Risoluzione dei problemi relativi all'avviso di errore 802.1X recente nel dispositivo Meraki

Sommario

Introduzione

Questo documento descrive come risolvere il recente avviso di errore 802.1X nel dispositivo Meraki.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Comprendere le soluzioni base SDWAN (Wide Area Network) definite dal software Meraki
- Informazioni sulle regole di accesso di base e sull'autenticazione Radius

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

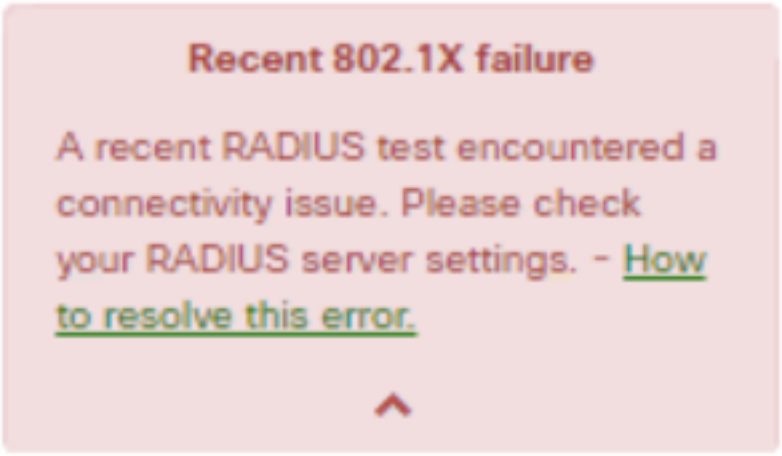
Problema

I dispositivi Meraki usano la configurazione delle policy del server AAA Radius per autenticare l'utente finale.

Cos'è il test RADIUS nei dispositivi Meraki?

Il recente avviso di errore 802.1X ha indicato che, se i messaggi periodici di richiesta di accesso inviati ai server RADIUS configurati non sono raggiungibili, è necessario utilizzare un periodo di timeout di 10 secondi.

I dispositivi Meraki inviano periodicamente messaggi di richiesta di accesso ai server RADIUS configurati che utilizzano l'identità **meraki_8021x_test** per garantire che i server RADIUS siano raggiungibili. Queste richieste di accesso hanno un timeout di 10 secondi e se il server RADIUS non risponde, considera i server RADIUS irraggiungibili e richiede il messaggio di avviso "Errore recente 802.1X". Fare riferimento allo screenshot dell'avviso visualizzato sul dispositivo:



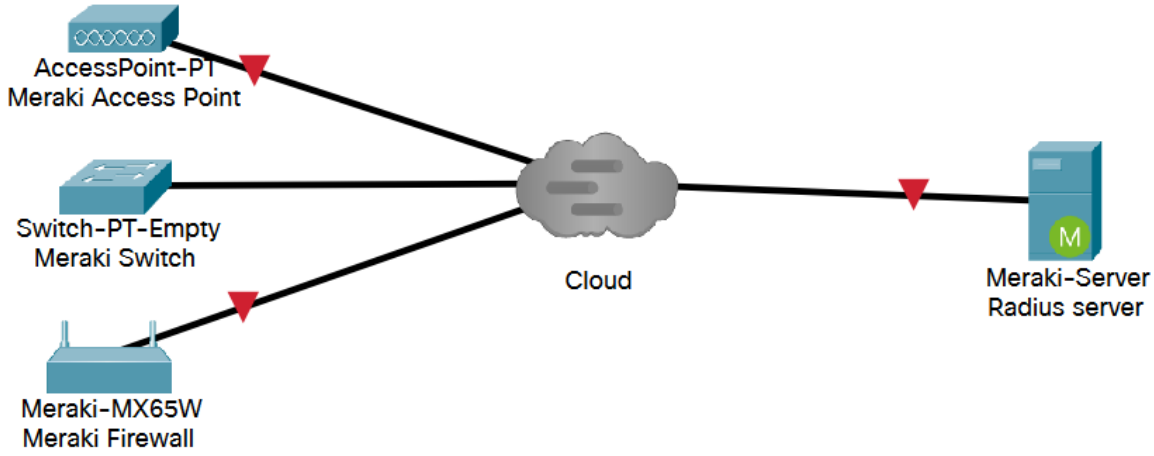
Un test è considerato riuscito se il dispositivo Meraki riceve una risposta RADIUS legittima (Access-Accept/Reject/Challenge) dal server.

Se il test RADIUS è abilitato, tutti i server RADIUS vengono mantenuti in esecuzione su ogni nodo almeno una volta ogni 24 ore, indipendentemente dal risultato del test. Se un test RADIUS non riesce per un determinato nodo, viene eseguito di nuovo ogni ora finché non si verifica un risultato positivo. Un passaggio successivo indica che il server è raggiungibile, cancella l'avviso e torna al ciclo di test di 24 ore.

Configurazione

Esempio di rete

Di seguito è riportato un semplice diagramma della topologia che descrive l'installazione:



Verifica E Risoluzione Dei Problemi

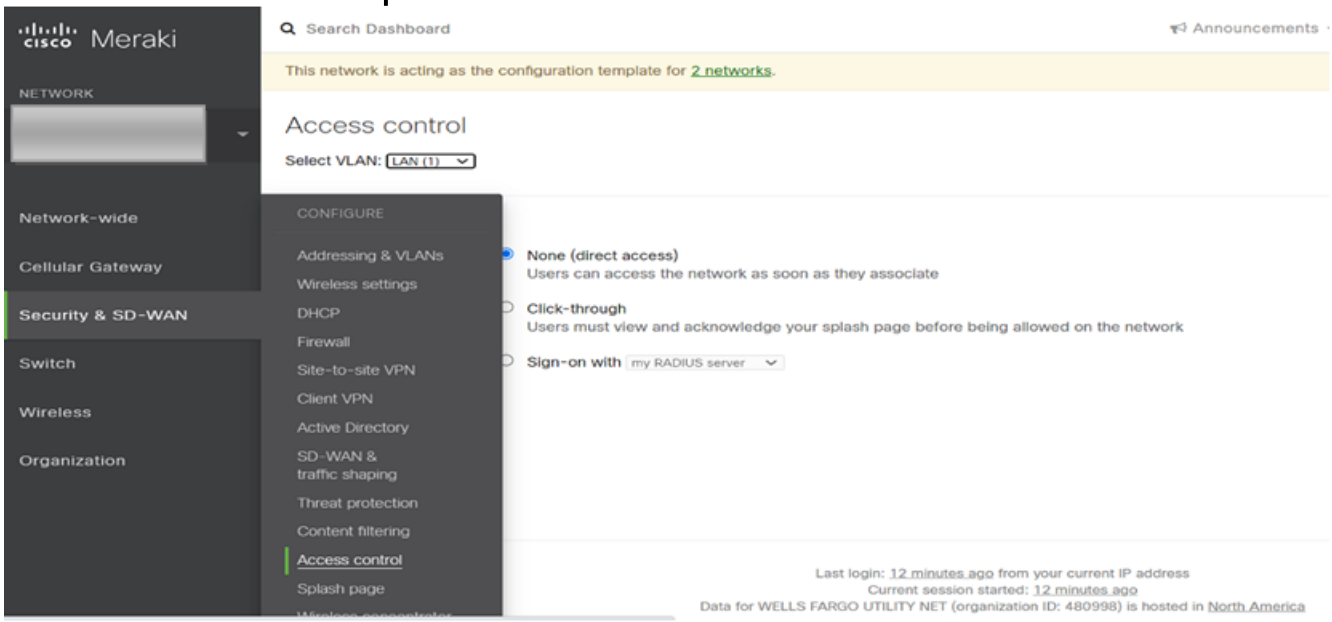
Configurazione 802.1X

La configurazione RADIUS 802.1X è disponibile nel percorso indicato, che dipende dal modello del prodotto Meraki.

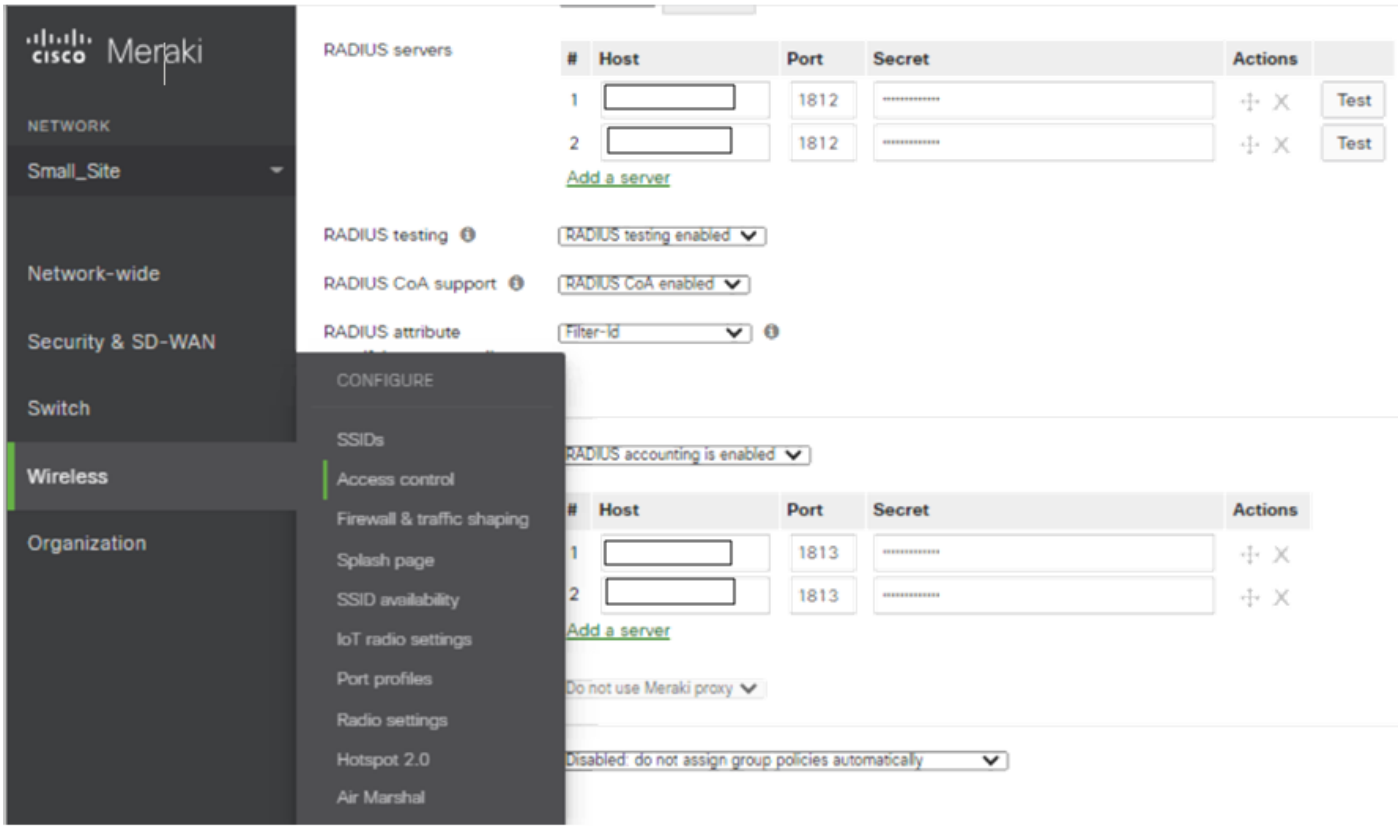
1. Appliance MX-Security (configurata per porte di accesso o wireless)

- Per porte di accesso
  Sicurezza e SD-WAN > Indirizzamento e VLAN

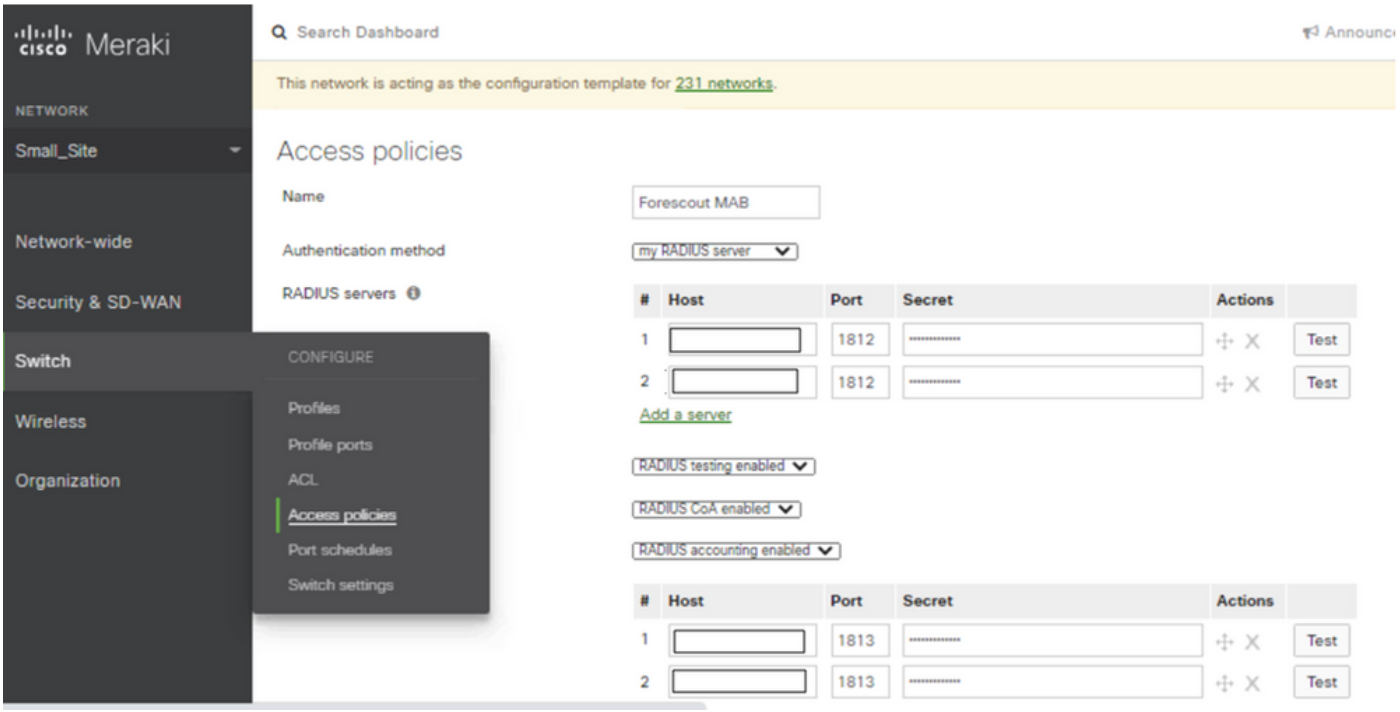
- Per wireless
  Sicurezza e SD-WAN > Impostazioni wireless



2. Punti di accesso MR (abilitati in base agli SSID (Service Set Identifier)):
Wireless > Controllo degli accessi



3. Switch MS
Cambia > Criteri di accesso

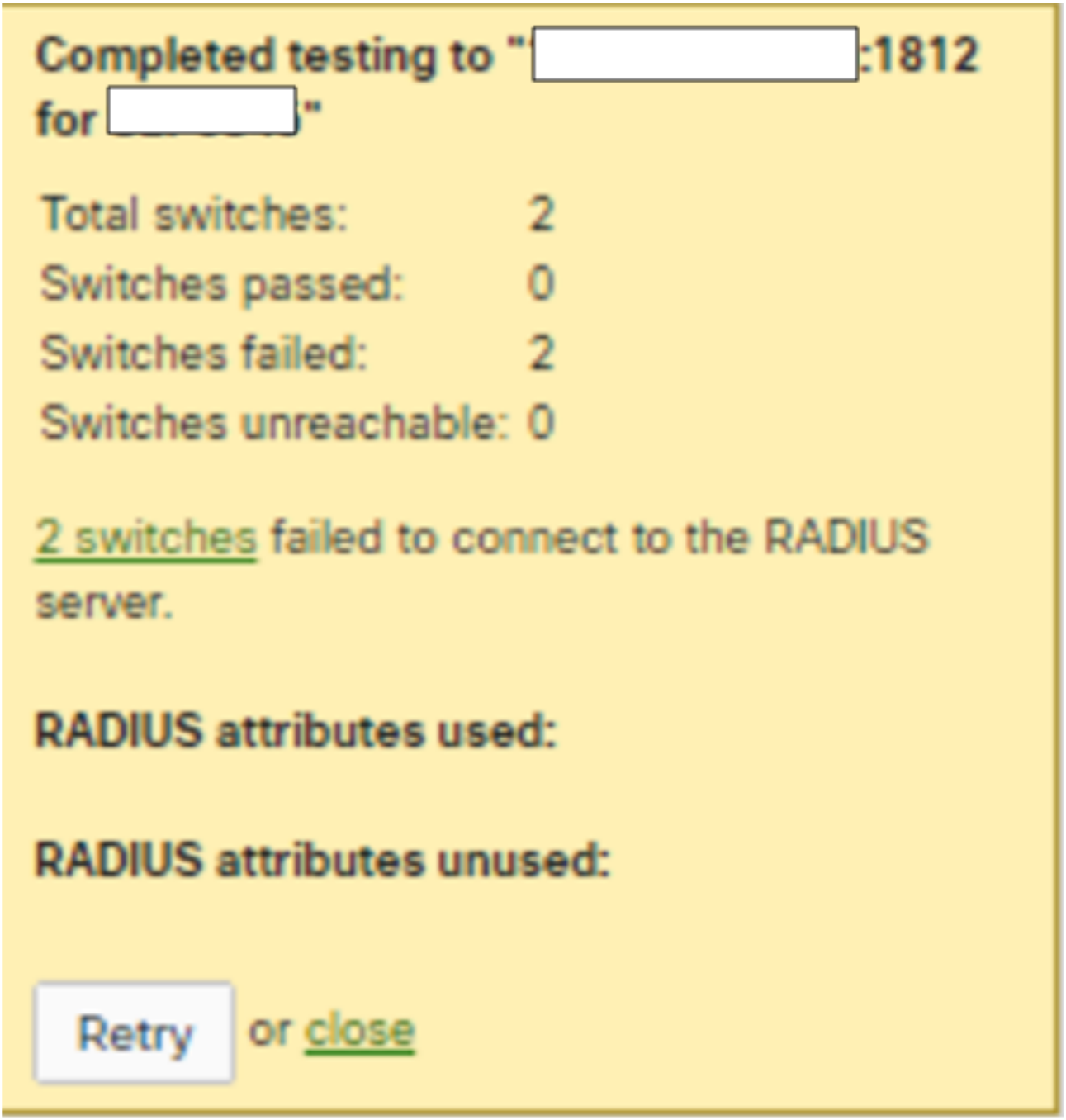


Test di verifica della configurazione 802.1X

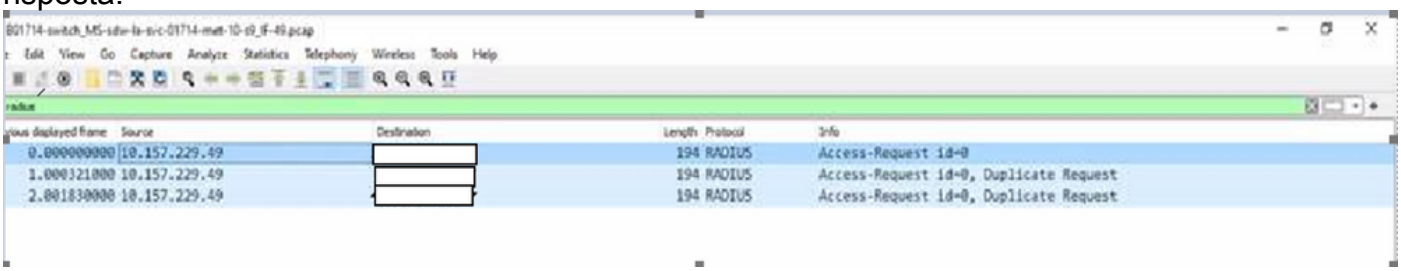
- **Dashboard Meraki > Modello Di Rete > Switch > Policy Di Accesso > Server Radius > Test**
- **Dashboard Meraki > Modello di rete > Wireless > Controllo dell'accesso > Server Radius > Test**

1. Se il risultato del test viene rilevato come **tutti gli access point non siano riusciti a connettere il**

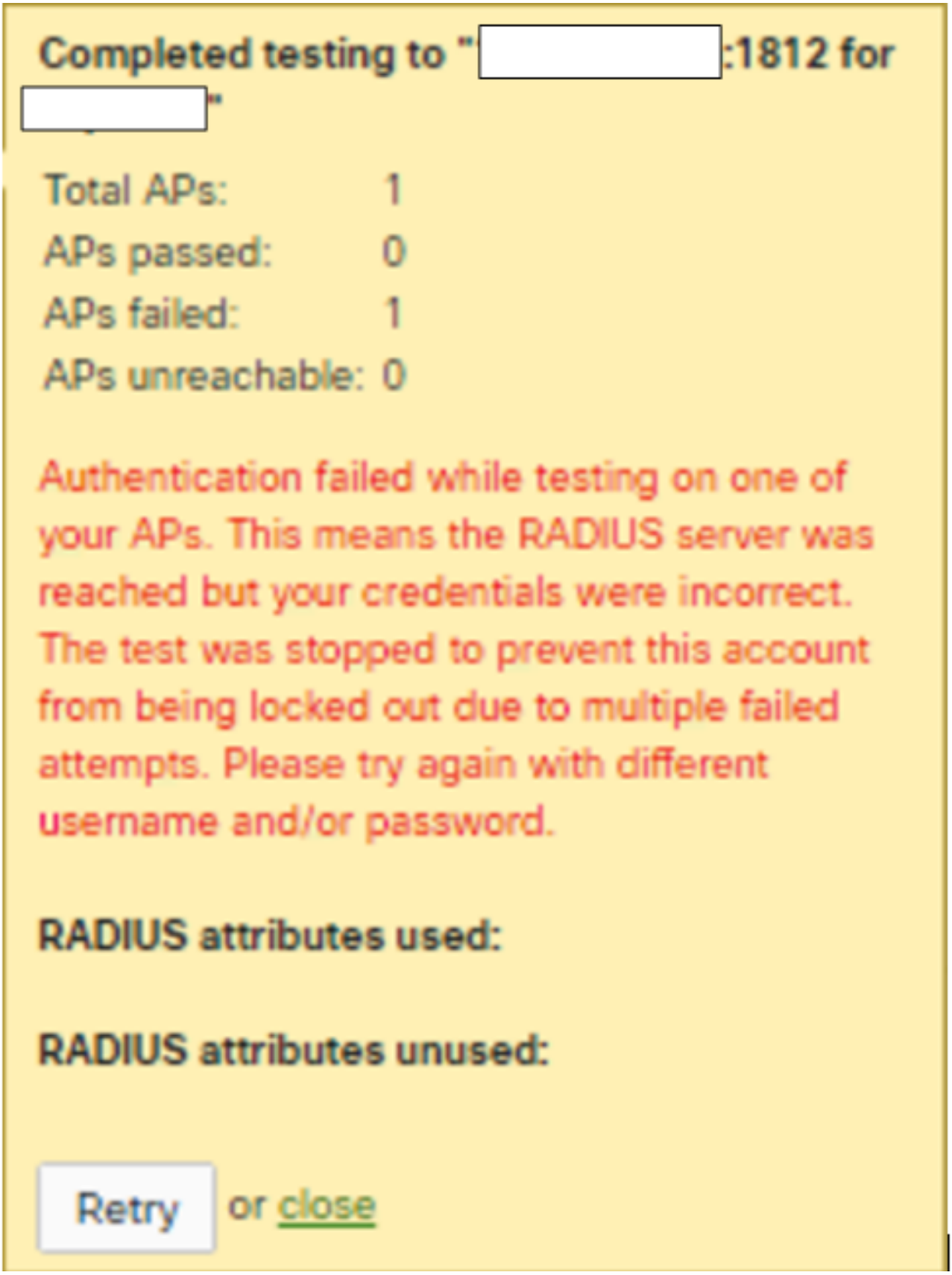
server radius, è necessario controllare dove la richiesta di accesso è stata eliminata.



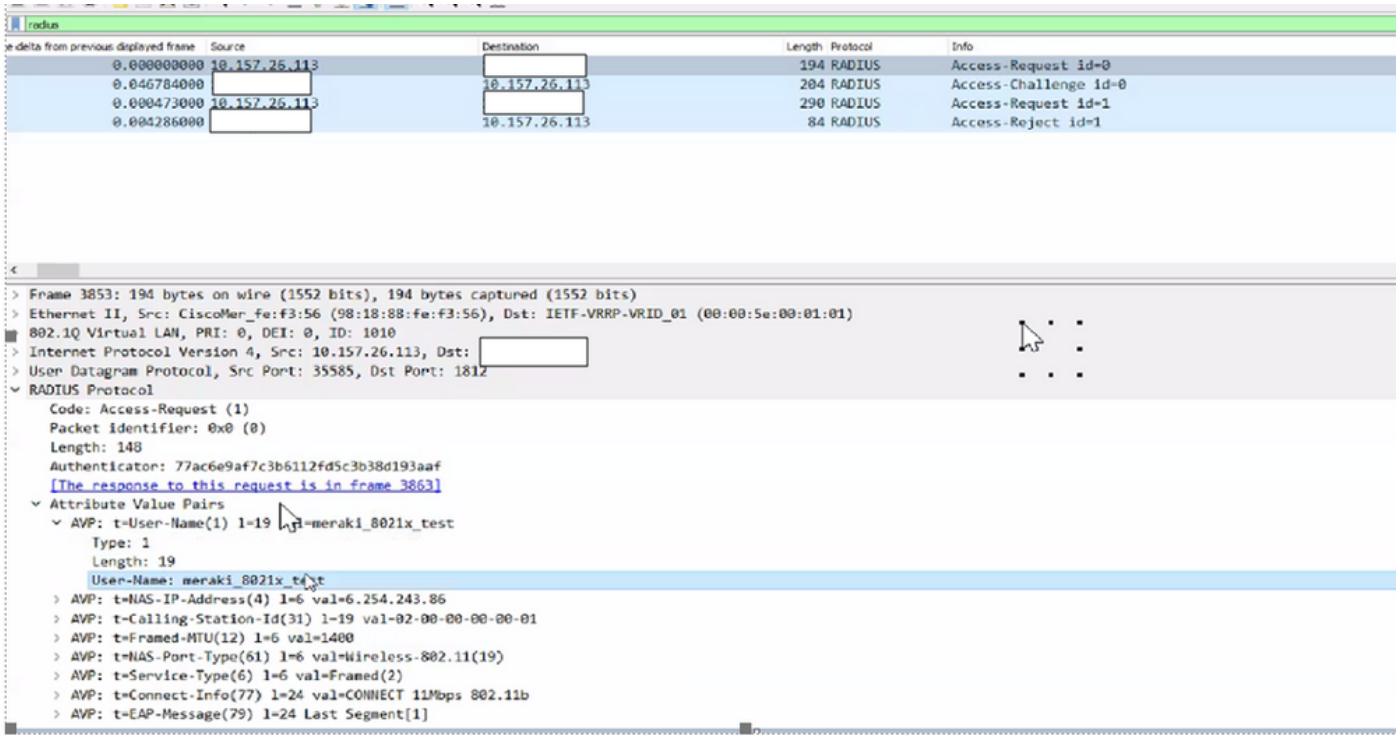
2. Eseguire l'acquisizione dei pacchetti sulla porta uplink e verificare il flusso di richiesta di accesso. Fare riferimento alla schermata di packet capture access - La richiesta non riceve alcuna risposta.



3. Se il risultato del test viene segnalato come credenziali di accettazione/rifiuto/negazione/risposta/errate, significa che il server RADIUS è attivo.

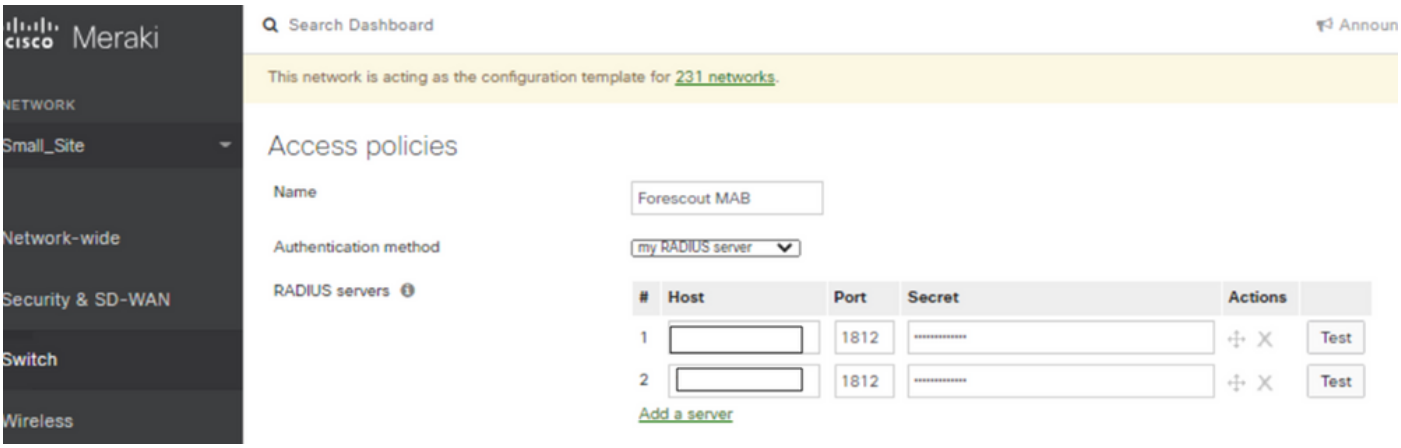


4. Eseguire l'acquisizione dei pacchetti sulla porta uplink e verificare il flusso di richiesta di accesso. Fare riferimento allo screenshot dell'accesso all'acquisizione del pacchetto - La richiesta ha ricevuto una risposta.

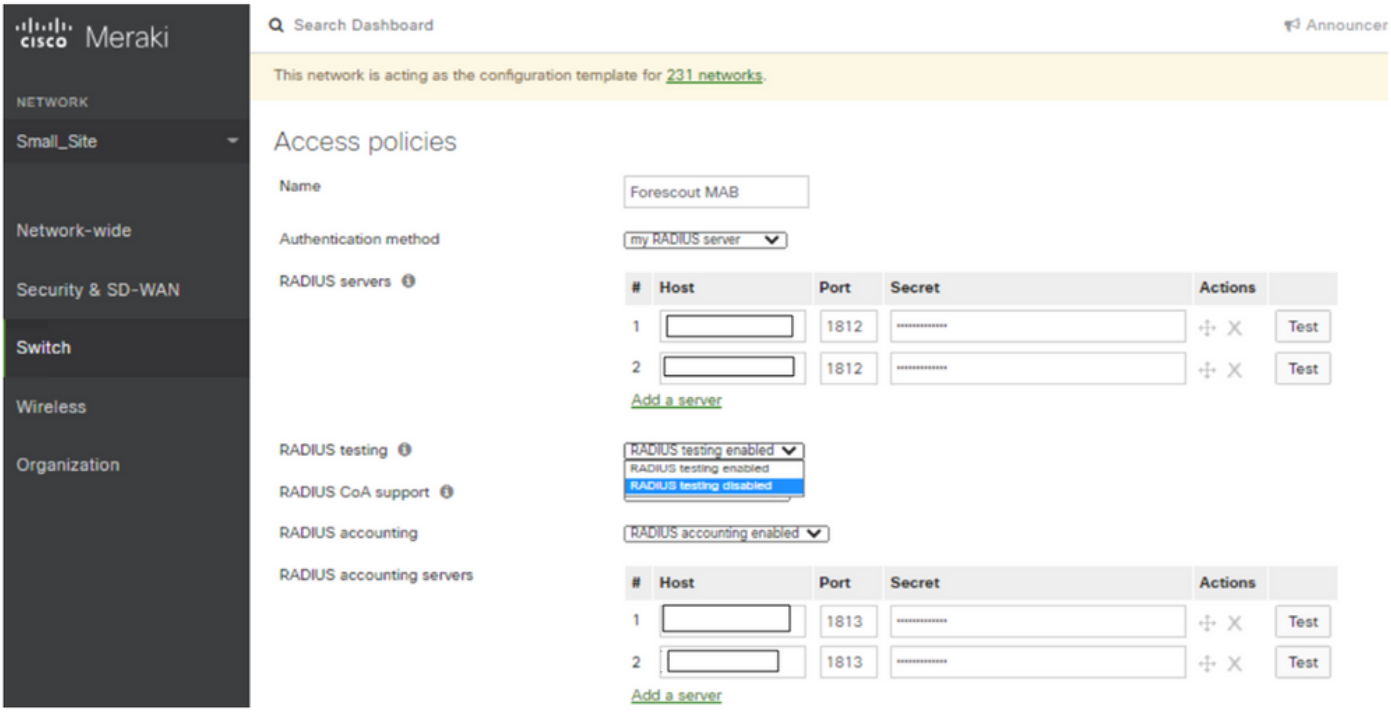


Verifica configurazione criteri di accesso

1. È necessario verificare che il parametro indicato nei criteri di accesso sia corretto e includa l'indirizzo IP dell'host, il numero di porta e la chiave privata.



2. Gli indirizzi IP dei server RADIUS configurati sono fittizi o non vengono utilizzati nella produzione oppure i criteri di accesso non sono in uso. È consigliabile rimuovere i criteri di accesso. Se si desidera mantenerla, è possibile disattivare l'**impostazione del test del raggio.**



Informazioni correlate

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- Documentazione e supporto tecnico – Cisco Systems

Nota

- Quando i server radius eseguono il polling dei dispositivi Meraki usando l'IP LAN e il nome utente predefinito "meraki_8021x_test", il dashboard Meraki ha usato l'indirizzo MAC Meraki come origine.
- Meraki ha dato visibilità a questi allarmi da ottobre 2021.