RADIUS en LNO configureren op industriële draadloze toegangspunten in URWB-modus

Inhoud

Inleiding

Dit document beschrijft de configuratie van RADIUS-verificatie en Large Network Optimization (LNO) op IW9165- en IW9167-radio's in de URWB-modus.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basisinstructies voor CLI-navigatie en -opdrachten
- Inzicht in IW URWB-mode radio's

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- IW9165- en IW9167-radio's

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

RADIUS - Remote Authentication Dial-In User Service is een netwerkprotocol dat wordt gebruikt voor gecentraliseerd verificatie-, autorisatie- en boekhoudbeheer (AAA) voor gebruikers of apparaten die verbinding maken met en gebruik maken van een netwerkservice. Voor industriële draadloze apparaten in de URWB-modus kan Radius worden gebruikt om apparaten te verifiëren

voordat ze zich bij een netwerk kunnen aansluiten.

Parameters voor Radius-configuratie kunnen worden geconfigureerd op de IW-apparaten, hetzij vanuit GUI of vanuit CLI-toegang of ook vanuit IoT OD.

CLI-configuratie van Radius-parameters:

Deze parameters kunnen worden geconfigureerd vanuit de activeringsmodus op de CLI van de apparaten.

1. Verificatie van radius mogelijk maken:

Met deze parameter kunt u Radius-verificatie op de apparaten inschakelen. Dit moet worden uitgevoerd na het toevoegen van andere verplichte parameters die vereist zijn voor radiusverificatie.

Radio1#configure radius enabled

2. Radius-verificatie uitschakelen:

Met deze parameter kunt u de Radius-verificatie op de apparaten uitschakelen.

Radio1#configure radius disabled

3. Doorgang:

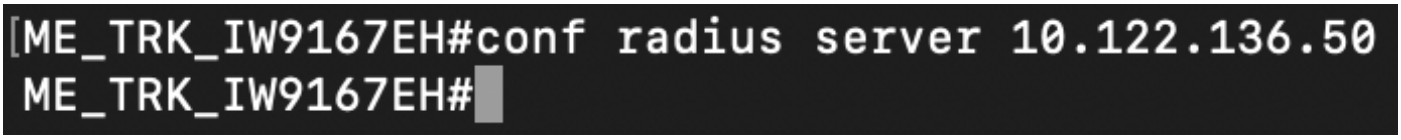
Deze parameter moet alleen worden geconfigureerd op de infrastructuurradio's. Door infrastructuurradio's met passthrough-parameter te configureren, kunnen de voertuigradio's zichzelf verifiëren via de infrastructuurradio's, waardoor ook communicatie mogelijk is tussen de geverifieerde voertuigradio's en de niet-geverifieerde infrastructuurradio's.

Radio1#configure radius passthrough

4. Radius-server toevoegen:

Deze parameter wordt gebruikt om het IP-adres van de Radius-server op te geven waarmee het apparaat moet communiceren.

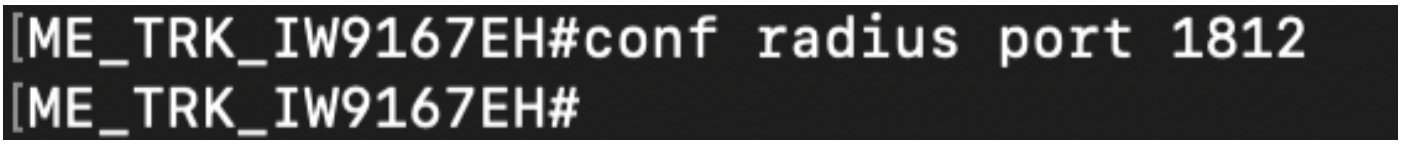
Radio1#configure radius server



5. Straalpoort:

Deze parameter wordt gebruikt om de poort van de Radius-server op te geven waarmee het apparaat moet communiceren. De standaardpoort voor Radius-verificatie is 1812.

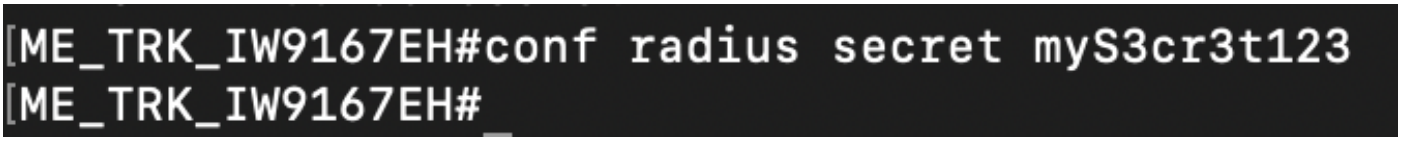
Radio1#configure radius server



6. Straalgeheim:

Deze parameter wordt gebruikt om de vooraf gedeelde sleutel op te geven die met de Radius-server moet worden gebruikt.

Radio1#configure radius secret



7. IP en poort van de secundaire server:

Deze parameters worden gebruikt om het IP-adres en poortnummer van een tweede Radius-server op te geven, die moet worden gebruikt als het apparaat de primaire server niet kan bereiken.

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. Time-out straal:

Deze parameter wordt gebruikt om de hoeveelheid tijd in seconden op te geven die de client wacht op een reactie van de primaire Radius-server voordat deze probeert verbinding te maken met de secundaire server. De standaardwaarde is ingesteld op 10 seconden.

Radio1#configure radius timeout

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

9. Authenticatieparameters:

Deze parameter wordt gebruikt om de verificatiemethode Radius en de bijbehorende parameters die moeten worden doorgegeven, op te geven. Er zijn verschillende opties om te gebruiken.

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
```

Als u deze methoden gebruikt: GTC (Generic token card), MD5 (Message-Digest Algorithm 5) of MSCHAPV2 (Microsoft Challenge Handshake Authentication Protocol versie 2), kunnen zowel gebruikersnaam als wachtwoord worden toegevoegd met de volgende opdrachten:

Radio1#configure radius authentication gtc

Radio1#configure radius authentication md5

Radio1#configure radius authentication mschapv2

Als u deze methoden gebruikt: PEAP (Protected Extensible Authentication Protocol) of EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) voor verificatie, moet u ook een andere interne verificatiemethode opgeven. Het kan zowel gtc, md5 of mschapv2 zijn.

Radio1#configure radius authentication peap

inner-auth-method

Radio1#configure radius authentication ttls

inner-auth-method

10. Switch:

Deze parameter geeft het aantal toegestane radiusverificatiepogingen voor de hoofdserver op voordat de client naar de tweede server switches. De standaardwaarde is 3.

Radio1#configure radius switch <1-6>

11. Terugverdientijd:

Deze parameter geeft de waarde van de tijd in seconden aan waarop de client moet wachten, nadat het maximum aantal pogingen voor verificatie is overschreden.

Radio1#configure radius backoff-time

12. Vervaltijd:

Deze parameter geeft de waarde van de tijd in seconden op. Als de Radius-verificatie niet is

voltooid, wordt de verificatiepoging opgegeven.

Radio1#configure radius expiration

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

13. Verzend verzoek:

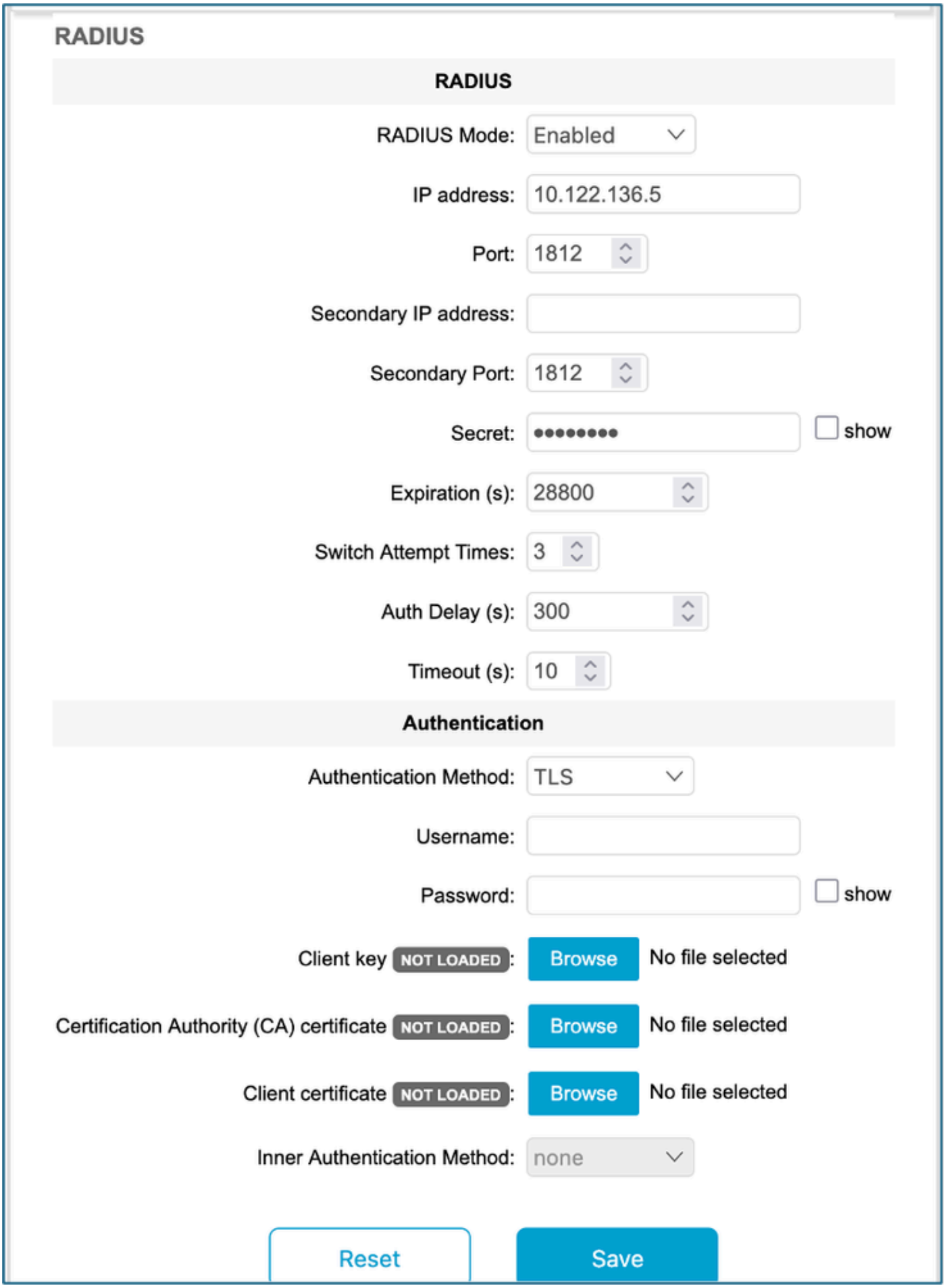
Deze parameter wordt gebruikt om een radiusverificatieverzoek te starten voor de primaire of de secundaire geconfigureerde Radius-server.

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).
```

Dezelfde parameters kunnen worden geconfigureerd op de Industrial Wireless-radio's in de URWB-modus via de GUI en onder het tabblad 'Radius' op de webpagina.



Opdrachten weergeven:

De huidige Radius-configuratie kan worden geverifieerd via CLI met show-opdrachten.

1.

#straal tonen

Met deze opdracht wordt aangegeven of Radius is ingeschakeld of uitgeschakeld op het apparaat.

```
[ME_TRK_IW9167EH#show radius
```

2.

#RADIUS-boekhouding weergeven

#RADIUS AUTH-METHOD-TLS tonen

#RADIUS-verificatie weergeven

Deze tonen opdrachten tonen de huidige configuratie van de geconfigureerde radius-accountingserver, de verificatieserver en de verificatiemethode tls-parameters.

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

Radius Authenticatie sequentie met LNO

LNO of Large Network Optimization is een functie die wordt voorgesteld om te worden ingeschakeld op grote netwerken met 50 of meer infrastructuurradio's om de pseudowire-formatie tussen alle apparaten in het netwerk te optimaliseren. Het wordt gebruikt in zowel Layer 2- als Layer 3-netwerken.

In netwerken waar zowel LNO als Radius zijn ingeschakeld, verifiëren de infrastructuurradio's zichzelf sequentieel (van laagste Mesh ID tot hoogste Mesh ID). Het inschakelen van LNO dwingt alle infrastructuurradio's om alleen pseudodraden te bouwen naar het maaseinde en zal ook het doorsturen van BPDU's uitschakelen.

In dit artikel wordt de volgorde van Radius-verificatie beschreven op een Fluidity-opstelling met één Mesh End- en 4 Mesh Point Infrastructure-radio's.

De Mesh End-radio is de standaard "bekabelde coördinator" van het Fluidity-netwerk. Dat betekent dat het automatisch geopend is en fungeert als het ingress / egress-punt van het netwerk.

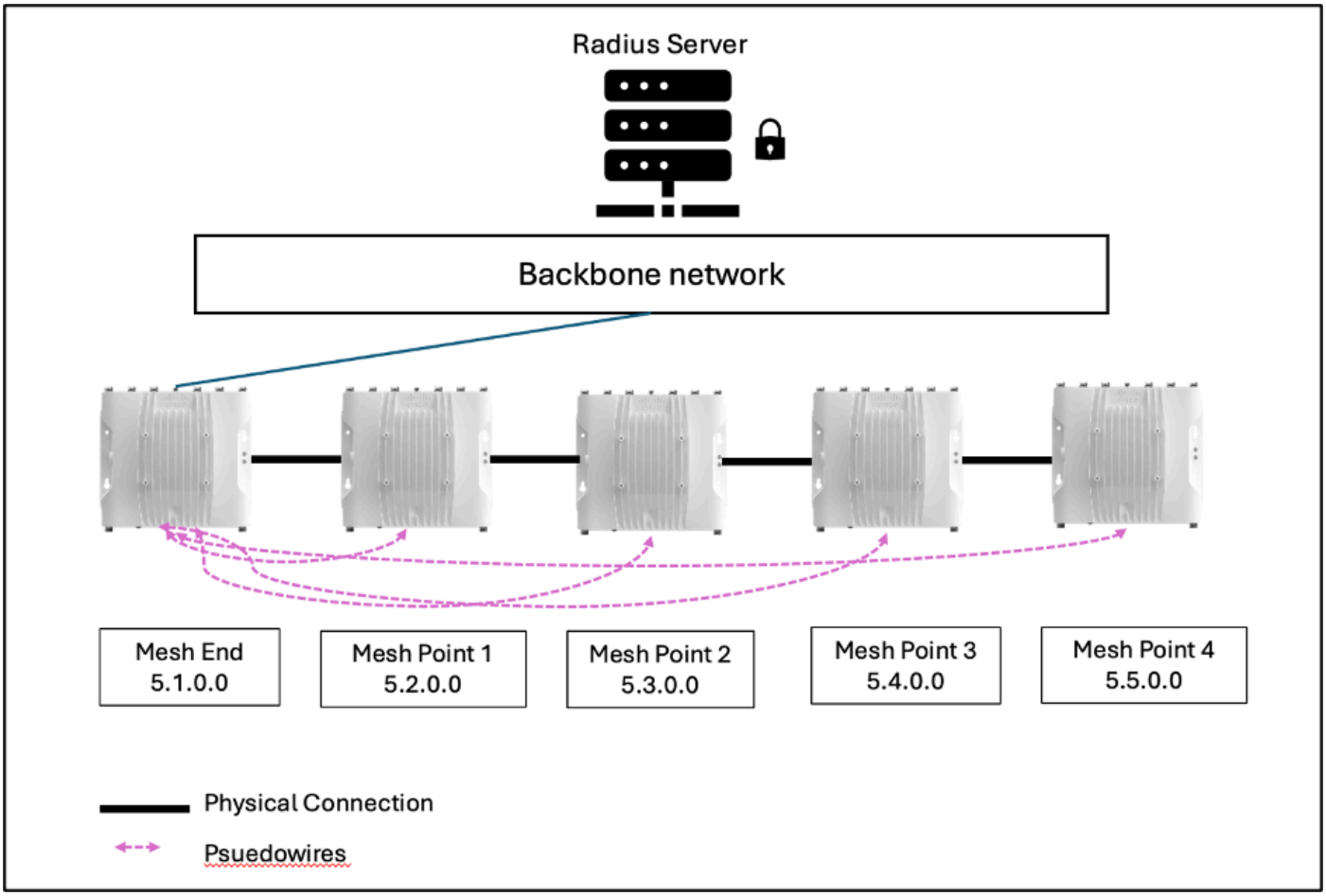
Alle andere infrastructuurradio's zijn ingesteld als Mesh-punten en ze hebben allemaal een fysieke

verbinding met het Mesh End via switches die met elkaar zijn verbonden.

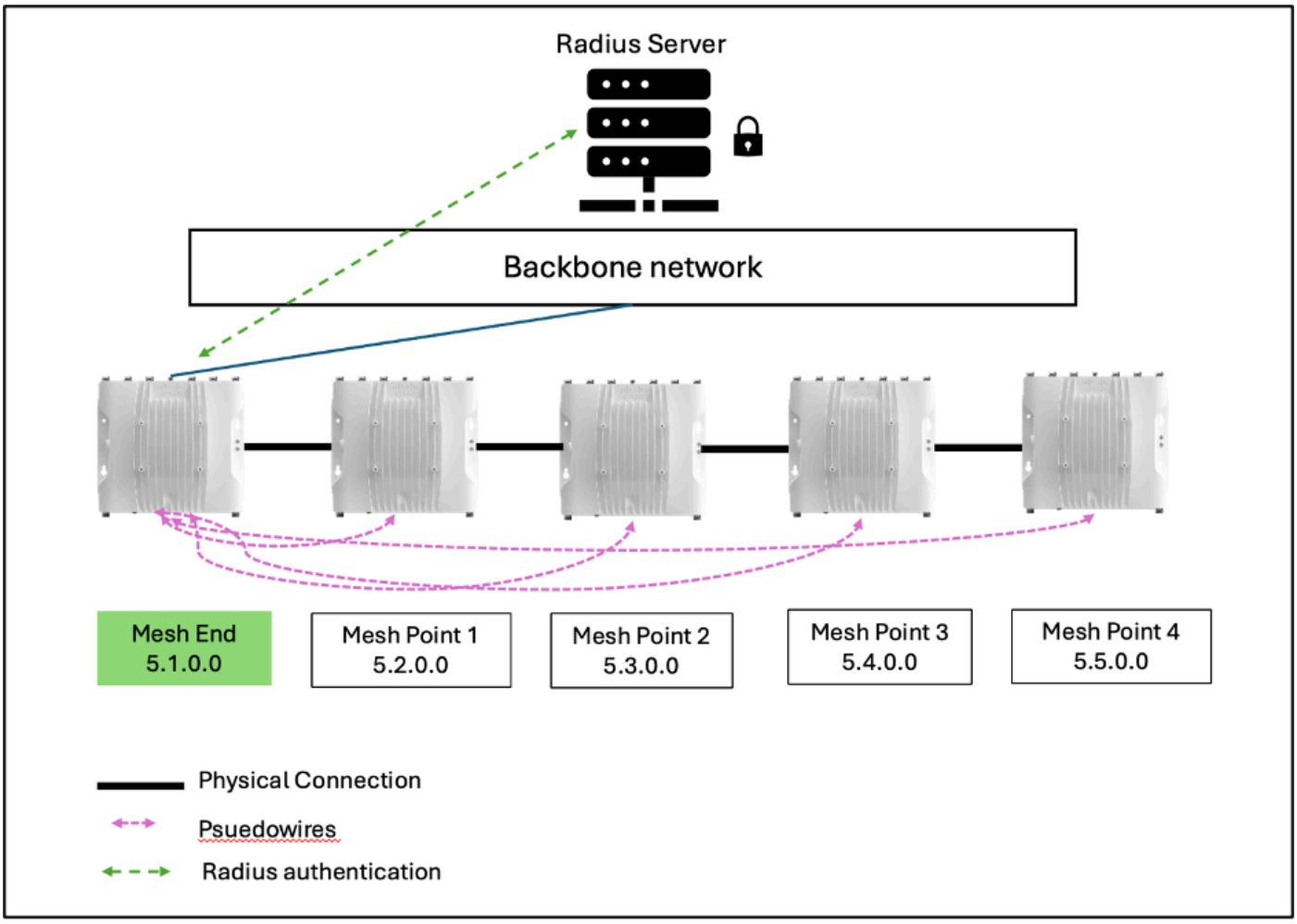
De Mesh End-radio is verbonden met het backbonenetwerk, meestal via een glasvezelverbinding en via het backbonenetwerk kan deze de Radius-server van het netwerk bereiken.

Elk apparaat kan de Radius-server alleen bereiken als:

1. Het is een bekabelde coördinator.
2. Het heeft een pseudowire gebouwd met de bedrade master, dat wil zeggen Mesh End.



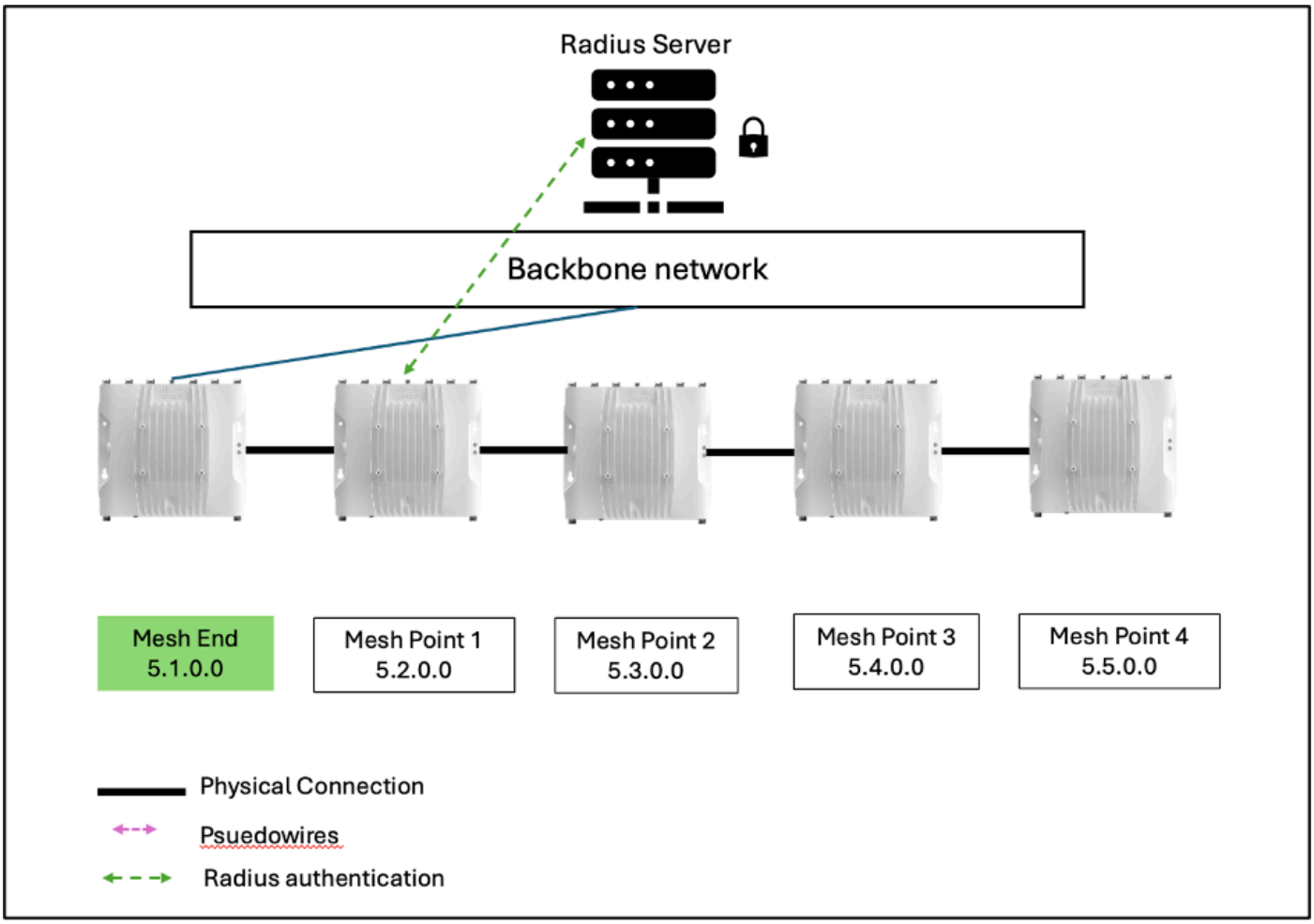
Stap 1: Alle eenheden zijn niet-geverifieerd.



In het begin zijn alle eenheden, inclusief het maaseinde, niet-geverifieerd. De automatische tap wordt alleen geopend op de Mesh End-radio, die het Ingress / Egress-punt van het hele netwerk is. Als een infrastructuurapparaat de Radius-server wil bereiken om zichzelf te verifiëren, moet het een Mesh End zijn of een pseudowire naar de Mesh End hebben.

Nu stuurt de Mesh End-radio 5.1.0.0 een verificatieverzoek naar de Radius-server via het Backbone-netwerk. Zodra het communicatie terug ontvangt, wordt het geverifieerd en wordt het vervolgens 'onzichtbaar' voor de rest van de niet-geverifieerde infrastructuurmesh-punten, zoals de vereiste voor AAA met Radius.

Stap 2: Mesh End 5.1.0.0. is geverifieerd, de rest is niet geverifieerd.

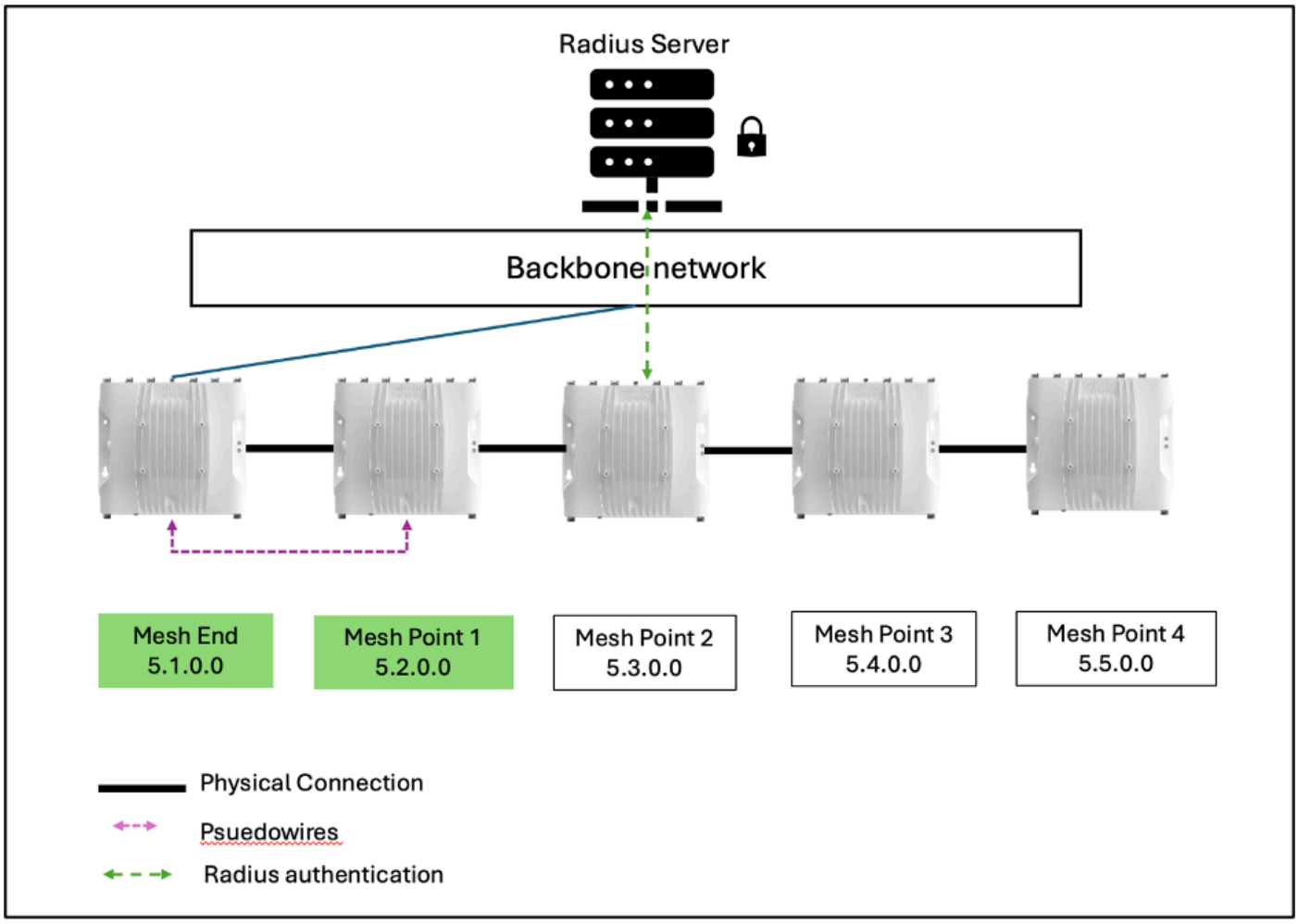


Nu Mesh End 5.1.0.0 is geverifieerd en onzichtbaar is voor de rest van het netwerk, zullen de resterende Mesh Points een selectie uitvoeren en het apparaat met de laagste Mesh ID kiezen om de volgende bekabelde coördinator te zijn. In dit voorbeeld zou dat Mesh Point 1 zijn met Mesh ID 5.2.0.0. Autotap zal dan open zijn op Mesh Point 1.

Omdat LNO is ingeschakeld, worden er geen pseudowires gevormd naar Mesh Point 1. Alle overige radio's moeten sequentieel worden geverifieerd wanneer hun Autotap is geopend.

Nu kan Mesh Point 1 een verificatieverzoek verzenden naar Radius Server en zichzelf verifiëren.

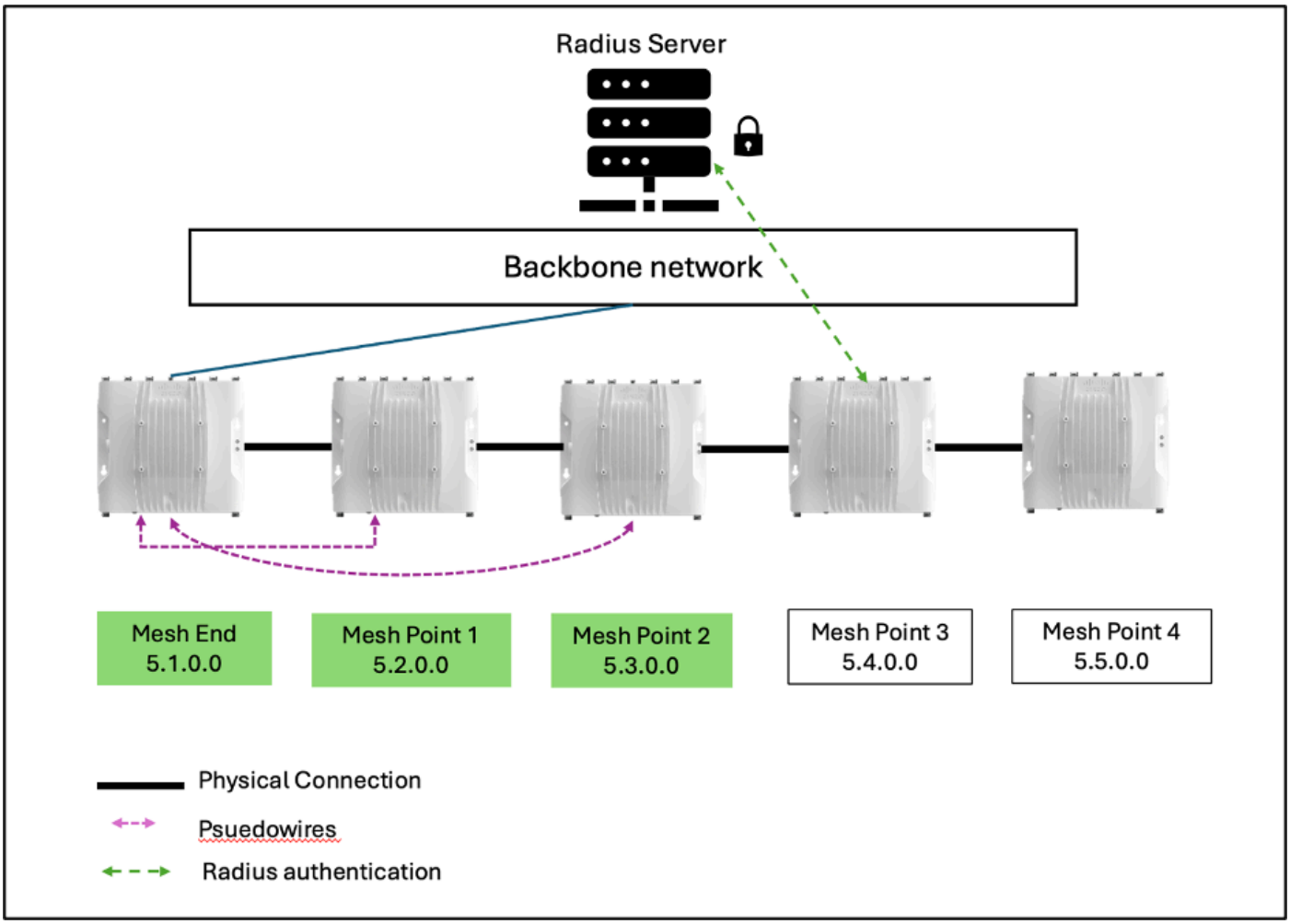
Stap 3: Mesh End, Mesh Point 1 is geverifieerd en andere zijn niet-geverifieerd.



Nu Mesh Point 1 ook is geverifieerd, vormt het een pseudowire met het geverifieerde Mesh End en wordt het ook onzichtbaar voor de rest van de niet-geverifieerde infrastructuurradio's.

De rest van de niet-geverifieerde radio's voert de selectie opnieuw uit en kiest Mesh Point 2 met de laagste Mesh ID 5.3.0.0 als de nieuwe bekabelde coördinator en die radio stuurt een verificatieverzoek naar de Radius-server omdat de Autotap nu is geopend.

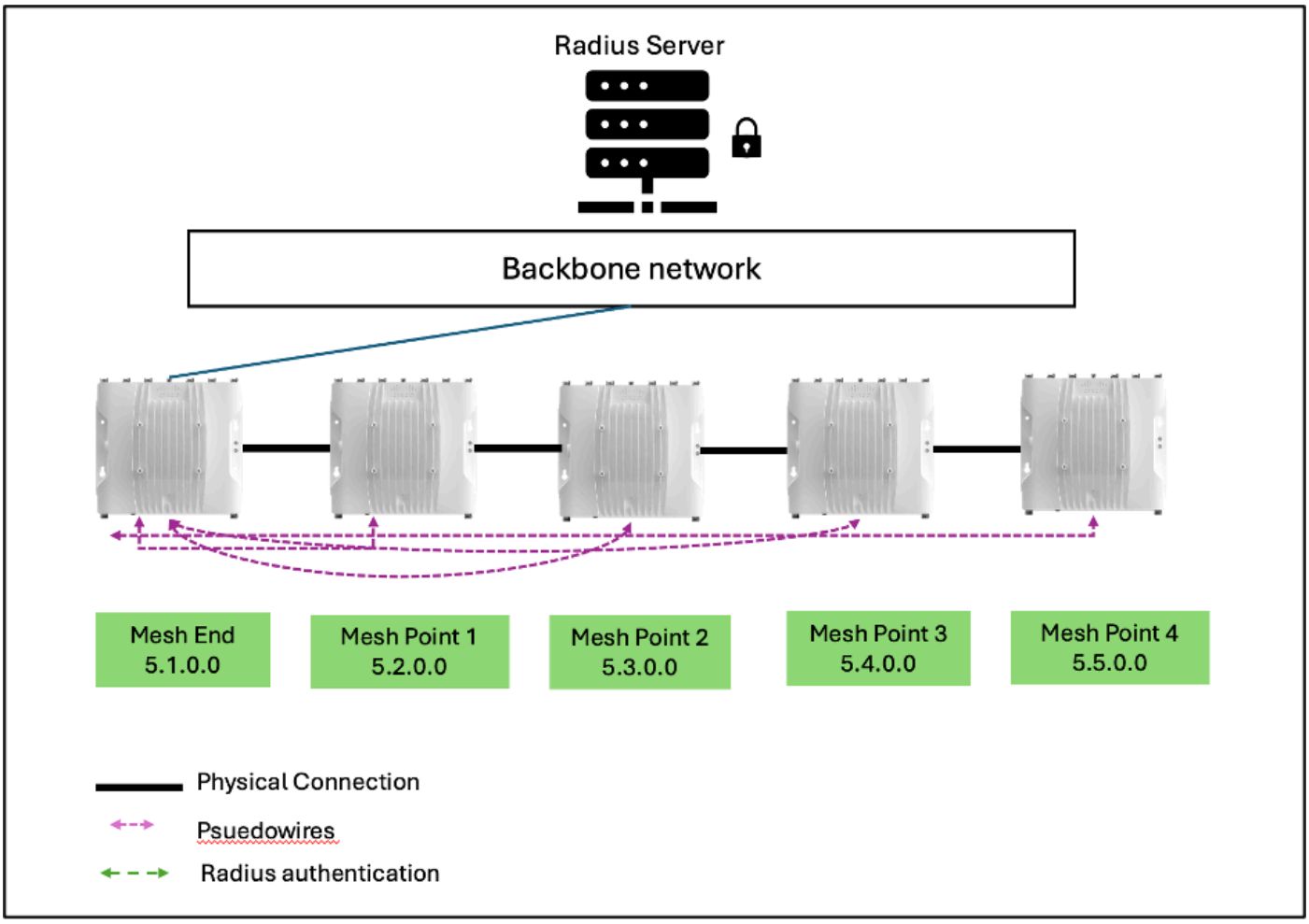
Stap 4: Mesh End, MP 1 en MP 2 zijn geverifieerd.



Het proces herhaalt zich dan met Mesh Point 2 wordt geverifieerd en vormen Pseudowire met het Mesh End apparaat.

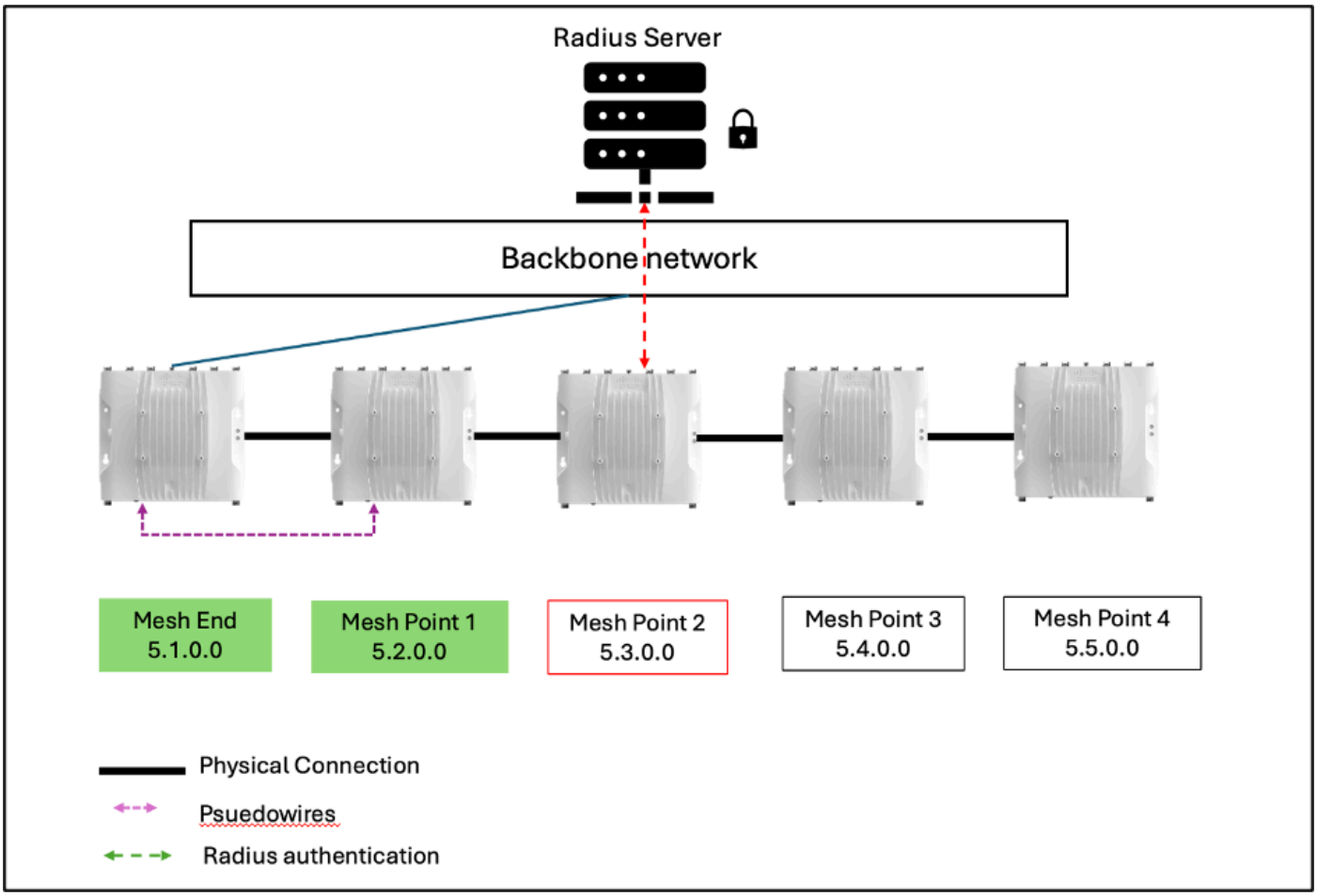
De rest van de Infrastructuur-radio's authenticeren zichzelf om de beurt, in de volgorde van laagste tot hoogste Mesh ID's, als en wanneer hun eigen autotap wordt geopend.

Stap 5: Alle radio's zijn geverifieerd.



Misconfiguratie of probleemgevallen:

Als een van de infrastructuurvermaasde punten verkeerde referenties heeft of Radius per ongeluk heeft uitgeschakeld, heeft dit invloed op andere radio's die niet kunnen worden geverifieerd. Controleer altijd de referenties en instellingen voordat u radio's in productie neemt.



In dit voorbeeld, als Mesh Point 2 verkeerde creds heeft, blijft het niet-geverifieerd en op zijn beurt krijgen Mesh Point 3 en Mesh Point 4 nooit de kans om zichzelf te verifiëren, omdat er geen Pseudowire van hen naar Mesh Point 2 is gevormd omdat LNO is ingeschakeld.

De radio's die niet zijn geverifieerd, zijn afhankelijk van de Mesh ID van de verkeerd geconfigureerde radio. Radio's met een Mesh ID die hoger is dan de huidige bekabelde coördinator, blijven niet-geverifieerd en veroorzaken problemen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.