Configuration de RADIUS et LNO sur les points d'accès sans fil industriels en mode URWB

Table des matières

Introduction

Ce document décrit la configuration de l'authentification RADIUS et de l'optimisation du réseau étendu (LNO) sur les radios IW9165 et IW9167 en mode URWB.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Navigation et commandes de base CLI
- Présentation des radios en mode IW URWB

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Radios IW9165 et IW9167

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

RADIUS - Remote Authentication Dial-In User Service est un protocole réseau utilisé pour fournir une gestion centralisée de l'authentification, de l'autorisation et de la comptabilité (AAA) pour les utilisateurs ou les périphériques qui se connectent et utilisent un service réseau. Pour les périphériques sans fil industriels en mode URWB, Radius peut être utilisé pour authentifier les

périphériques avant qu'ils ne puissent se connecter à un réseau.

Les paramètres de configuration de Radius peuvent être configurés sur les périphériques IW à partir de l'interface utilisateur graphique, de l'accès CLI ou de l'IoT OD.

Configuration CLI des paramètres Radius :

Ces paramètres peuvent être configurés à partir du mode enable sur l'interface de ligne de commande des périphériques.

1. Activation de l'authentification Radius :

Ce paramètre permet d'activer l'authentification Radius sur les périphériques. Cette opération doit être exécutée après l'ajout d'autres paramètres obligatoires requis pour l'authentification RADIUS.

Radio1#configure radius enabled

2. Désactivation de l'authentification Radius :

Ce paramètre permet de désactiver l'authentification Radius sur les périphériques.

Radio1#configure radius disabled

3. Passthrough :

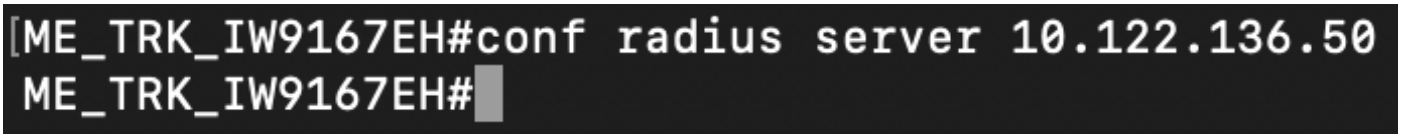
Ce paramètre doit uniquement être configuré sur les radios d'infrastructure. La configuration des radios d'infrastructure avec un paramètre de transfert permet aux radios de véhicule de s'authentifier via les radios d'infrastructure, permettant également la communication entre les radios de véhicule authentifiées et les radios d'infrastructure non authentifiées.

Radio1#configure radius passthrough

4. Ajout du serveur Radius :

Ce paramètre est utilisé pour spécifier l'adresse IP du serveur Radius avec lequel le périphérique doit communiquer.

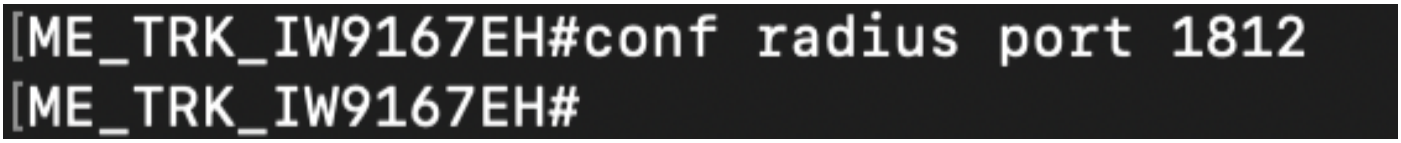
Radio1#configure radius server



5. Port Radius :

Ce paramètre est utilisé pour spécifier le port du serveur Radius avec lequel le périphérique doit communiquer. Le port par défaut pour l'authentification Radius est 1812.

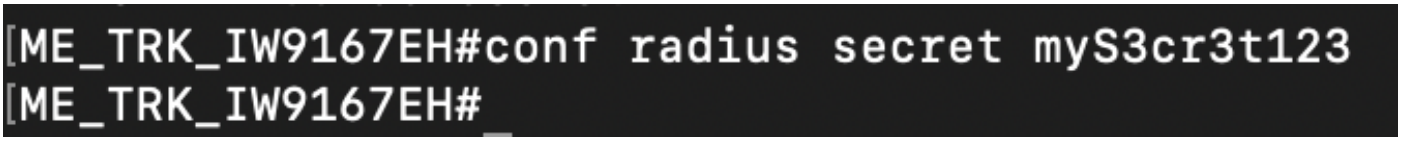
Radio1#configure radius server



6. Radius Secret :

Ce paramètre est utilisé pour spécifier la clé pré-partagée à utiliser avec le serveur Radius.

Radio1#configure radius secret



7. Adresse IP et port du serveur secondaire :

Ces paramètres sont utilisés pour spécifier l'adresse IP et le numéro de port d'un second serveur

Radius, à utiliser dans le cas où le périphérique ne peut pas atteindre le serveur principal.

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. Délai d'attente Radius :

Ce paramètre est utilisé pour spécifier la durée en secondes pendant laquelle le client attendra une réponse du serveur Radius principal avant d'essayer de se connecter au serveur secondaire. La valeur par défaut est de 10 secondes.

Radio1#configure radius timeout

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

9. Paramètres d’authentification :

Ce paramètre est utilisé pour spécifier la méthode d'authentification Radius et les paramètres correspondants à passer. Il existe plusieurs options à utiliser.

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
```

Si vous utilisez ces méthodes : Les commandes GTC (Generic token card), MD5 (Message-Digest Algorithm 5) ou MSCHAPV2 (Microsoft Challenge Handshake Authentication Protocol version 2) peuvent être ajoutées avec le nom d'utilisateur et le mot de passe suivants :

Radio1#configure radius authentication gtc

Radio1#configure radius authentication md5

Radio1#configure radius authentication mschapv2

Si vous utilisez ces méthodes : PEAP (Protected Extensible Authentication Protocol) ou EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) pour l'authentification, une autre méthode d'authentification interne doit également être fournie. Il peut être soit gtc, md5 ou mschapv2.

Radio1#configure radius authentication peap

inner-auth-method

Radio1#configure radius authentication ttls

inner-auth-method

10. Tentatives de commutation :

Ce paramètre spécifie le nombre de tentatives d'authentification RADIUS autorisées vers le serveur principal avant que le client ne bascule vers le serveur secondaire. La valeur par défaut est 3.

Radio1#configure radius switch <1-6>

11. Délai de réémission :

Ce paramètre spécifie la valeur du délai d'attente du client en secondes, après avoir dépassé le nombre maximal de tentatives d'authentification.

Radio1#configure radius backoff-time

12. Délai d'expiration :

Ce paramètre spécifie la valeur du temps en secondes si, pendant lequel l'authentification Radius n'est pas terminée, la tentative d'authentification sera abandonnée.

Radio1#configure radius expiration

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

13. Envoyer la demande :

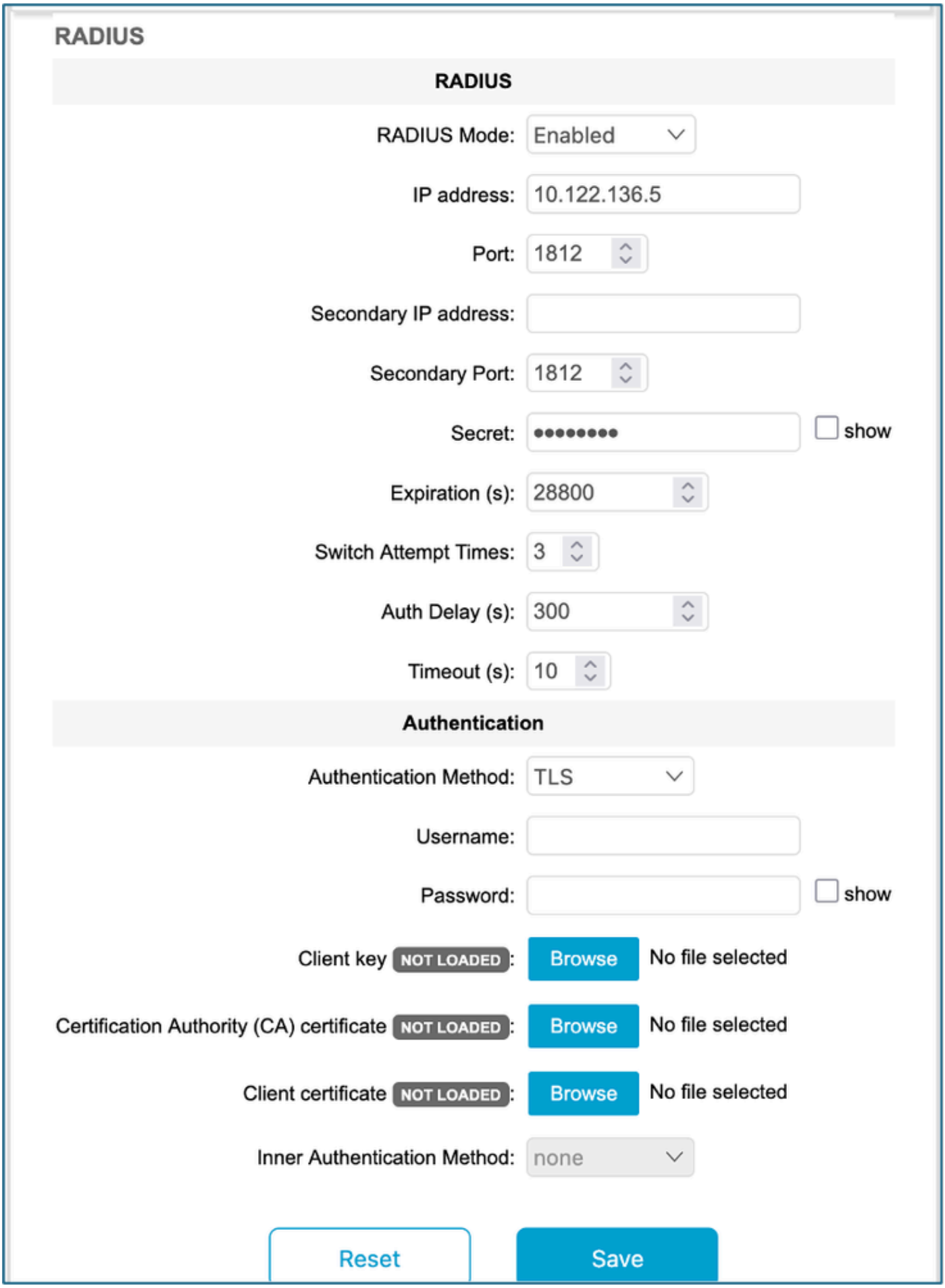
Ce paramètre est utilisé pour initier une demande d'authentification RADIUS au serveur RADIUS principal ou secondaire configuré.

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).
```

Les mêmes paramètres peuvent être configurés sur les radios sans fil industrielles en mode URWB via l'interface graphique utilisateur ainsi que sous l'onglet « Radius » sur la page Web.



Commandes show :

La configuration Radius actuelle peut être vérifiée via l'interface de ligne de commande avec les commandes show.

1.

#show radius

Cette commande show indique si Radius est activé ou désactivé sur le périphérique.

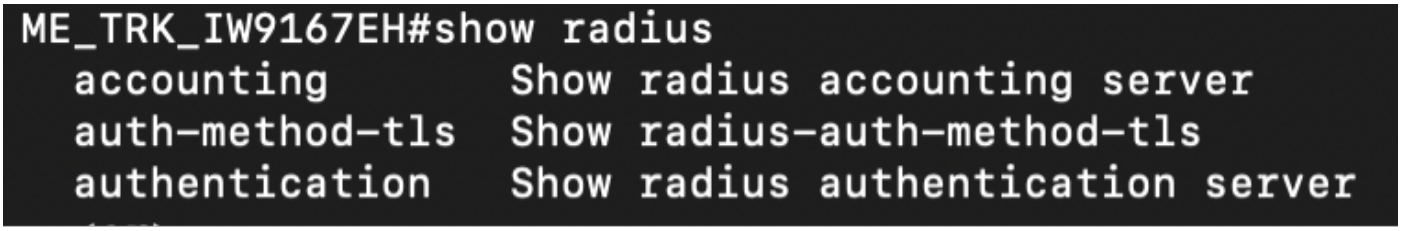
2.

#show radius accounting

#show radius auth-method-tls

#show radius authentication

Ces commandes show affichent la configuration actuelle du serveur de comptabilité radius, du serveur d'authentification et des paramètres tls de la méthode d'authentification configurés.



Séquence d'authentification Radius avec LNO

L'optimisation LNO ou Large Network Optimization est une fonctionnalité que l'on suggère d'activer sur les grands réseaux avec 50 radios d'infrastructure ou plus pour optimiser la formation de pseudo-fils entre tous les périphériques du réseau. Il est utilisé dans les réseaux de couche 2 et 3.

Dans les réseaux où LNO et Radius sont activés, les radios d'infrastructure s'authentifient séquentiellement (de l'ID de maillage le plus bas à l'ID de maillage le plus élevé). L'activation de LNO forcera toutes les radios d'infrastructure à construire des pseudo-fils UNIQUEMENT à l'extrémité maillée et désactivera également le transfert BPDU.

Cet article décrit la séquence d'authentification Radius sur une configuration Fluidité avec une extrémité maillée et 4 radios d'infrastructure de point maillé.

La radio Mesh End est le « coordinateur filaire » par défaut du réseau Fluidité. En d'autres termes, il est ouvert automatiquement et agit comme point d'entrée/de sortie du réseau.

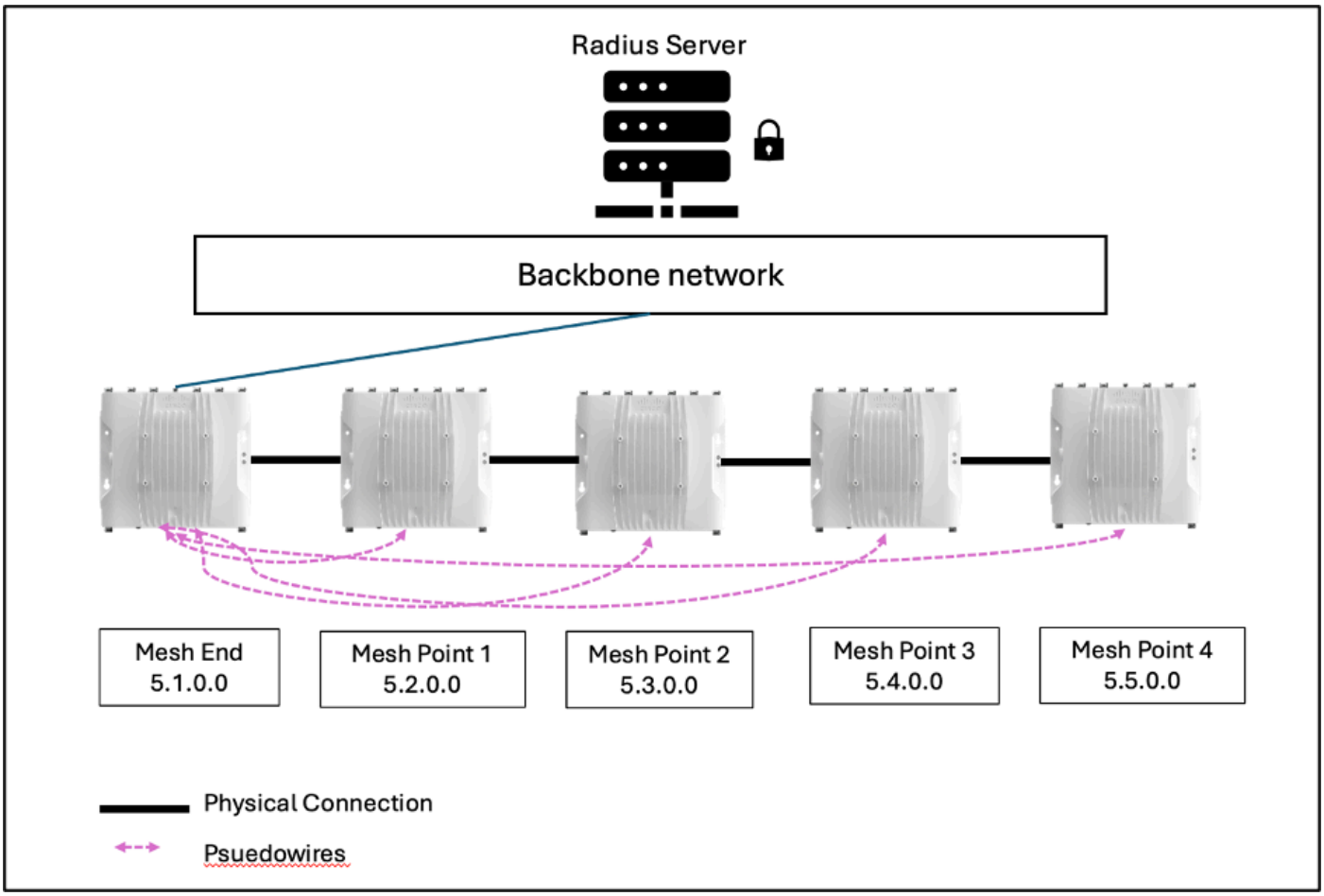
Toutes les autres radios d'infrastructure sont configurées en tant que points maillés et elles ont

toutes une connexion physique à l'extrémité maillée via des commutateurs connectés les uns aux autres.

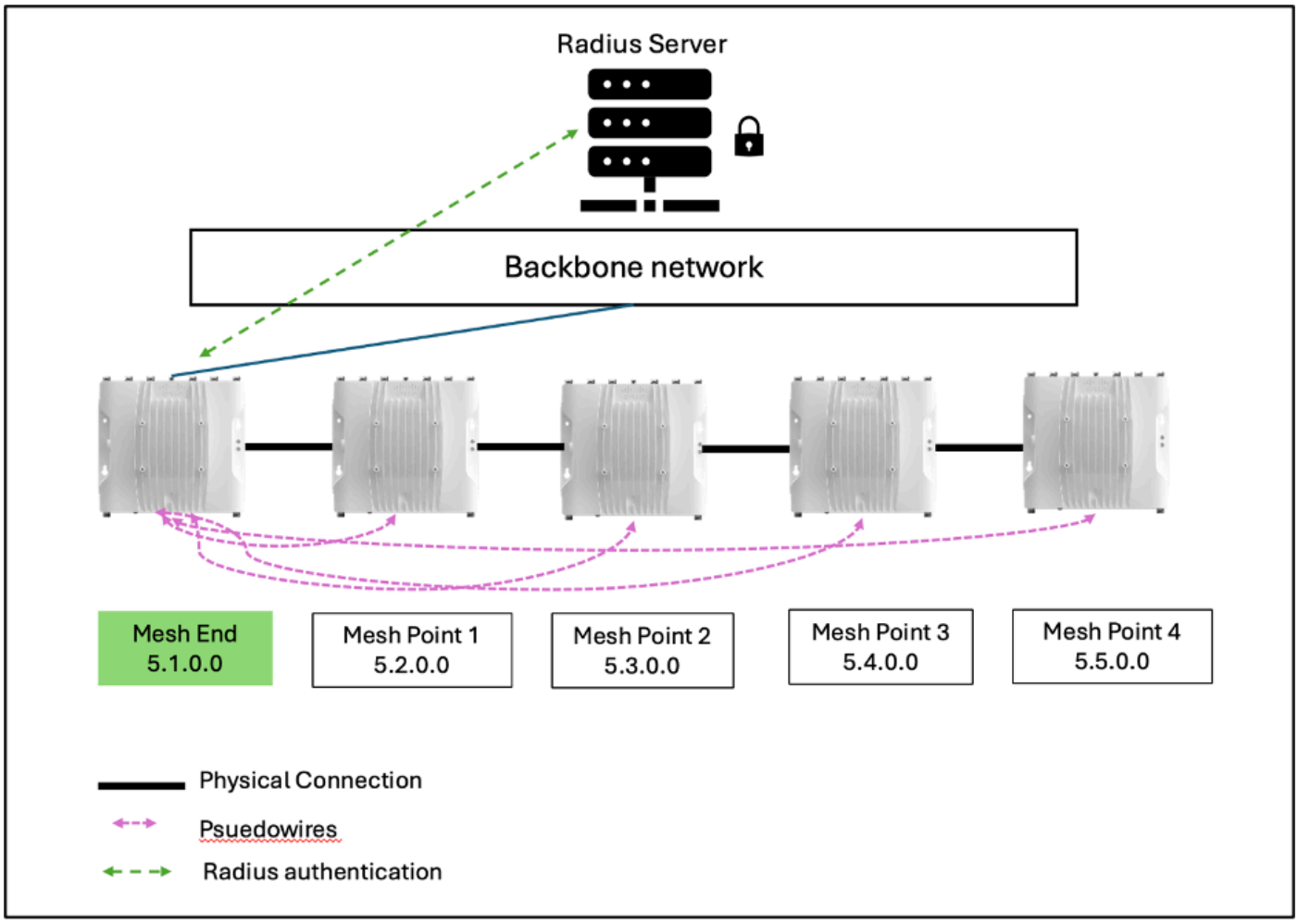
La radio Mesh End est connectée au réseau fédérateur généralement via une connexion par fibre optique et via le réseau fédérateur, elle peut atteindre le serveur Radius du réseau.

Tout périphérique peut accéder au serveur Radius uniquement si :

1. Il s'agit d'un coordinateur filaire.
2. Il a un pseudo-fil construit avec le maître filaire, c'est-à-dire Mesh End.



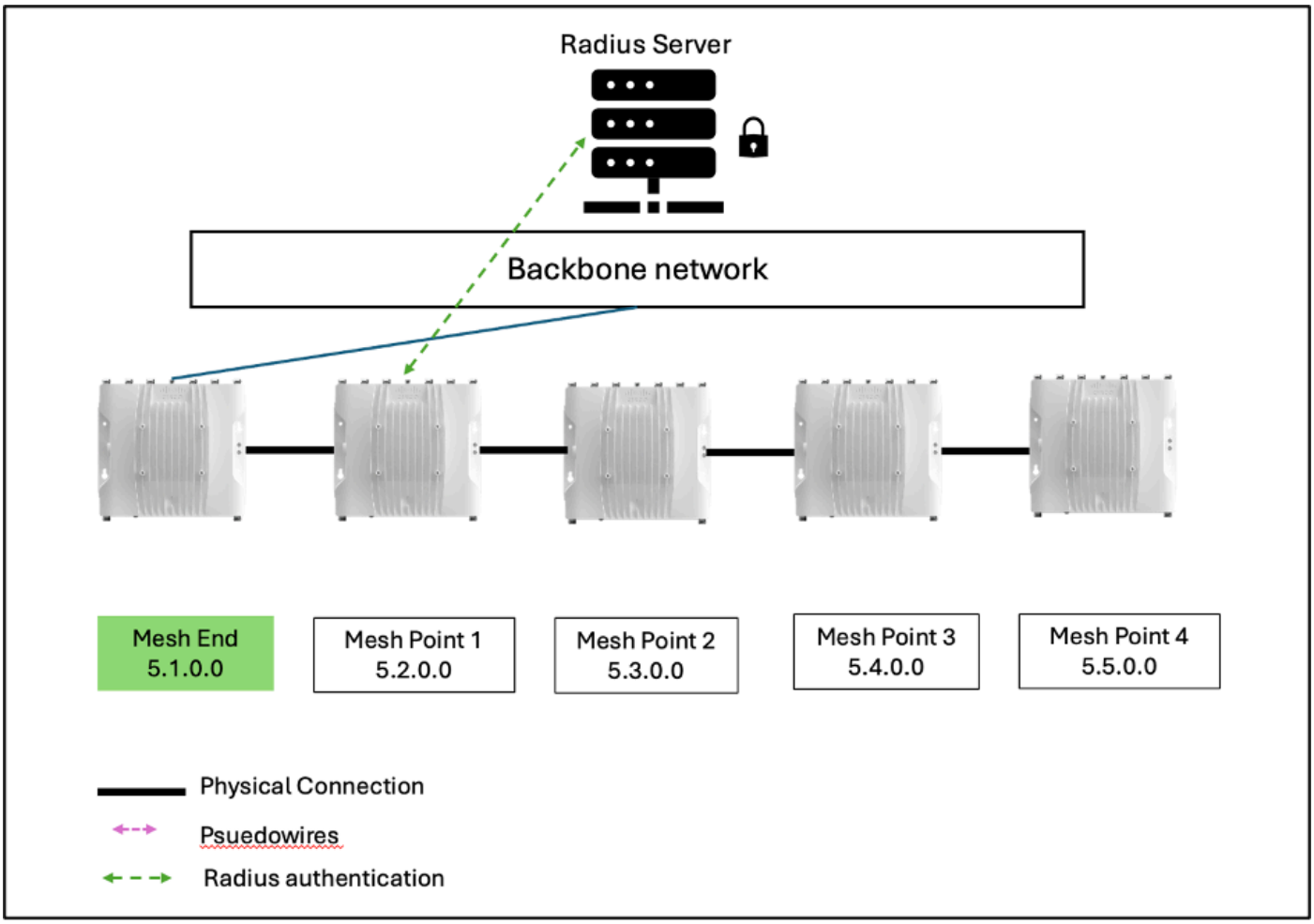
Étape 1 : Toutes les unités ne sont pas authentifiées.



Au début, toutes les unités, y compris l'extrémité maillée, ne sont pas authentifiées. L'autotap s'ouvre uniquement sur la radio Mesh End qui est le point d'entrée/sortie de l'ensemble du réseau. Pour qu'un périphérique Infrastructure puisse atteindre le serveur Radius pour s'authentifier, il doit s'agir d'une extrémité maillée ou d'un pseudo-fil vers l'extrémité maillée.

Maintenant, la radio Mesh End 5.1.0.0 envoie une requête d'authentification au serveur Radius via le réseau fédérateur. Une fois la communication reçue, elle est authentifiée et devient « invisible » pour les autres points de maillage d'infrastructure non authentifiés, comme c'est le cas pour AAA avec Radius.

Étape 2 : Mesh End 5.1.0.0. est authentifié, les autres sont non authentifiés.

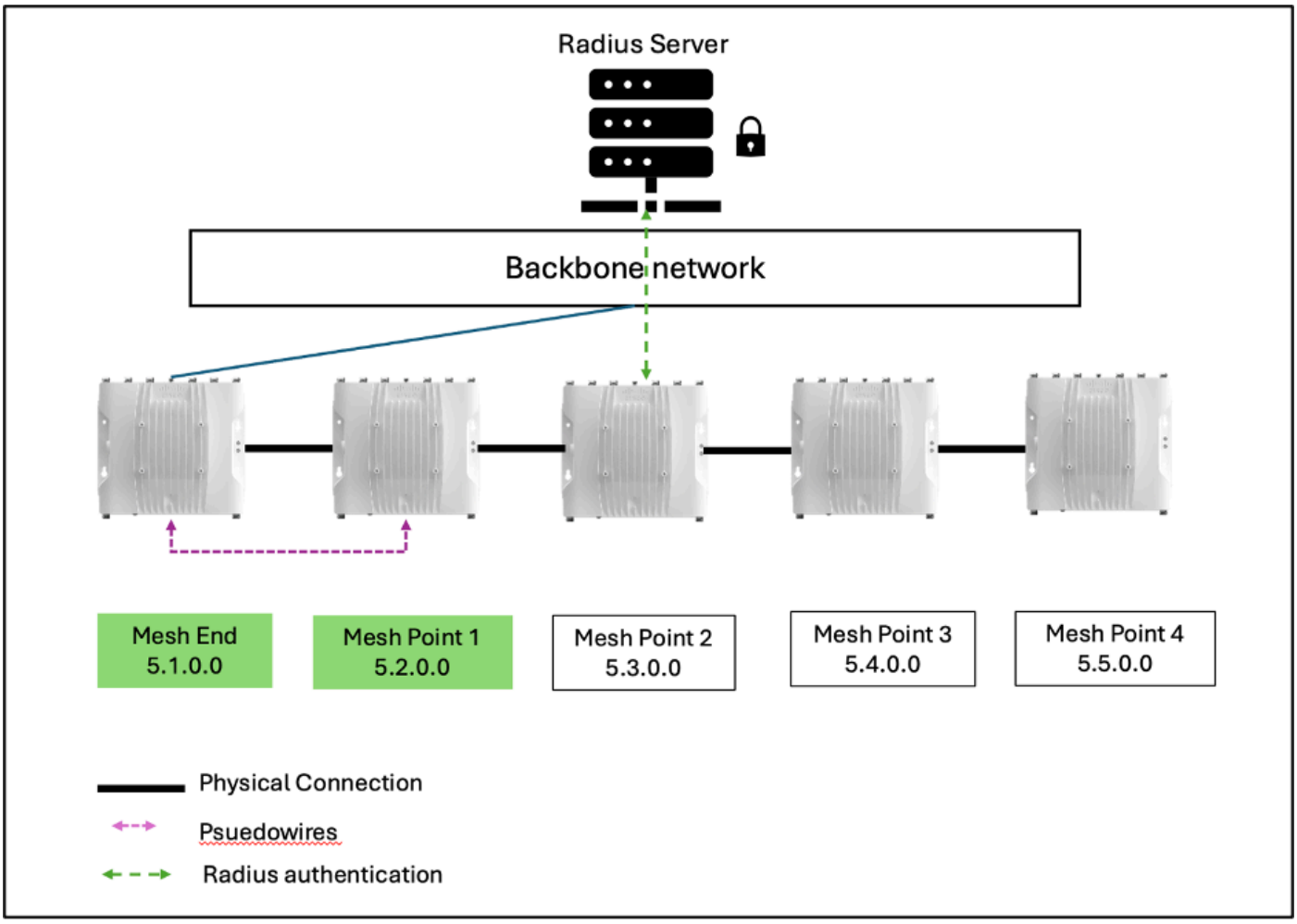


Maintenant que l'extrémité de maillage 5.1.0.0 est authentifiée et invisible pour le reste du réseau, les points de maillage restants exécuteront une sélection et choisiront le périphérique ayant l'ID de maillage le plus faible pour être le prochain coordinateur filaire. Dans cet exemple, il s'agirait du point de maillage 1 avec l'ID de maillage 5.2.0.0. L'autotap sera alors ouvert sur le point de maillage 1.

En raison de l'activation de LNO, aucun pseudo-fil ne se formera au point de maillage 1. Toutes les radios restantes devront s'authentifier séquentiellement lorsque leur point d'accès automatique sera ouvert.

Le point de maillage 1 peut maintenant envoyer une demande d'authentification au serveur Radius et s'authentifier.

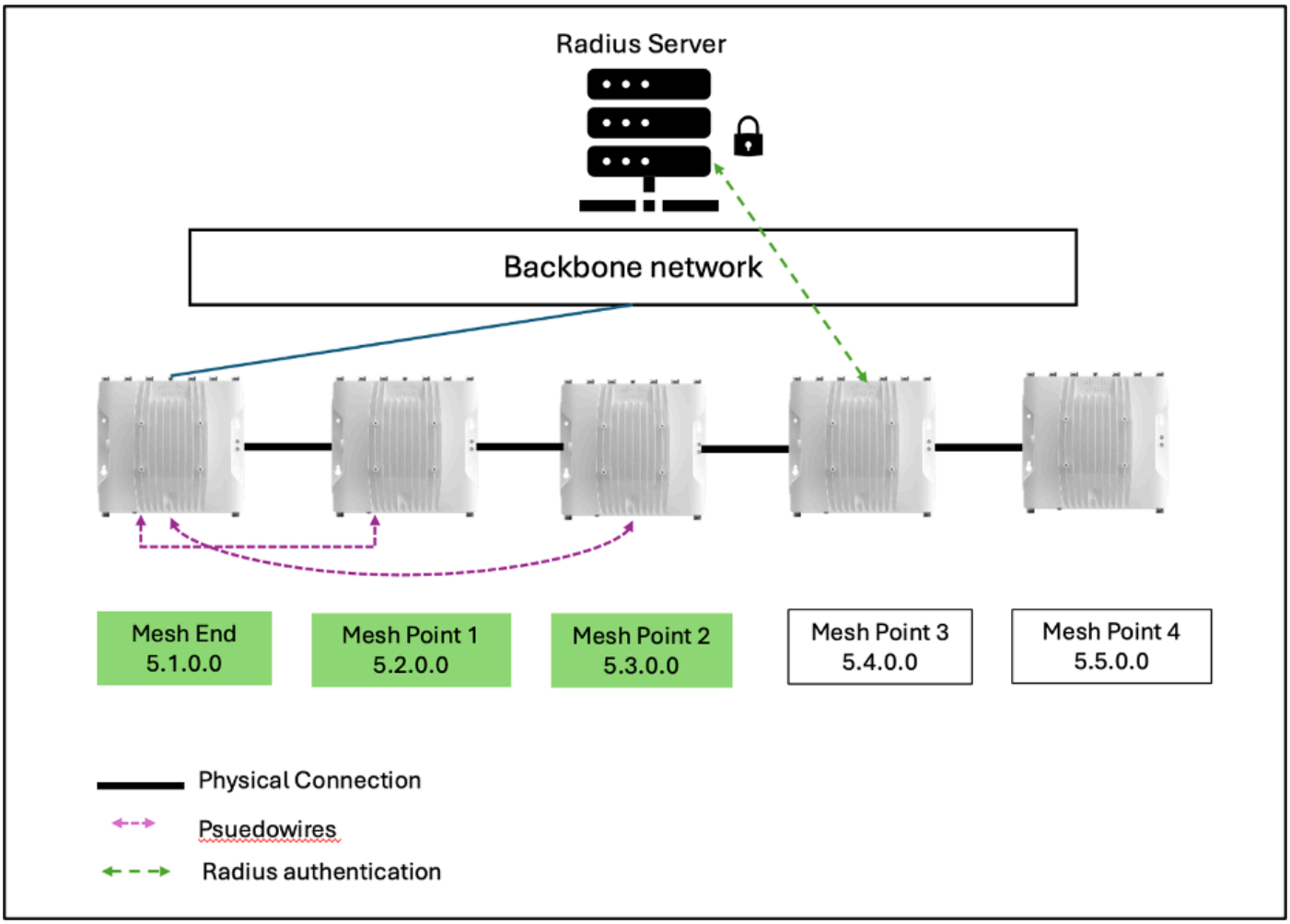
Étape 3 : Extrémité du maillage, le point de maillage 1 est authentifié et les autres ne le sont pas.



Maintenant que le point de maillage 1 est également authentifié, il forme un pseudo-fil avec l'extrémité de maillage authentifiée et devient également invisible pour le reste des radios d'infrastructure non authentifiées.

Les autres radios non authentifiées réexécutent la sélection et choisissent le point de maillage 2 avec l'ID de maillage le plus bas 5.3.0.0 comme nouveau coordinateur filaire et cette radio envoie une demande d'authentification au serveur Radius alors que son autotap est maintenant ouvert.

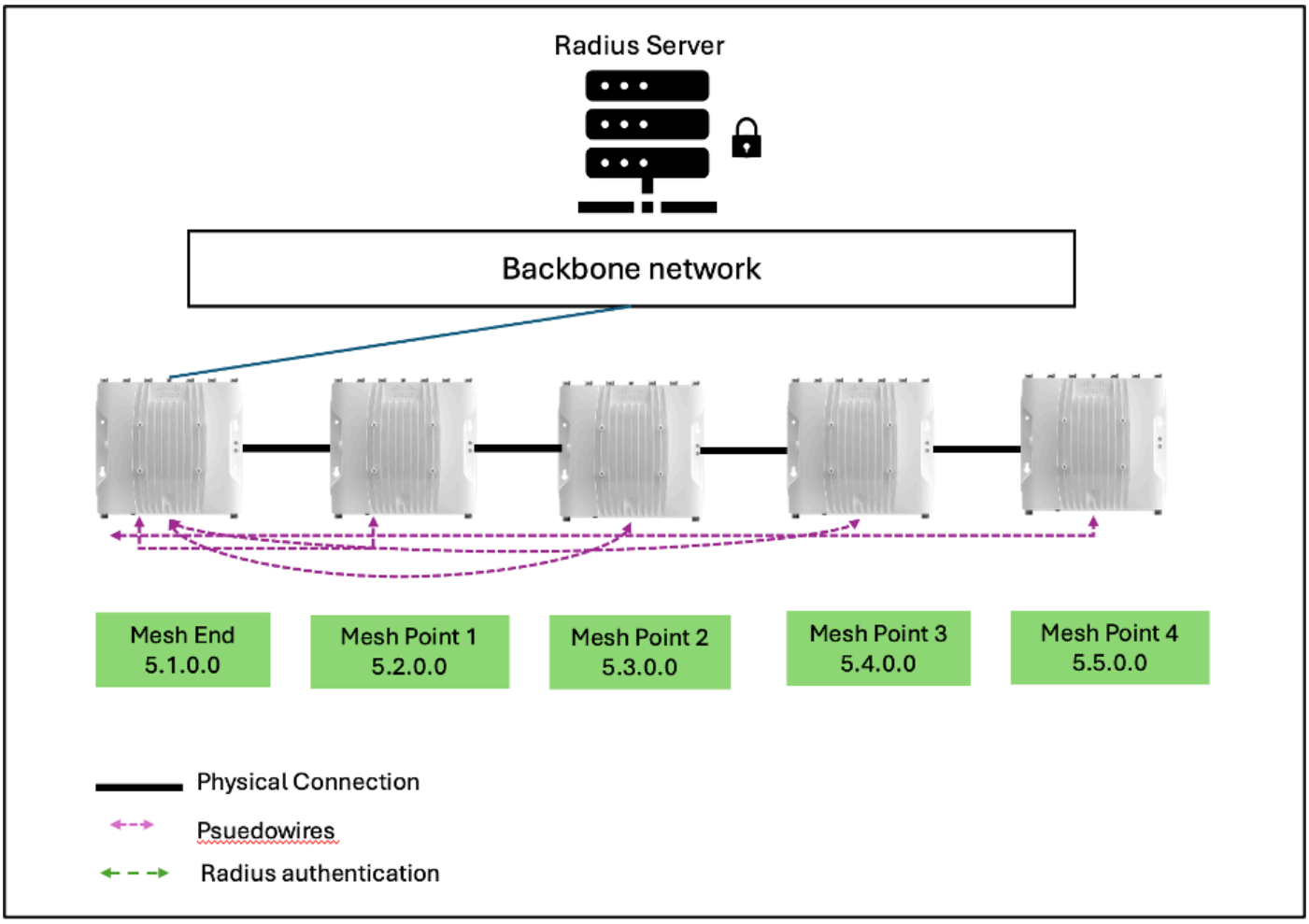
Étape 4 : L'extrémité de maillage, MP1 et MP2 sont authentifiés.



Le processus se répète ensuite avec le point de maillage 2 authentifié et formant un pseudo-fil avec le dispositif d'extrémité de maillage.

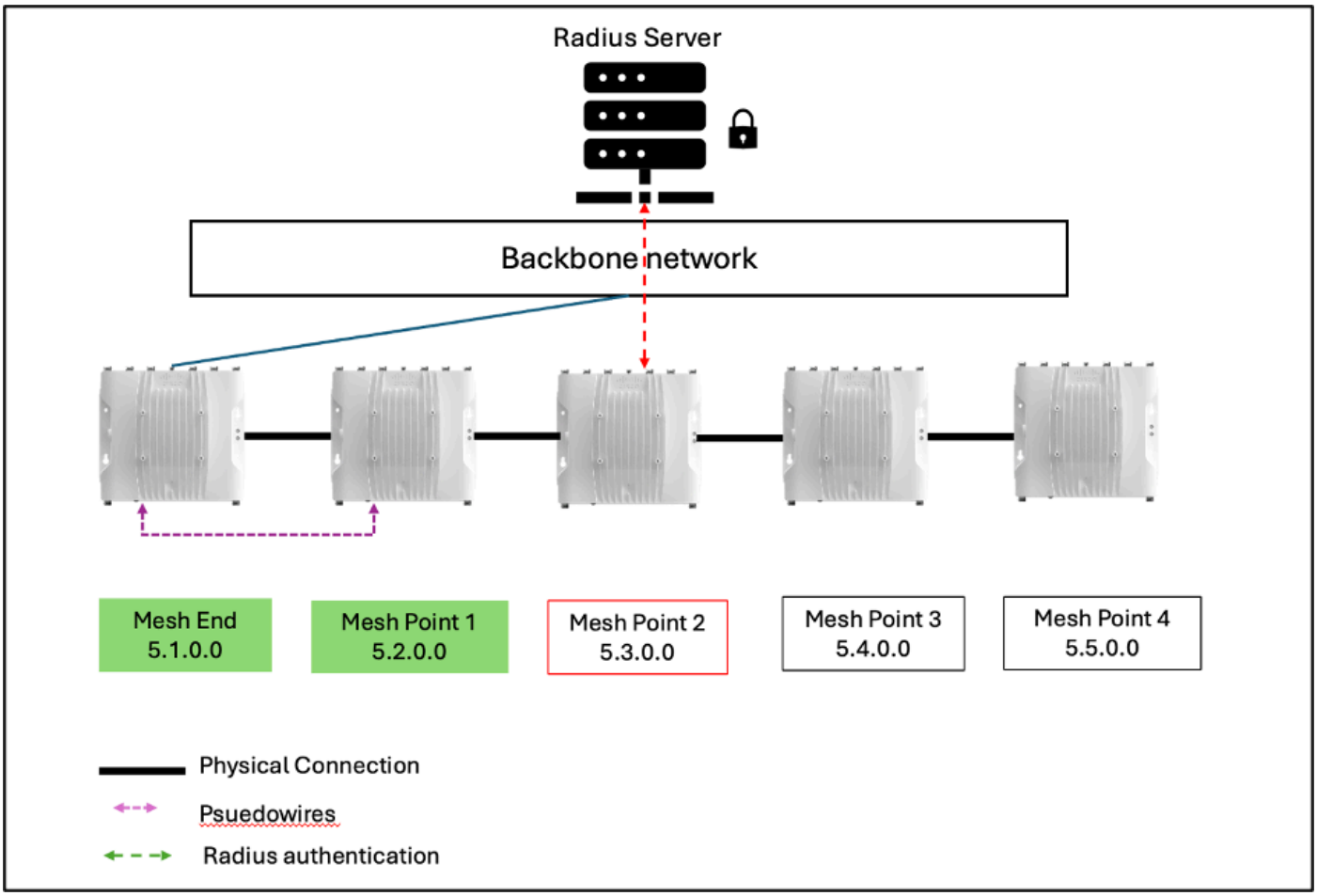
Les autres radios d'infrastructure s'authentifient à tour de rôle, dans l'ordre des ID de maillage les plus faibles à les plus élevés, au fur et à mesure de l'ouverture de leur propre autotap.

Étape 5 : Toutes les radios sont authentifiées.



Mauvaise configuration ou cas de problème :

Si l'un des points de maillage de l'infrastructure comporte des informations d'identification erronées ou si Radius est désactivé par erreur, cela empêchera les autres radios de s'authentifier. Assurez-vous toujours de vérifier les informations d'identification et les paramètres avant de déployer des radios en production.



Dans cet exemple, si le point de maillage 2 a des informations de connexion erronées, il ne sera pas authentifié et, à son tour, le point de maillage 3 et le point de maillage 4 n'auront jamais la chance de s'authentifier eux-mêmes, car aucun pseudo-fil n'est formé à partir d'eux vers le point de maillage 2 en raison de l'activation de LNO.

Les radios qui ne sont pas authentifiées dépendent de l'ID de maillage de la radio mal configurée. Toute radio avec un ID de maillage supérieur au coordinateur filaire actuel ne sera pas authentifiée et causera des problèmes.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.