Konfigurieren von RADIUS und LNO auf Industrial Wireless Access Points im URWB-Modus

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der RADIUS-Authentifizierung und der LNO-Funktion (Large Network Optimization) für IW9165- und IW9167-Funkmodule im URWB-Modus beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegende CLI-Navigation und -Befehle
- Verständnis von IW-URWB-Modusradios

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- IW9165- und IW9167-Funkeinheiten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

RADIUS - Remote Authentication Dial-In User Service ist ein Netzwerkprotokoll zur zentralisierten AAA-Verwaltung (Authentication, Authorization, Accounting) für Benutzer oder Geräte, die eine Verbindung mit einem Netzwerkdienst herstellen und diesen nutzen. Für industrielle Wireless-Geräte im URWB-Modus kann Radius verwendet werden, um Geräte zu authentifizieren, bevor sie einem Netzwerk beitreten können.

Die Parameter für die Radius-Konfiguration können auf den IW-Geräten entweder über die GUI, den CLI-Zugriff oder auch über das IoT-OD konfiguriert werden.

CLI-Konfiguration der Radius-Parameter:

Diese Parameter können über den privilegierten Modus (enable mode) in der CLI der Geräte konfiguriert werden.

1. Aktivieren der Radius-Authentifizierung:

Mit diesem Parameter kann die Radius-Authentifizierung auf den Geräten aktiviert werden. Dies muss ausgeführt werden, nachdem weitere erforderliche Parameter für die RADIUS-Authentifizierung hinzugefügt wurden.

Radio1#configure radius enabled

2. Deaktivieren der Radius-Authentifizierung:

Mit diesem Parameter kann die Radius-Authentifizierung auf den Geräten deaktiviert werden.

Radio1#configure radius disabled

3. Passthrough:

Dieser Parameter muss nur für die Infrastruktur-Funkmodule konfiguriert werden. Durch die Konfiguration von Infrastrukturradios mit Passthrough-Parametern können sich die Fahrzeugradios über die Infrastrukturradios authentifizieren und eine Kommunikation zwischen den authentifizierten Fahrzeugradios und den nicht authentifizierten Infrastrukturradios ermöglichen.

Radio1#configure radius passthrough

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

4. RADIUS-Server hinzufügen:

Dieser Parameter gibt die IP-Adresse des Radius-Servers an, mit dem das Gerät kommunizieren soll.

Radio1#configure radius server

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

5. Radius-Port:

Mit diesem Parameter wird der Port des Radius-Servers festgelegt, mit dem das Gerät kommunizieren soll. Der Standardport für die Radius-Authentifizierung ist 1812.

Radio1#configure radius server

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

6. Radius Secret:

Mit diesem Parameter wird der vorinstallierte Schlüssel für den Radius-Server festgelegt.

Radio1#configure radius secret

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

7. Sekundäre Server-IP und Port:

Mit diesen Parametern werden die IP-Adresse und die Port-Nummer eines zweiten Radius-Servers festgelegt, der verwendet werden soll, wenn das Gerät den primären Server nicht erreichen kann.

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-Timeout:

Dieser Parameter gibt die Zeit in Sekunden an, die der Client auf eine Antwort vom primären Radius-Server wartet, bevor er versucht, eine Verbindung zum sekundären Server herzustellen. Der Standardwert ist 10 Sekunden.

Radio1#configure radius timeout

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

9. Authentifizierungsparameter:

Dieser Parameter wird verwendet, um die Radius-Authentifizierungsmethode und die entsprechenden zu übergebenden Parameter anzugeben. Es gibt mehrere Optionen zu verwenden.

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
```

Bei Verwendung dieser Methoden: GTC (Generic Token Card), MD5 (Message-Digest Algorithm 5) oder MSCHAPV2 (Microsoft Challenge Handshake Authentication Protocol Version 2) können Benutzername und Passwort mit den folgenden Befehlen hinzugefügt werden:

Radio1#configure radius authentication gtc

Radio1#configure radius authentication md5

Radio1#configure radius authentication mschapv2

Bei Verwendung dieser Methoden: PEAP (Protected Extensible Authentication Protocol) oder EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) für die Authentifizierung muss zusätzlich eine andere innere Authentifizierungsmethode bereitgestellt werden. Es kann sich um gtc, md5 oder mschapv2 handeln.

Radio1#configure radius authentication peap

inner-auth-method

Radio1#configure radius authentication ttls

inner-auth-method

10. Switch-Versuche:

Dieser Parameter gibt die Anzahl der RADIUS-Authentifizierungsversuche an, die für den primären Server zulässig sind, bevor der Client zum sekundären Server wechselt. Der Standardwert ist 3.

Radio1#configure radius switch <1-6>

11. Backoff-Zeit:

Dieser Parameter gibt den Wert der Zeit in Sekunden an, auf die der Client warten muss, nachdem die maximale Anzahl von Authentifizierungsversuchen überschritten wurde.

Radio1#configure radius backoff-time

12. Verfallszeit:

Dieser Parameter gibt den Wert für die Zeit in Sekunden an, während der die Radius-Authentifizierung nicht abgeschlossen ist und der Authentifizierungsversuch abgebrochen wird.

Radio1#configure radius expiration

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

13. Bitte senden:

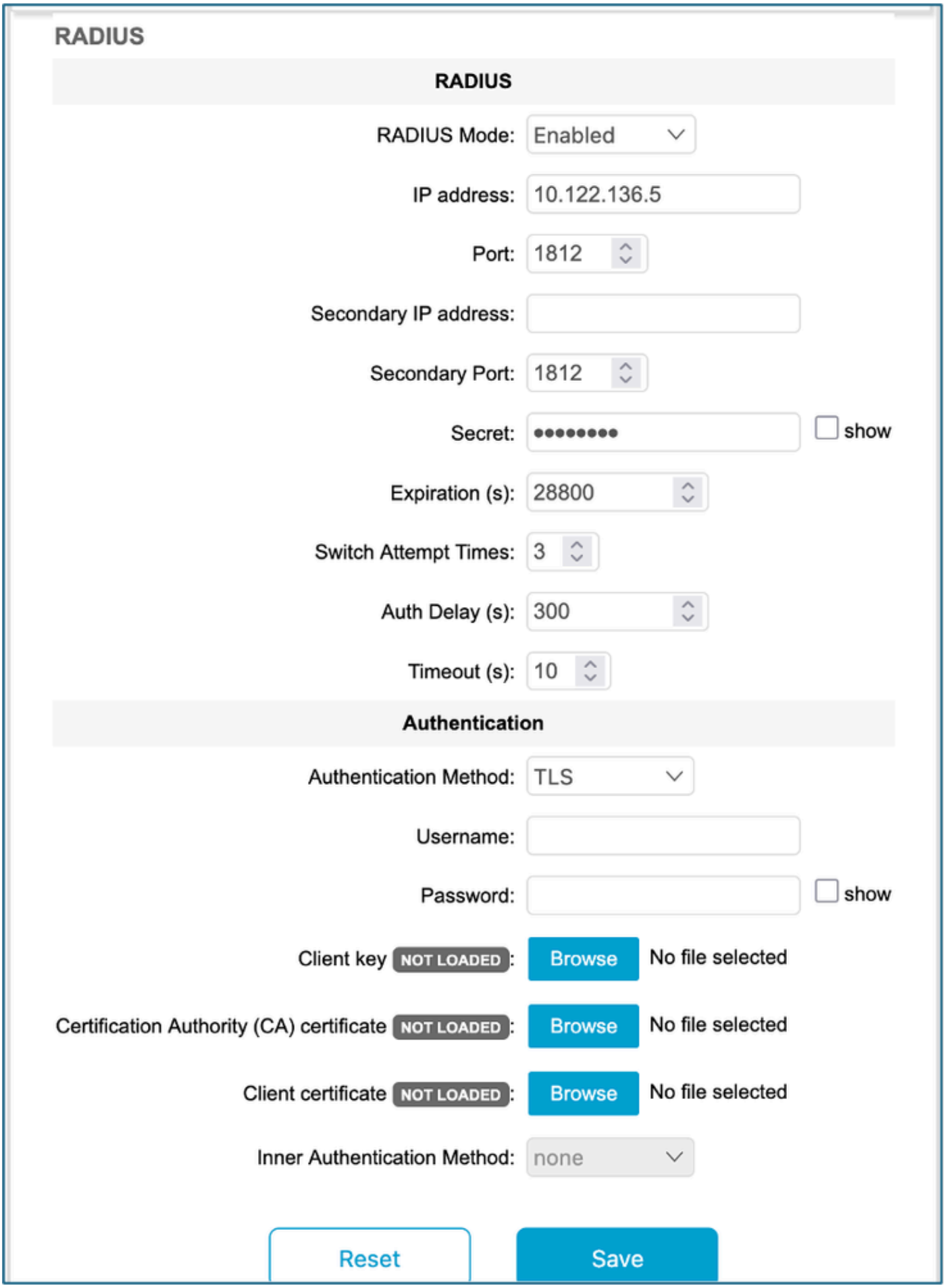
Dieser Parameter wird verwendet, um eine RADIUS-Authentifizierungsanforderung an den konfigurierten primären oder sekundären RADIUS-Server zu initiieren.

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).
```

Dieselben Parameter können auf den Industrial Wireless-Funkmodulen im URWB-Modus über die Benutzeroberfläche sowie auf der Registerkarte "Radius" auf der Webseite konfiguriert werden.



Show-Befehle:

Die aktuelle Radius-Konfiguration kann über die CLI mit show-Befehlen überprüft werden.

1.

#show Radius

Dieser Befehl show gibt an, ob Radius auf dem Gerät aktiviert oder deaktiviert ist.

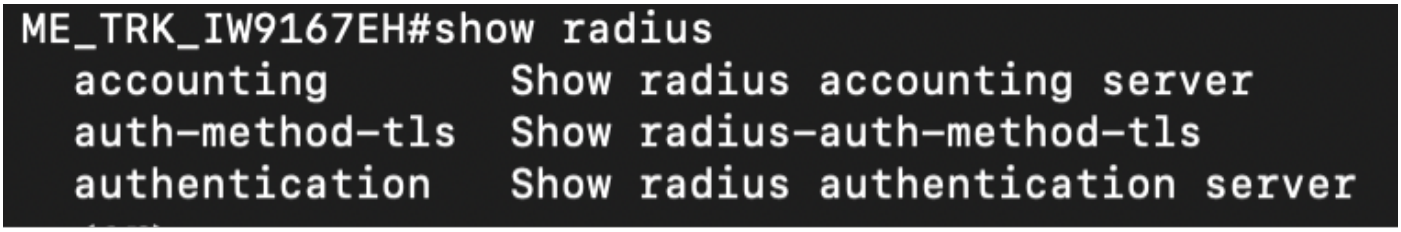
2.

#show Radius-Accounting

#show radius auth-method-tls

#show RADIUS-Authentifizierung

Diese Befehle zeigen die aktuelle Konfiguration des Radius-Abrechnungsservers, des Authentifizierungsservers und der konfigurierten Authentifizierungsmethode tls an.



Radius-Authentifizierungssequenz mit LNO

Die LNO- oder die Optimierung großer Netzwerke ist eine Funktion, die in großen Netzwerken mit 50 oder mehr Funkeinheiten der Infrastruktur aktiviert werden sollte, um die Pseudodrahterzeugung zwischen allen Geräten im Netzwerk zu optimieren. Es wird sowohl in Layer-2- als auch Layer-3-Netzwerken verwendet.

In Netzwerken, in denen sowohl LNO als auch Radius aktiviert sind, authentifizieren sich die Infrastruktur-Funkeinheiten der Reihe nach (von der niedrigsten bis zur höchsten Mesh-ID). Die Aktivierung von LNO zwingt alle Infrastruktur-Funkmodule dazu, NUR Pseudodrähte zum Mesh-End aufzubauen, und deaktiviert außerdem die BPDU-Weiterleitung.

In diesem Artikel wird die Sequenz der Radius-Authentifizierung bei einer Fluidity-Konfiguration mit einem Mesh End- und 4 Mesh Point Infrastructure-Funkmodulen beschrieben.

Das Mesh-End-Funkmodul ist der standardmäßige "Wired-Koordinator" des Fluidity-Netzwerks. Das bedeutet, dass er sich automatisch öffnet und als Eingangs-/Ausgangspunkt für das Netzwerk fungiert.

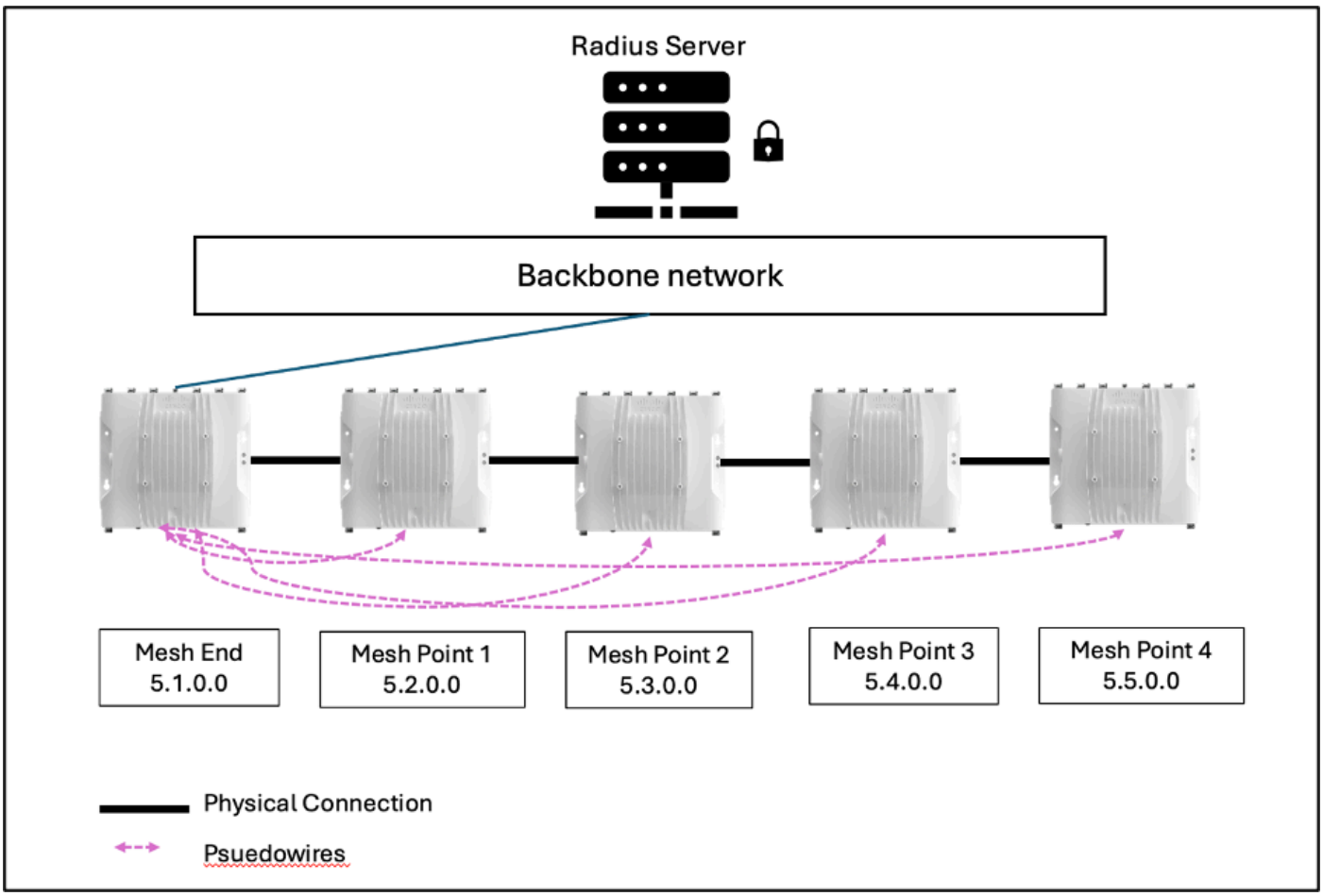
Alle anderen Infrastruktur-Funkmodule sind als Mesh-Punkte eingerichtet und verfügen über

physische Verbindungen zum Mesh-End über miteinander verbundene Switches.

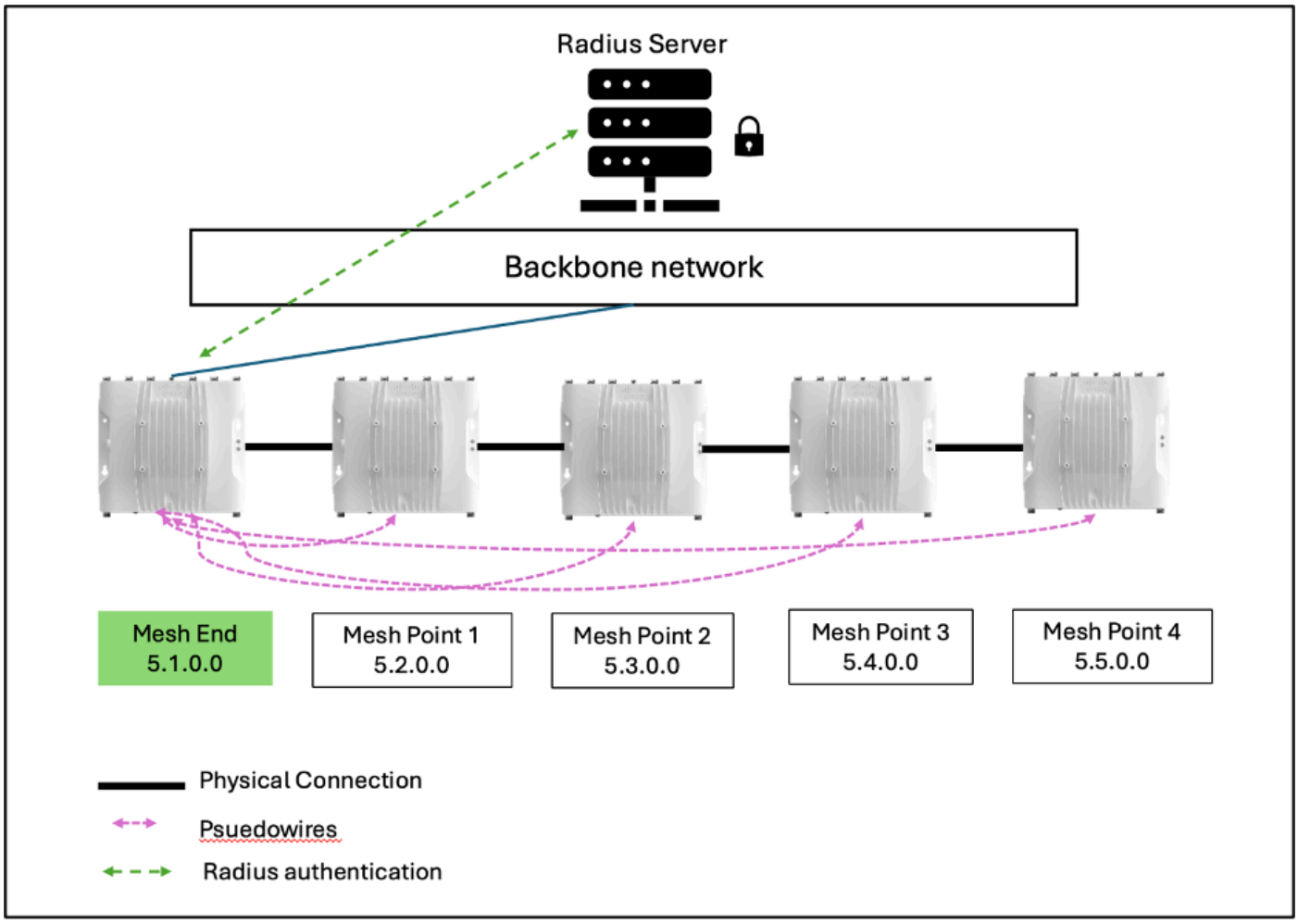
Die Mesh End-Funkeinheit ist normalerweise über eine Glasfaserverbindung mit dem Backbone-Netzwerk verbunden. Über das Backbone-Netzwerk kann sie den Radius-Server des Netzwerks erreichen.

Jedes Gerät kann den Radius-Server nur erreichen, wenn:

1. Es ist ein verdrahteter Koordinator.
2. Es verfügt über einen Pseudowire, der mit dem verdrahteten Master, d. h. Mesh End, aufgebaut ist.



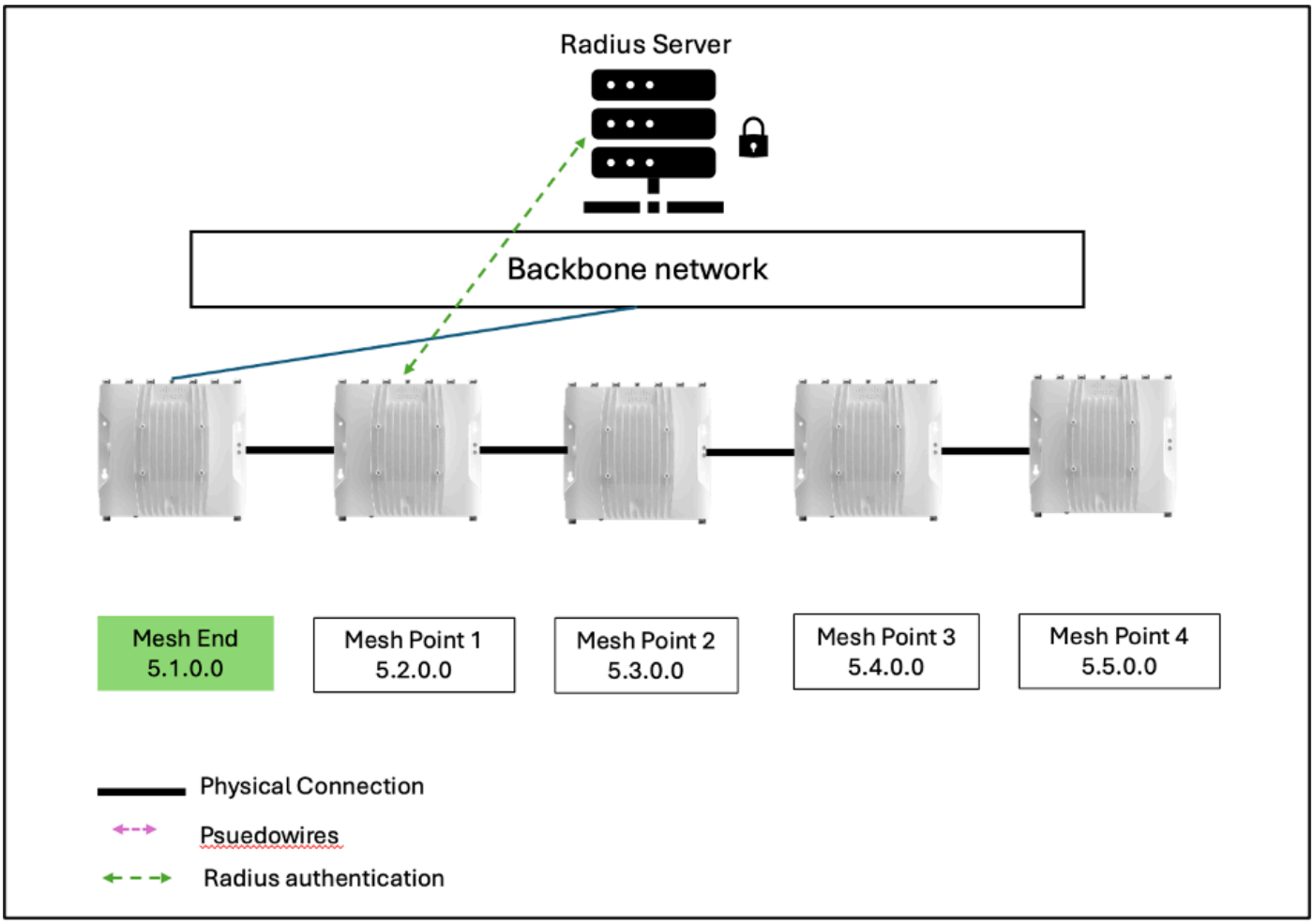
Schritt 1: Alle Einheiten sind nicht authentifiziert.



Am Anfang werden alle Einheiten einschließlich des Mesh-Endes nicht authentifiziert. Der automatische Abgriff öffnet sich nur am Mesh End, dem Eingangs-/Ausgangspunkt des gesamten Netzwerks. Damit ein Infrastrukturgerät den Radius-Server erreichen kann, um sich selbst zu authentifizieren, muss es entweder ein Mesh End sein oder über einen Pseudowire zum Mesh End verfügen.

Nun sendet das Mesh End Radio 5.1.0.0 eine Authentifizierungsanfrage über das Backbone-Netzwerk an den Radius-Server. Sobald die Kommunikation wieder aufgenommen wird, wird sie authentifiziert und für den Rest der nicht authentifizierten Infrastruktur-Mesh-Punkte "unsichtbar", wie es für AAA mit Radius erforderlich ist.

Phase 2: Mesh End 5.1.0.0. ist authentifiziert, Rest sind nicht authentifiziert.

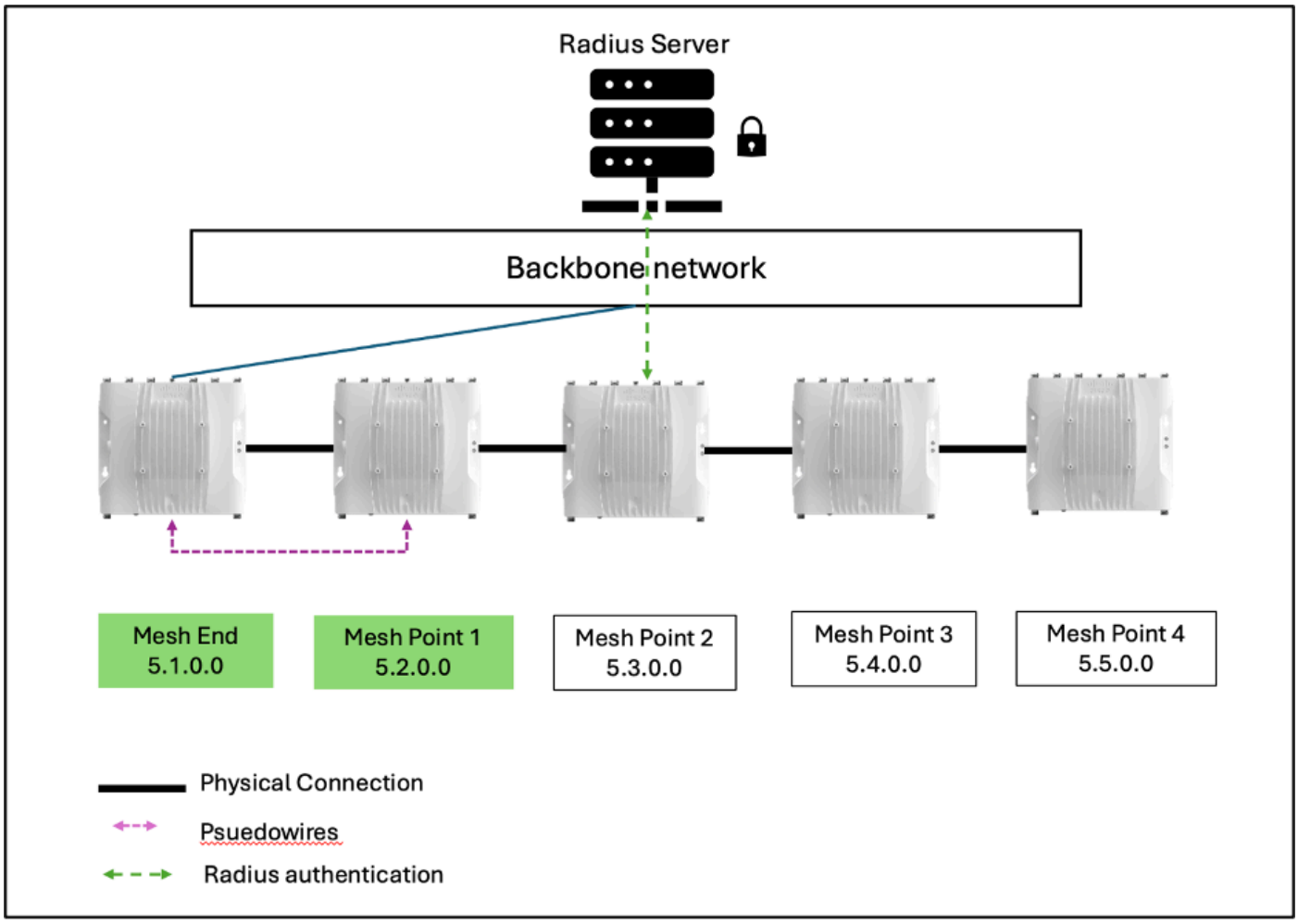


Nachdem das Mesh-Ende 5.1.0.0 authentifiziert und für den Rest des Netzwerks unsichtbar ist, werden die verbleibenden Mesh-Punkte ausgewählt und das Gerät mit der niedrigsten Mesh-ID zum nächsten verdrahteten Koordinator ausgewählt. In diesem Beispiel wäre dies Mesh Point 1 mit Mesh ID 5.2.0.0. Autotap ist dann auf Mesh Point 1 geöffnet.

Aufgrund der Aktivierung von LNO bilden sich keine Pseudowire-Emulation zu Mesh Point 1. Alle verbleibenden Funkgeräte müssen sich sequenziell authentifizieren, wenn ihr Autotap geöffnet ist.

Nun kann Mesh Point 1 eine Authentifizierungsanfrage an Radius Server senden und sich selbst authentifizieren.

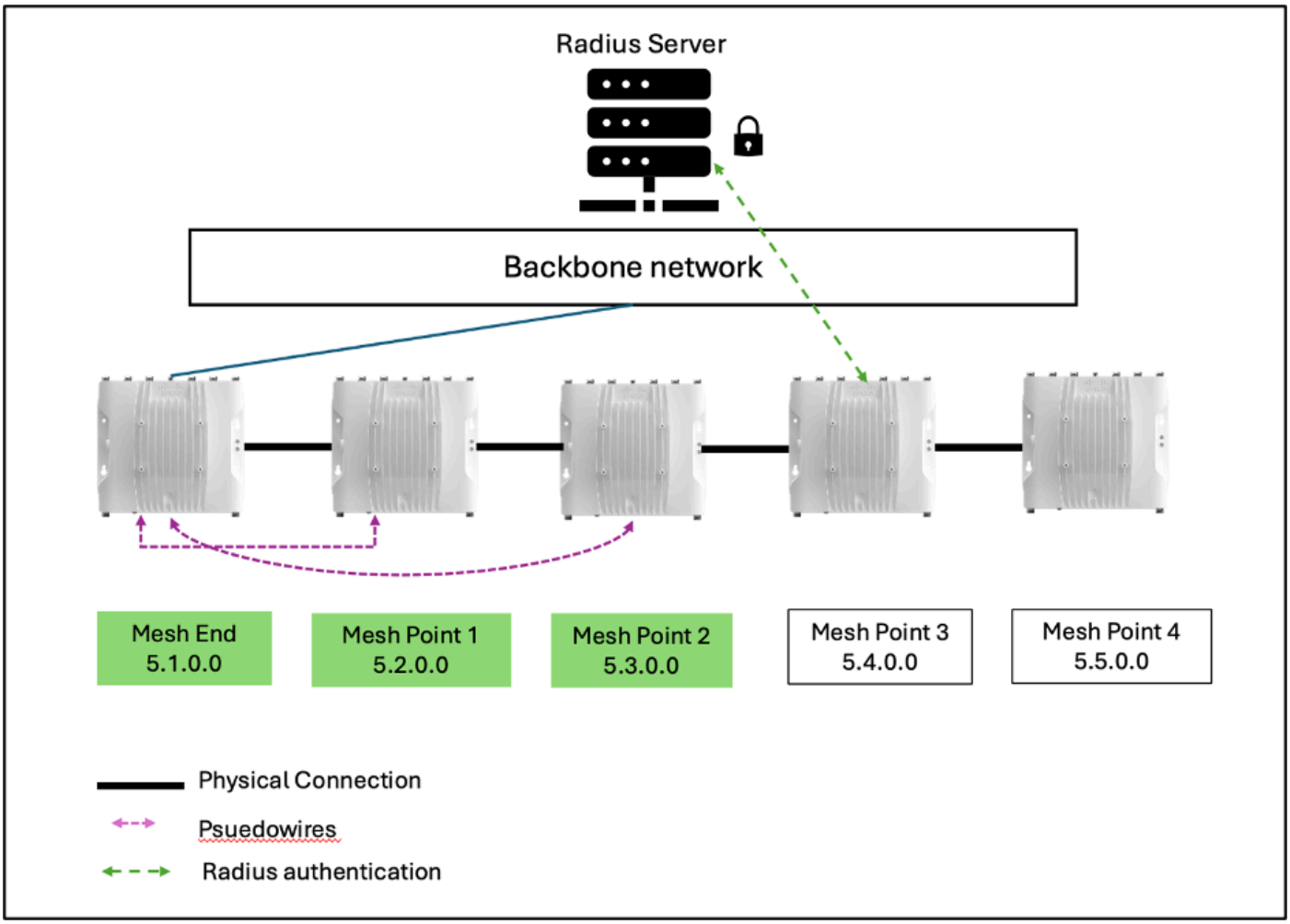
Schritt 3: Mesh End, Mesh Point 1 wird authentifiziert, andere nicht.



Nachdem Mesh Point 1 ebenfalls authentifiziert wurde, wird ein Pseudowire mit dem authentifizierten Mesh End gebildet, und auch für die restlichen nicht authentifizierten Infrastrukturradios wird er unsichtbar.

Der Rest der nicht authentifizierten Funkmodule führt die Auswahl erneut aus und wählt Mesh Point 2 mit der niedrigsten Mesh-ID 5.3.0.0 als neuen verdrahteten Koordinator aus. Diese Funkeinheit sendet eine Authentifizierungsanfrage an den Radius-Server, da ihr Autotap jetzt geöffnet ist.

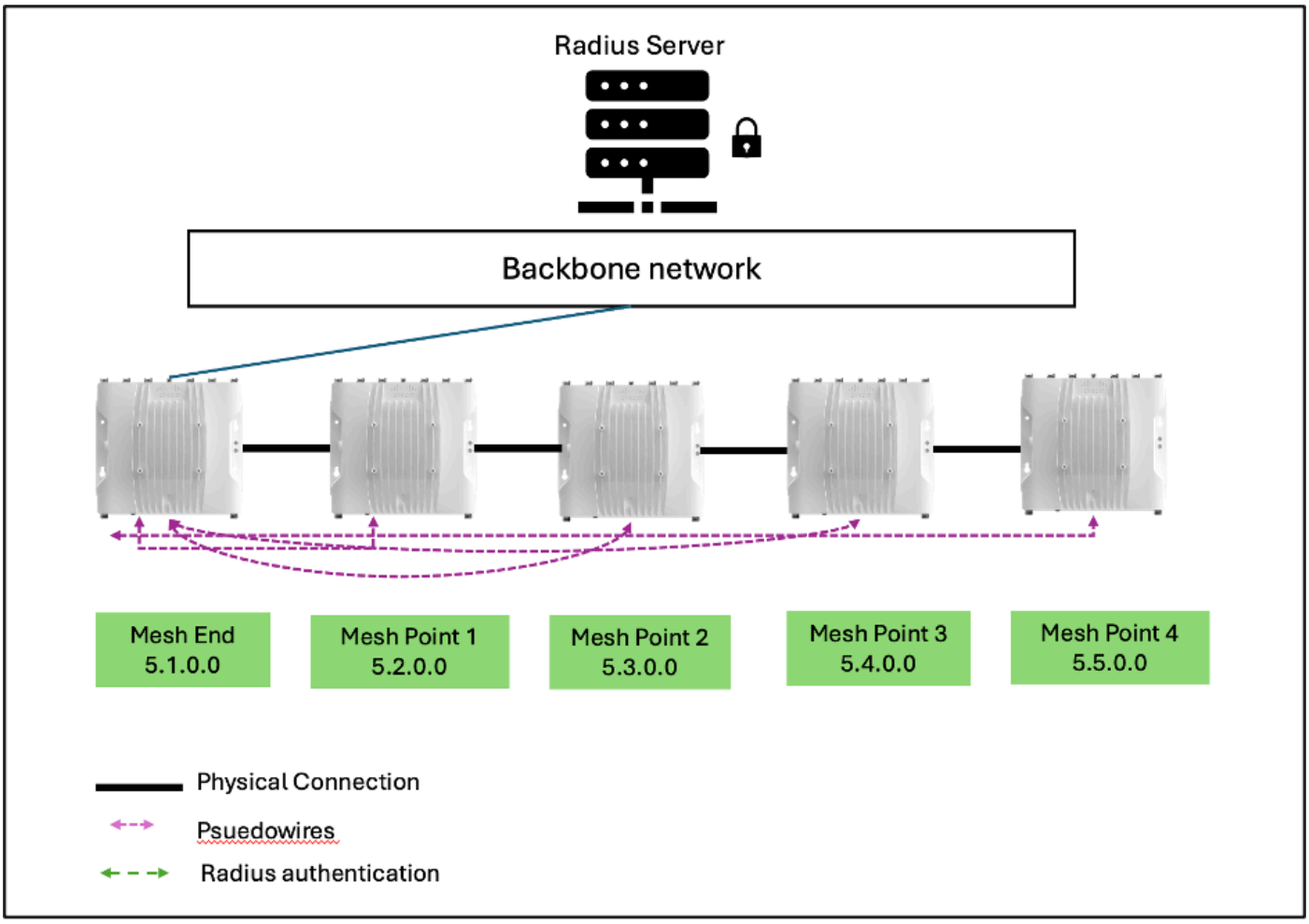
Schritt 4: Mesh End, MP 1 und MP 2 werden authentifiziert.



Der Prozess wiederholt sich dann mit Mesh Point 2 authentifiziert und bildet Pseudowire mit dem Mesh End-Gerät.

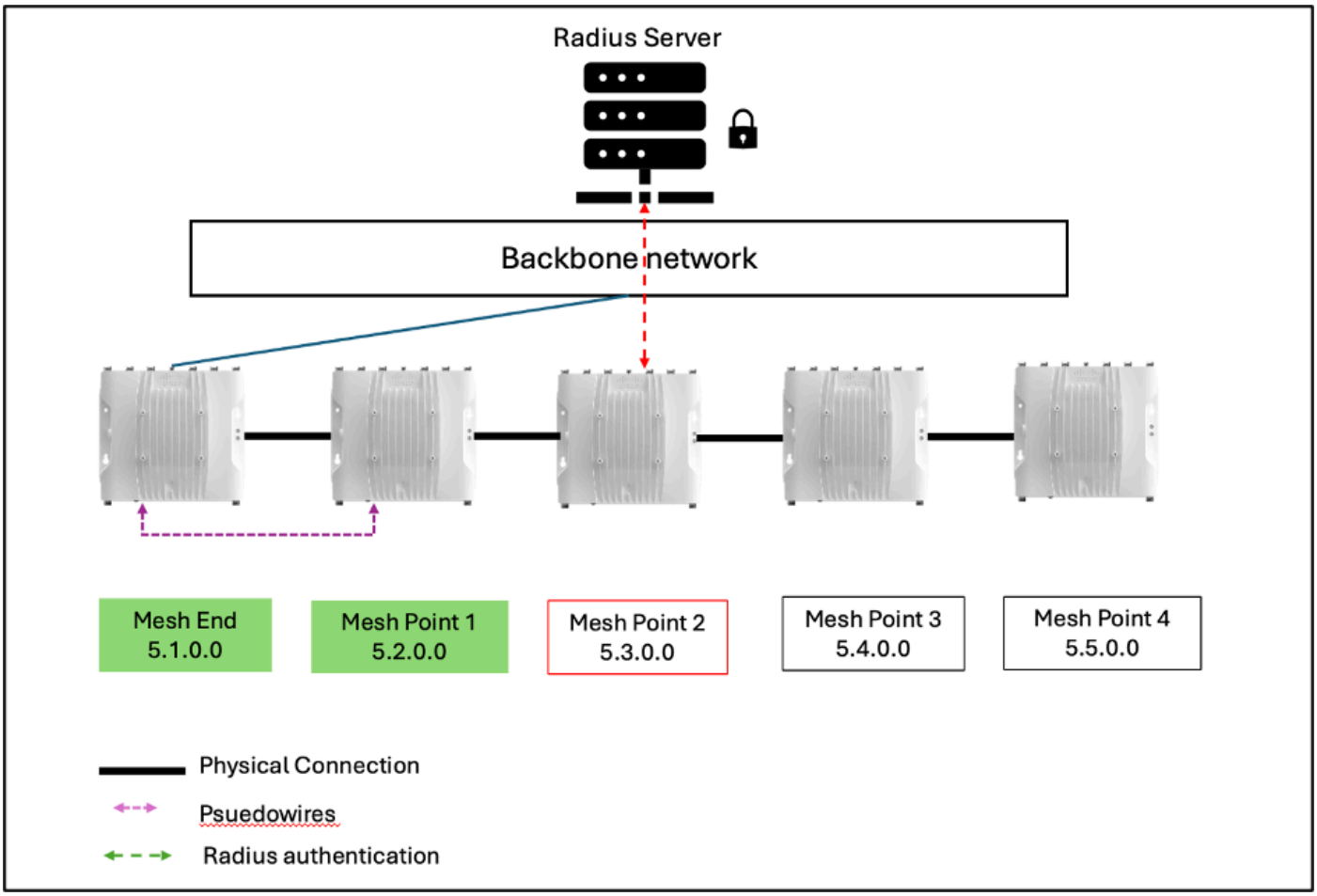
Die übrigen Infrastruktur-Funkeinheiten authentifizieren sich abwechselnd, in der Reihenfolge der niedrigsten bis höchsten Mesh-IDs, wenn ihr eigener Autotap geöffnet wird.

Schritt 5: Alle Funkmodule sind authentifiziert.



Fehlkonfiguration oder Problemfälle:

Wenn bei einem der Mesh-Punkte der Infrastruktur falsche Anmeldeinformationen angegeben sind oder Radius versehentlich deaktiviert wurde, kann dies die Authentifizierung anderer Funkgeräte beeinträchtigen. Überprüfen Sie stets die Anmeldeinformationen und Einstellungen, bevor Sie Funkmodule in der Produktionsumgebung bereitstellen.



Wenn in diesem Beispiel Mesh Point 2 falsche Creds hat, bleibt es nicht authentifiziert, und wiederum erhalten Mesh Point 3 und Mesh Point 4 nie die Chance, sich zu authentifizieren, da kein Pseudowire von ihnen zu Mesh Point 2 gebildet wird, weil LNO aktiviert ist.

Welche Funkmodule nicht authentifiziert werden können, hängt von der Mesh-ID des falsch konfigurierten Funkmoduls ab. Alle Funkmodule mit einer höheren Mesh-ID als der aktuelle verdrahtete Koordinator bleiben nicht authentifiziert und verursachen Probleme.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.