URWBモードの産業用ワイヤレスアクセスポイントでのRADIUSおよびLNOの設定

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[背景説明](#)

[LNOを使用したRADIUS認証シーケンス](#)

はじめに

このドキュメントでは、URWBモードのIW9165およびIW9167無線でのRADIUS認証(RADIUS)および大規模ネットワーク最適化(LNO)の設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 基本的なCLIナビゲーションとコマンド
- IW URWBモード無線の理解

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IW9165およびIW9167無線

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

RADIUS:Remote Authentication Dial-In User Service（リモート認証ダイヤルインユーザサービス）は、ネットワークサービスに接続して使用するユーザまたはデバイスに対して、中央集中型の認証、許可、アカウンティング(AAA)管理を提供するために使用されるネットワーキングプロトコルです。URWBモードの産業用ワイヤレスデバイスでは、Radiusを使用して、デバイスがネッ

トワークに参加する前にデバイスを認証できます。

RADIUS設定のパラメータは、GUIまたはCLIアクセスから、あるいはIoT ODからもIWデバイスで設定できます。

RADIUSパラメータのCLI設定：

これらのパラメータは、デバイスのCLIのイネーブルモードから設定できます。

1. Radius認証を有効にします。

このパラメータを使用すると、デバイスでRADIUS認証を有効にできます。これは、RADIUS認証に必要な他の必須パラメータを追加した後で実行する必要があります。

Radio1#configure radius enabled

2. RADIUS認証を無効にする：

このパラメータを使用すると、デバイスのRADIUS認証を無効にできます。

Radio1#configure radius disabled

3. パススルー：

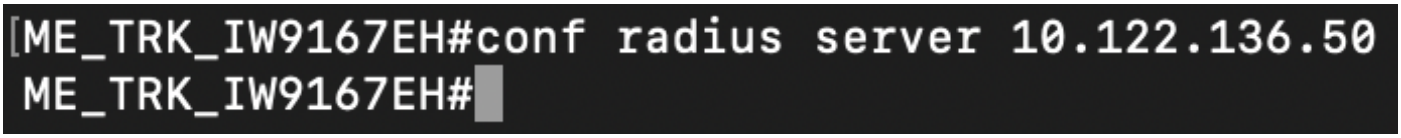
このパラメータは、インフラストラクチャ無線でのみ設定できます。インフラストラクチャ無線にパススルーパラメータを設定すると、Vehicle無線がインフラストラクチャ無線を介して自身を認証できるようになります。また、認証された車両無線と認証されていないインフラストラクチャ無線との通信も可能になります。

Radio1#configure radius passthrough

4. Radiusサーバを追加します。

このパラメータは、デバイスが通信するRADIUSサーバのIPアドレスを指定するために使用されます。

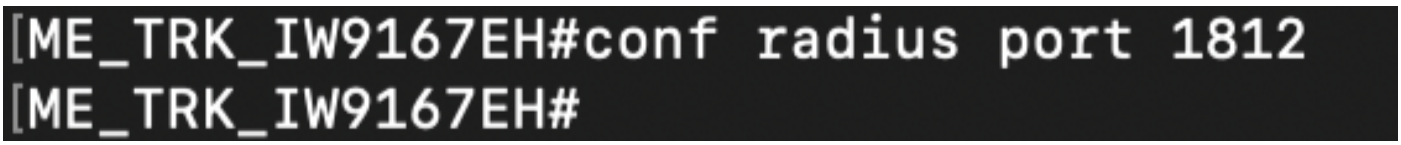
Radio1#configure radius server



5. RADIUSポート：

このパラメータは、デバイスが通信するRADIUSサーバのポートを指定するために使用されます。Radius認証のデフォルトポートは1812です。

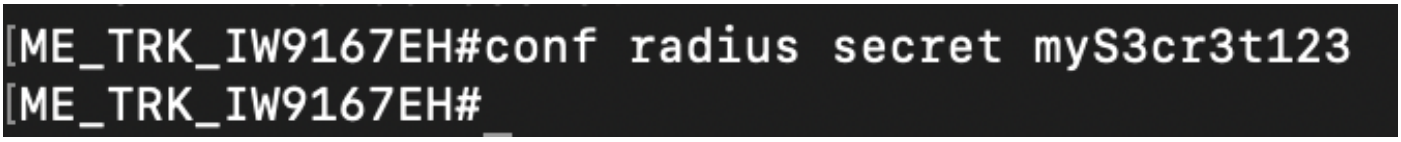
Radio1#configure radius server



6. Radiusシークレット：

このパラメータは、RADIUSサーバで使用する事前共有キーを指定するために使用します。

Radio1#configure radius secret



7. セカンダリサーバのIPとポート：

これらのパラメータは、デバイスがプライマリサーバに到達できない場合に使用する、2番目の

Radiusサーバ のIPアドレスとポート番号を指定するために使用されます。

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タイムアウト：

このパラメータは、クライアントがセカンダリ・サーバへの接続を試行する前に、プライマリRadiusサーバからの応答を待機する時間を秒単位で指定するために使用されます。デフォルト値は10秒に設定されています。

Radio1#configure radius timeout

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

9. 認証パラメータ：

このパラメータは、RADIUS認証方式と、それに対応して渡されるパラメータを指定するために使用されます。使用するオプションはいくつかあります。

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
```

これらの方法を使用する場合：GTC(Generic token card)、MD5(Message-Digest Algorithm 5)、またはMSCHAPV2(Microsoft Challenge Handshake Authentication Protocol version 2)では、ユーザ名とパスワードの両方を次のコマンドで追加できます。

Radio1#configure radius authentication gtc

Radio1#configure radius authentication md5

Radio1#configure radius authentication mschapv2

認証にPEAP(Protected Extensible Authentication Protocol)またはEAP-TTLS(Extensible Authentication Protocol-Tunneled Transport Layer Security)を使用する場合は、別の内部認証方式も指定する必要があります。gtc、md5、mschapv2のいずれかを指定できます。

Radio1#configure radius authentication peap

inner-auth-method

Radio1#configure radius authentication ttls

inner-auth-method

10. 切り替えの試行：

このパラメータには、クライアントがセカンダリサーバに切り替わるまでにプライマリサーバに対して許可されるRADIUS認証の試行回数を指定します。デフォルト値は 3 です。

Radio1#configure radius switch <1-6>

11. バックオフ時間：

このパラメータには、認証の最大試行回数を超えた後にクライアントが待機する時間を秒単位で指定します。

Radio1#configure radius backoff-time

12. 有効期限：

このパラメータには、Radius認証が完了していない間に認証の試行が破棄される時間を秒数で指定します。

Radio1#configure radius expiration

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

13. 要求の送信：

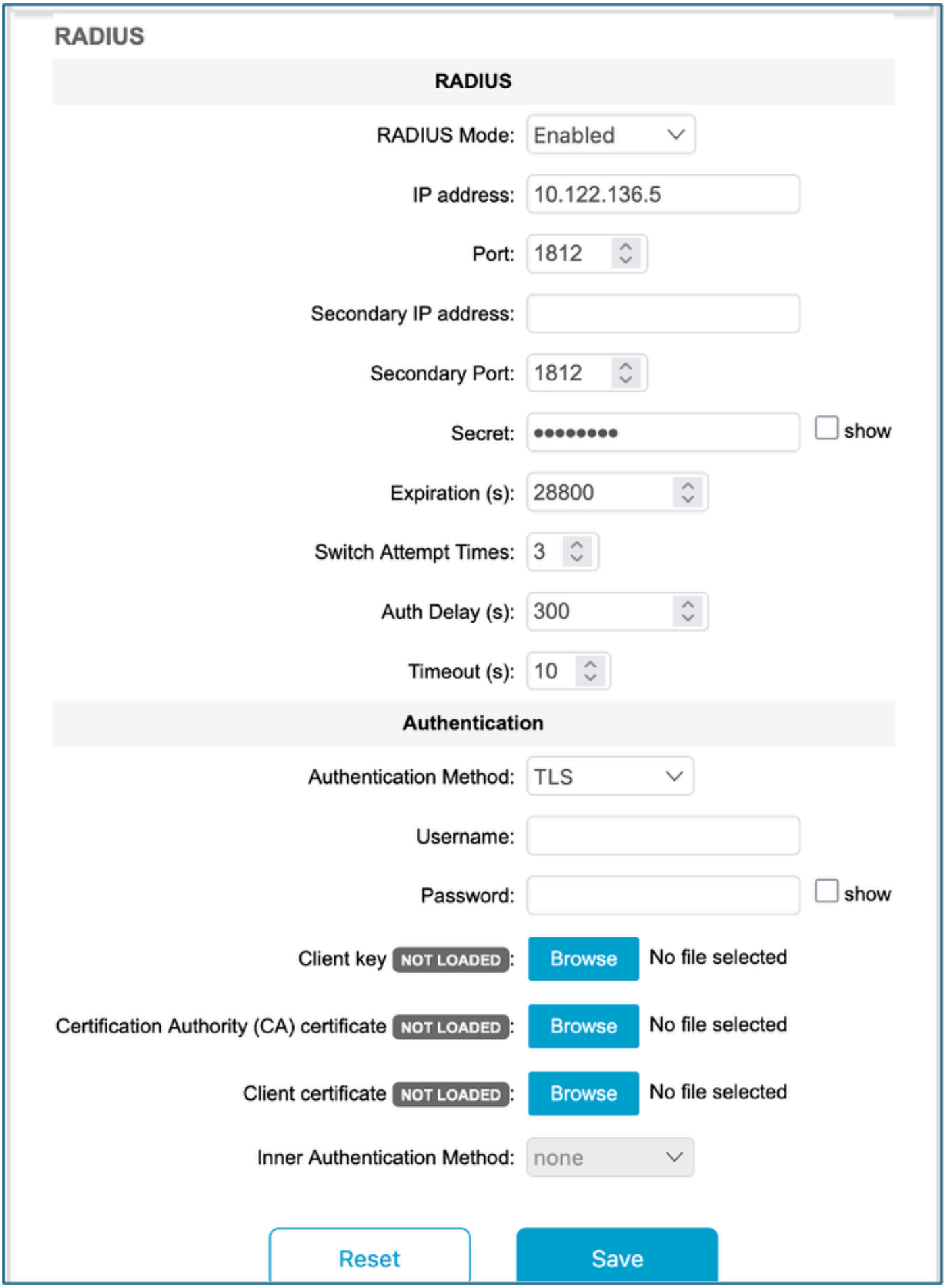
このパラメータは、設定されたプライマリまたはセカンダリRadiusサーバに対してRADIUS認証要求を開始するために使用されます。

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).
```

URWBモードの産業用ワイヤレス無線でも、GUIおよびWebページの「Radius」タブで同じパラメータを設定できます。


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 コマンド：

現在のRADIUS設定は、CLIでshowコマンドを使用して確認できます。

1.

#show半径

次のshowコマンドは、デバイスでRADIUSが有効か無効かを示します。

```
[ME_TRK_IW9167EH#show radius
```

2.

***#show RADIUS*アカウンティング**

***#show radius auth-method-tls*（オプション）**

***#show RADIUS*認証**

次のshowコマンドは、設定されたradiusアカウンティングサーバ、認証サーバ、および認証方式tlsパラメータの現在の設定を表示します。

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

LNOを使用したRADIUS認証シーケンス

LNO(Large Network Optimization)は、50以上のインフラストラクチャ無線を備えた大規模なネットワークで有効にし、ネットワーク内のすべてのデバイス間の疑似配線形成を最適化することを推奨する機能です。レイヤ2とレイヤ3の両方のネットワークで使用される

LNOとRADIUSの両方が有効になっているネットワークでは、インフラストラクチャ無線は自分自身を（最低のメッシュIDから最高のメッシュIDまで）順番に認証します。 LNOを有効にすると、すべてのインフラストラクチャ無線でメッシュ終端への疑似配線のみが構築され、BPDU転送も無効になります。

この記事では、1つのメッシュエンド無線と4つのメッシュポイントインフラストラクチャ無線を使用したFluidity設定でのRADIUS認証のシーケンスについて説明します。

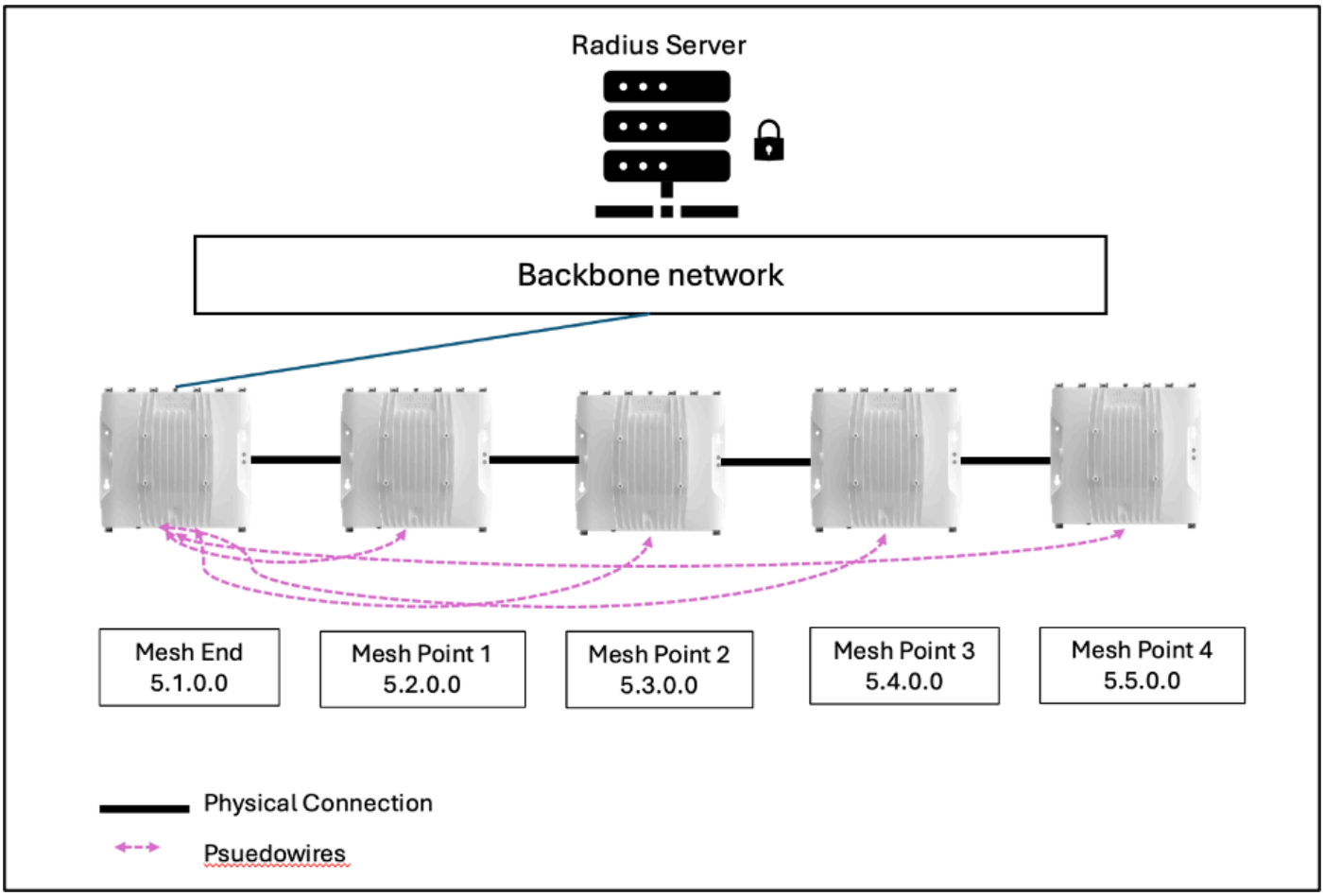
Mesh End無線は、Fluidityネットワークのデフォルトの「有線コーディネータ」です。つまり、オートタップが開いていて、ネットワークの入力/出力ポイントとして機能します。

他のすべてのインフラストラクチャ無線はメッシュポイントとして設定され、相互に接続されたスイッチを介してメッシュエンドに物理的に接続されています。

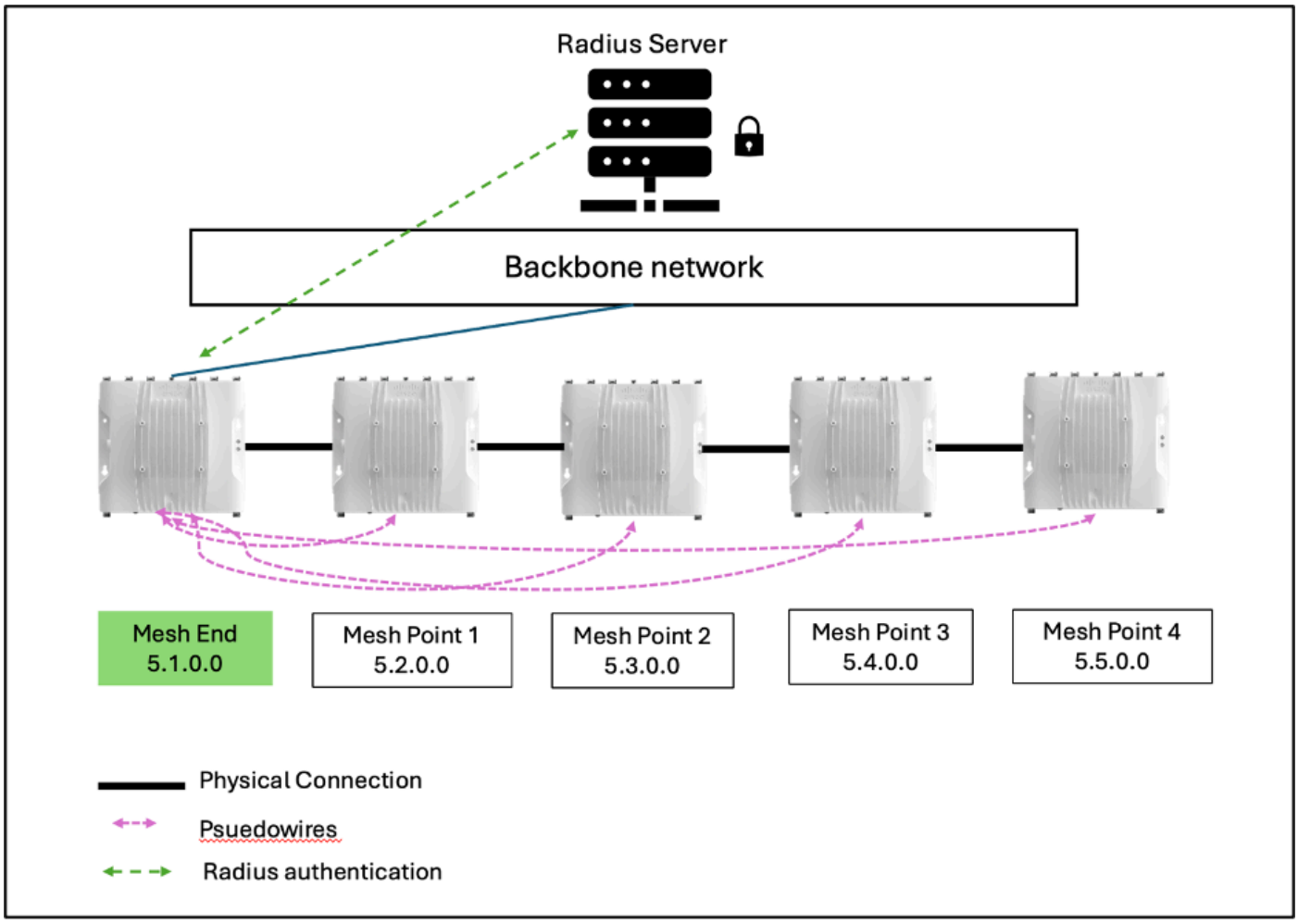
メッシュエンド無線は、通常はファイバ接続を介してバックボーンネットワークに接続され、バックボーンネットワークを介してネットワークのRADIUSサーバに到達できます。

どのデバイスも、次の場合にのみRADIUSサーバに到達できます。

1. 有線のコーディネータです。
2. これは、メッシュエンドなどの有線マスターで構築された疑似配線を備えています。



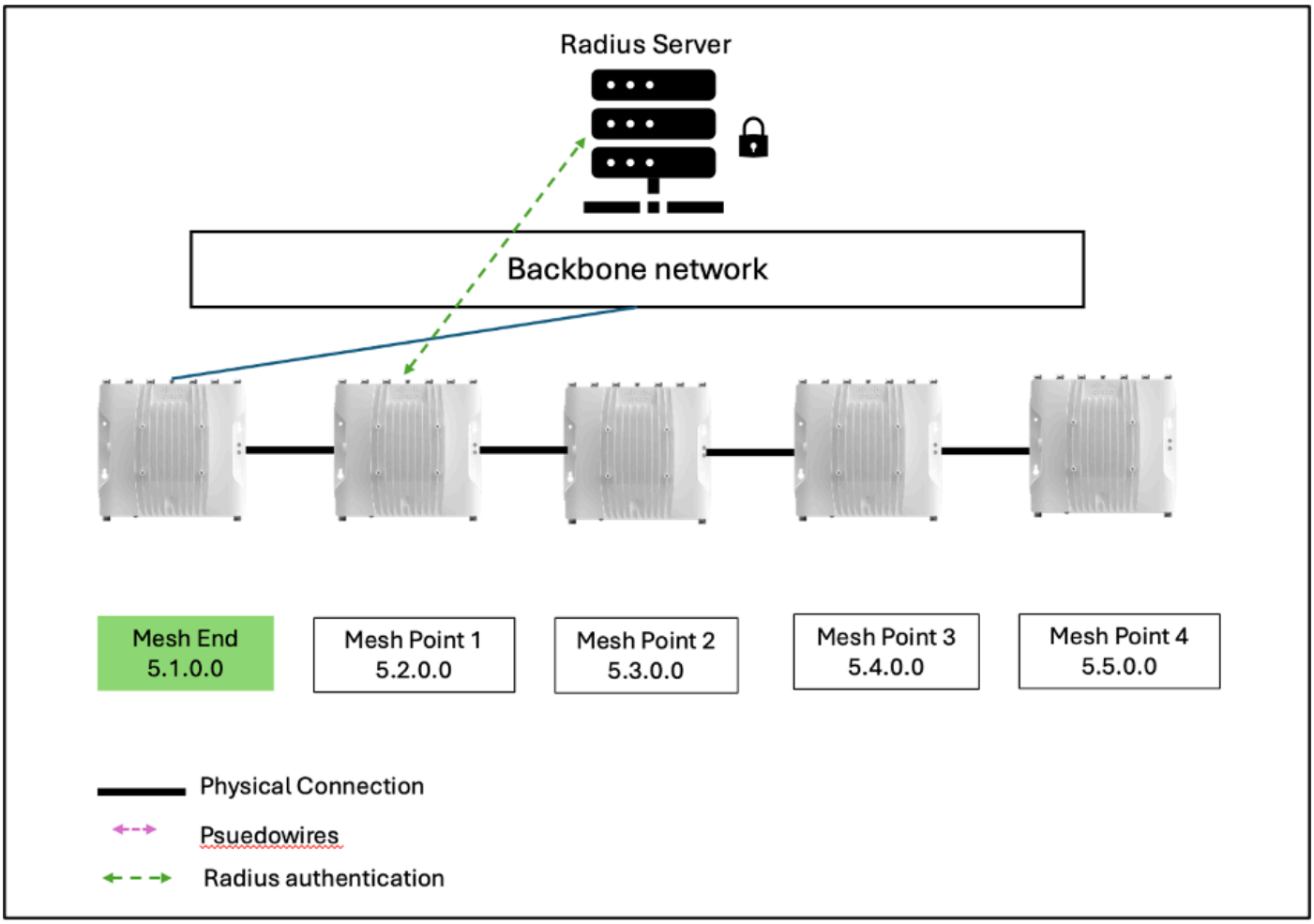
ステップ1：すべてのユニットが認証されていません。



最初は、メッシュの終端を含むすべてのユニットが認証されません。自動タップは、ネットワーク全体の入力/出力ポイントであるメッシュ終端無線でのみ開きます。インフラストラクチャデバイスがRadiusサーバに到達して自身を認証するには、そのデバイスがメッシュ端であるか、メッシュ端への疑似配線を備えている必要があります。

ここで、メッシュエンドの無線5.1.0.0は、バックボーンネットワーク経由でRadiusサーバに認証要求を送信します。通信が返されると、認証が行われ、Radiusを使用するAAAの要件に従って、認証されていないインフラストラクチャメッシュポイントの残りの部分に「見えない」状態になります。

手順2：メッシュの終端5.1.0.0が認証され、残りは認証されません。

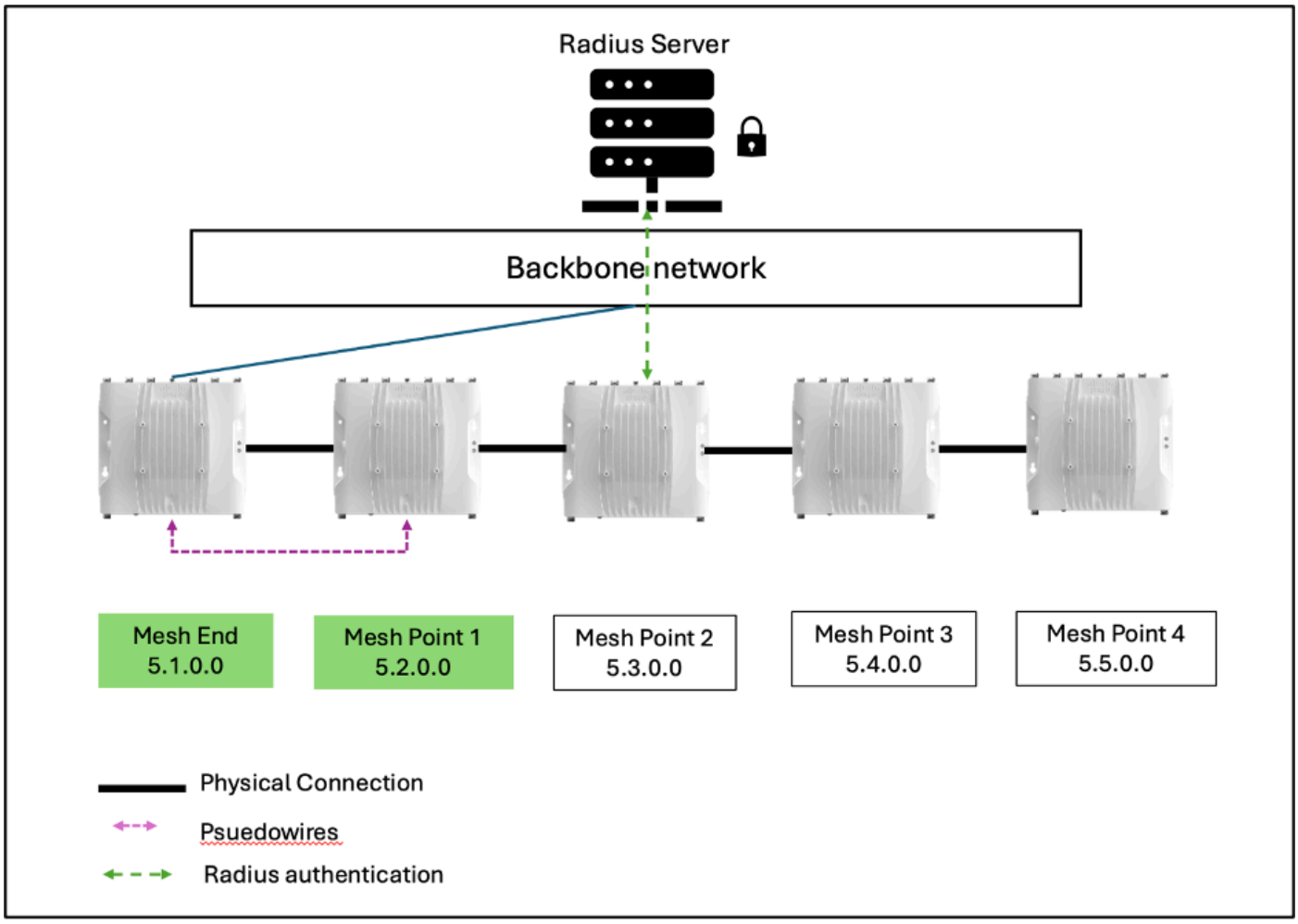


メッシュエンド5.1.0.0が認証され、ネットワークの他の部分からは見えなくなったので、残りのメッシュポイントが選択を実行し、最も低いメッシュIDを持つデバイスを次の有線コーディネータとして選択します。この例では、メッシュIDが5.2.0.0のメッシュポイント1です。その後、Autotapはメッシュポイント1で開きます。

LNOが有効になっているため、メッシュポイント1への擬似配線は形成されません。残りのすべての無線は、Autotapが開いているときに順次認証される必要があります。

これで、メッシュポイント1はRadiusサーバに認証要求を送信し、自身を認証できます。

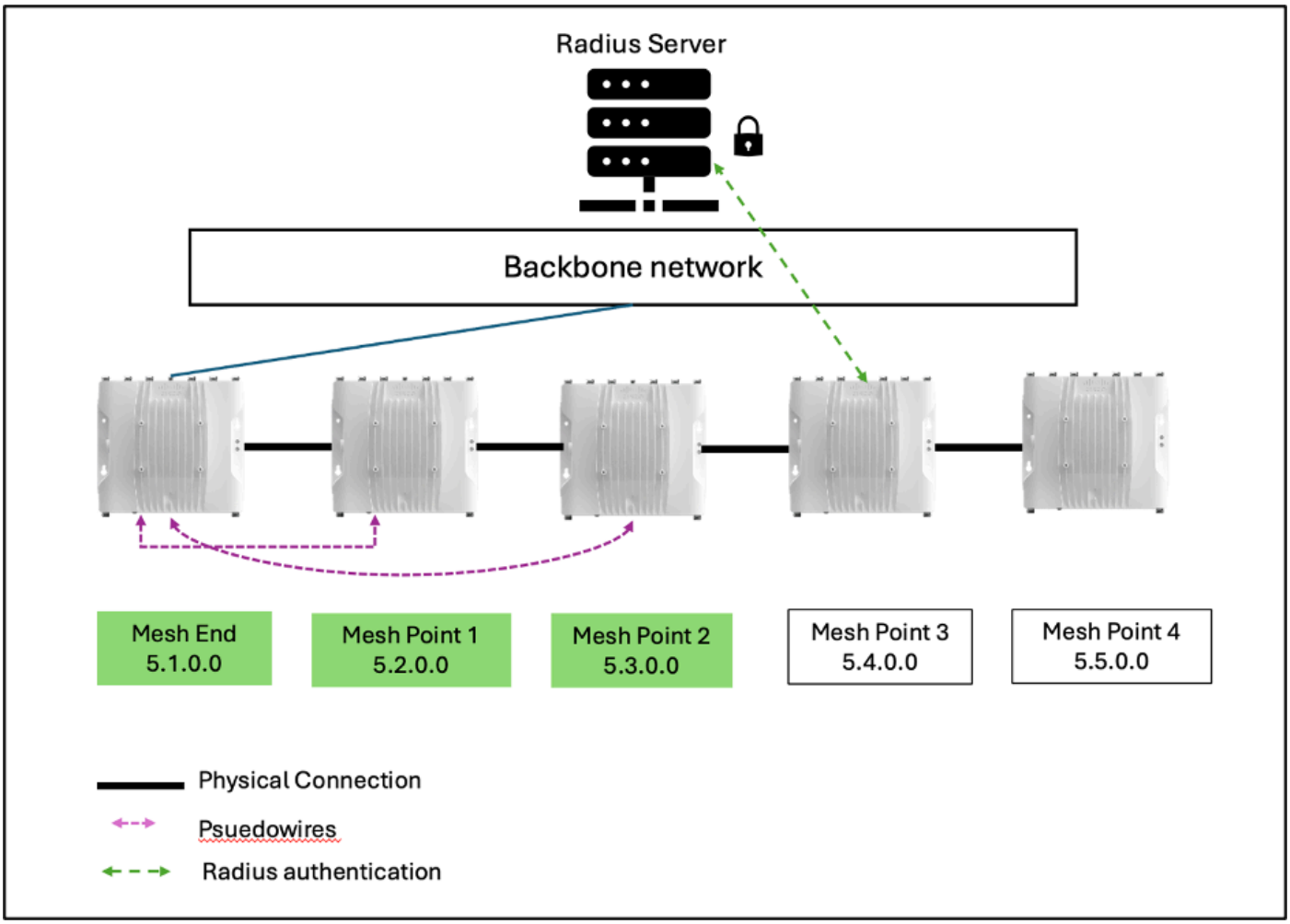
手順3：メッシュの終端、メッシュポイント1が認証され、他のポイントは認証されません。



メッシュポイント1も認証されたため、認証済みのメッシュエンドとの疑似配線が形成され、認証されていないインフラストラクチャ無線の残りの部分からも見えなくなります。

残りの未認証の無線は選出を再実行し、新しい有線コーディネータとして最小のメッシュID 5.3.0.0を持つメッシュポイント2を選択します。その無線は、Autotapが開いているため、Radiusサーバに認証要求を送信します。

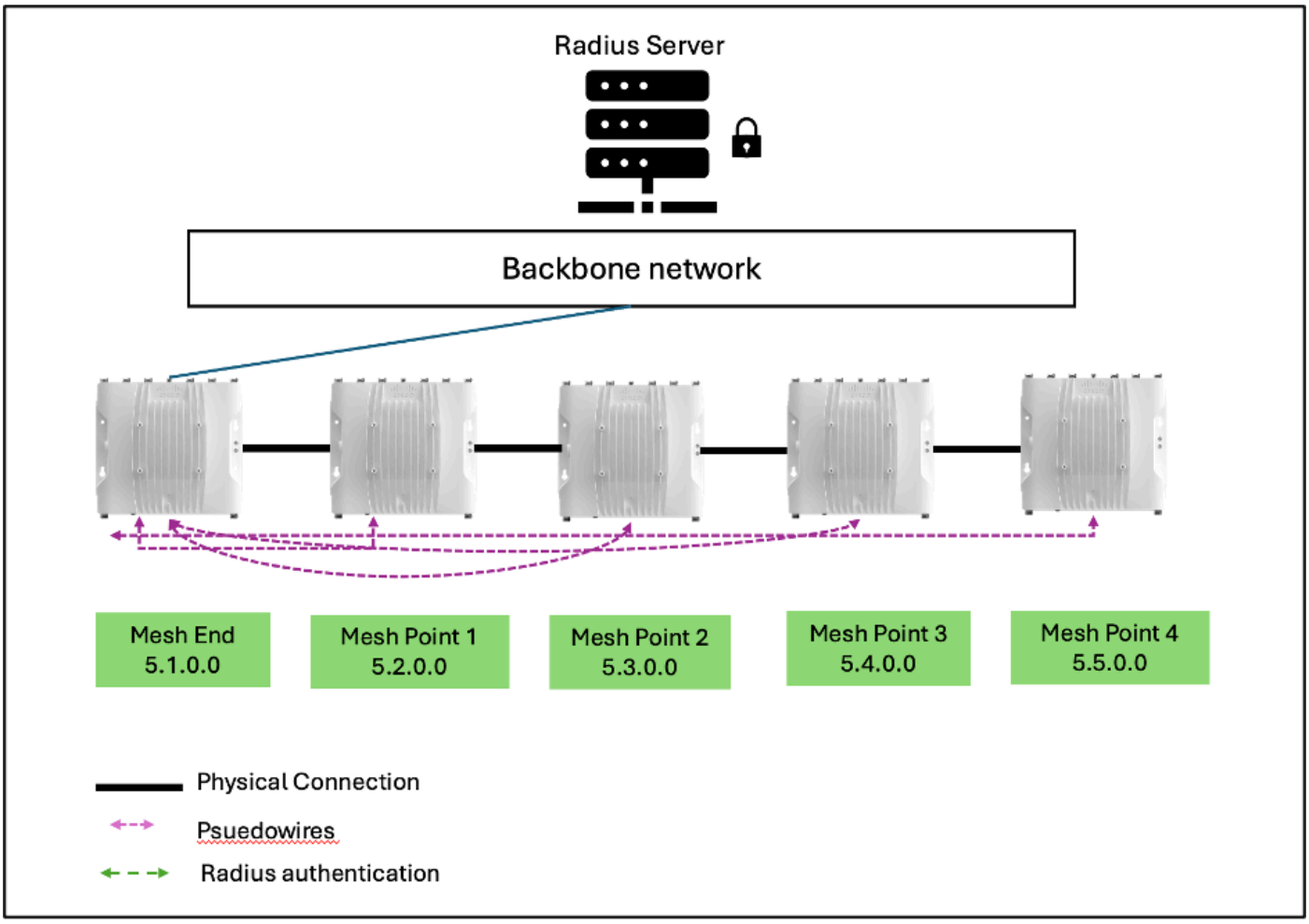
手順4：メッシュの終端、MP 1およびMP 2が認証されます。



このプロセスは、メッシュポイント2が認証され、メッシュエンドデバイスとの疑似配線が形成されるときにも繰り返されます。

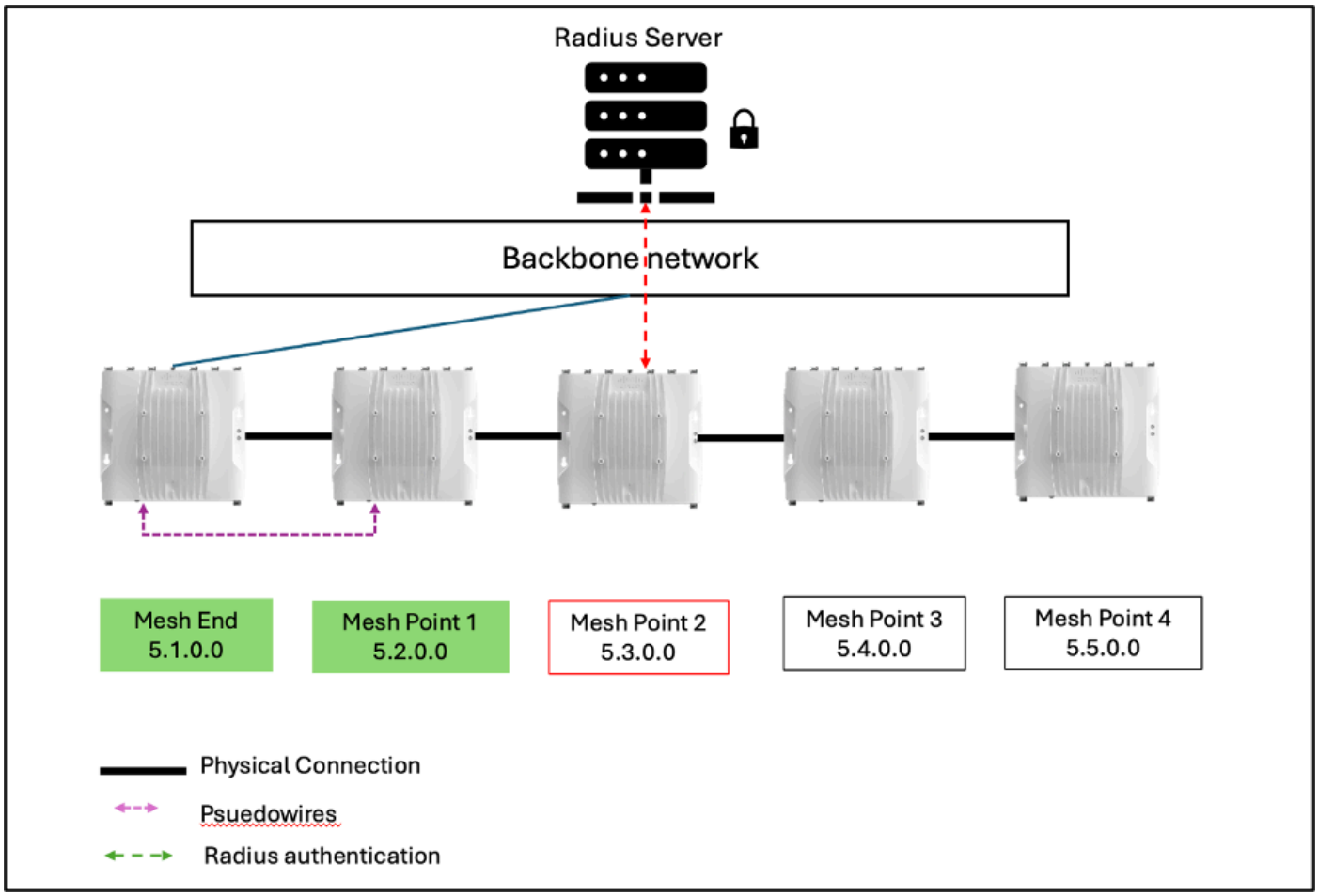
インフラストラクチャ無線の残りの部分は、低いメッシュIDから高いメッシュIDの順に、自身のオートタップが開かれたときに、順番に認証を受けます。

手順5：すべての無線が認証されます。



誤設定または問題のあるケース：

インフラストラクチャメッシュポイントのいずれかに誤ったクレデンシャルがあるか、誤ってRADIUSを無効にした場合、他の無線の認証に影響します。無線を実稼働環境に導入する前に、必ずクレデンシャルと設定を確認してください。



この例では、メッシュポイント2に不正なクレッドがある場合、LNOが有効になっているためメッシュポイント2への疑似回線が形成されないため、メッシュポイント2は未認証のままになり、メッシュポイント3とメッシュポイント4は自身を認証する機会がありません。

認証されないままの無線は、誤って設定された無線のメッシュIDに依存します。現在の有線コーディネータよりも高いメッシュIDを持つ無線は認証されないままになり、問題を引き起こします。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。