Solución de problemas de la reciente alerta de fallo 802.1X en el dispositivo Meraki

Contenido

Introducción

Este documento describe cómo resolver la alerta de falla 802.1X reciente en el dispositivo Meraki.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprender la solución básica de red de área extensa (SDWAN) definida por software Meraki
- Comprender la política de acceso básica y la autenticación Radius

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

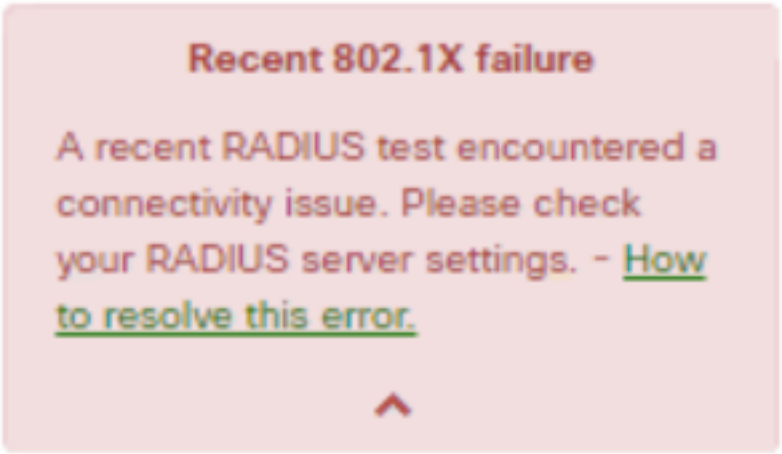
Problema

Los dispositivos Meraki utilizan la configuración de política de servidor RADIUS AAA para autenticar al usuario final.

¿Cuál es la prueba RADIUS en los dispositivos Meraki?

La reciente alerta de falla 802.1X mostraba que, si los mensajes periódicos de solicitud de acceso enviados a los servidores RADIUS configurados son inalcanzables, debe utilizar un período de tiempo de espera de 10 segundos.

Los dispositivos Meraki envían periódicamente mensajes de solicitud de acceso a los servidores RADIUS configurados que utilizan la identidad **meraki_8021x_test** para asegurarse de que los servidores RADIUS son accesibles. Estas solicitudes de acceso tienen un tiempo de espera de 10 segundos y si el servidor RADIUS no responde, considera que los servidores RADIUS son inalcanzables y envía el mensaje de alerta "Falla 802.1X reciente". Consulte la captura de pantalla de la alerta vista en el dispositivo:



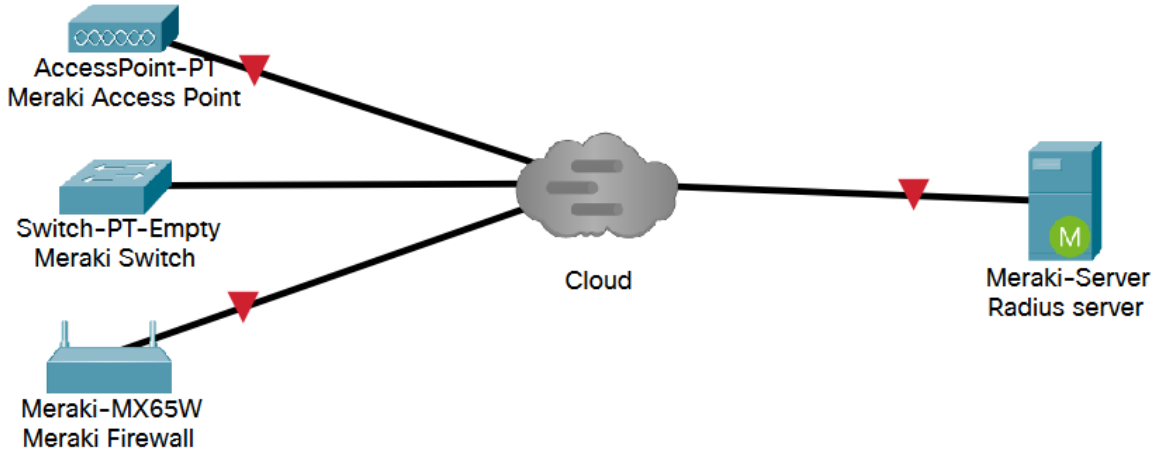
Una prueba se considera exitosa si el dispositivo Meraki recibe cualquier respuesta RADIUS legítima (Access-Accept/Reject/Challenge) del servidor.

Con la prueba RADIUS activada, todos los servidores RADIUS se mantienen en ejecución de prueba en cada nodo al menos una vez cada 24 horas, independientemente del resultado de la prueba. Si una prueba RADIUS falla para un nodo determinado, se prueba de nuevo cada hora hasta que se produzca un resultado que pase. Una pasada posterior marca el servidor alcanzable, borra la alerta y vuelve al ciclo de prueba de 24 horas.

Configurar

Diagrama de la red

Este es un diagrama de topología simple que describe la configuración:



Verificación y resolución de problemas

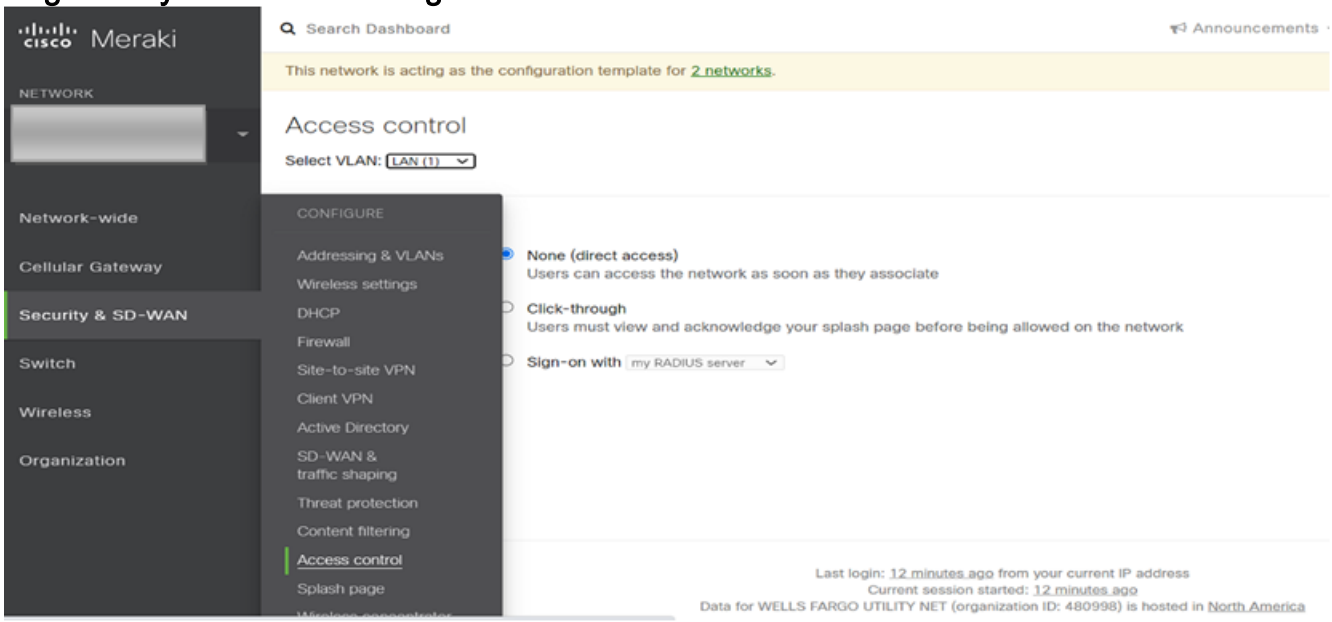
Configuración de 802.1X

La configuración RADIUS 802.1X se puede encontrar en la trayectoria mostrada que depende del modelo de producto Meraki.

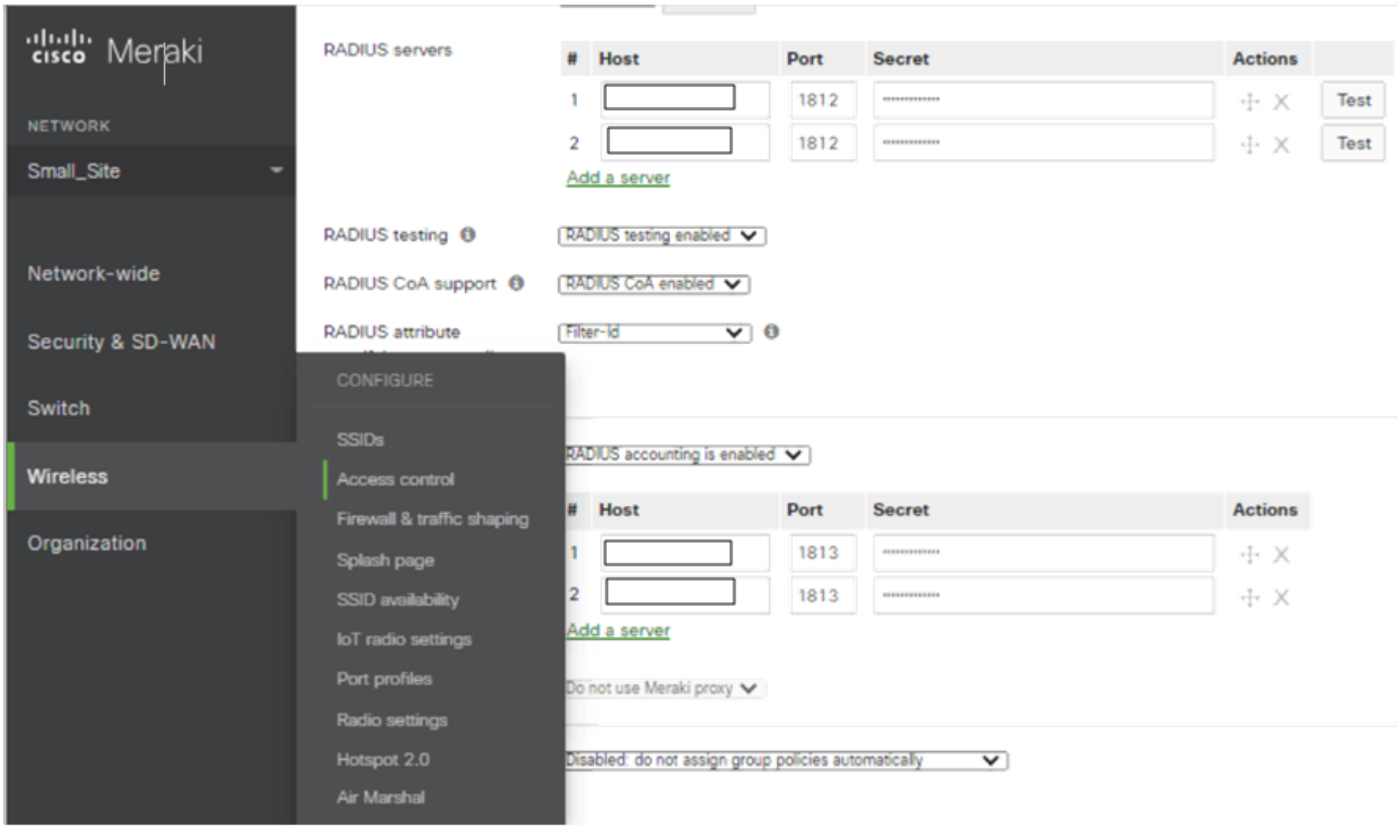
1. Dispositivo de seguridad MX (configurado para puertos de acceso o inalámbrico)

- Para puertos de acceso
  Seguridad y SD-WAN > Direccionamiento y VLAN

- Para redes inalámbricas
  Seguridad y SD-WAN > Configuración inalámbrica

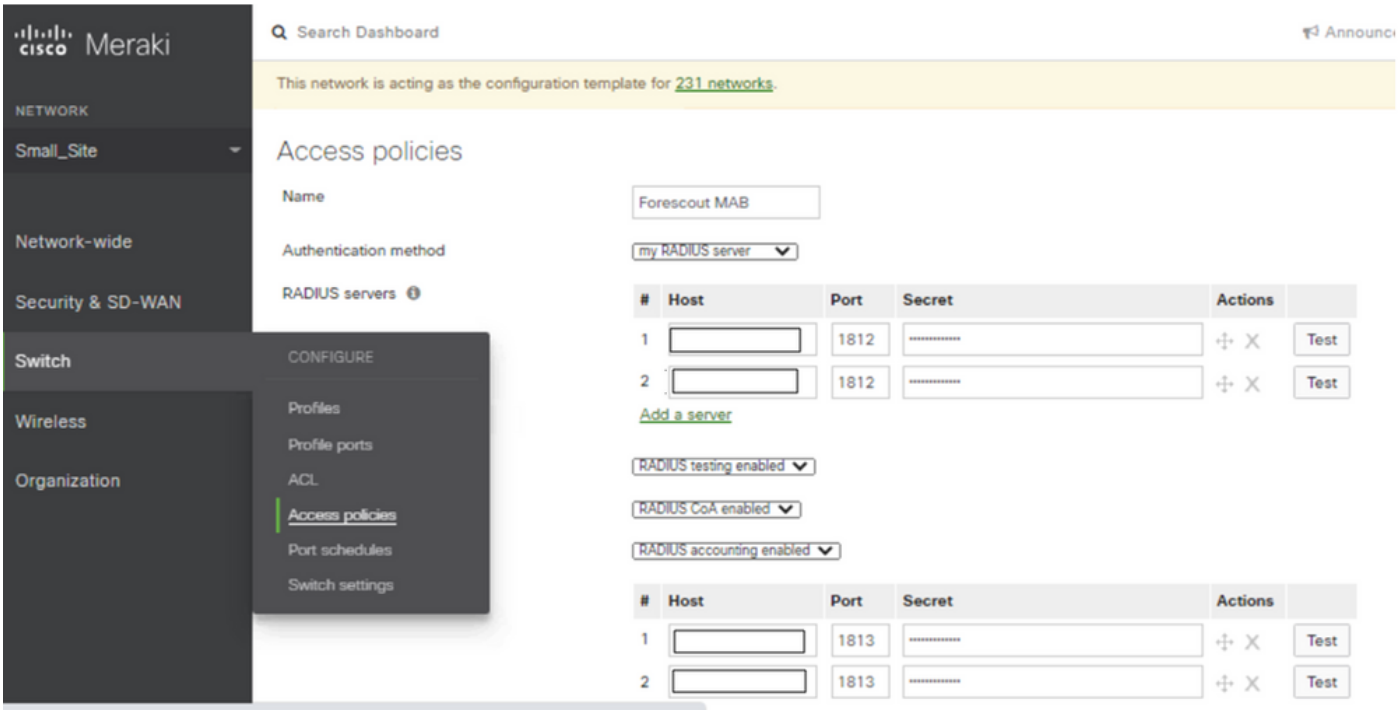


2. Puntos de acceso MR (activados por identificador de conjunto de servicios (SSID)):
Wireless > Access control



3. MS-Switches

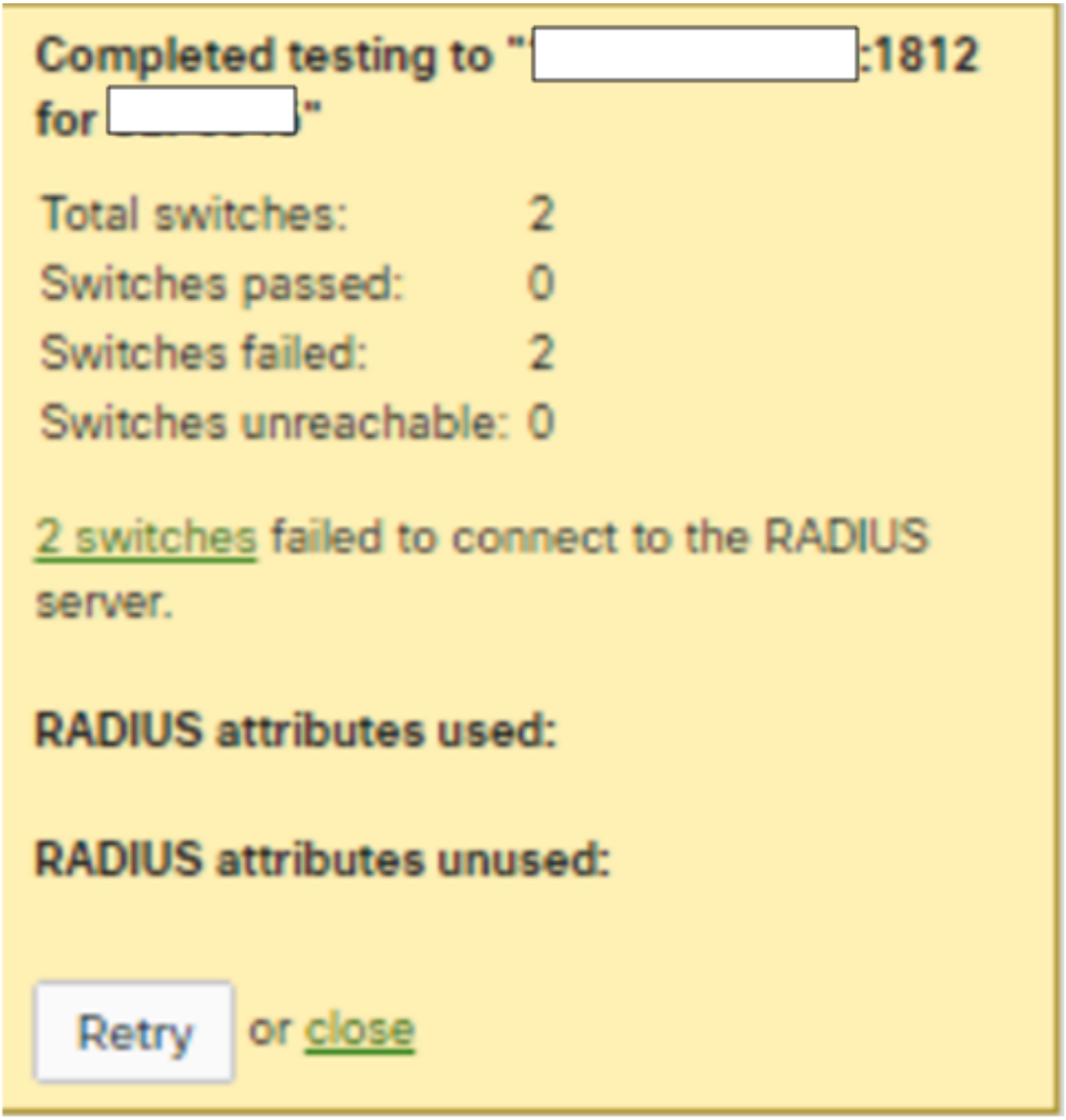
Switch > Políticas de acceso



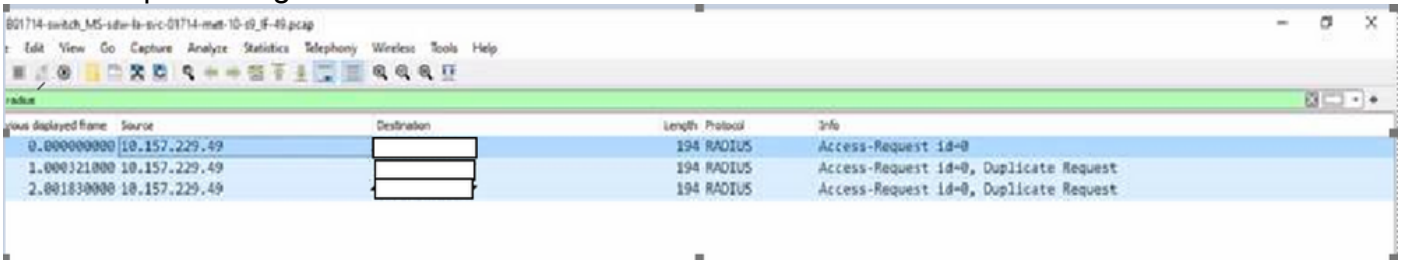
Prueba de verificación de la configuración 802.1X

- **Panel de Meraki > Plantilla de Red > Switch > Políticas de Acceso > Servidores Radius > Prueba**
- **Panel Meraki > Plantilla de red > Tecnología inalámbrica > Control de acceso > Servidores Radius > Prueba**

1. Si el resultado de la prueba se observa como **Todos los AP no pudieron conectar el servidor RADIUS**, debe verificar dónde se descartó la solicitud de acceso.

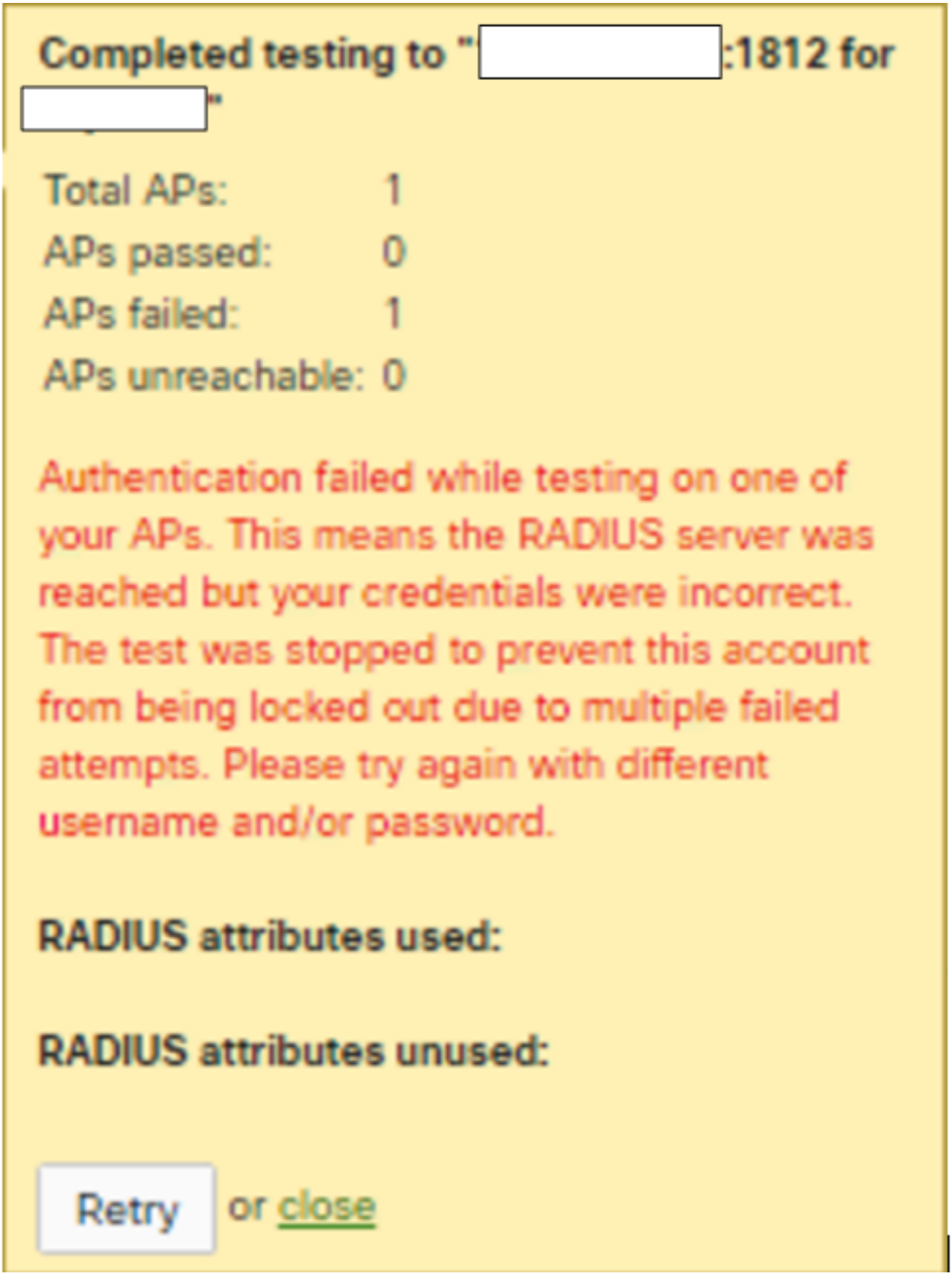


2. Ejecute la captura de paquetes en el puerto de link ascendente y verifique el flujo de solicitud de acceso. Consulte la captura de pantalla del acceso a la captura de paquetes - La solicitud no recibe respuesta alguna.

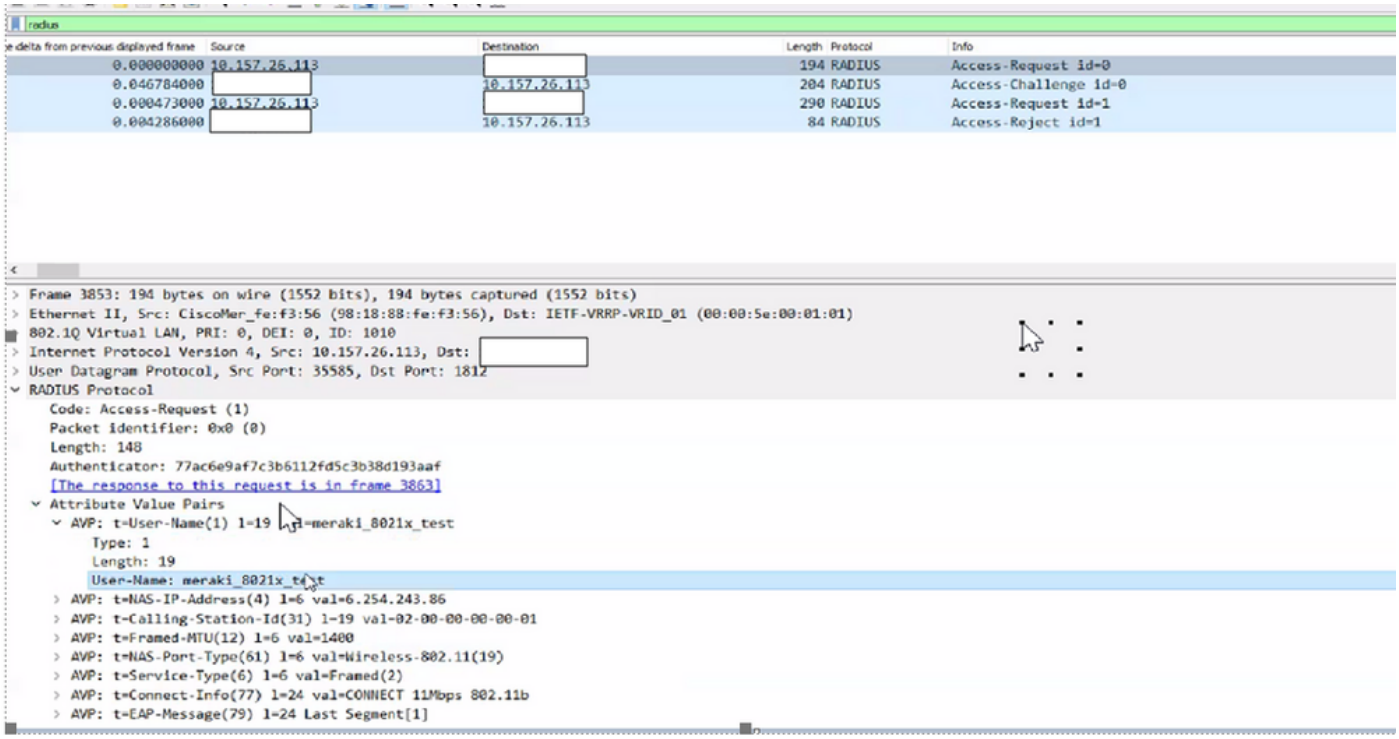


3. Si el resultado de la prueba observado se contesta como aceptar/rechazar/rechazar/responder/credenciales incorrectas, significa que el servidor radius

está vivo.

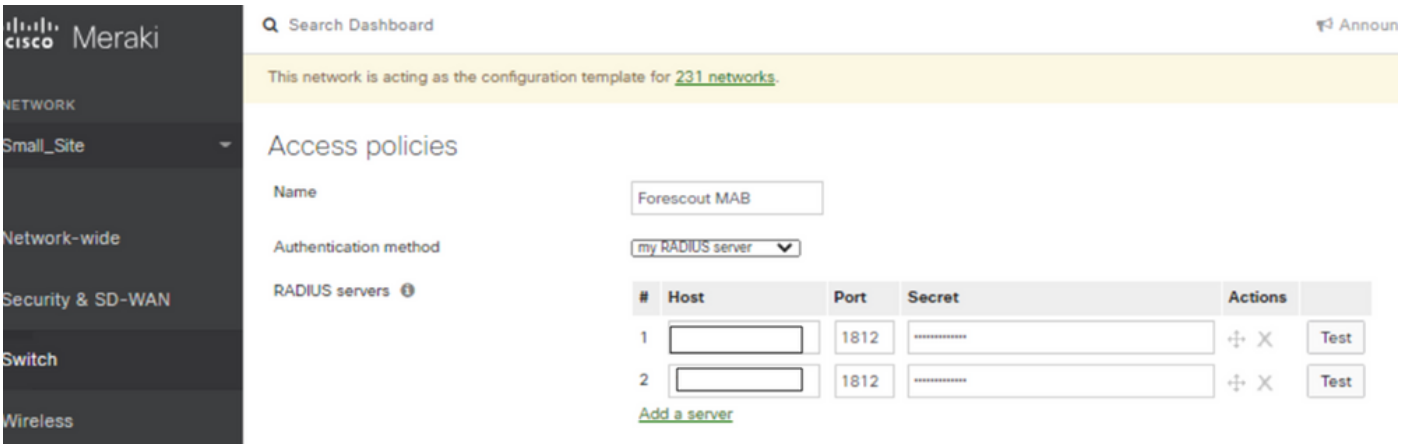


4. Ejecute la captura de paquetes en el puerto de link ascendente y verifique el flujo de solicitud de acceso. Consulte la captura de pantalla del acceso a la captura de paquetes: la solicitud obtuvo una respuesta.

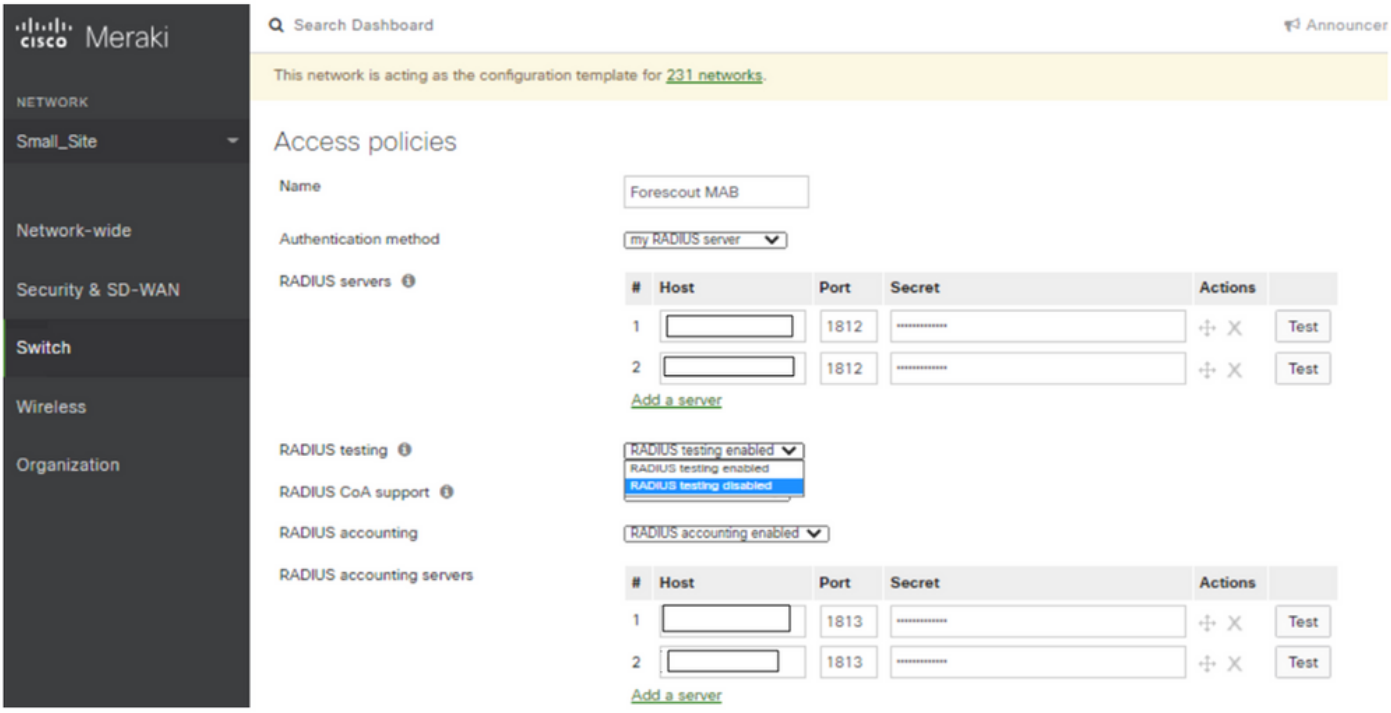


Verificación de la configuración de la política de acceso

1. Es necesario verificar que el parámetro mencionado en la política de acceso sea correcto e incluya la dirección IP del host, el número de puerto y la clave secreta.



2. Las IP configuradas del servidor RADIUS son falsas o no se utilizan en la producción o la política de acceso no está en uso. Se recomienda quitar la política de acceso. Si desea conservarlo, puede desactivar la **configuración de prueba de Radius.**



Información Relacionada

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- Soporte Técnico y Documentación - Cisco Systems

Nota

- Cuando los servidores de radio sondean los dispositivos Meraki utilizando la IP de LAN y el nombre de usuario predeterminado "meraki_8021x_test", el panel de Meraki utilizó la dirección MAC de Meraki como origen.
- Meraki proporcionó visibilidad de estas alertas desde octubre de 2021.