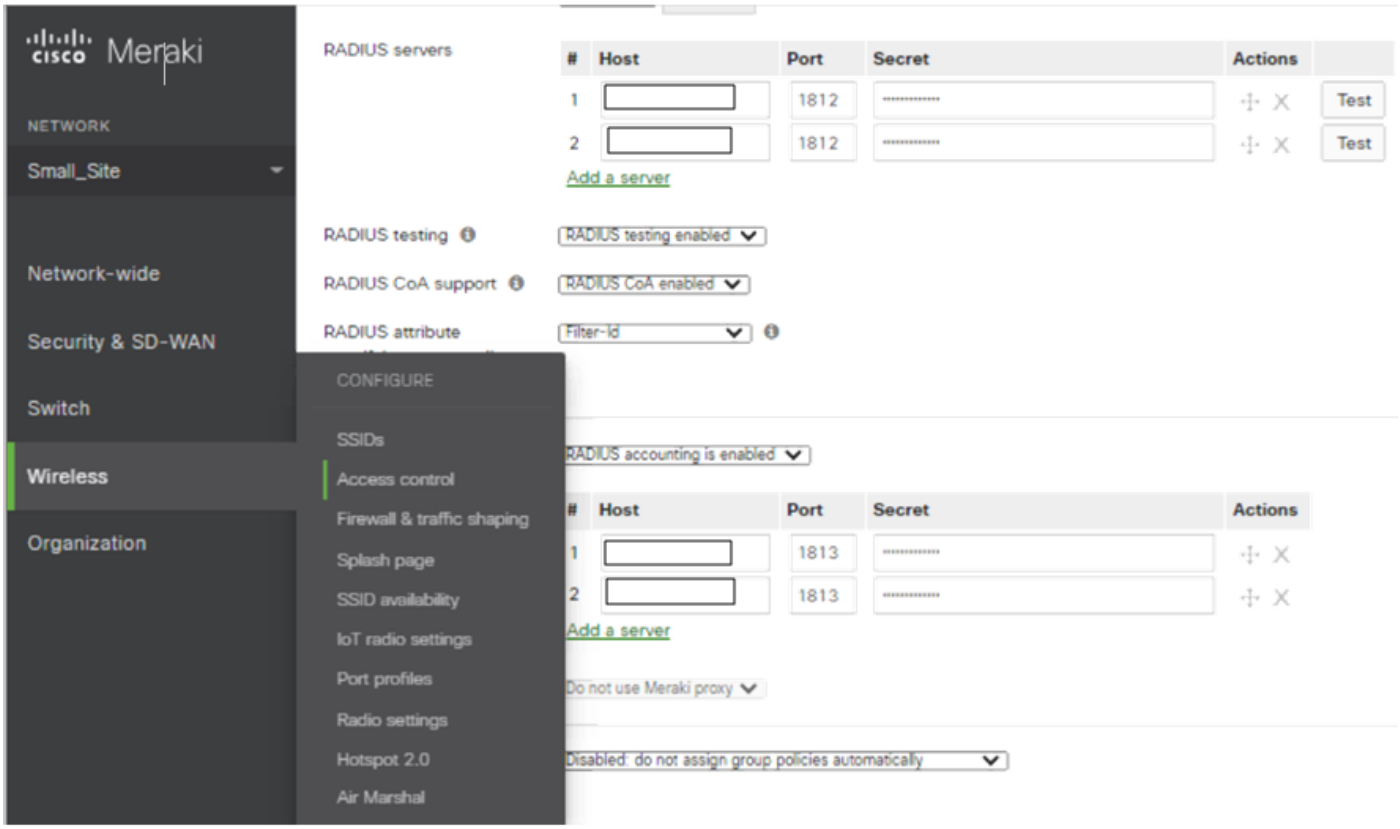
1. Dispositivo de segurança MX (configurado para portas de acesso ou sem fio)

- Para portas de acesso
  Segurança e SD-WAN > Endereçamento e VLANs

- Para redes sem fio
  Segurança e SD-WAN > Configurações sem fio

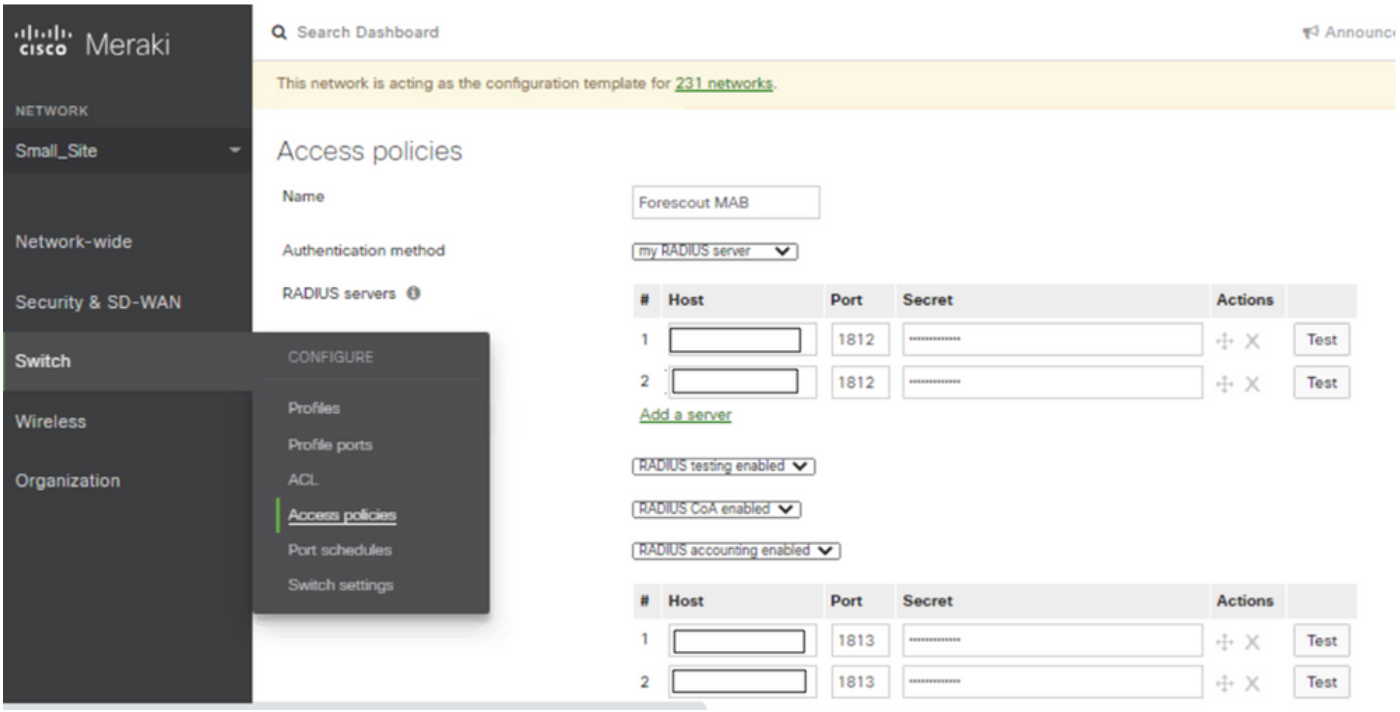


2. Pontos de acesso MR (habilitado por SSID (Service Set Identifier):
Sem fio > Controle de acesso



3. Switches MS

Switch > Políticas de acesso

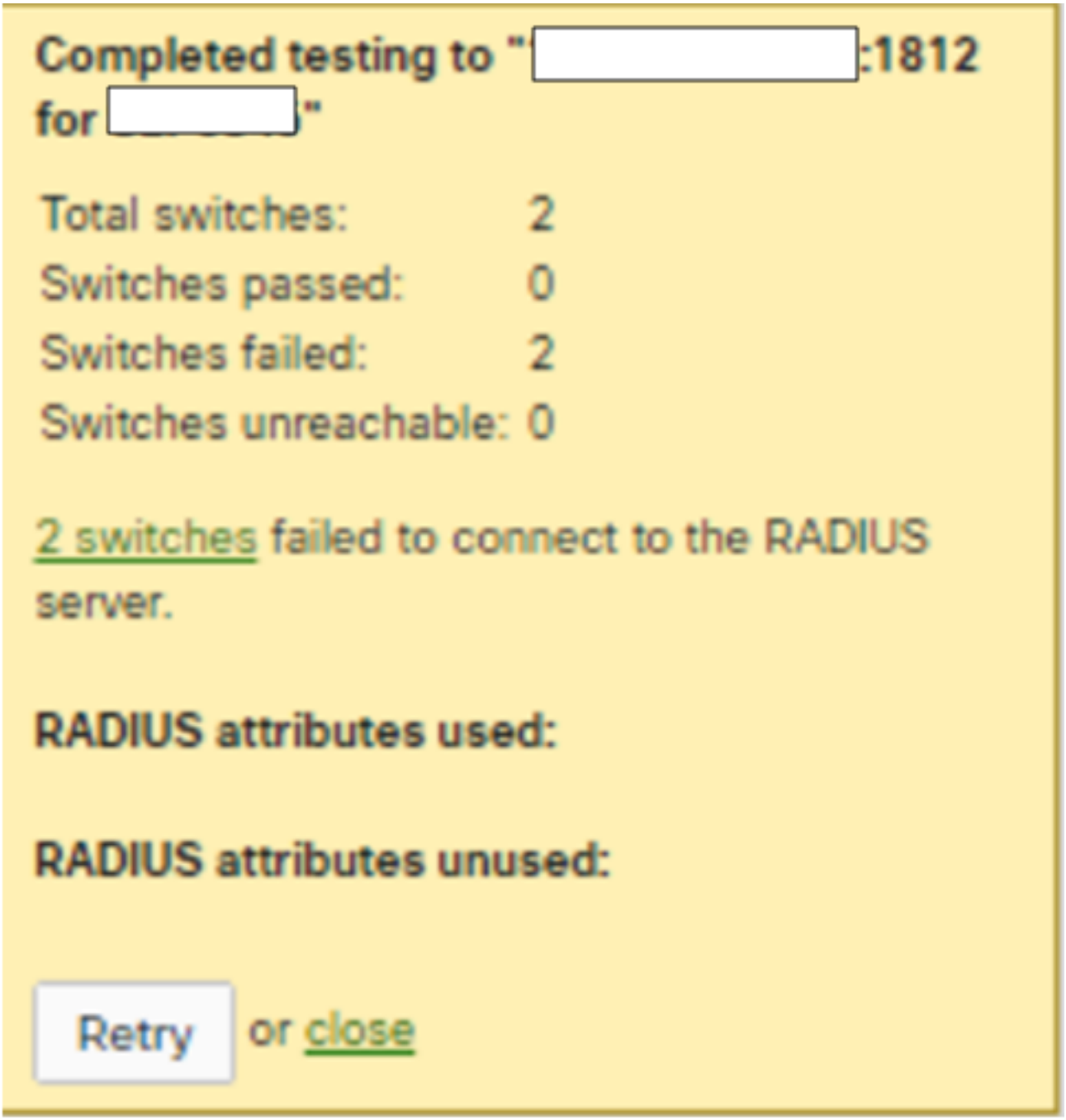


Teste de verificação de configuração 802.1X

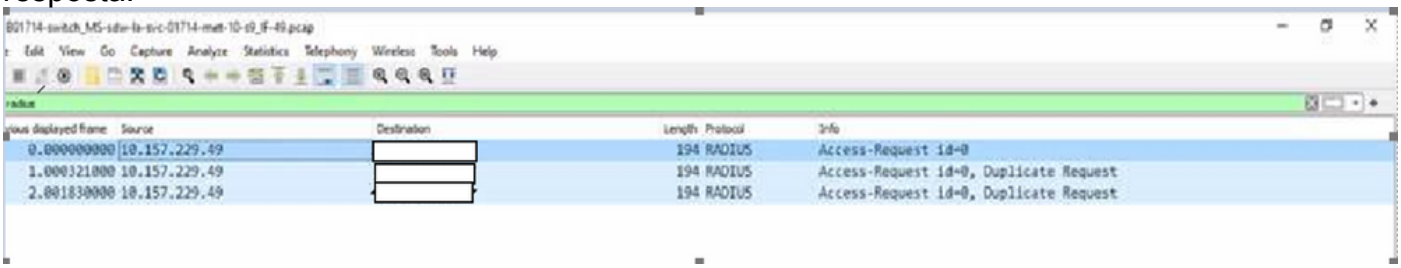
- **Painel Meraki > Modelo de rede > Switch > Políticas de acesso > Servidores Radius > Teste**
- **Painel Meraki > Modelo de Rede > Tecnologia Wireless > Controle de acesso > Servidores Radius > Teste**

1. Se o resultado do teste for notado como **All AP failed to connect radius server**, você precisará

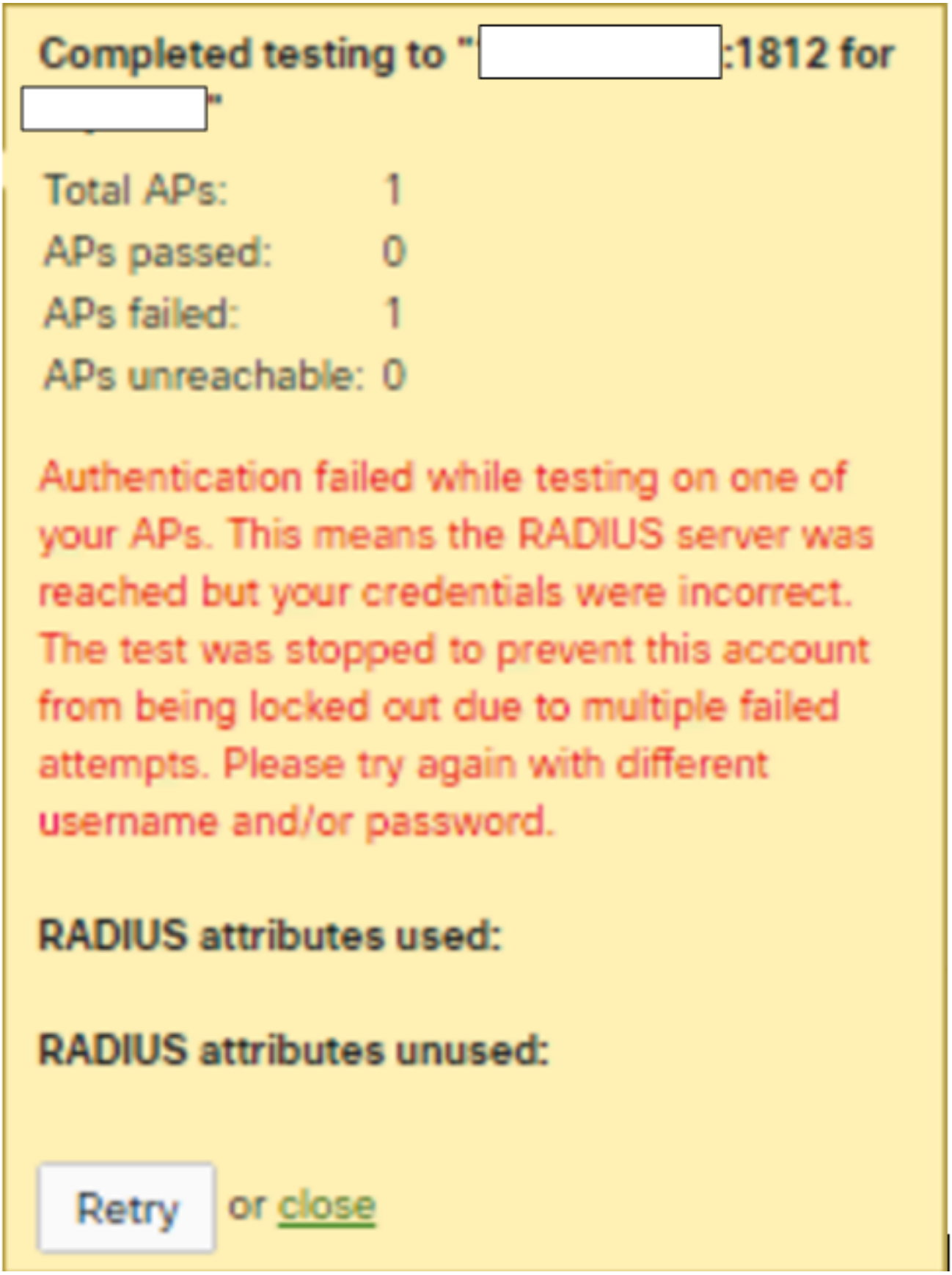
verificar onde a solicitação de acesso foi removida.



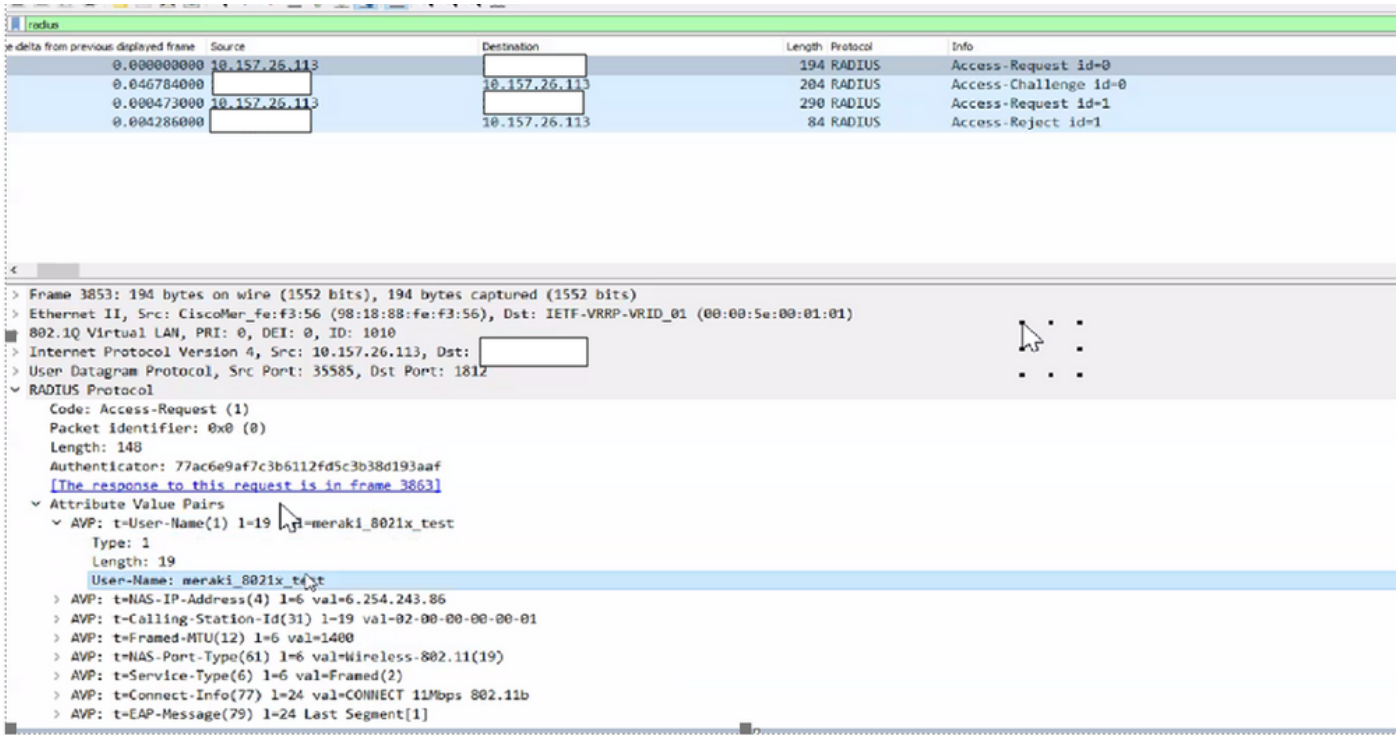
2. Execute a captura de pacotes na porta de uplink e verifique o fluxo de solicitação de acesso. Consulte a captura de tela do acesso à captura de pacotes - A solicitação não recebe nenhuma resposta.



3. Se o resultado do teste observado for retornado como credenciais de aceitação/rejeição/negação/resposta/incorreta, significa que o servidor radius está ativo.

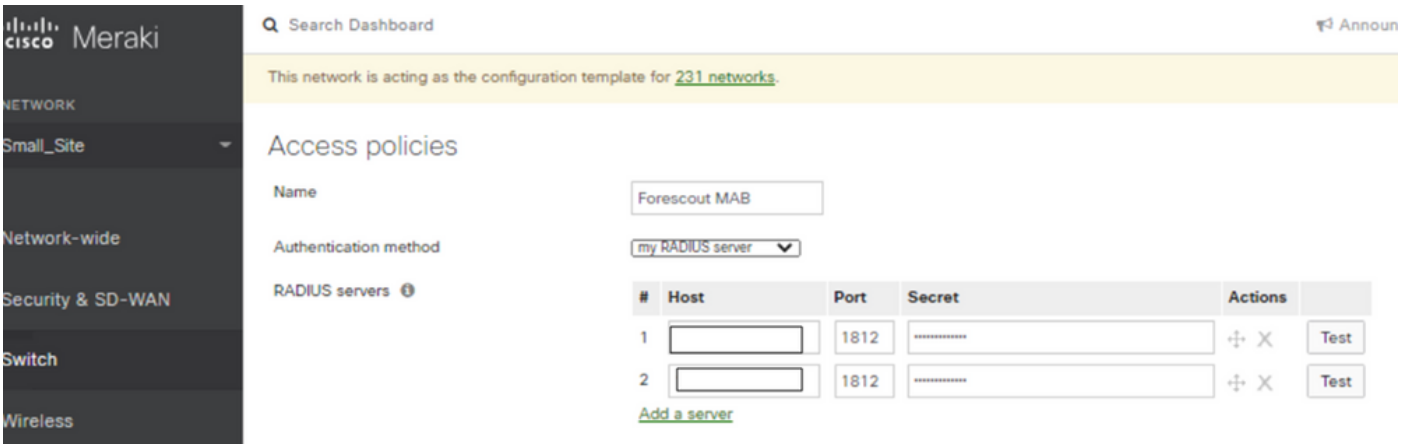


4. Execute a captura de pacotes na porta de uplink e verifique o fluxo de solicitação de acesso. Consulte a captura de tela do acesso de captura de pacote - A solicitação recebeu uma resposta.

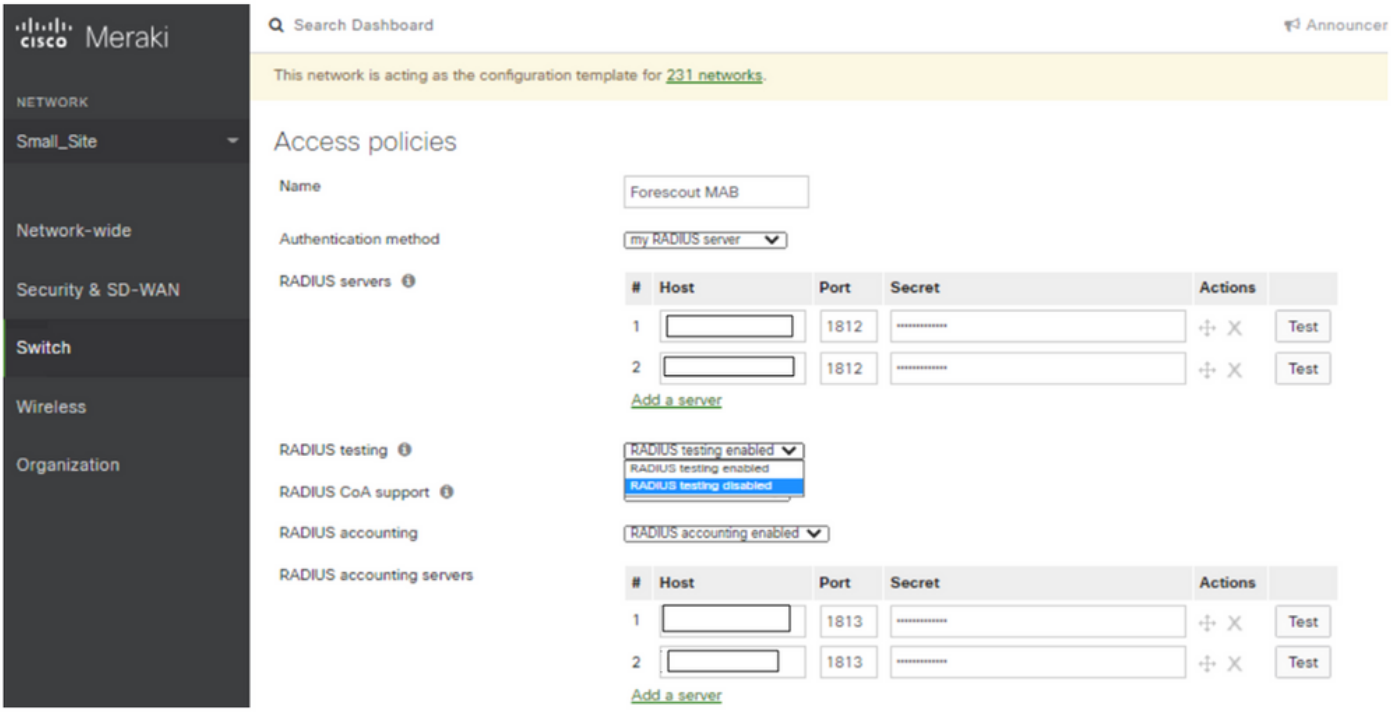


Verificação da configuração da política de acesso

1. É necessário verificar se o parâmetro mencionado na política de acesso está correto e inclui o IP do host, o número da porta e a chave secreta.



2. Os IPs do servidor radius configurados são fictícios ou não são usados na produção ou a política de acesso não está em uso. Recomenda-se remover a política de acesso. Se quiser mantê-lo, você pode desativar a **configuração de teste de RADIUS.**



Informações Relacionadas

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- Suporte Técnico e Documentação - Cisco Systems

Nota

- Quando os servidores radius pesquisam os dispositivos Meraki usam o IP da LAN e o nome de usuário padrão "meraki_8021x_test", o painel da Meraki usou o endereço MAC da Meraki como origem.
- A Meraki disponibilizou visibilidade para esses alertas desde outubro de 2021.