在URWB模式下配置工業無線接入點的RADIUS和LNO

目錄

簡介

本檔案介紹在URWB模式的IW9165和IW9167無線電上設定RADIUS驗證和大型網路最佳化(LNO)。

必要條件

需求

思科建議您瞭解以下主題：

- 基本CLI導航和命令
- 瞭解IW URWB模式無線電

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- IW9165和IW9167無線電

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

RADIUS — 遠端驗證撥入使用者服務是一種網路通訊協定，用於為連線和使用網路服務的使用者或裝置提供集中式驗證、授權和計量(AAA)管理。對於URWB模式下的工業無線裝置，可以在裝置加入網路之前使用Radius對其進行身份驗證。

Radius配置的引數可在IW裝置上通過GUI、CLI訪問或通過IoT OD配置。

Radius引數的CLI設定：

這些引數可在裝置的CLI上從啟用模式進行配置。

1.啟用Radius身份驗證：

此引數允許在裝置上啟用Radius身份驗證。必須在新增radius驗證所需的其他強制引數後執行該操作。

Radio1#configure radius enabled

```
ME_TRK_IW9167EH#configure radius enabled
```

2.禁用Radius身份驗證：

此引數允許停用裝置上的Radius驗證。

Radio1#configure radius disabled

```
ME_TRK_IW9167EH#configure radius disabled
```

3.直通：

此引數只能在基礎設施無線電上配置。使用直通引數配置基礎設施無線電允許車輛無線電通過基礎設施無線電驗證其自身，也允許在已驗證的車輛無線電與未驗證的基礎設施無線電之間進行通訊。

Radio1#configure radius passthrough

```
ME_TRK_IW9167EH#configure radius passthrough
```

4.新增Radius伺服器：

此引數用於指定Radius伺服器的IP地址，以便裝置與其通訊。

Radio1#configure radius server

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

5. Radius埠：

此引數用於指定Radius伺服器的埠，以便與裝置進行通訊。Radius驗證的預設連線埠為1812。

Radio1#configure radius server

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

6. Radius密碼：

此引數用於指定要與Radius伺服器一起使用的預共用金鑰。

Radio1#configure radius secret

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

7.輔助伺服器IP和埠：

這些引數用於指定第二台Radius伺服器的IP地址和埠號，以便在裝置無法到達主伺服器時使用。

Radio1#configure radius secondary server

Radio1#configure radius secondary port

```
ME_TRK_IW9167EH#conf radius secondary server 10.122.136.51
ME_TRK_IW9167EH#conf radius secondary port 1812
```

8. Radius超時：

此引數用於指定客戶端在嘗試連線到輔助伺服器之前等待來自主Radius伺服器的響應的時間量（以秒為單位）。預設值設定為10秒。

Radio1#configure radius timeout

```
[ME_TRK_IW9167EH#conf radius timeout 20
[ME_TRK_IW9167EH#
```

9.驗證引數：

此引數用於指定Radius身份驗證方法和要傳遞的相應引數。有幾種方法可供使用。

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
```

如果使用這些方法：可以使用以下命令新增GTC（通用令牌卡）、MD5（消息摘要演算法5）或MSCHAPV2（Microsoft質詢握手身份驗證協定版本2）使用者名稱和密碼：

Radio1#configure radius authentication gtc

Radio1#configure radius authentication md5

Radio1#configure radius authentication mschapv2

如果使用這些方法：PEAP（受保護的可擴展身份驗證協定）或EAP-TTLS（可擴展身份驗證協定隧道傳輸層安全）用於身份驗證，還必須提供另一種內部身份驗證方法。它可以是gtc、md5或mschapv2。

Radio1#configure radius authentication peap

inner-auth-method

Radio1#configure radius authentication ttls

inner-auth-method

10.交換嘗試：

此引數指定在客戶端切換到輔助伺服器之前，允許對主伺服器進行radius身份驗證嘗試的次數。預設值為 3。

Radio1#configure radius switch <1-6>

```
[ME_TRK_IW9167EH#conf radius switch 4
[ME_TRK_IW9167EH#
```

11.回退時間：

此引數指定客戶端在超過最大身份驗證嘗試次數後等待的時間值（以秒為單位）。

Radio1#configure radius backoff-time

```
[ME_TRK_IW9167EH#conf radius backoff-time 30
```

十二、到期時間：

此引數指定時間值（以秒為單位），如果Radius身份驗證未完成，則身份驗證嘗試將被放棄。

Radio1#configure radius expiration

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

13.傳送請求：

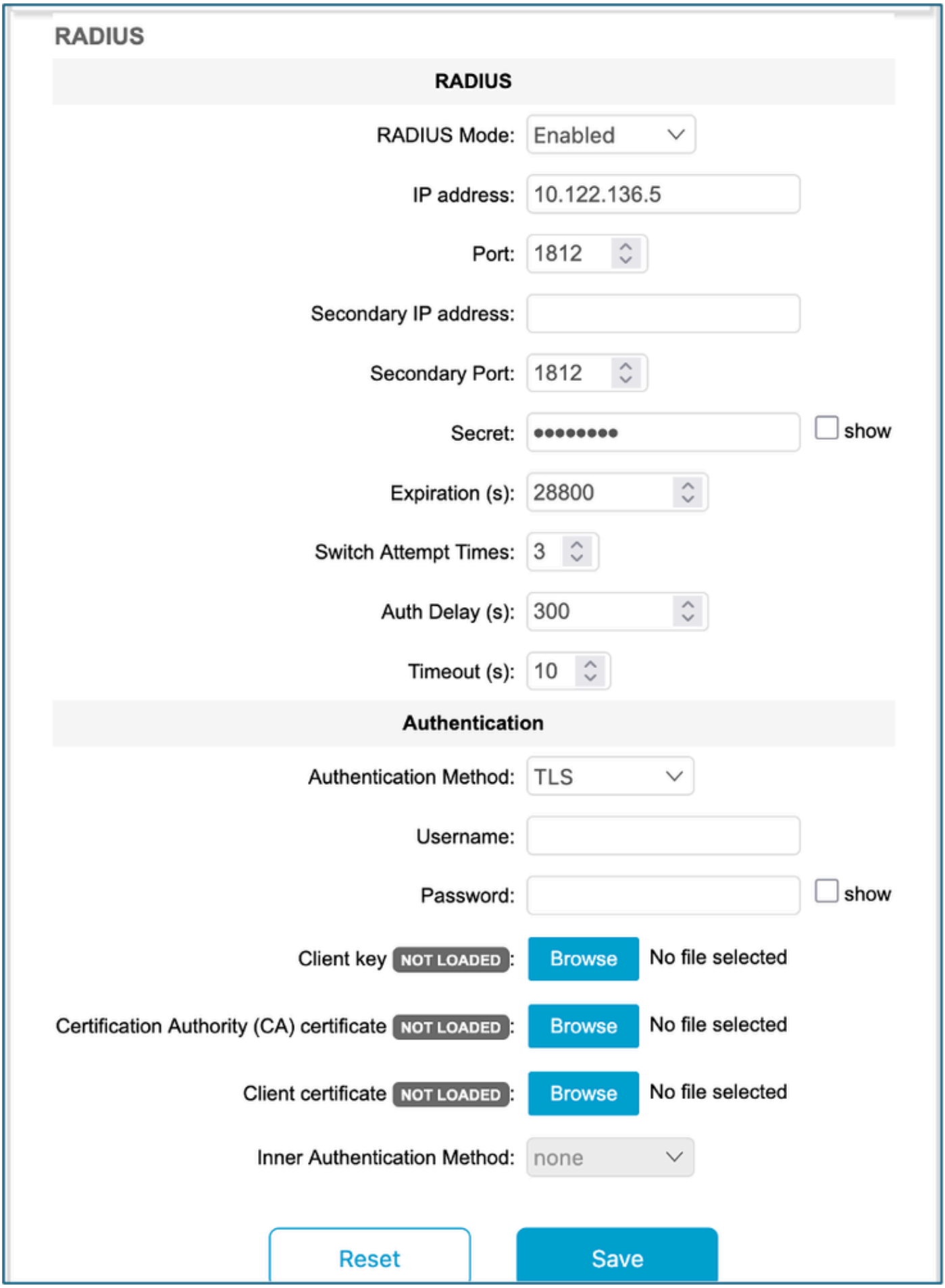
此引數用於向配置的主或輔助Radius伺服器發起RADIUS身份驗證請求。

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).
```

通過GUI在URWB模式的工業無線無線電上以及網頁上的「Radius」頁籤下可以配置相同的引數。


RADIUS
RADIUS
RADIUS Mode: Enabled
IP address: 10.122.136.5
Port: 1812
Secondary IP address:
Secondary Port: 1812
Secret: ••••••••
show
Expiration (s): 28800
Switch Attempt Times: 3
Auth Delay (s): 300
Timeout (s): 10
Authentication
Authentication Method: TLS
Username:
Password:
show
Client key NOT LOADED: Browse No file selected
Certification Authority (CA) certificate NOT LOADED: Browse No file selected
Client certificate NOT LOADED: Browse No file selected
Inner Authentication Method: none
Reset
Save

Show命令：

目前的Radius組態可以透過CLI使用show指令進行驗證。

1.

#show radius

此show命令會說明裝置上是否啟用或禁用Radius。

```
[ME_TRK_IW9167EH#show radius
```

2.

***#show radius*計量**

#show radius auth-method-tls

***#show radius*驗證**

這些show命令將顯示radius記帳伺服器、身份驗證伺服器的當前配置以及配置的身份驗證方法tls引數。

```
ME_TRK_IW9167EH#show radius
  accounting        Show radius accounting server
  auth-method-tls   Show radius-auth-method-tls
  authentication    Show radius authentication server
```

使用LNO的RADIUS驗證序列

LNO或大型網路最佳化是建議在具有50個或更多基礎設施無線電的大型網路上啟用的功能，以最佳化網路中所有裝置之間的偽線形成。它同時用於第2層和第3層網路。

在同時啟用LNO和Radius的網路中，基礎設施無線電按順序進行身份驗證（從最低的網狀ID到最高網狀ID）。 啟用LNO將強制所有基礎設施無線電僅建立到網狀端的偽線，並且也將禁用BPDU轉發。

本文將描述在具有一個網狀終端和4個網狀點基礎設施無線電的流動性設定上的Radius身份驗證序列。

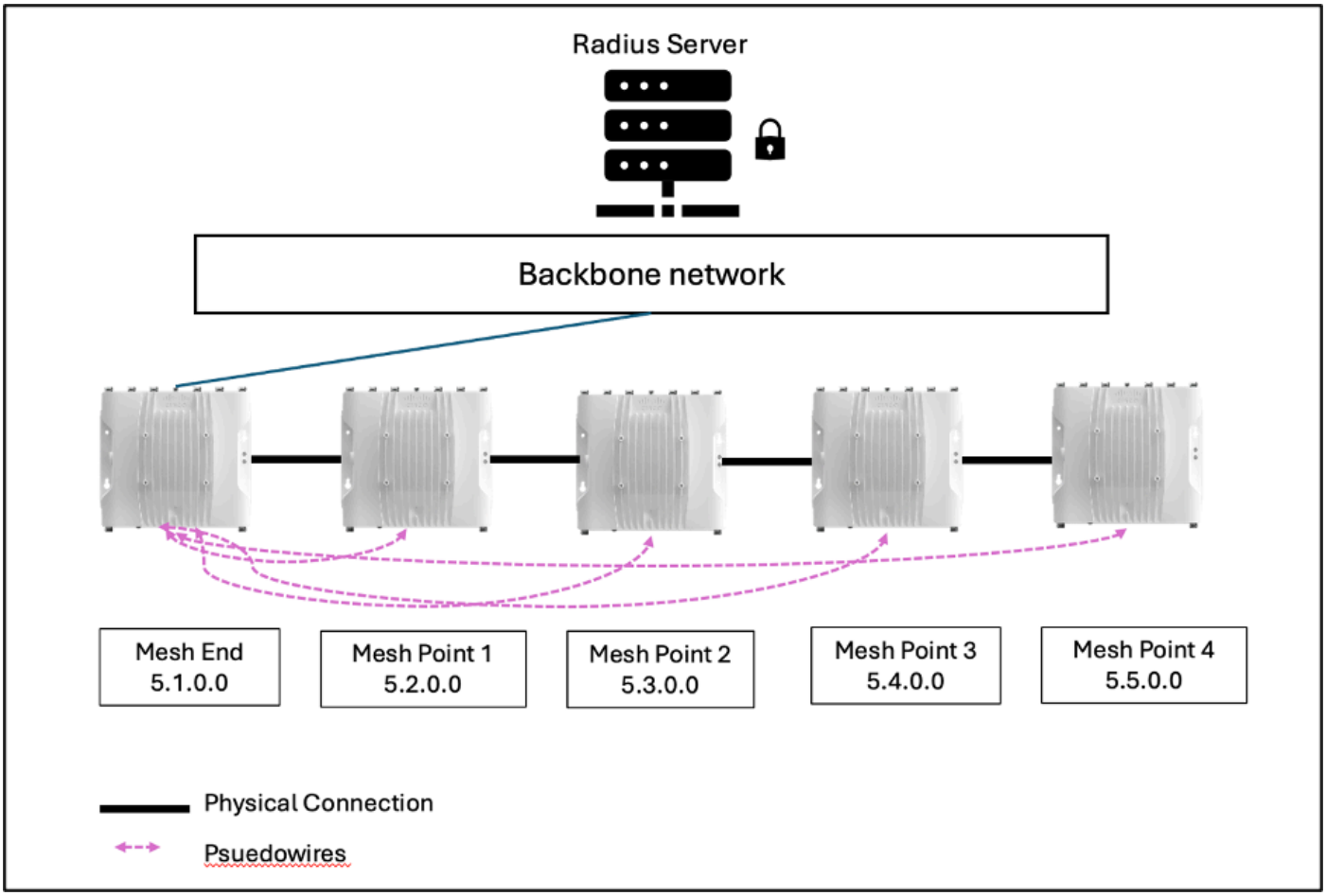
網狀終端無線電是流動性網路的預設「有線協調器」。也就是說，它開啟了autotap，並充當網路的輸入/輸出點。

所有其它基礎設施無線電都設定為網狀點，並且它們都通過相互連線的交換機與網狀端建立物理連線。

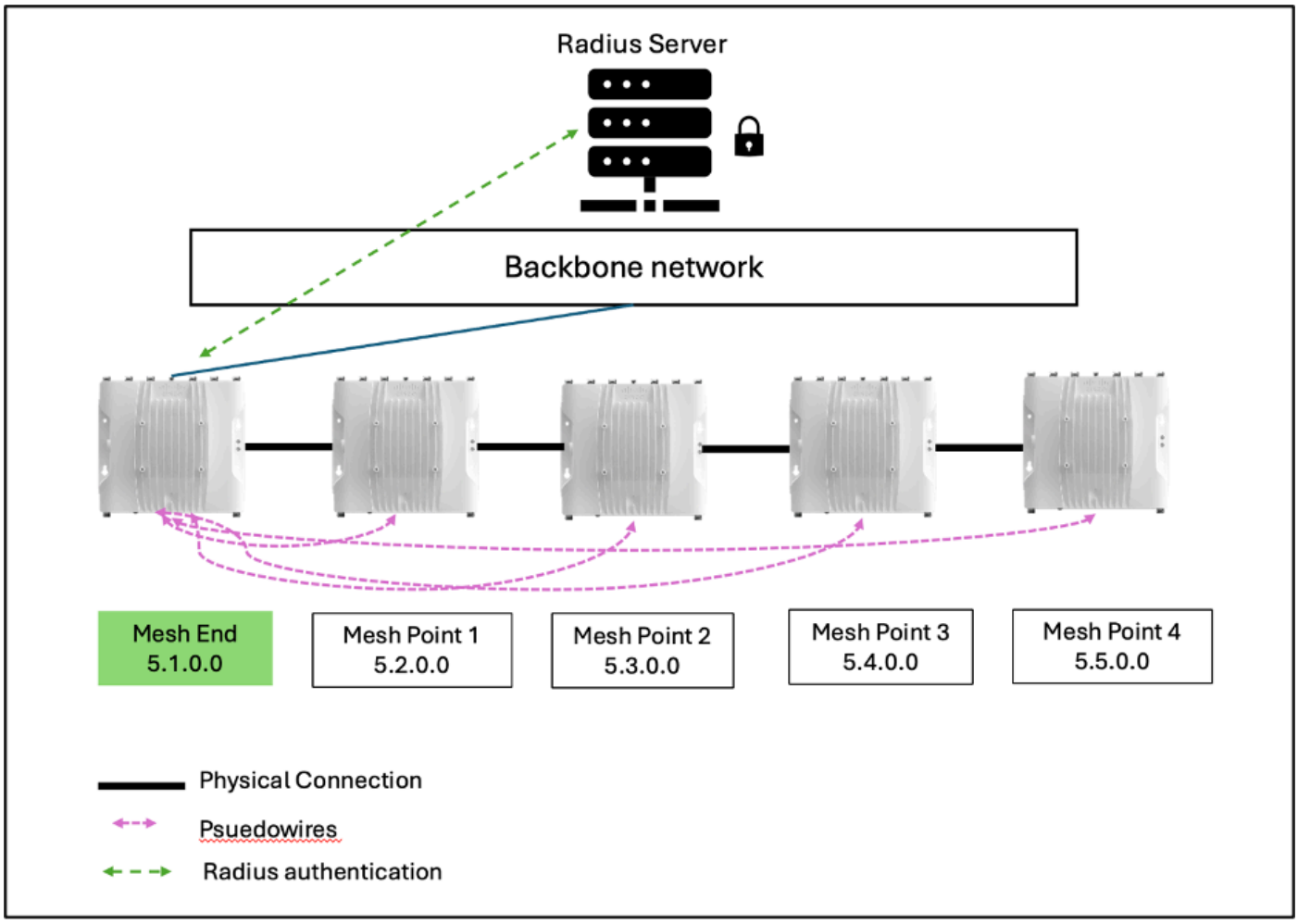
網狀端無線電通常透過光纖連線連線到主幹網路，並可透過主幹網路連線到網路的Radius伺服器。

只有發生以下情況時，任何裝置才能到達Radius伺服器：

1. 是一個有線協調器。
2. 它使用有線主機（即Mesh End）構建偽線。



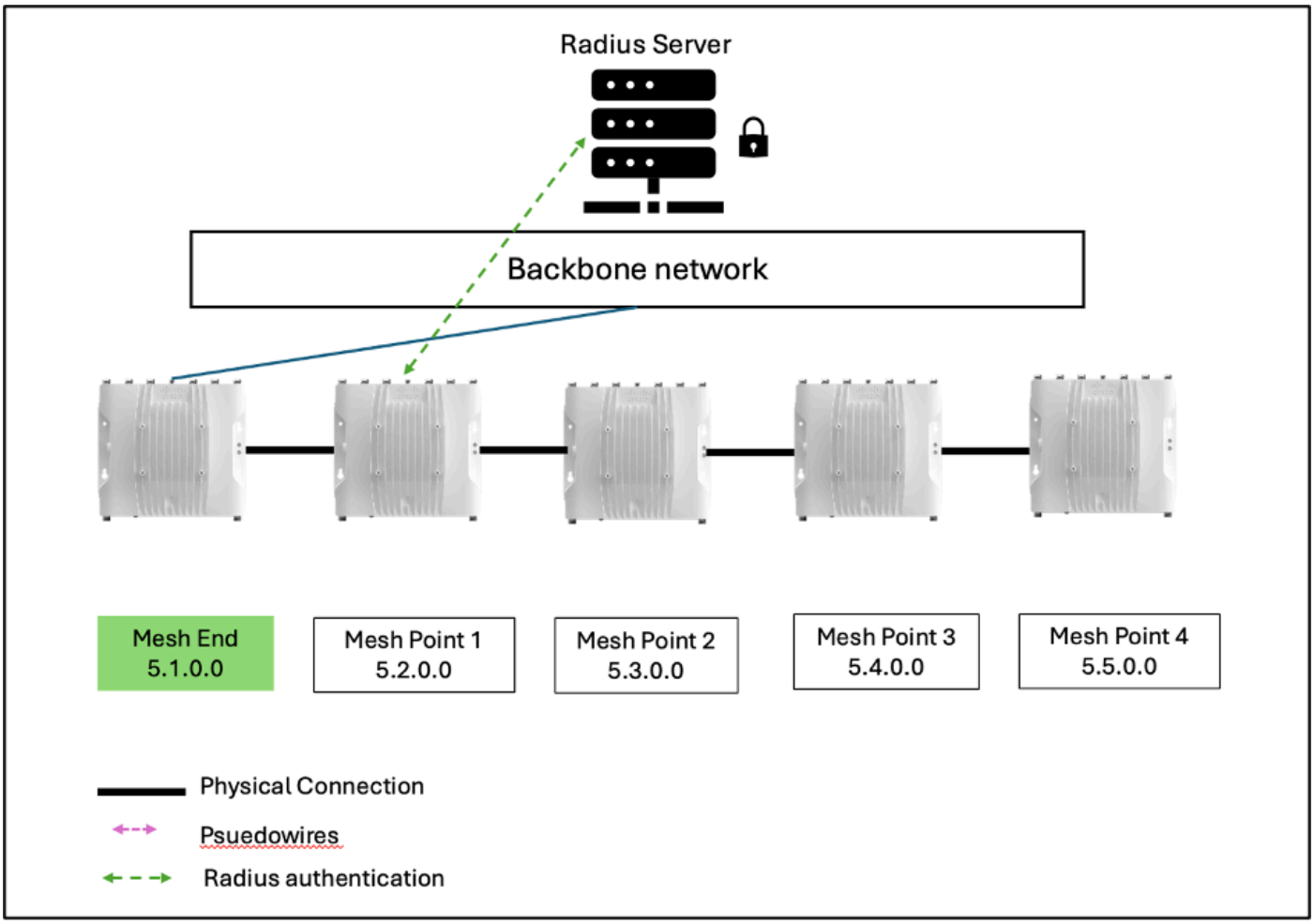
步驟 1:所有裝置均未經身份驗證。



開始時，所有單元(包括「網格端」(Mesh End))均未經身份驗證。自動分流器將僅在網狀終端無線電上開啟，網狀終端無線電是整個網路的輸入/輸出點。任何基礎架構裝置若要到達Radius伺服器以進行自我驗證，它必須是網狀端或具有到網狀端的偽線。

現在，網狀終端無線電5.1.0.0將通過骨幹網路向Radius伺服器發出身份驗證請求。收到回傳的通訊後，會進行驗證，然後對未驗證的基礎架構網狀點的其餘部分變得「不可見」，如同使用Radius的AAA的要求一樣。

步驟 2:Mesh End 5.1.0.0通過身份驗證，其餘部分未經身份驗證。

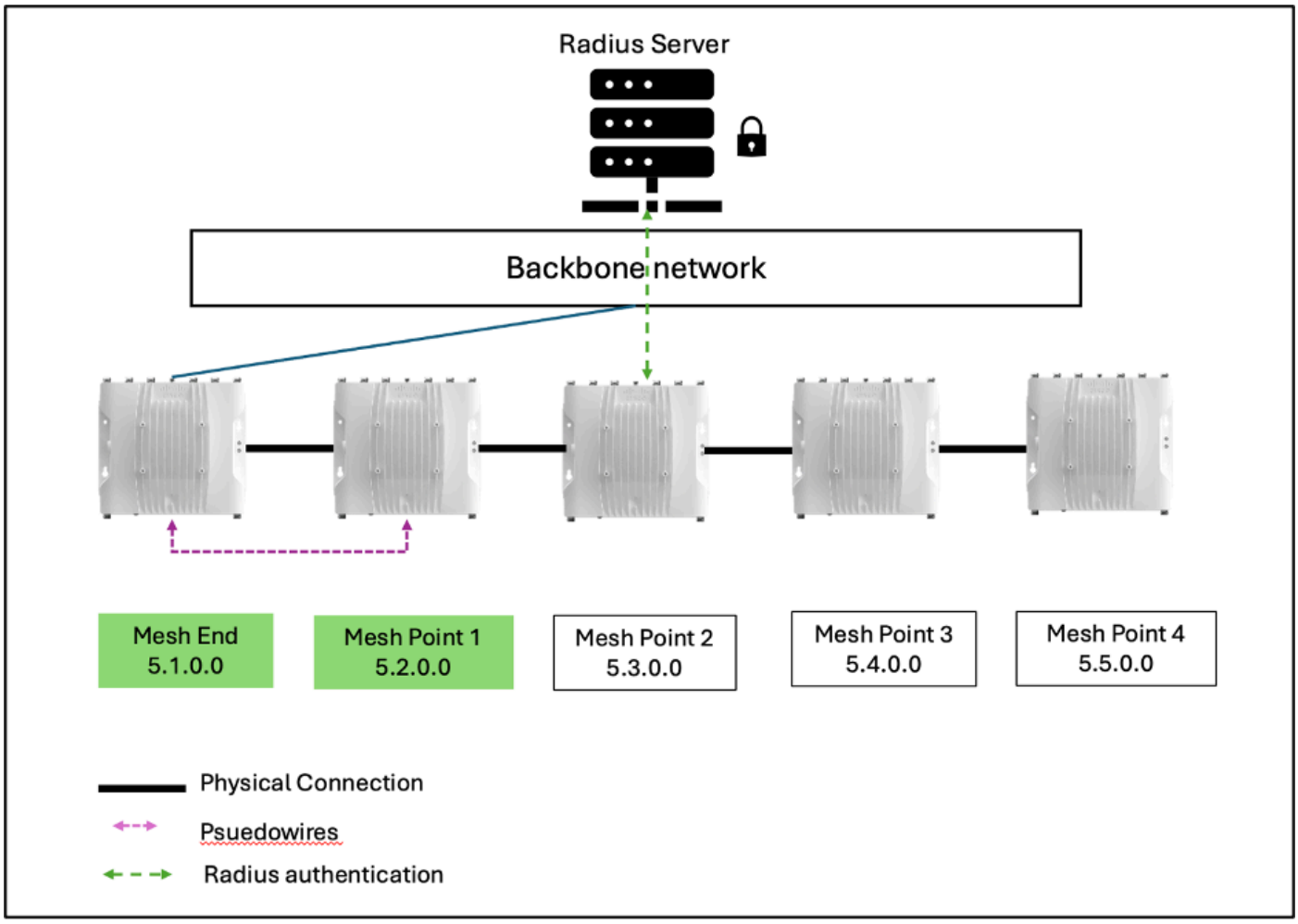


現在，網狀終端5.1.0.0已經過身份驗證，並且網路其餘部分看不到它，其餘的網狀點將運行選擇並選擇具有最低網狀ID的裝置作為下一個有線協調器。在本示例中，該網格點為網格ID為5.2.0.0的網格點1。然後，將在網格點1上開啟自動分接頭。

由於啟用了LNO，不會形成網狀點1的偽線。所有其餘無線電在其自動分路開啟時將必須按順序進行身份驗證。

現在，網狀點1可以向Radius伺服器傳送驗證要求並進行驗證。

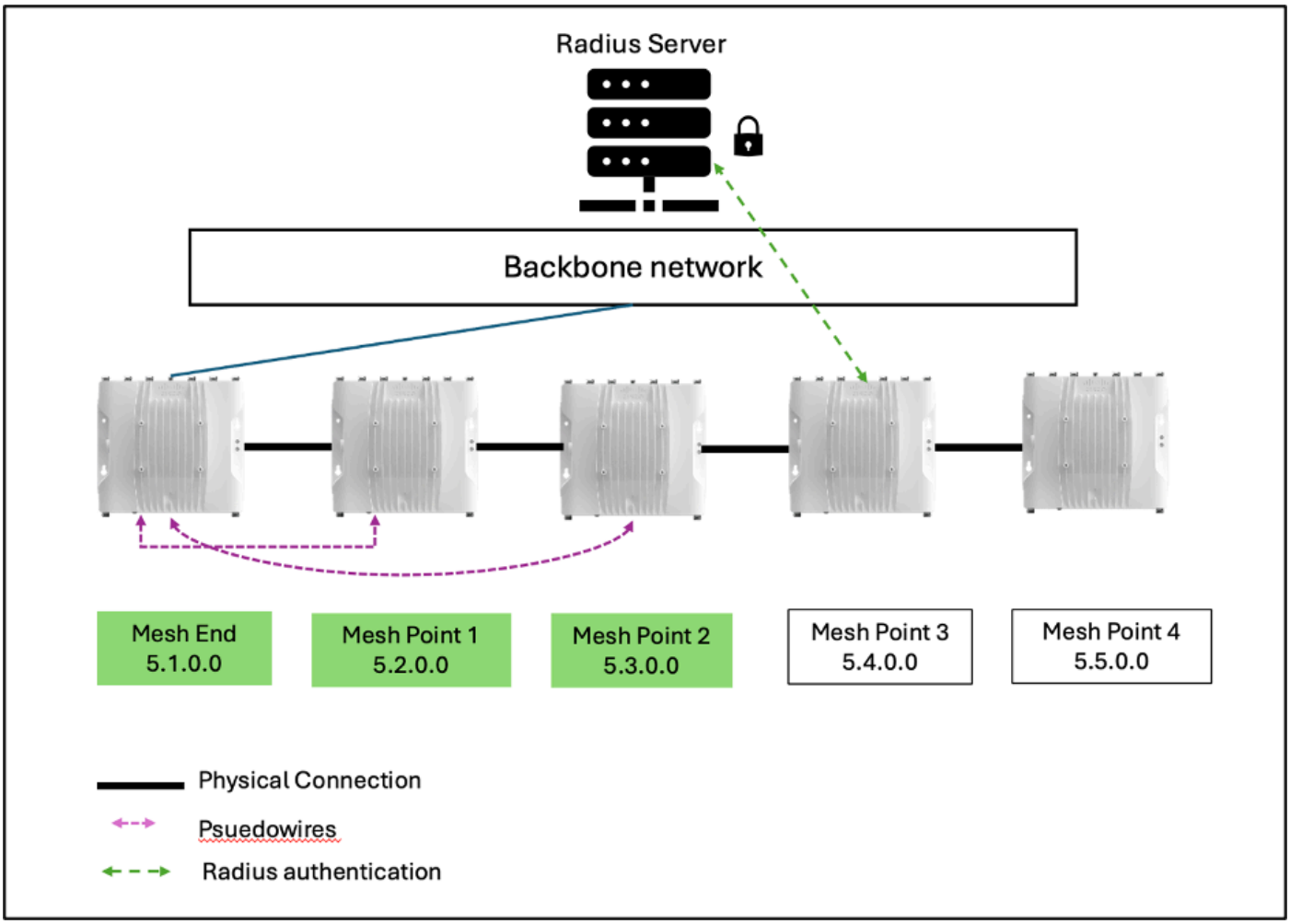
步驟 3:Mesh End、Mesh Point 1被驗證，而其它未被驗證。



現在，網狀點1也經過身份驗證，它將與經過身份驗證的網狀終端形成一條虛線，並且對於未經身份驗證的基礎設施無線電，它也會變得不可見。

其餘未經身份驗證的無線電重新運行選擇，並選擇具有最低網狀ID 5.3.0.0的網狀點2作為新的有線協調器，並且無線電會在其自動分流器現在開啟時向Radius伺服器發出身份驗證請求。

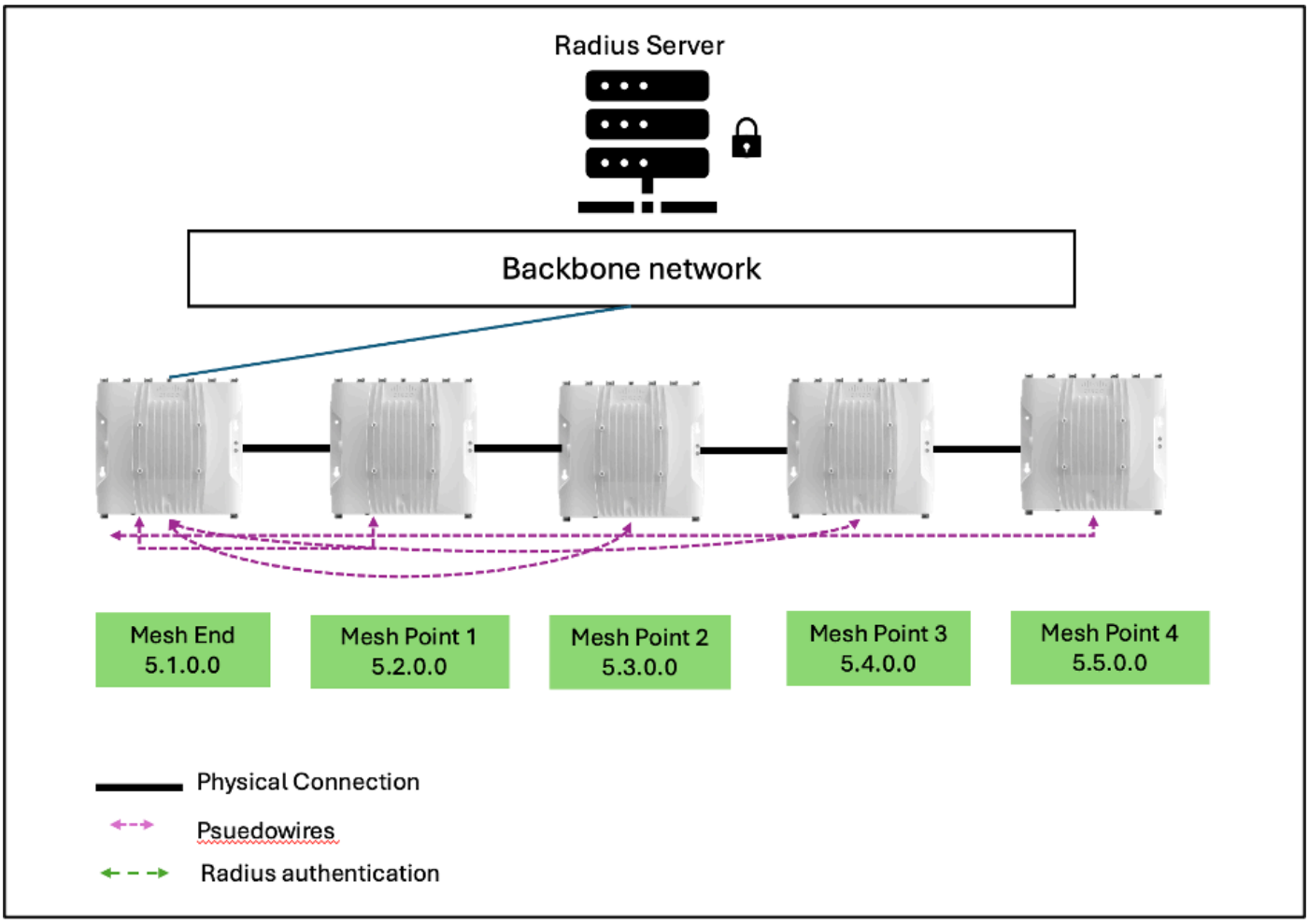
步驟 4:Mesh End、MP 1和MP 2進行身份驗證。



然後重複該過程，網格點2通過驗證並與網格端點裝置形成偽線。

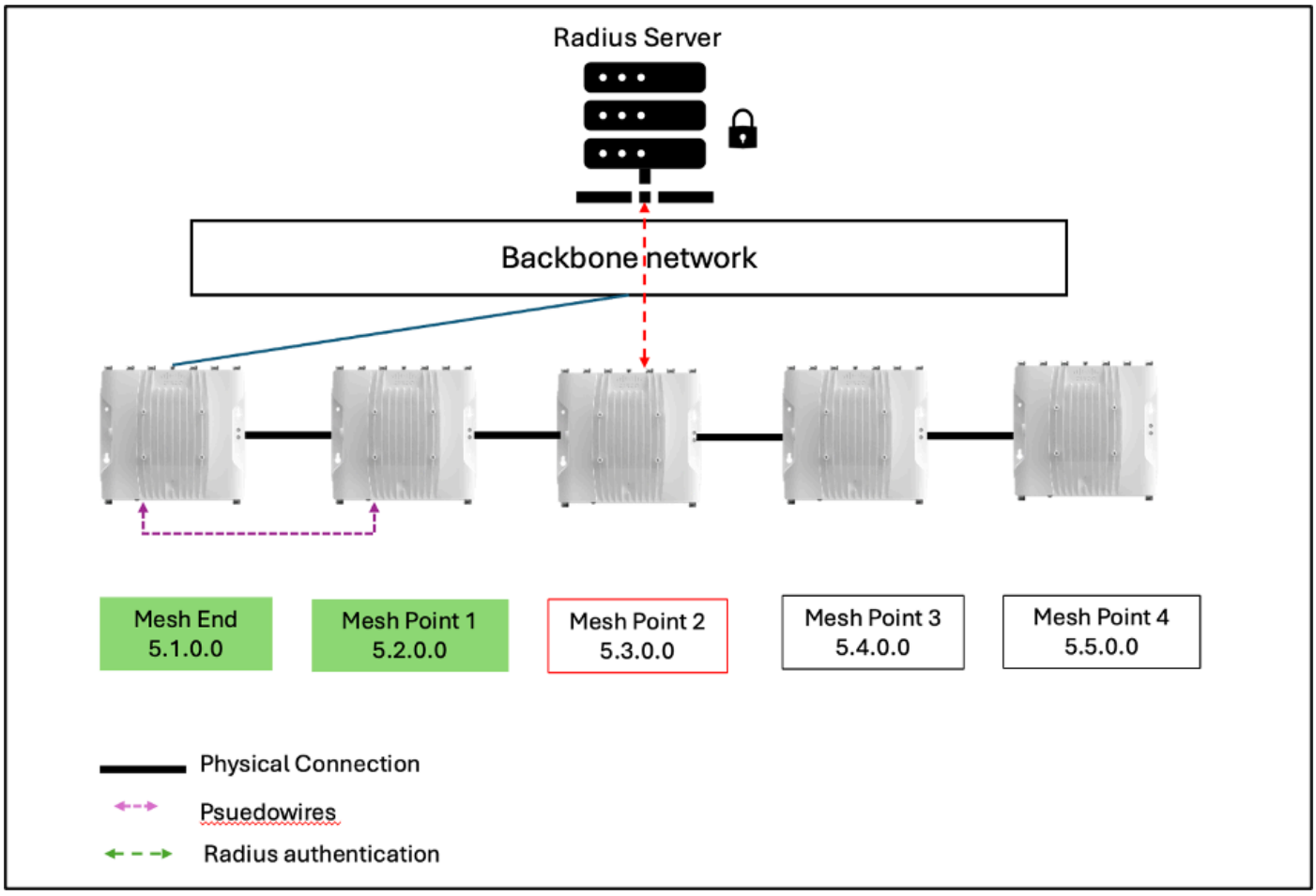
其餘的基礎架構無線電在開啟其自己的自動分路器時，按最低到最高網狀ID的順序輪流驗證自己。

步驟 5:所有無線電都經過身份驗證。



配置錯誤或問題案例：

如果任何基礎架構網狀點上的憑證錯誤或錯誤停用Radius，則會影響其他無線電進行驗證。在將無線電部署到生產環境之前，始終確保檢查憑據和設定。



在此範例中，如果網狀點2具有錯誤的摺痕，則會保持未經驗證的狀態，而網狀點3和網狀點4則永遠不會有機會驗證自己，因為啟用LNO後，從它們到網狀點2沒有形成偽線。

未通過身份驗證的無線電取決於錯誤配置的無線電的網狀ID。網狀ID高於當前有線協調器的任何無線電都保持未經驗證的狀態，並會導致問題。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。