Troubleshoot Recent 802.1X Failure Alert in Meraki Device

Contents

Introduction

This document describes how to resolve the recent 802.1X failure alert in the Meraki device.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Understand basic Meraki Software-Defined Wide Area Network (SDWAN) solution
- Understand basic Access Policy & Radius authentication

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

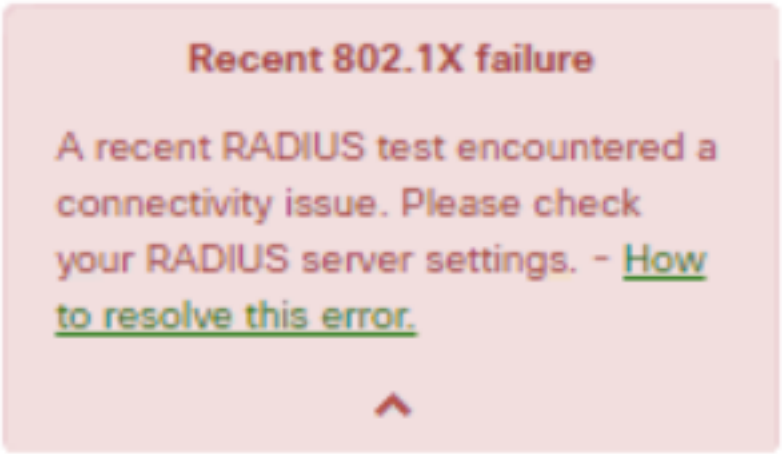
Problem

Meraki devices use the AAA radius server policy configuration to authenticate the end-user.

What is the RADIUS test in Meraki devices?

The recent 802.1X failure alert displayed that, if the periodic access-request messages sent to the configured RADIUS servers are unreachable, you must use a timeout period of 10 seconds.

Meraki devices periodically send Access-Request messages to the configured RADIUS servers that use identity **meraki_8021x_test** to ensure that the RADIUS servers are reachable. These Access-Requests have a timeout of 10 seconds and if the RADIUS server does not respond then it considers radius servers are unreachable and prompts the alert "Recent 802.1X failure" message. Refer to the screenshot of the alert seen on the device:



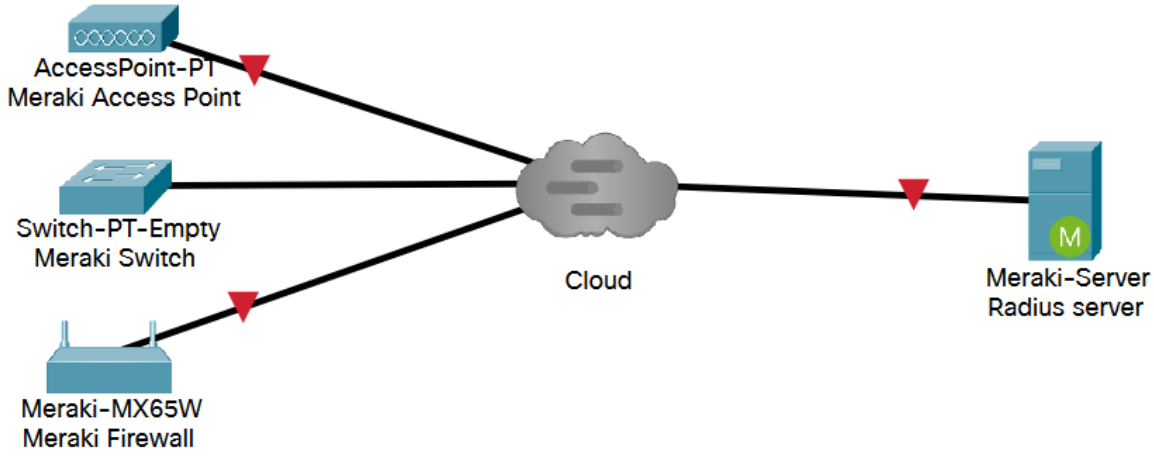
A test is considered successful if the Meraki device receives any legitimate RADIUS response (Access-Accept/Reject/Challenge) from the server.

With the RADIUS test enabled, all RADIUS servers are kept test run on every node at least once per 24 hours regardless of a test result. If a RADIUS test fails for a given node, it tests again every hour until a result that passes occurs. A subsequent pass marks the server reachable, clears the alert, and returns to the 24-hour test cycle.

Configure

Network Diagram

Here is a simple topology diagram that describes the setup:



Verify And Troubleshoot

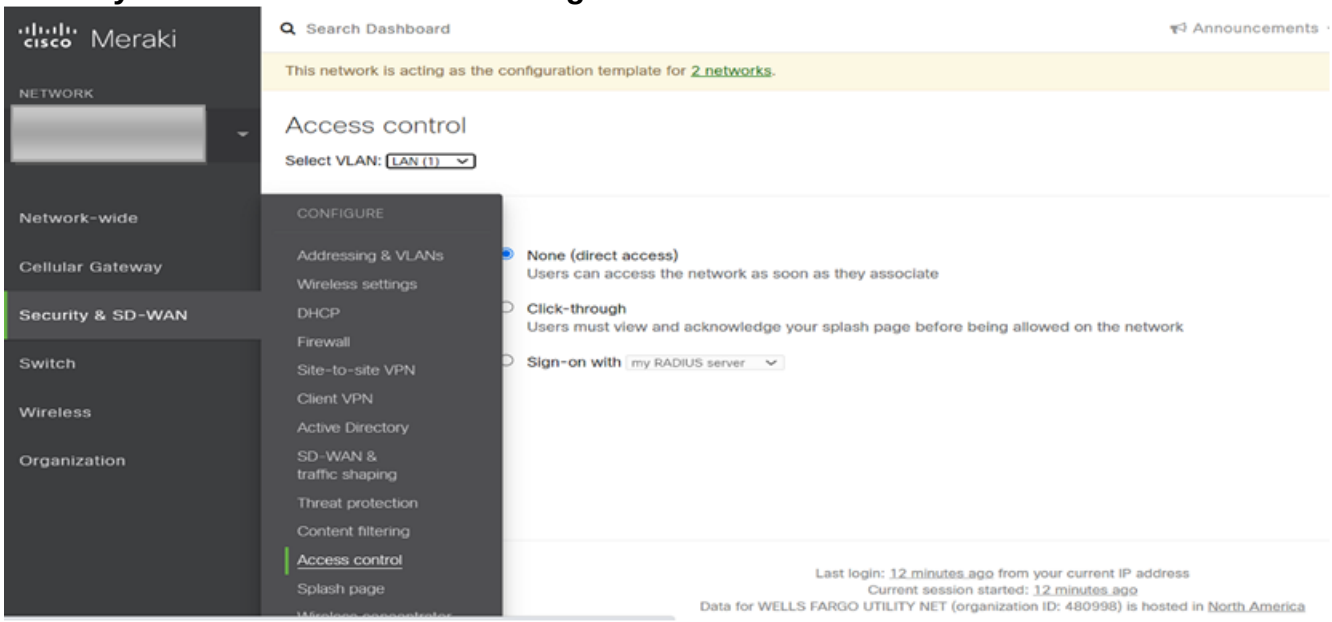
802.1X Configuration

802.1X RADIUS configuration can be found in the path shown that depends on the Meraki product Model.

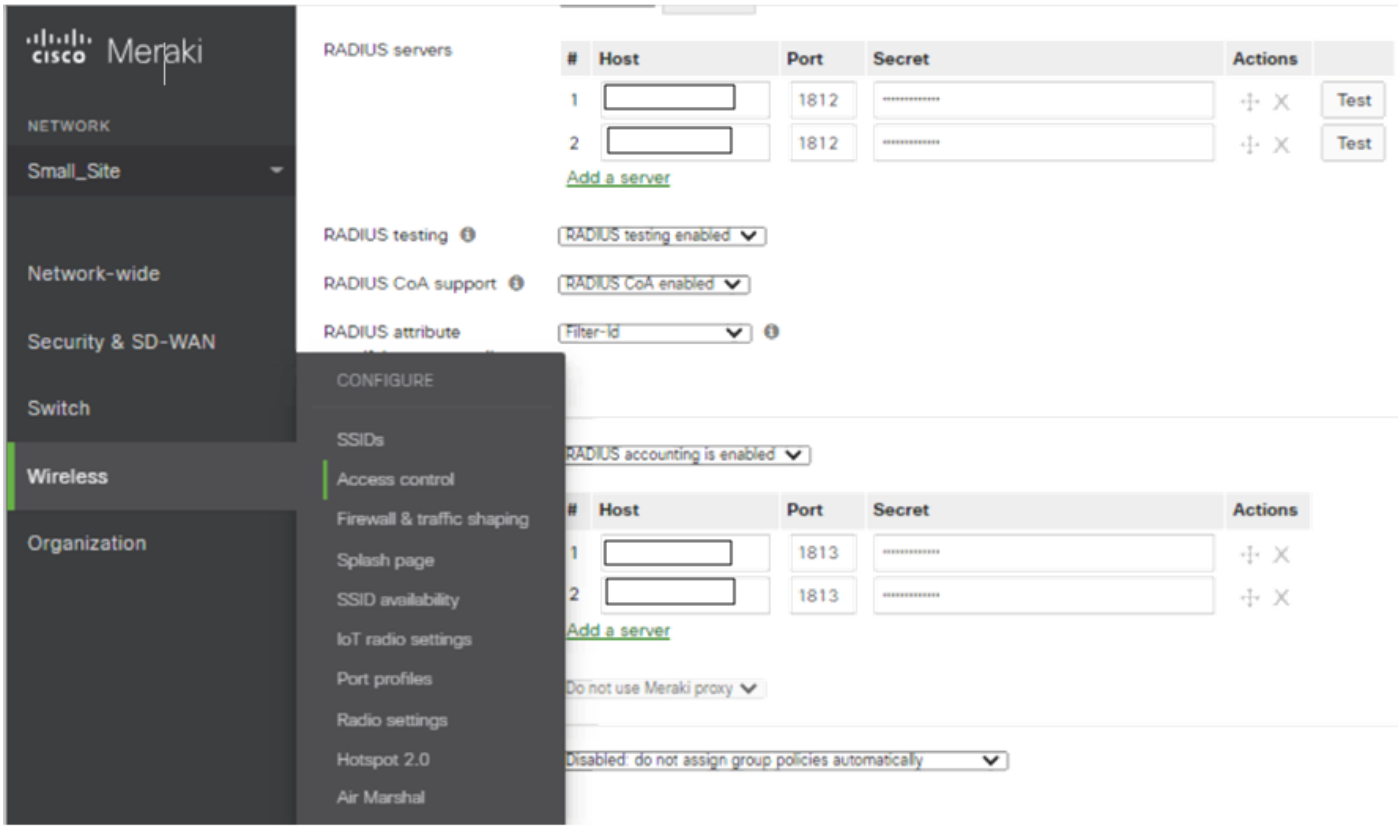
1. MX-Security appliance (configured either for access ports or wireless)

- For Access Ports
  Security & SD-WAN > **Addressing & VLANs**

- For Wireless
  Security & SD-WAN > **Wireless settings**

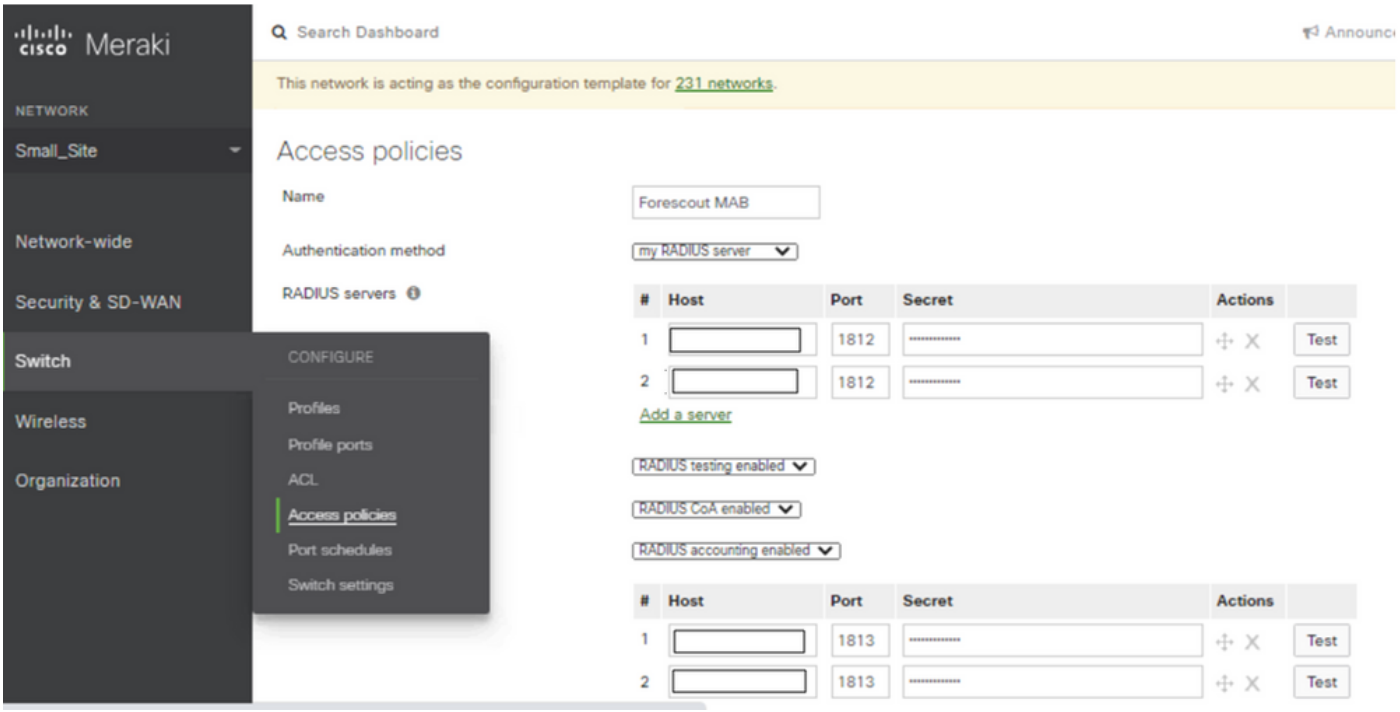


2. MR-Access points (enabled on a per Service Set Identifier (SSID) basis):
Wireless > **Access control**



3. MS-Switches

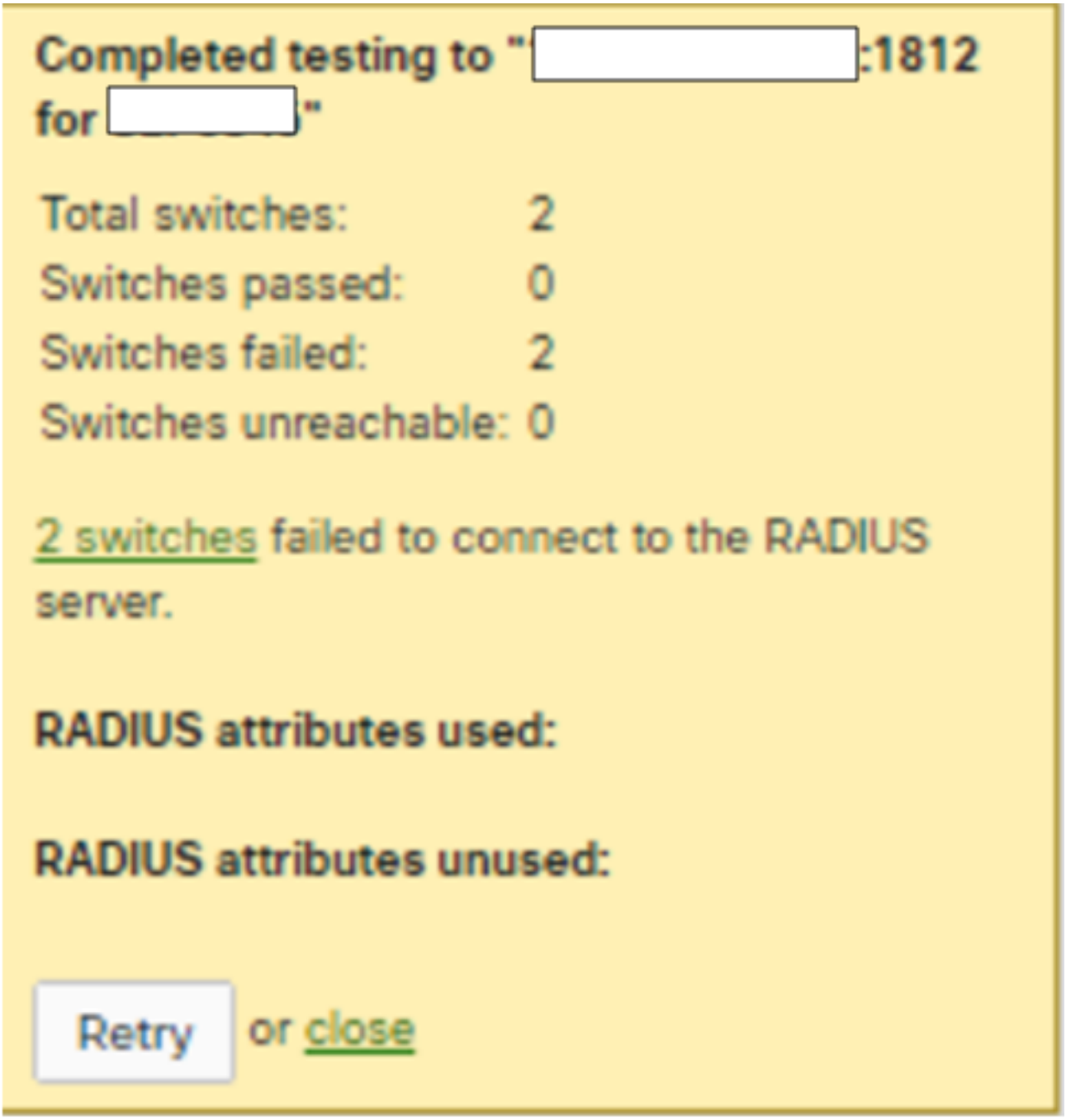
Switch > **Access Policies**



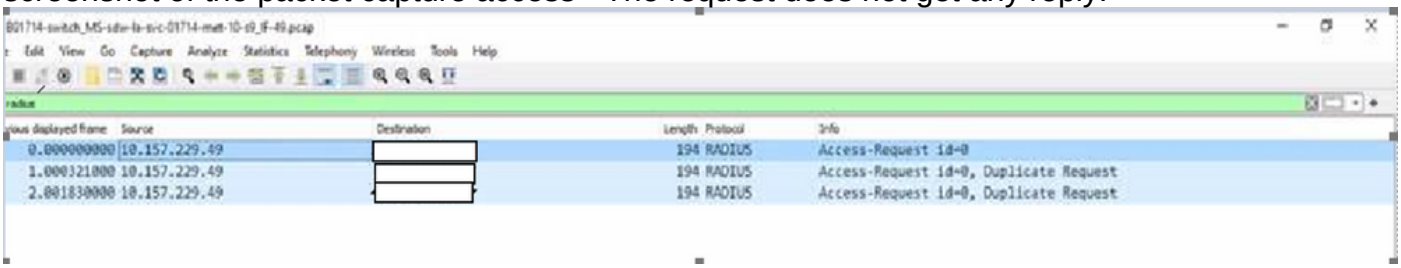
802.1X Configuration Verification Test

- **Meraki Dashboard** > **Network Template** > **Switch** > **Access Policies** > **Radius Servers** > **Test**
- **Meraki Dashboard** > **Network Template** > **Wireless** > **Access Control** > **Radius Servers** > **Test**

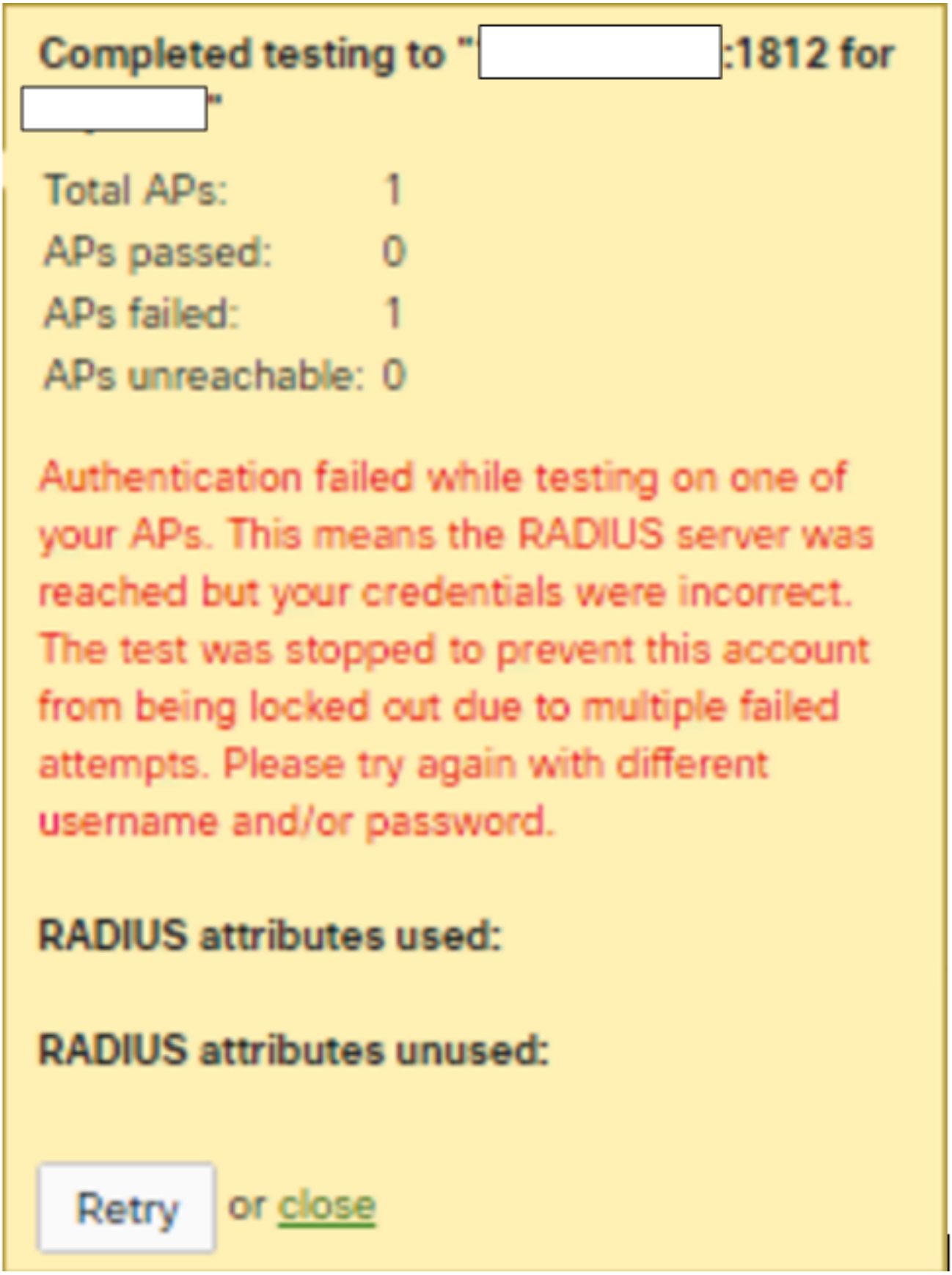
1. If the test result is noticed as **All AP failed to connect radius server**, you need to check where the access-Request got dropped.



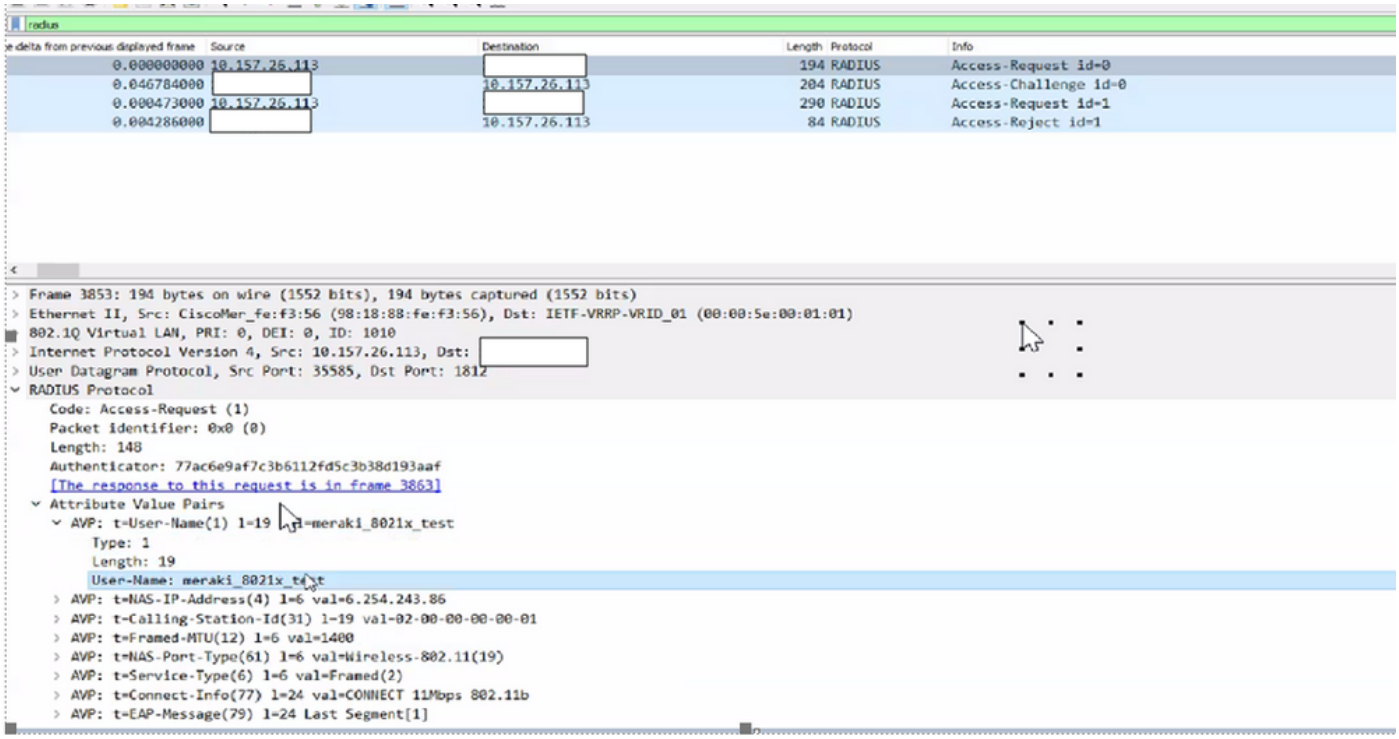
2. Run the packet capture on the uplink port and verify the access-request flow. Refer to the screenshot of the packet capture access - The request does not get any reply.



3. If noticed test result gets replied as accept/reject/deny/response/incorrect credentials, it means the radius server is alive.

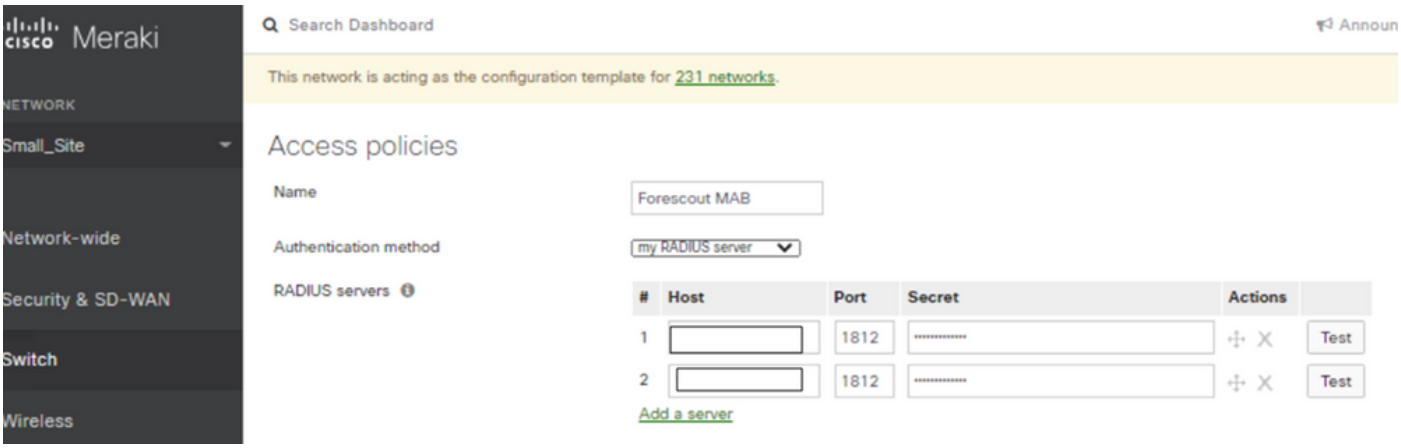


4. Run the packet capture on the uplink port and verify the access-request flow. Refer to the screenshot of the packet capture access - The request got a reply.

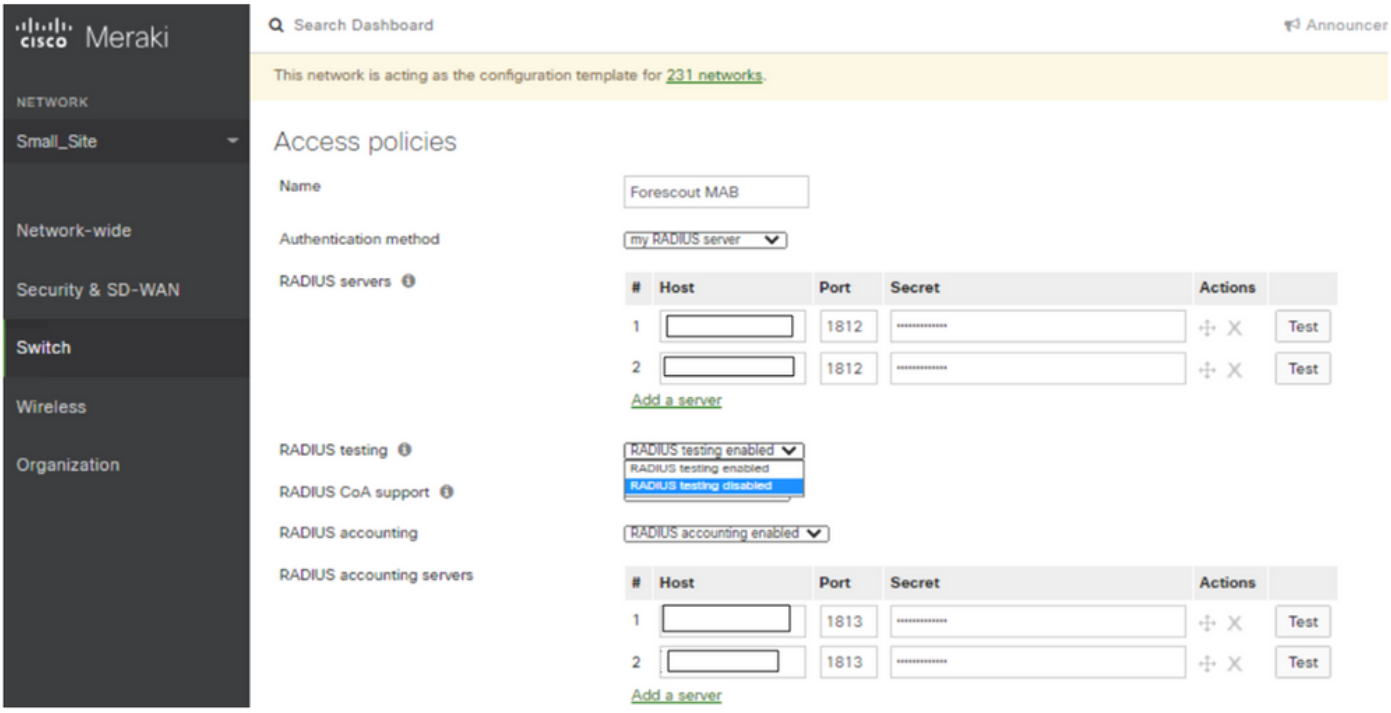


Access Policy Configuration Verification

1. Need to check the parameter mentioned in the access policy is correct and includes Host IP, Port Number, and Secret Key.



2. Configured radius server IPs are dummy or not used in production or Access policy is not in use. It is recommended to remove the access policy. If you want to keep it, you can disable the **Radius testing setting.**



Related Information

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- Technical Support & Documentation - Cisco Systems

Note

- When the radius servers poll Meraki devices use the LAN IP and Default username “meraki_8021x_test”, the Meraki dashboard used the Meraki MAC address as the source.
- Meraki provided visibility to these alerts since October 2021.