排除Meraki设备中最近的802.1X故障警报

目录

简介

本文档介绍如何解决Meraki设备中最近的802.1X故障警报。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解基本的Meraki软件定义广域网(SDWAN)解决方案
- 了解基本访问策略和Radius身份验证

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

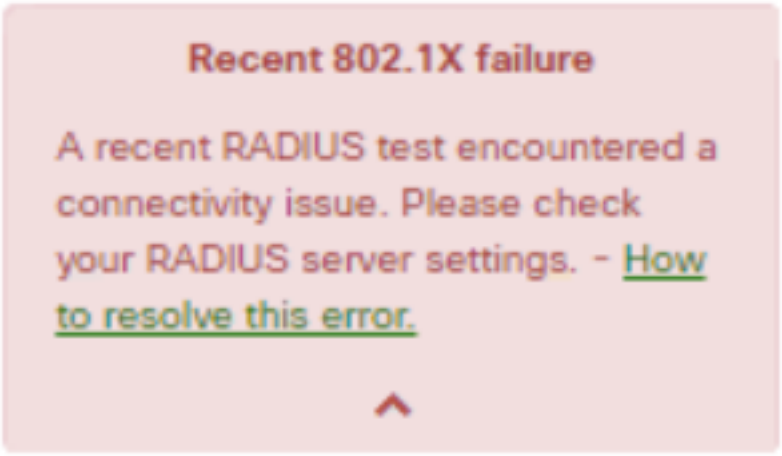
问题

Meraki设备使用AAA RADIUS服务器策略配置对最终用户进行身份验证。

Meraki设备中的RADIUS测试是什么？

最近的802.1X故障警报显示，如果发送到已配置RADIUS服务器的定期访问请求消息无法访问，则必须使用10秒的超时时间。

Meraki设备定期向使用身份meraki_8021x_test的已配置RADIUS服务器发送访问请求消息，**以确保RADIUS服**务器可访问。这些访问请求的超时时间为10秒，如果RADIUS服务器未响应，则会认为RADIUS服务器不可达并提示“最近802.1X故障”警报消息。请参阅设备上显示的警报截图：



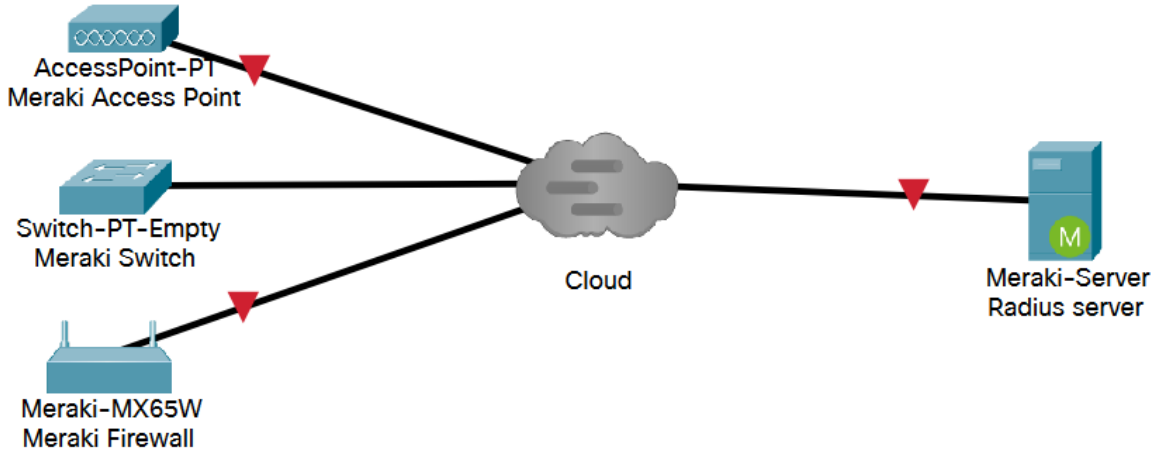
如果Meraki设备收到来自服务器的任何合法RADIUS响应(Access-Accept/Reject/Challenge)，则测试被视为成功。

启用RADIUS测试后，所有RADIUS服务器都将在每个节点上至少每24小时运行一次测试，而不管测试结果如何。如果给定节点的RADIUS测试失败，它会每小时重新测试一次，直到结果通过。随后的通行将标记服务器可访问，清除警报并返回24小时测试周期。

配置

网络图

以下是描述设置的简单拓扑图：



验证与故障排除

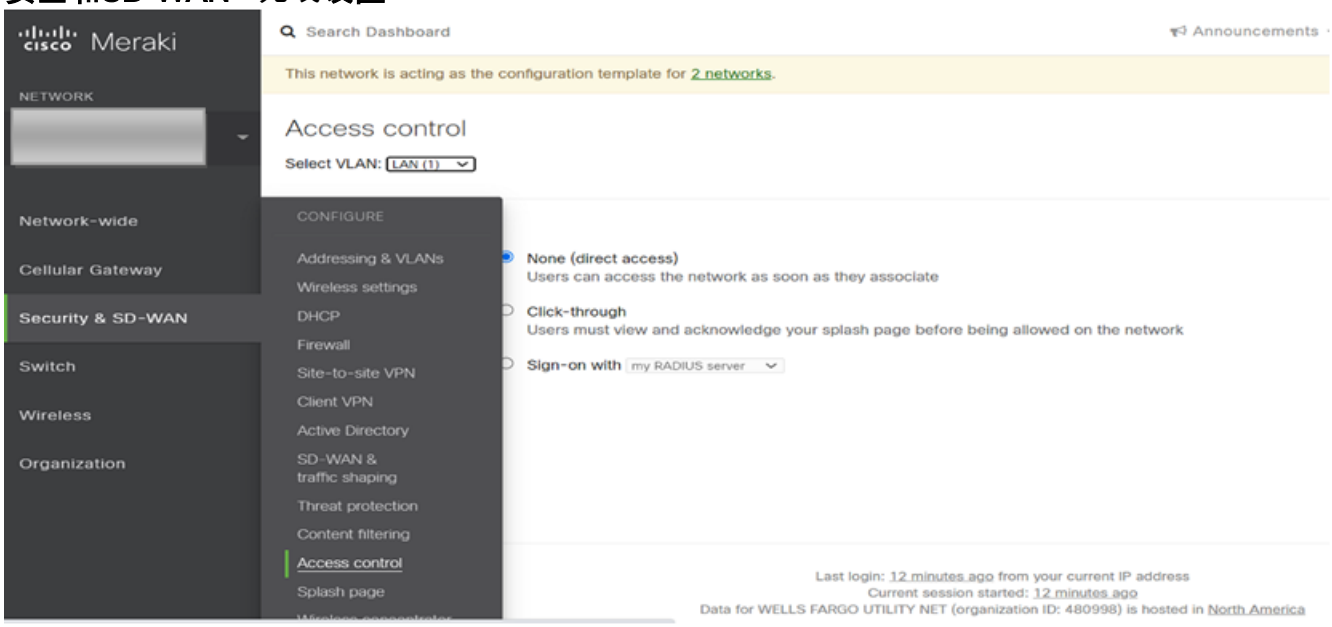
802.1X配置

802.1X RADIUS配置可在显示的路径中找到，具体取决于Meraki产品型号。

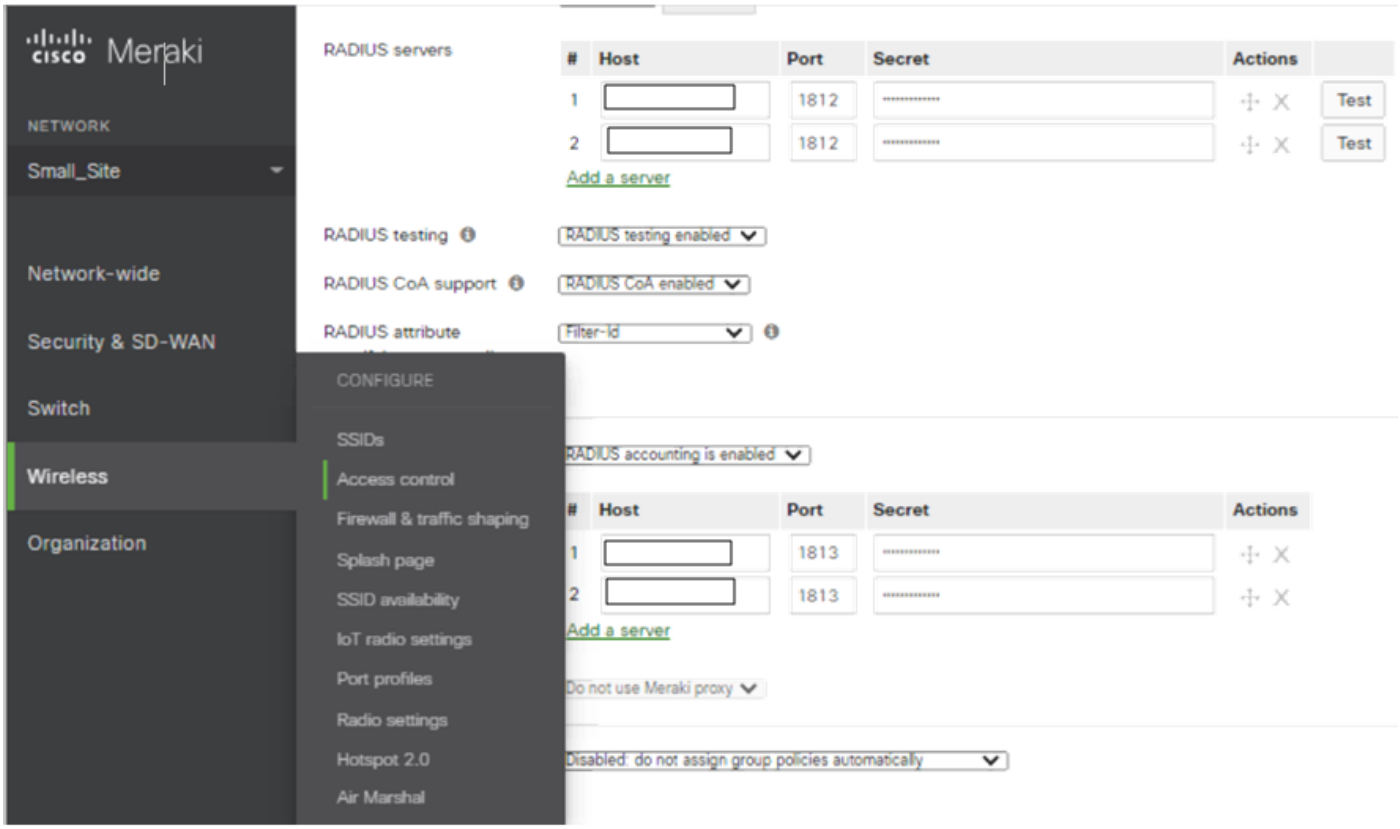
1. MX-Security设备（为接入端口或无线配置）

- 对于接入端口
  安全和SD-WAN >编址和VLAN

- 无线
  安全和SD-WAN >无线设置

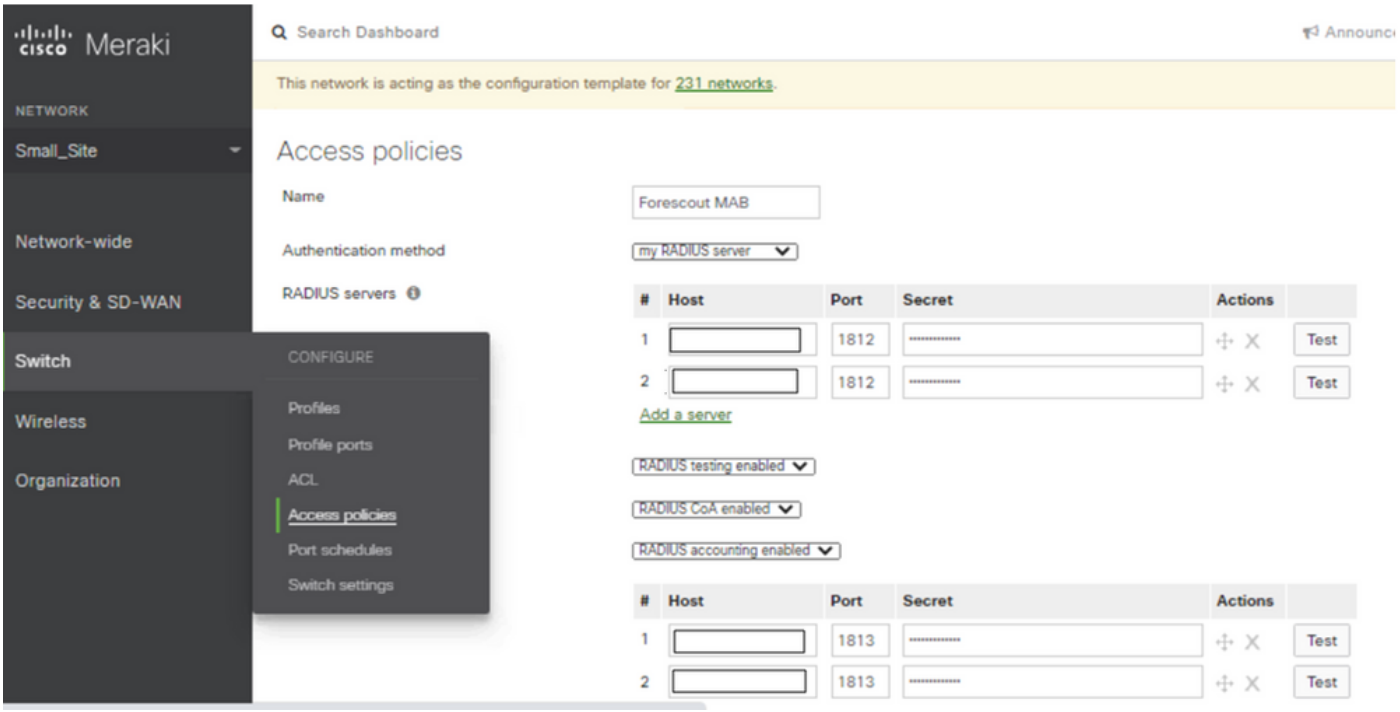


2. MR — 接入点(根据服务集标识符(SSID)启用):
无线>访问控制



3. MS-Switch

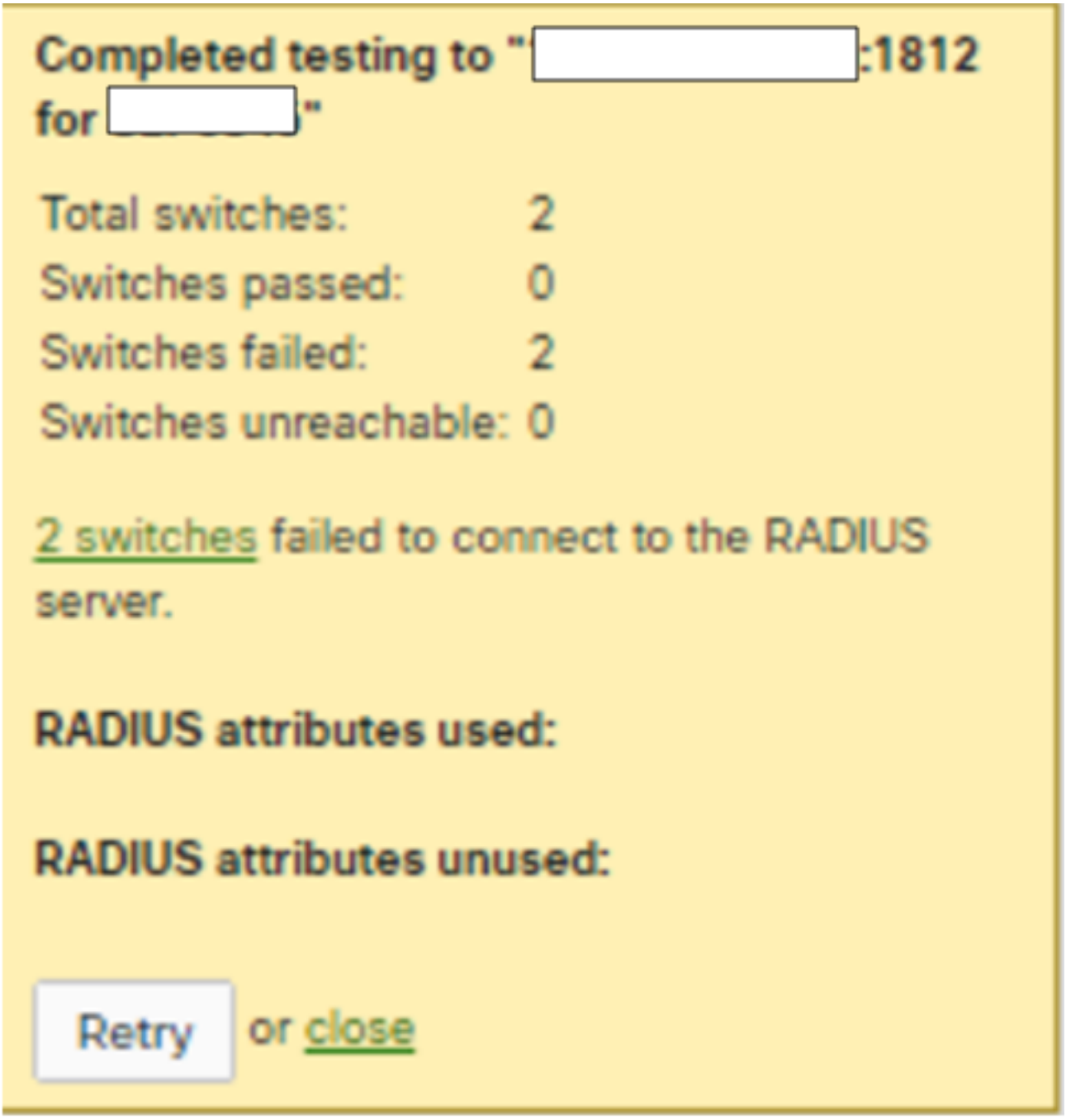
交换机> 访问策略



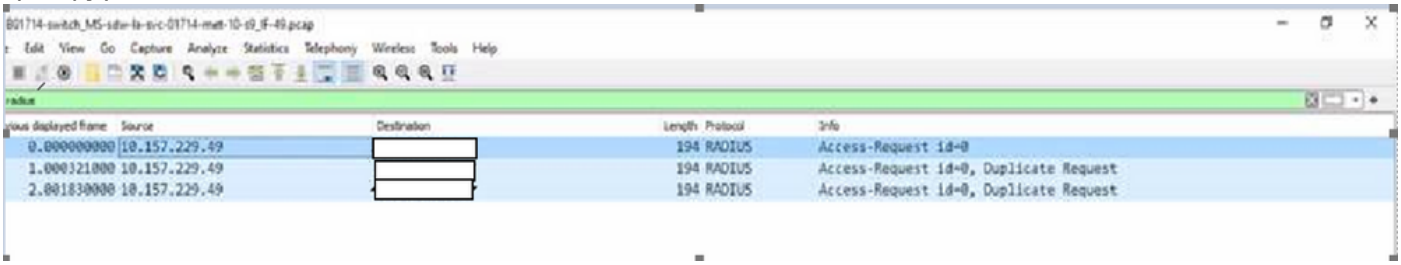
802.1X配置验证测试

- **Meraki控制面板>网络模板> 交换机> 访问策略> Radius服务器> 测试**
- **Meraki控制面板 > 网络模板 > 无线 > 访问控制 > RADIUS 服务器 > 测试**

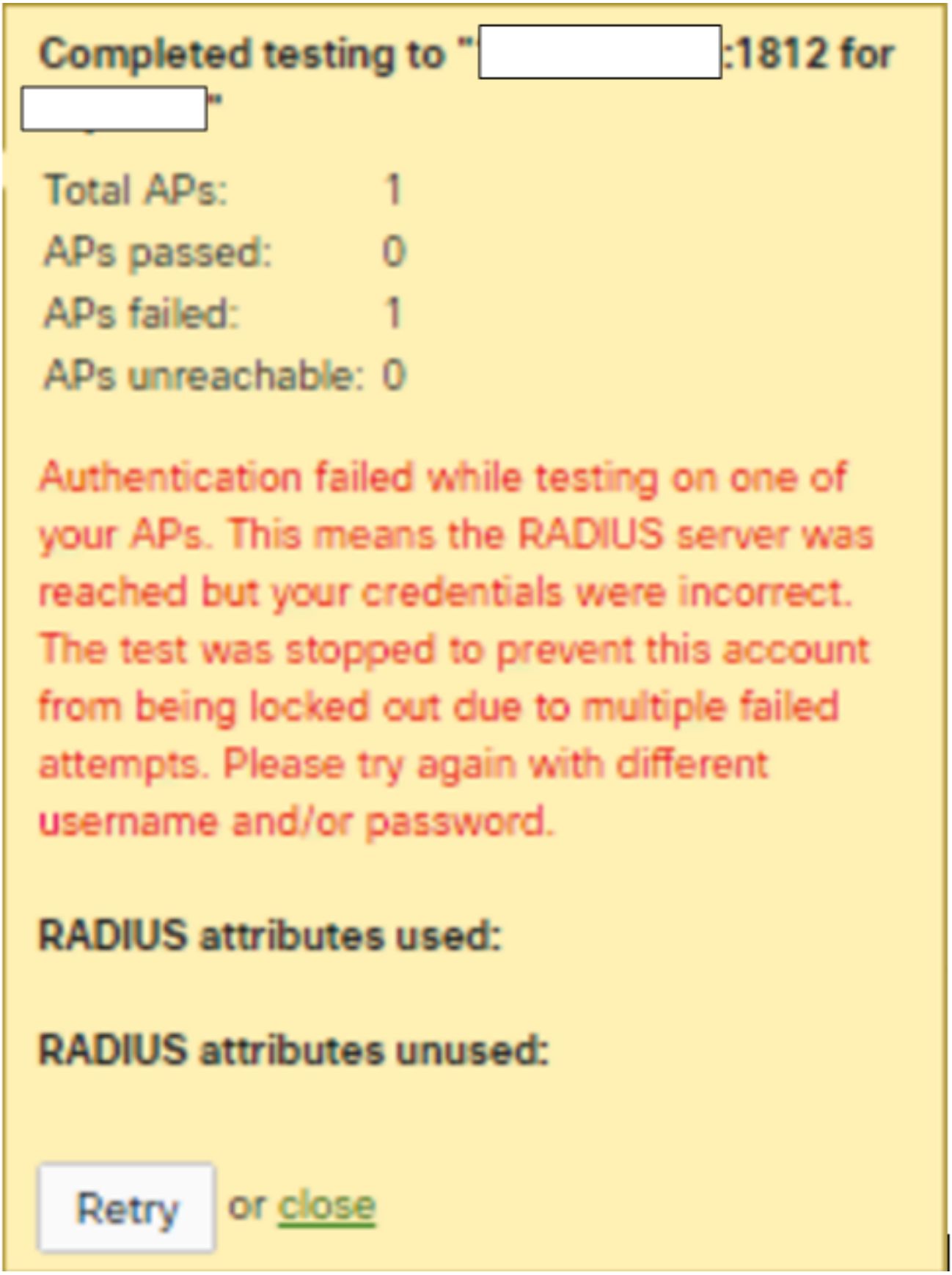
1.如果在All AP failed to connect radius server(所有AP无**法连接RADIUS服务器)中注意到测试结果**，则需要检查访问请求被丢弃的位置。



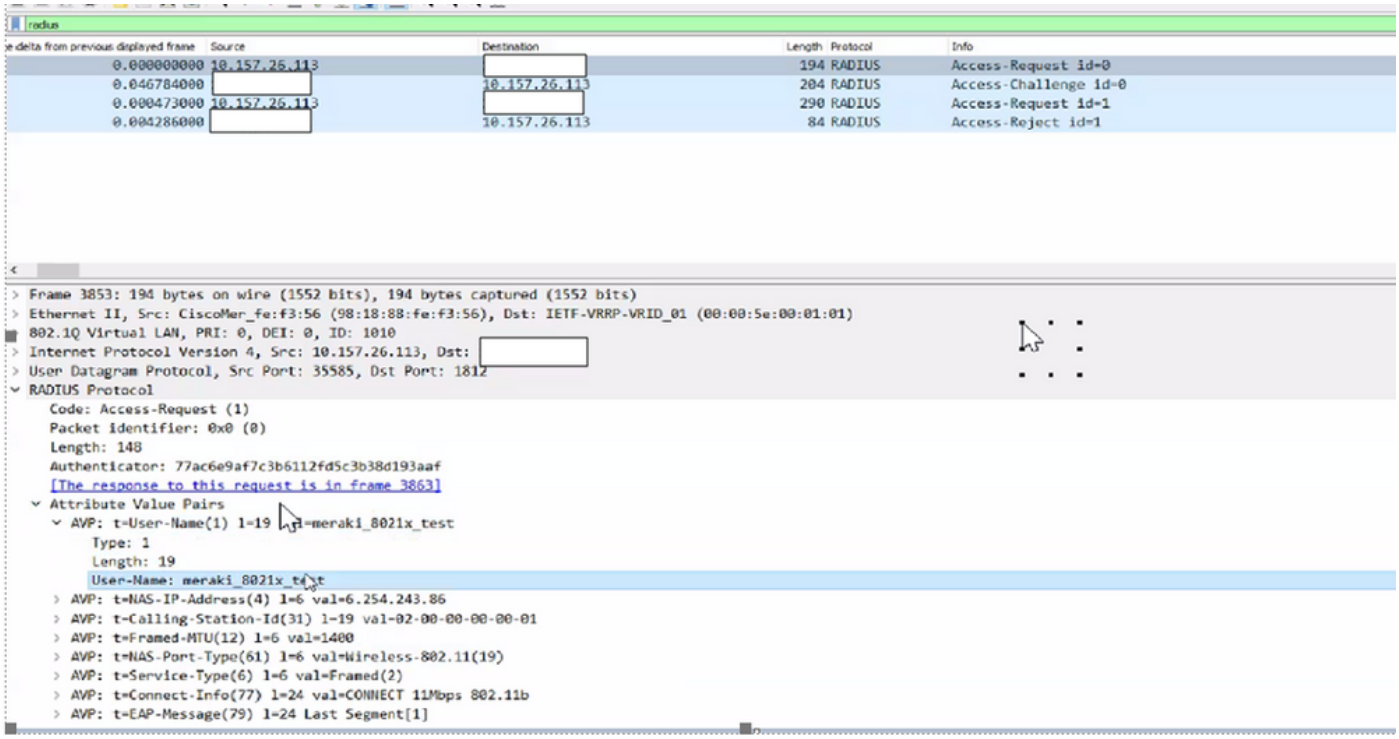
2.在上行链路端口上运行数据包捕获并检验访问请求流。请参阅数据包捕获访问权限的截图 — 请求未获得任何回复。



3.如果已注意到的测试结果被回复为接受/拒绝/拒绝/响应/不正确的凭据，则表示RADIUS服务器处于活动状态。

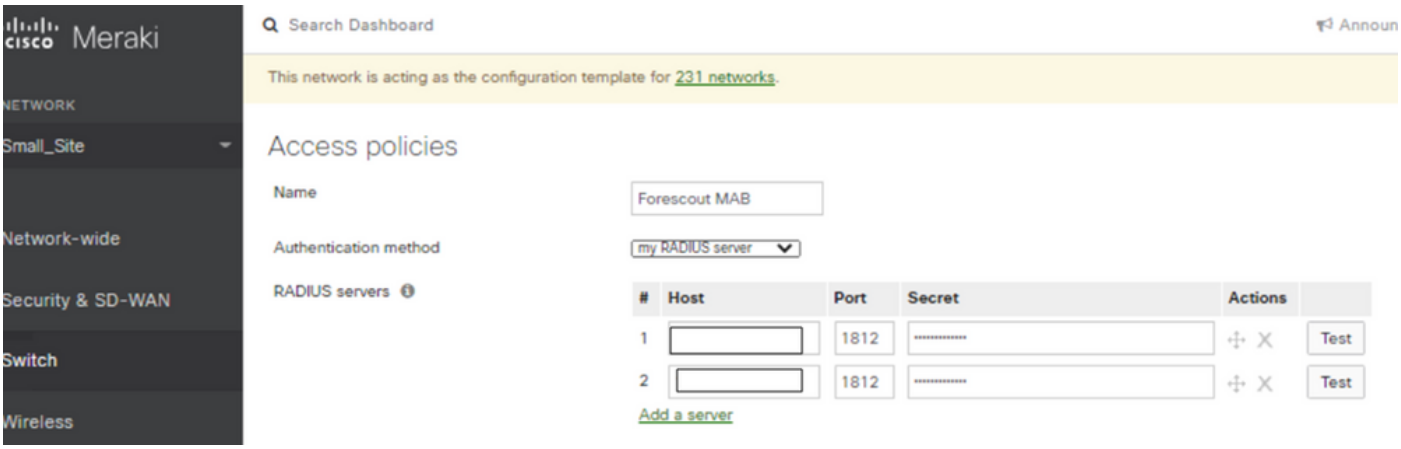


4.在上行链路端口上运行数据包捕获并检验访问请求流。请参阅数据包捕获访问权限的截图 — 请求得到应答。

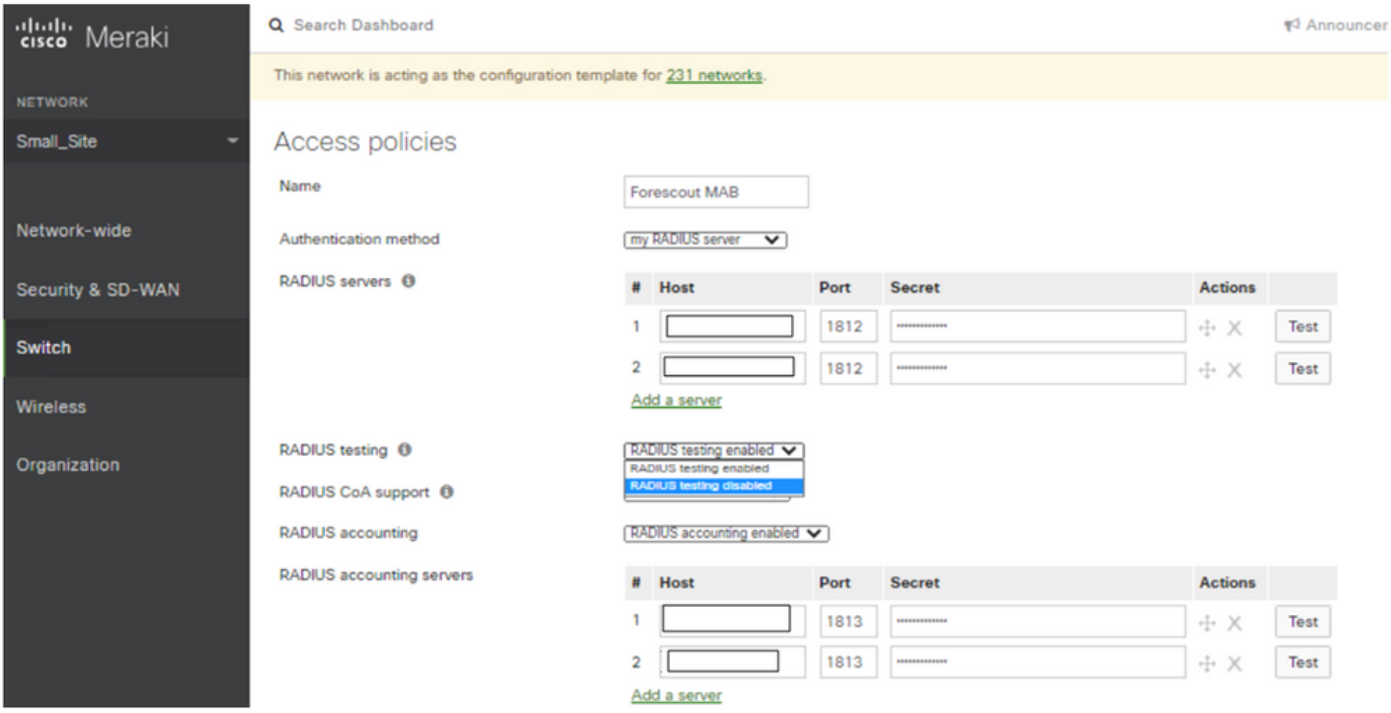


访问策略配置验证

1.需要检查访问策略中提到的参数是否正确，包括主机IP、端口号和密钥。



2.配置的RADIUS服务器IP是虚构的或未在生产中使用或访问策略未在使用。建议删除访问策略。如果要保留它，可以禁用**Radius测试设置。**



相关信息

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- 技术支持和文档 - Cisco Systems

备注

- 当RADIUS服务器轮询Meraki设备时，使用LAN IP和默认用户名“meraki_8021x_test”，Meraki控制面板使用Meraki MAC地址作为源。
- 自2021年10月起，Meraki提供了这些警报的可视性。