Configurazione di RADIUS e LNO sui punti di accesso wireless industriali in modalità URWB

Sommario

Introduzione

In questo documento viene descritta la configurazione dell'autenticazione RADIUS e di Large Network Optimization (LNO) sulle radio IW9165 e IW9167 in modalità URWB.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Navigazione e comandi CLI di base
- Informazioni sulle radio in modalità URWB IW

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Radio IW9165 e IW9167

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.

Premesse

RADIUS - Remote Authentication Dial-In User Service è un protocollo di rete utilizzato per fornire la gestione centralizzata di autenticazione, autorizzazione e accounting (AAA) per utenti o dispositivi che si connettono e utilizzano un servizio di rete. Per i dispositivi wireless industriali in

modalità URWB, è possibile utilizzare Radius per autenticare i dispositivi prima che possano essere collegati a una rete.

I parametri per la configurazione Radius possono essere configurati sui dispositivi IW dalla GUI o dall'accesso CLI o dal sistema operativo IoT.

Configurazione CLI dei parametri Radius:

Questi parametri possono essere configurati dalla modalità di abilitazione nella CLI dei dispositivi.

1. Abilitazione dell'autenticazione Radius:

Questo parametro consente di abilitare l'autenticazione Radius sui dispositivi. Questa operazione deve essere eseguita dopo aver aggiunto altri parametri obbligatori necessari per l'autenticazione radius.

Radio1#configure radius enabled

2. Disattivazione autenticazione Radius:

Questo parametro consente di disabilitare l'autenticazione Radius sui dispositivi.

Radio1#configure radius disabled

3. Passthrough:

Questo parametro deve essere configurato solo sulle radio dell'infrastruttura. Configurando le radio dell'infrastruttura con il parametro pass-through, le radio del veicolo possono autenticarsi tramite le radio dell'infrastruttura, consentendo anche la comunicazione tra le radio del veicolo autenticate e le radio dell'infrastruttura non autenticate.

Radio1#configure radius passthrough

```
[ME_TRK_IW9167EH#configure radius passthrough
```

4. Aggiunta del server Radius:

Questo parametro viene utilizzato per specificare l'indirizzo IP del server Radius con cui il dispositivo deve comunicare.

Radio1#configure radius server

```
[ME_TRK_IW9167EH#conf radius server 10.122.136.50
 ME_TRK_IW9167EH#
```

5. Porta Radius:

Questo parametro viene utilizzato per specificare la porta del server Radius con cui il dispositivo deve comunicare. La porta predefinita per l'autenticazione Radius è 1812.

Radio1#configure radius server

```
[ME_TRK_IW9167EH#conf radius port 1812
[ME_TRK_IW9167EH#
```

6. Segreto Radius:

Questo parametro viene utilizzato per specificare la chiave già condivisa da utilizzare con il server Radius.

Radio1#configure radius secret

```
[ME_TRK_IW9167EH#conf radius secret myS3cr3t123
[ME_TRK_IW9167EH#
```

7. Porta e indirizzo IP del server secondario:

Questi parametri vengono utilizzati per specificare l'indirizzo IP e il numero di porta di un secondo server Radius, da utilizzare nel caso in cui il dispositivo non sia in grado di raggiungere il server primario.

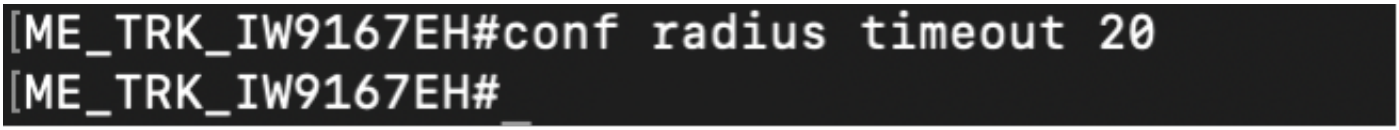
Radio1#configure radius secondary server

Radio1#configure radius secondary port

8. Timeout raggio:

Questo parametro viene utilizzato per specificare il periodo di tempo in secondi durante il quale il client attenderà una risposta dal server Radius primario prima di tentare la connessione al server secondario. Il valore predefinito è 10 secondi.

Radio1#configure radius timeout



9. Parametri di autenticazione:

Questo parametro viene utilizzato per specificare il metodo di autenticazione Radius e i parametri corrispondenti da passare. Sono disponibili diverse opzioni.

Radio1#configure radius authentication

```
[ME_TRK_IW9167EH#conf radius authentication
  gtc       Use Generic Token Card
  md5       Use Message Digest 5
  mschapv2  Use Microsoft Challenge-Handshake Authentication Protocol v2
  peap      Use Protected EAP
  tls       Use Transport Layer Security - Please note that you will need to
            upload the certificates
  ttls      Use EAP-TTLS
```

Se si utilizzano questi metodi: GTC (Generic token card), MD5 (Message-Digest Algorithm 5) o MSCHAPV2 (Microsoft Challenge Handshake Authentication Protocol versione 2). Il nome utente e la password possono essere aggiunti con questi comandi:

Radio1#configure radius authentication gtc

Radio1#configure radius authentication md5

Radio1#configure radius authentication mschapv2

Se si utilizzano questi metodi: Per l'autenticazione, PEAP (Protected Extensible Authentication Protocol) o EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) deve essere fornito anche un altro metodo di autenticazione interna. Può essere gtc, md5 o mschapv2.

Radio1#configure radius authentication peap

inner-auth-method

Radio1#configure radius authentication ttls

inner-auth-method

10. Tentativi di commutazione:

Questo parametro specifica il numero di tentativi di autenticazione radius consentiti verso il server primario prima che il client passi al server secondario. Il valore predefinito è 3.

Radio1#configure radius switch <1-6>

11. Tempo di arretrato:

Questo parametro specifica il tempo di attesa in secondi del client dopo il superamento del numero massimo di tentativi di autenticazione.

Radio1#configure radius backoff-time

12. Scadenza:

Questo parametro specifica il valore di tempo in secondi se durante il quale l'autenticazione

Radius non è completa, il tentativo di autenticazione verrà interrotto.

Radio1#configure radius expiration

```
[ME_TRK_IW9167EH#conf radius expiration 30000
[ME_TRK_IW9167EH#
```

13. Inviare la richiesta:

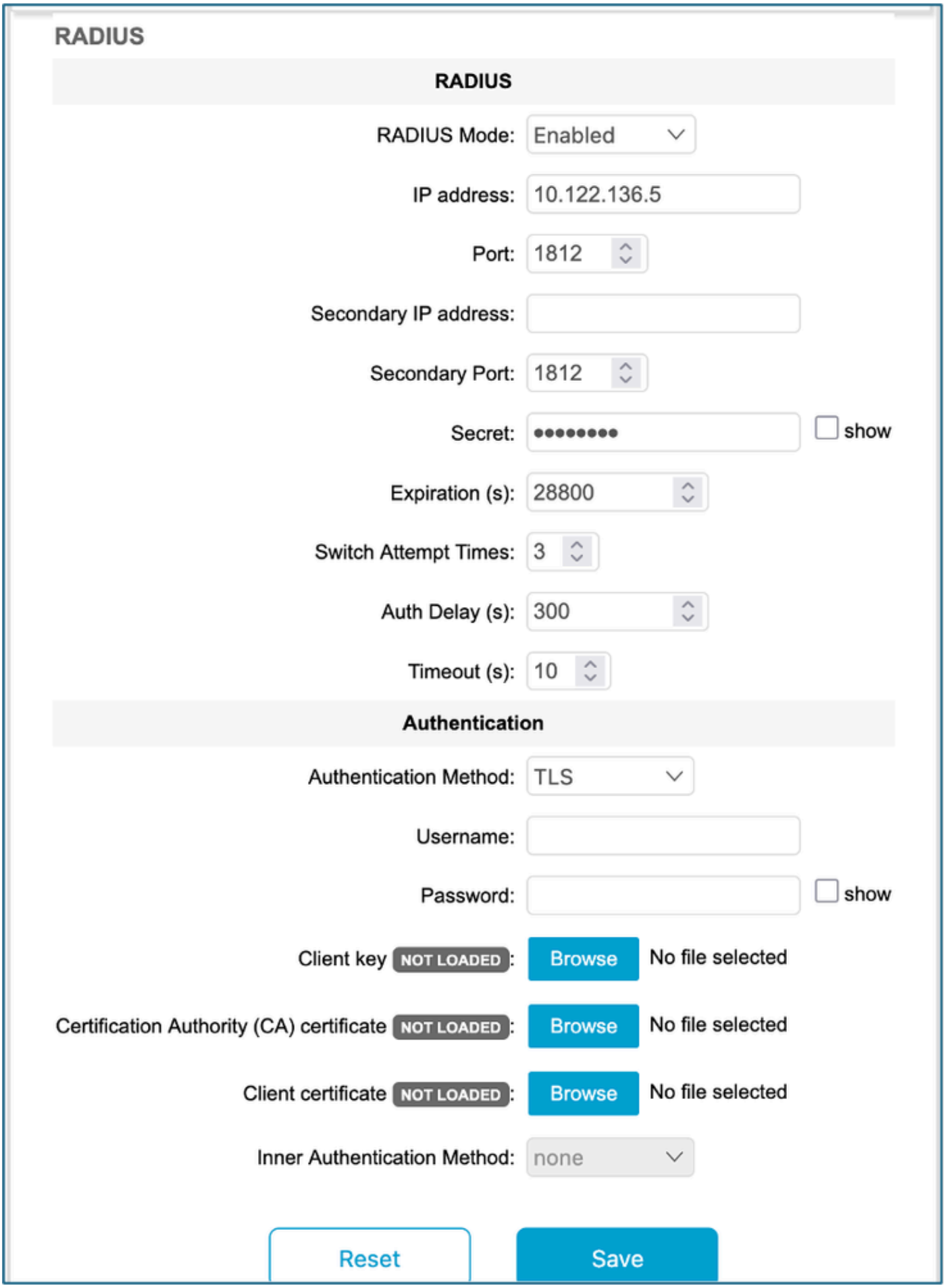
Questo parametro viene utilizzato per avviare una richiesta di autenticazione Radius per il server Radius primario o secondario configurato.

Radio1#configure radius send-request

```
[ME_TRK_IW9167EH#conf radius send-request primary
 Sending authentication request to Radius server: 10.122.136.50, (port: 1812).
```

```
[ME_TRK_IW9167EH#conf radius send-request secondary
Sending authentication request to Radius server: 10.122.136.51, (port: 1812).
```

Gli stessi parametri possono essere configurati sulle radio wireless industriali in modalità URWB tramite GUI e nella scheda ‘Radius’ sulla pagina Web.



Comandi show:

La configurazione Radius corrente può essere verificata tramite CLI con i comandi show.

1.

raggio #show

Questo comando show indica se Radius è abilitato o disabilitato sul dispositivo.

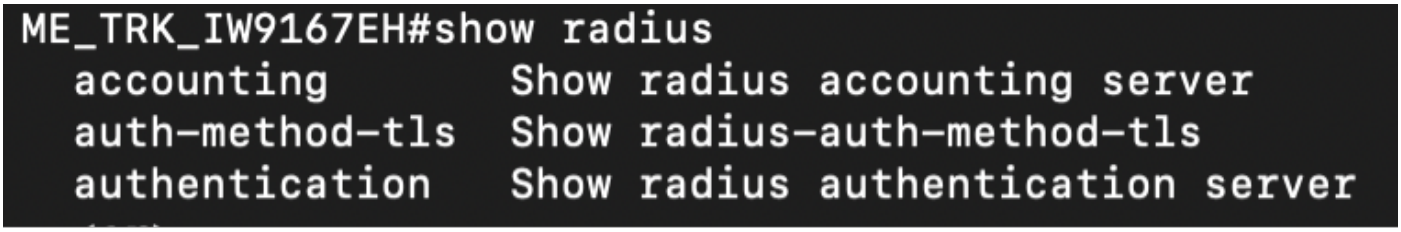
2.

#show radius accounting

#show radius auth-method-tls

autenticazione #show radius

Questi comandi show mostrano la configurazione corrente del server di accounting radius, del server di autenticazione e dei parametri tls del metodo di autenticazione configurati.



Sequenza di autenticazione Radius con LNO

L'ottimizzazione delle reti LNO o Large è una funzione che si consiglia di abilitare sulle reti di grandi dimensioni con 50 o più radio Infrastructure per ottimizzare la formazione dello pseudofilo tra tutti i dispositivi della rete. Viene utilizzato sia nelle reti di livello 2 che in quelle di livello 3.

Nelle reti in cui sono abilitati sia LNO che Radius, le radio dell'infrastruttura si autenticano in sequenza (dall'ID Mesh più basso all'ID Mesh più alto). L'abilitazione di LNO forzerà tutte le radio dell'infrastruttura a creare pseudofili SOLO fino all'estremità della rete, e disabiliterà anche l'inoltro BPDU.

Questo articolo descrive la sequenza di autenticazione Radius su un'impostazione di Fluidità con un'estremità della rete e 4 radio Mesh Point Infrastructure.

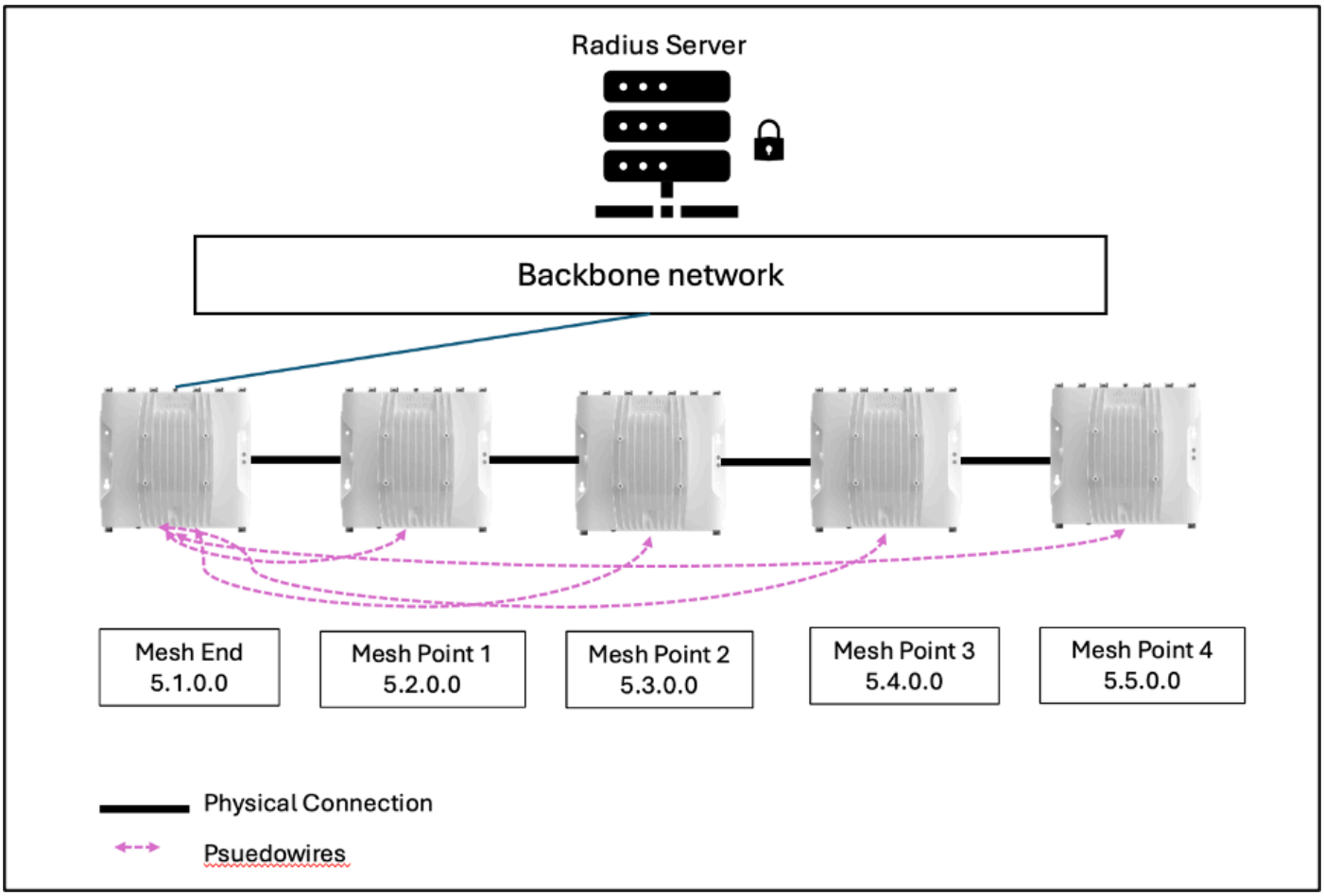
La radio Mesh End è il "coordinatore cablato" predefinito della rete Fluidity. Ciò significa che ha la funzione di autotap aperta e funge da punto di ingresso/uscita della rete.

Tutte le altre radio Infrastructure sono impostate come punti Mesh e tutte hanno una connessione fisica con l'estremità Mesh tramite switch collegati tra loro.

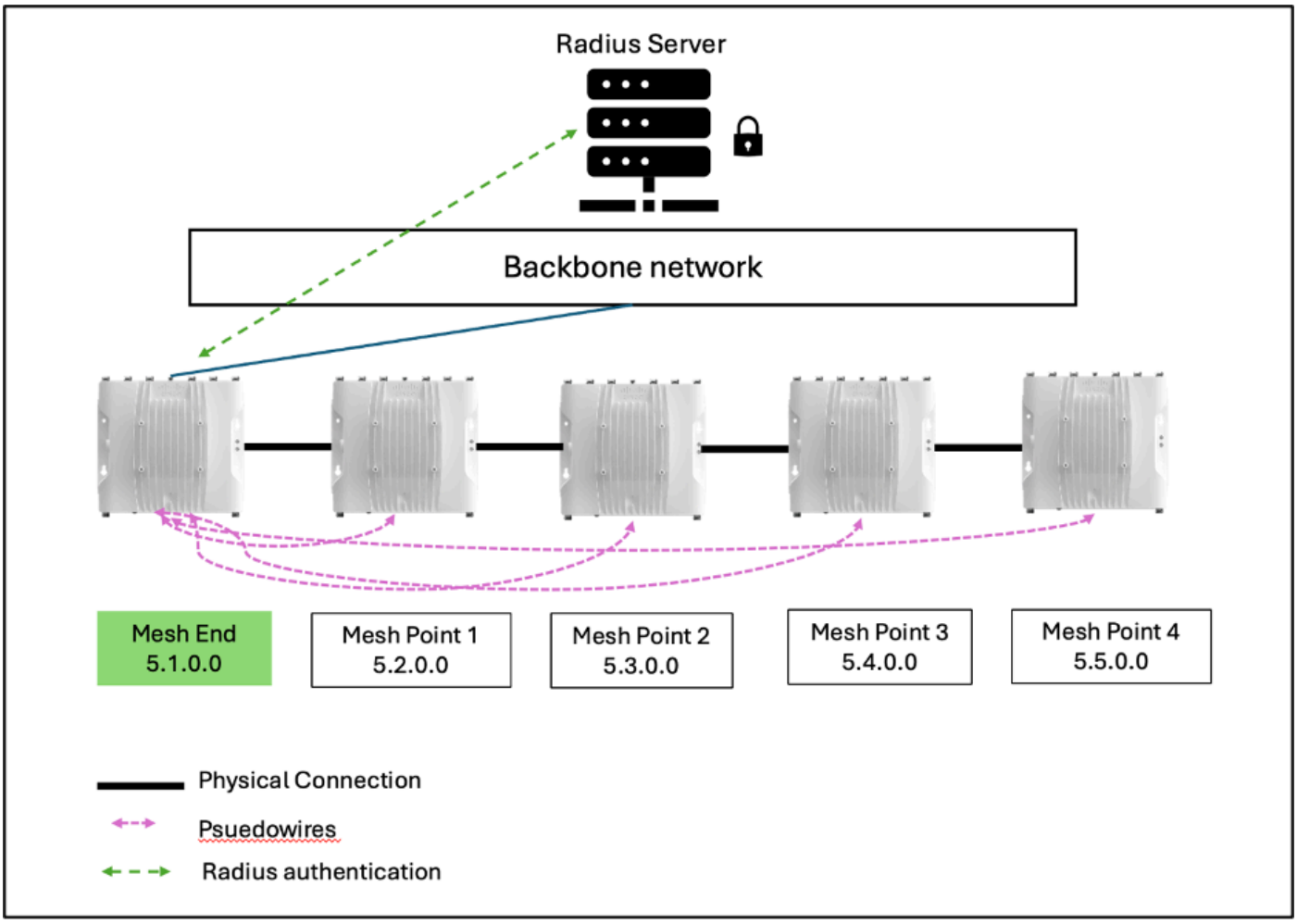
La radio Mesh End è connessa alla rete backbone generalmente tramite una connessione in fibra e tramite la rete backbone può raggiungere il server Radius della rete.

Qualsiasi dispositivo può raggiungere il server Radius solo se:

1. È un coordinatore cablato.
2. Ha uno pseudowire costruito con il master cablato, ad esempio Mesh End.



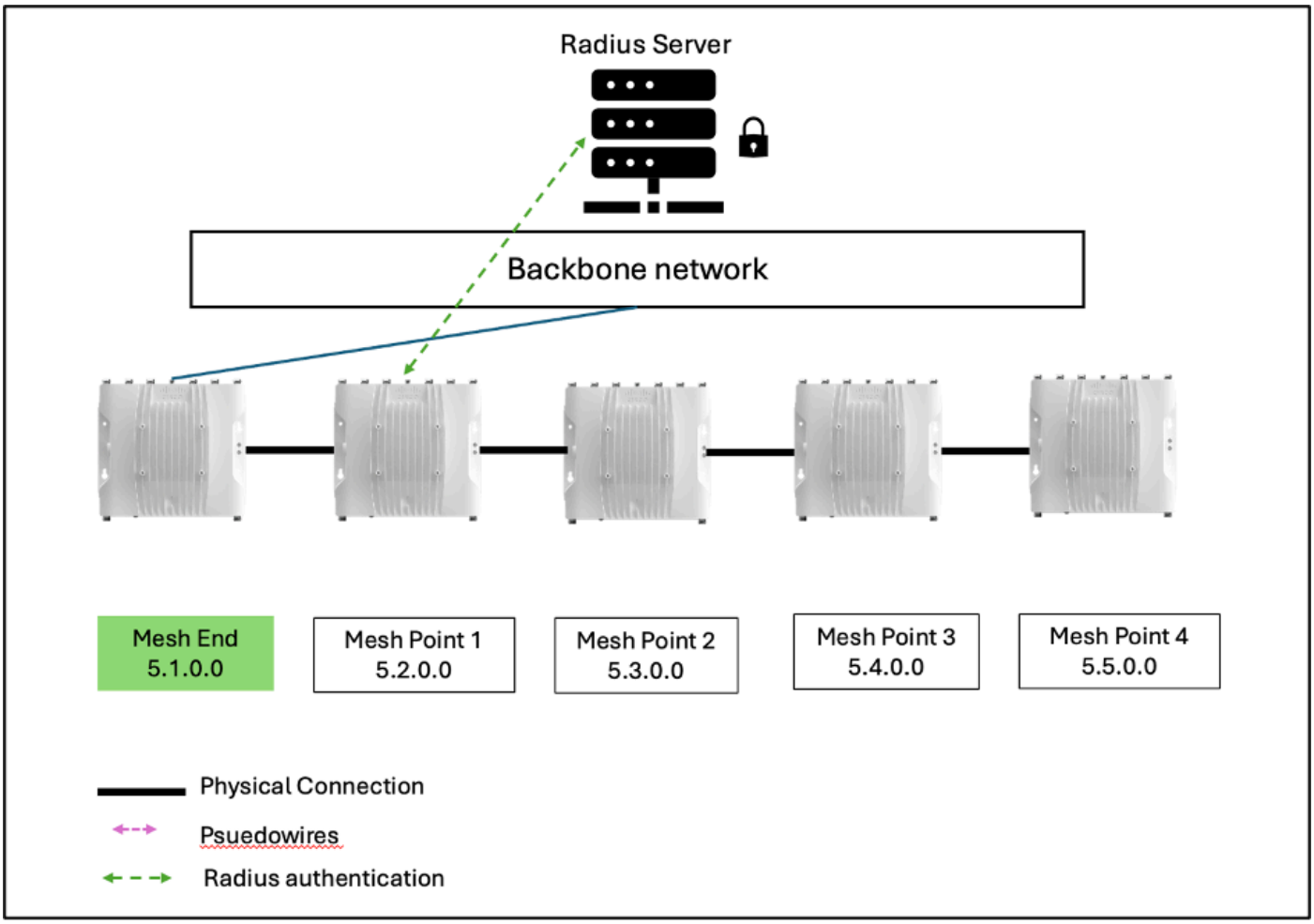
Passaggio 1: Tutte le unità non sono autenticate.



All'inizio, tutte le unità, compresa l'estremità della rete, non verranno autenticate. L'autotap si aprirà solo sulla radio Mesh End che è il punto di ingresso/uscita dell'intera rete. Affinché un dispositivo Infrastructure possa raggiungere il server Radius per autenticarsi, deve essere un'estremità della rete o avere uno pseudofilo all'estremità della rete.

Ora, la radio Mesh End 5.1.0.0 invierà una richiesta di autenticazione al server Radius tramite la rete Backbone. Una volta ricevuta la comunicazione, viene autenticata e quindi diventa "invisibile" al resto dei punti mesh dell'infrastruttura non autenticata, così come è richiesto per AAA con Radius.

Passaggio 2: Mesh End 5.1.0.0. è autenticato, mentre gli altri non lo sono.

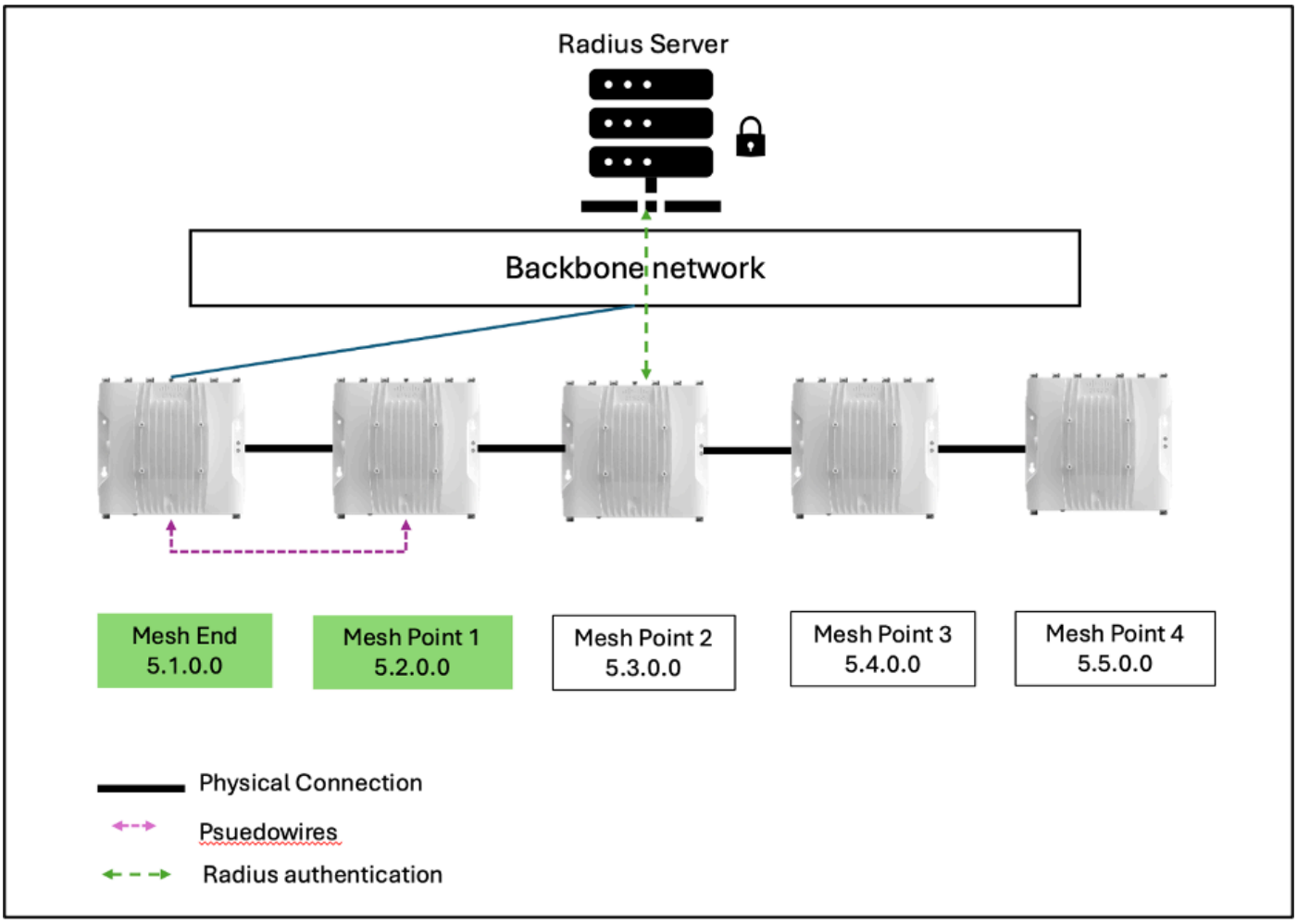


Ora che Mesh End 5.1.0.0 è autenticato e invisibile al resto della rete, i punti Mesh rimanenti eseguiranno una scelta e sceglieranno il dispositivo con ID Mesh più basso come coordinatore cablato successivo. In questo esempio, si tratterebbe di Mesh Point 1 con Mesh ID 5.2.0.0. Autotap sarà quindi aperto su Mesh Point 1.

Poiché LNO è abilitato, nessun oggetto Pseudowires si formerà in Mesh Point 1. Tutte le radio rimanenti dovranno essere autenticate in sequenza quando la relativa Autotap è aperta.

Ora Mesh Point 1 può inviare una richiesta di autenticazione a Radius Server e autenticarsi.

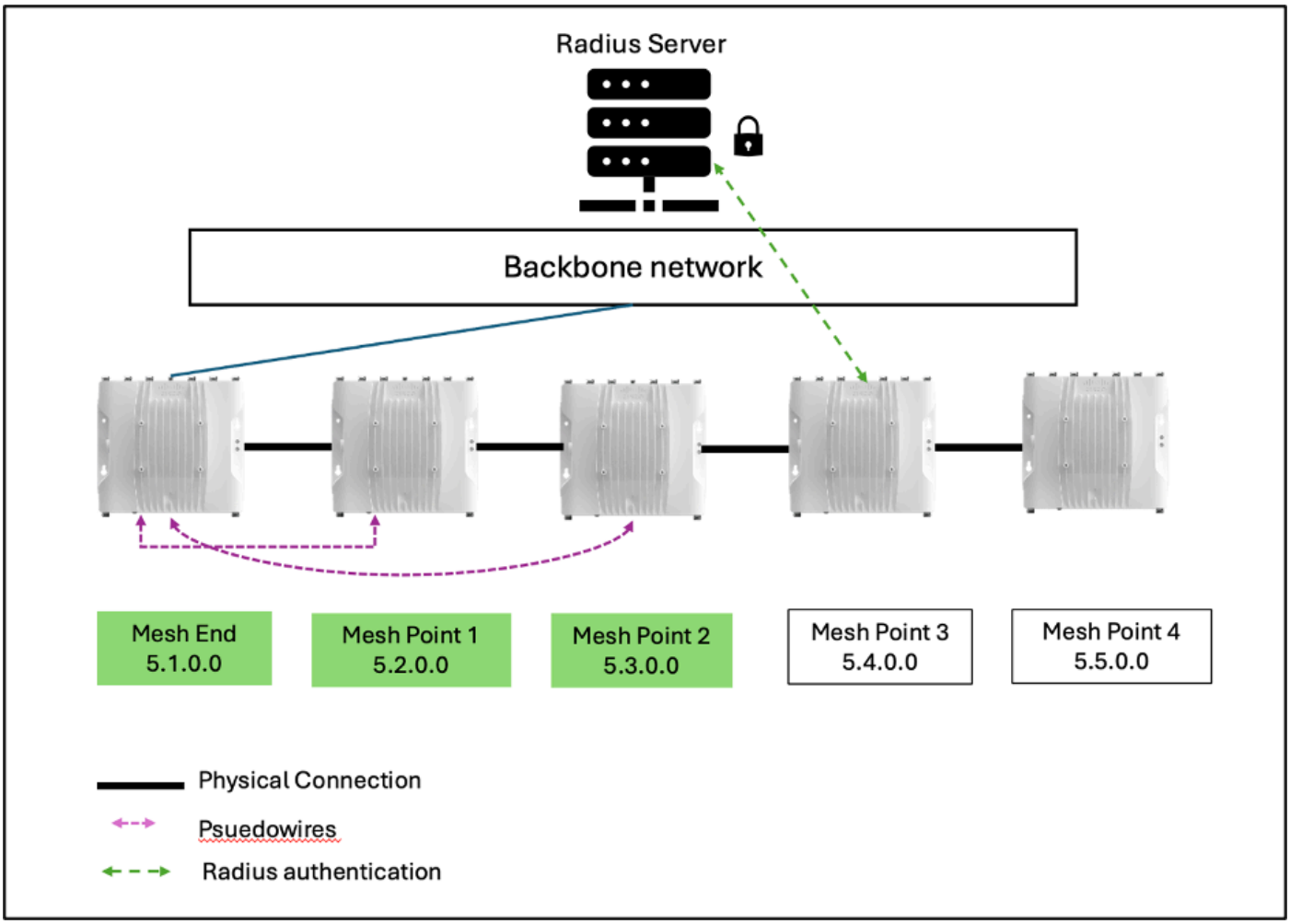
Passaggio 3: Mesh End, Mesh Point 1 è autenticato e gli altri non lo sono.



Ora che Mesh Point 1 è anche autenticato, formerà un psuedowire con Mesh End autenticato, e diventa anche invisibile per il resto delle radio non autenticate di Infrastructure.

Il resto delle radio non autenticate eseguono nuovamente la scelta e scelgono Mesh Point 2 con il più basso Mesh ID 5.3.0.0 come nuovo coordinatore cablato e quella radio invia una richiesta di autenticazione al server Radius mentre il suo Autotap è aperto.

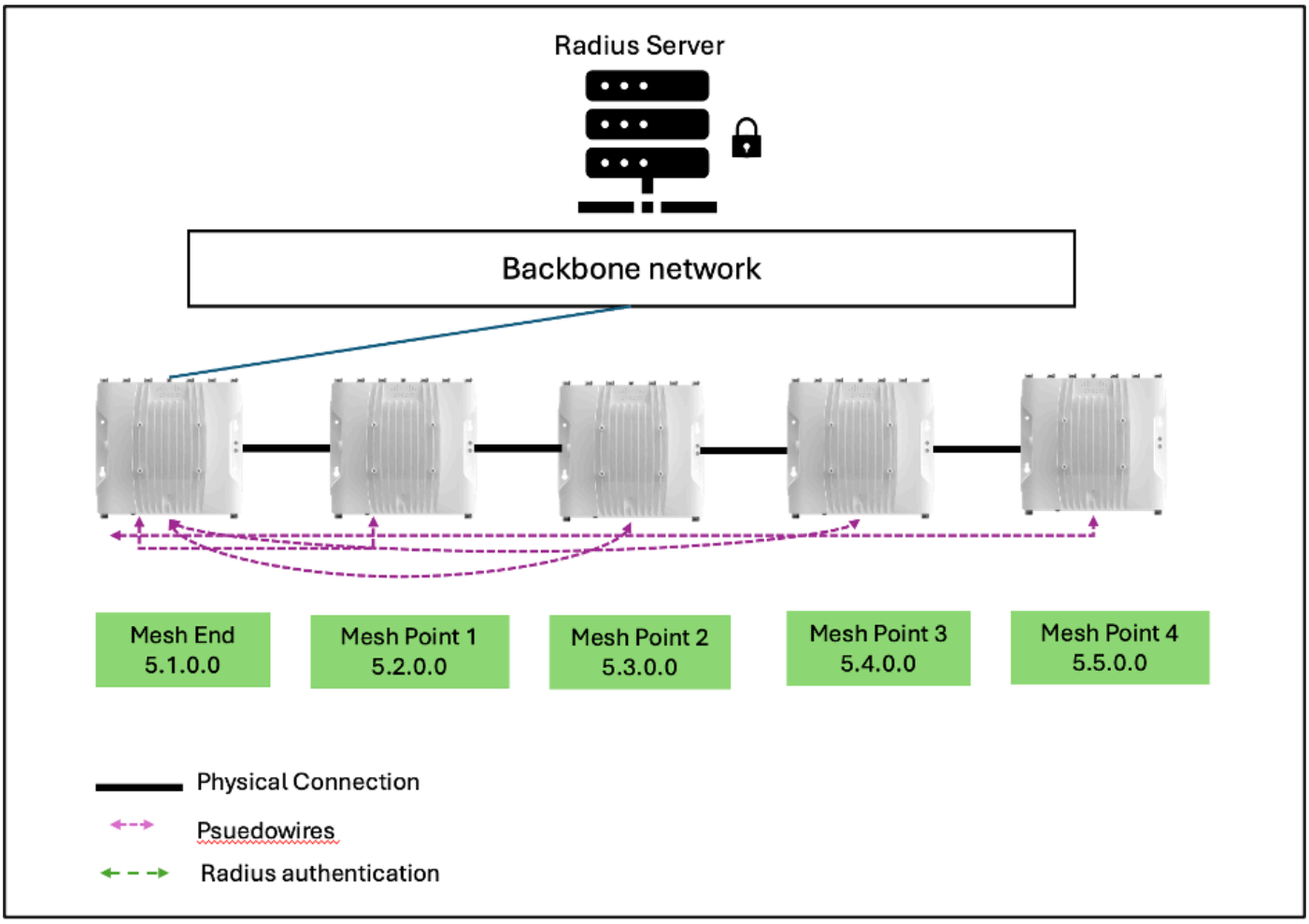
Passaggio 4: Mesh End, MP 1 e MP 2 sono autenticati.



Il processo si ripete con Mesh Point 2 che diventa autenticato e forma Pseudowire con il dispositivo Mesh End.

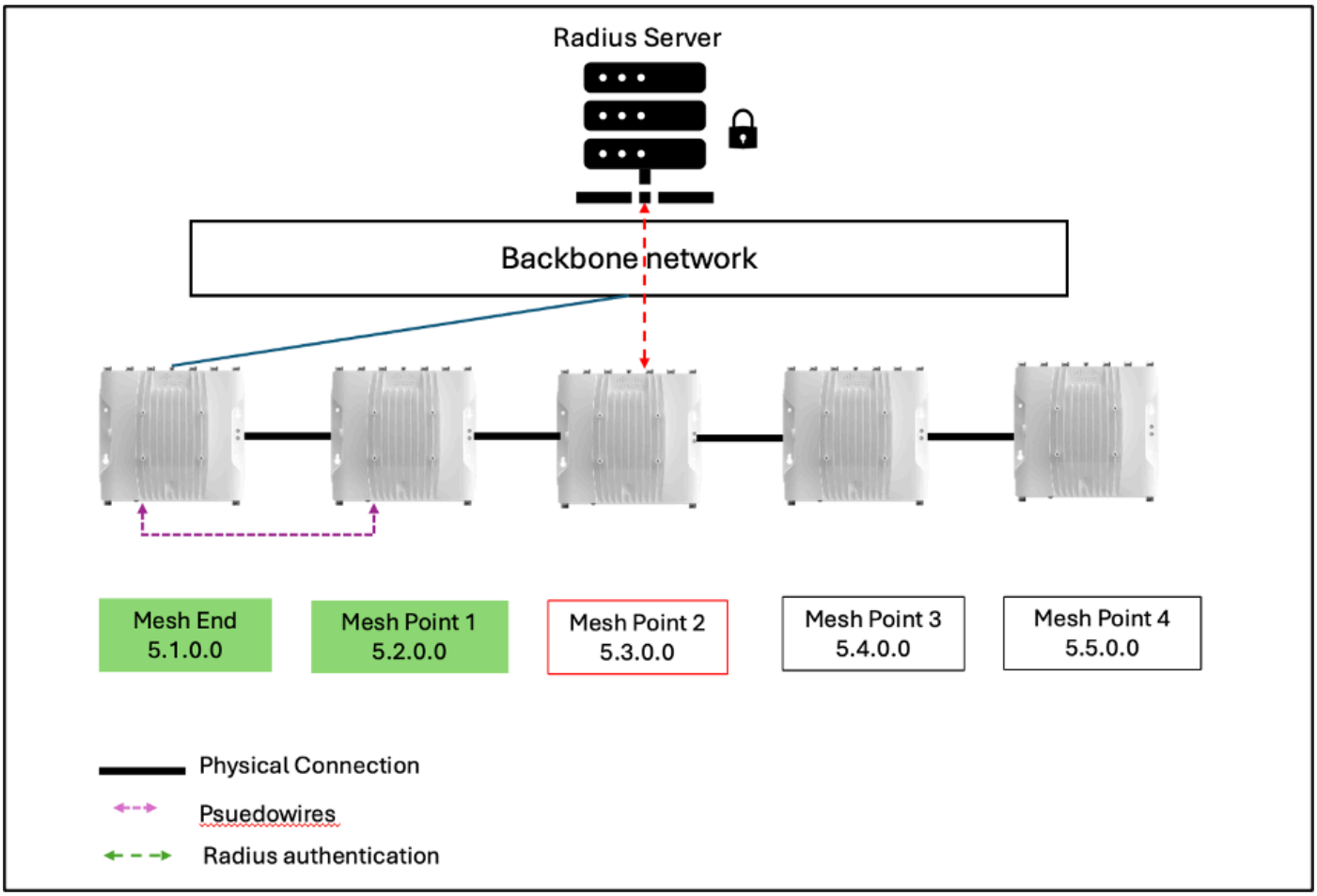
Le altre radio dell'infrastruttura si autenticano a turno, nell'ordine degli ID Mesh dal più basso al più alto, quando viene aperta la loro autotap.

Passaggio 5: Tutte le radio sono autenticate.



Configurazione errata o casi di problemi:

Se uno dei punti Mesh dell'infrastruttura ha credenziali errate su di essi o se Radius è stato disabilitato per errore, ciò influirà sull'autenticazione di altre radio. Verificare sempre le credenziali e le impostazioni prima di distribuire le radio in produzione.



In questo esempio, se Mesh Point 2 ha credenziali sbagliate, rimarrà non autenticato e a sua volta Mesh Point 3 e Mesh Point 4 non avranno mai la possibilità di autenticarsi poiché non c'è alcun Pseudowire formato da loro a Mesh Point 2 a causa dell'abilitazione di LNO.

Le radio non autenticate dipendono dall'ID Mesh della radio configurata in modo errato. Qualsiasi radio con ID Mesh superiore al coordinatore cablato corrente rimarrà non autenticata e causerà problemi.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).