在URWB模式下配置工业无线接入点的RADIUS和LNO

目录

简介

本文档介绍在URWB模式下的IW9165和IW9167无线电上配置RADIUS身份验证和大型网络优化(LNO)。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本CLI导航和命令
- 了解IW URWB模式无线电

使用的组件

本文档中的信息基于以下软件和硬件版本：

- IW9165和IW9167无线电

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

RADIUS — 远程身份验证拨入用户服务是一种网络协议，用于为连接和使用网络服务的用户或设备提供集中身份验证、授权和记帐(AAA)管理。对于URWB模式下的工业无线设备，可以在设备加入网络之前使用Radius对设备进行身份验证。

可以在IW设备上从GUI或CLI访问或从IoT OD配置Radius配置的参数。

Radius参数的CLI配置：

这些参数可在设备的CLI的启用模式下配置。

1.启用Radius身份验证：

此参数允许在设备上启用Radius身份验证。必须在添加radius身份验证所需的其他强制参数后执行此操作。

Radio1#configure radius enabled

2.禁用Radius身份验证：

此参数允许在设备上禁用Radius身份验证。

Radio1#configure radius disabled

3.直通：

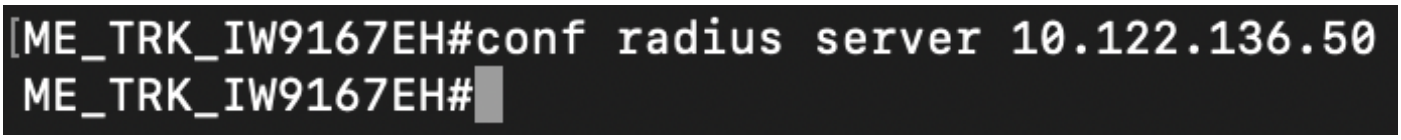
此参数只能在基础设施无线电上配置。使用直通参数配置基础设施无线电允许车辆无线电通过基础设施无线电对自身进行身份验证，也允许在已身份验证的车辆无线电与未身份验证的基础设施无线电之间进行通信。

Radio1#configure radius passthrough

4.添加Radius服务器：

此参数用于指定Radius服务器的IP地址，以便设备与之通信。

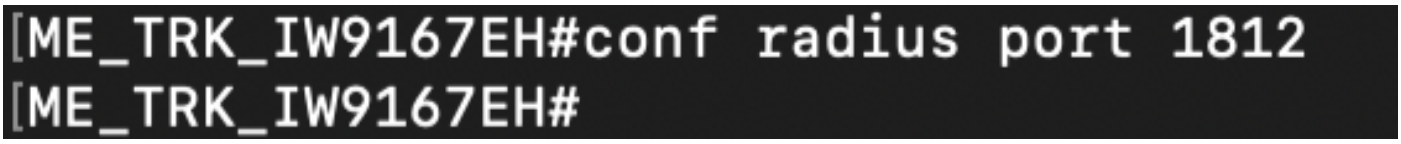
Radio1#configure radius server



5. RADIUS端口：

此参数用于指定Radius服务器的端口，以便设备与之通信。Radius身份验证的默认端口是1812。

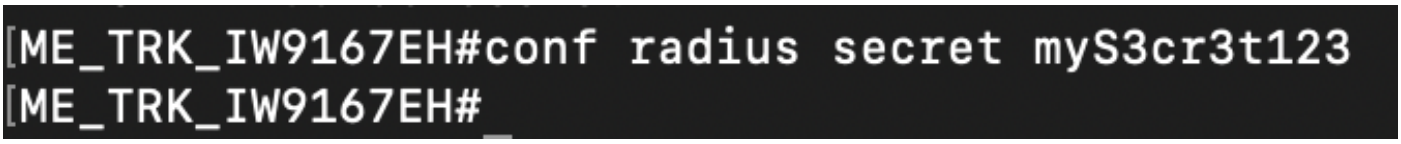
Radio1#configure radius server



6. Radius密码：

此参数用于指定要与Radius服务器一起使用的预共享密钥。

Radio1#configure radius secret



7.辅助服务器IP和端口：

这些参数用于指定第二个Radius服务器的IP地址和端口号，在设备无法到达主服务器时使用。

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超时：

此参数用于指定客户端在尝试连接到辅助服务器之前等待来自主Radius服务器的响应的时间（以秒为单位）。默认值设置为10秒。

Radio1#configure radius timeout

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

9.身份验证参数：

此参数用于指定Radius身份验证方法和要传递的相应参数。有几个选项可供使用。

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
```

如果使用这些方法：GTC（通用令牌卡）、MD5（消息摘要算法5）或MSCHAPV2（Microsoft质询握手身份验证协议版本2）用户名和密码都可以使用以下命令添加：

Radio1#configure radius authentication gtc

Radio1#configure radius authentication md5

Radio1#configure radius authentication mschapv2

如果使用这些方法：PEAP（受保护的可扩展身份验证协议）或EAP-TTLS（可扩展身份验证协议 — 隧道传输层安全）进行身份验证，还必须提供另一种内部身份验证方法。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.切换尝试：

此参数指定在客户端切换到辅助服务器之前允许对主服务器进行radius身份验证尝试的次数。默认值为 3。

Radio1#configure radius switch <1-6>

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

11.回退时间：

此参数指定客户端在超过身份验证的最大尝试次数后等待的时间值（以秒为单位）。

Radio1#configure radius backoff-time

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

十二、失效时间：

此参数指定时间值（以秒为单位），如果Radius身份验证未完成，身份验证尝试将被放弃。

Radio1#configure radius expiration

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

13.发送请求：

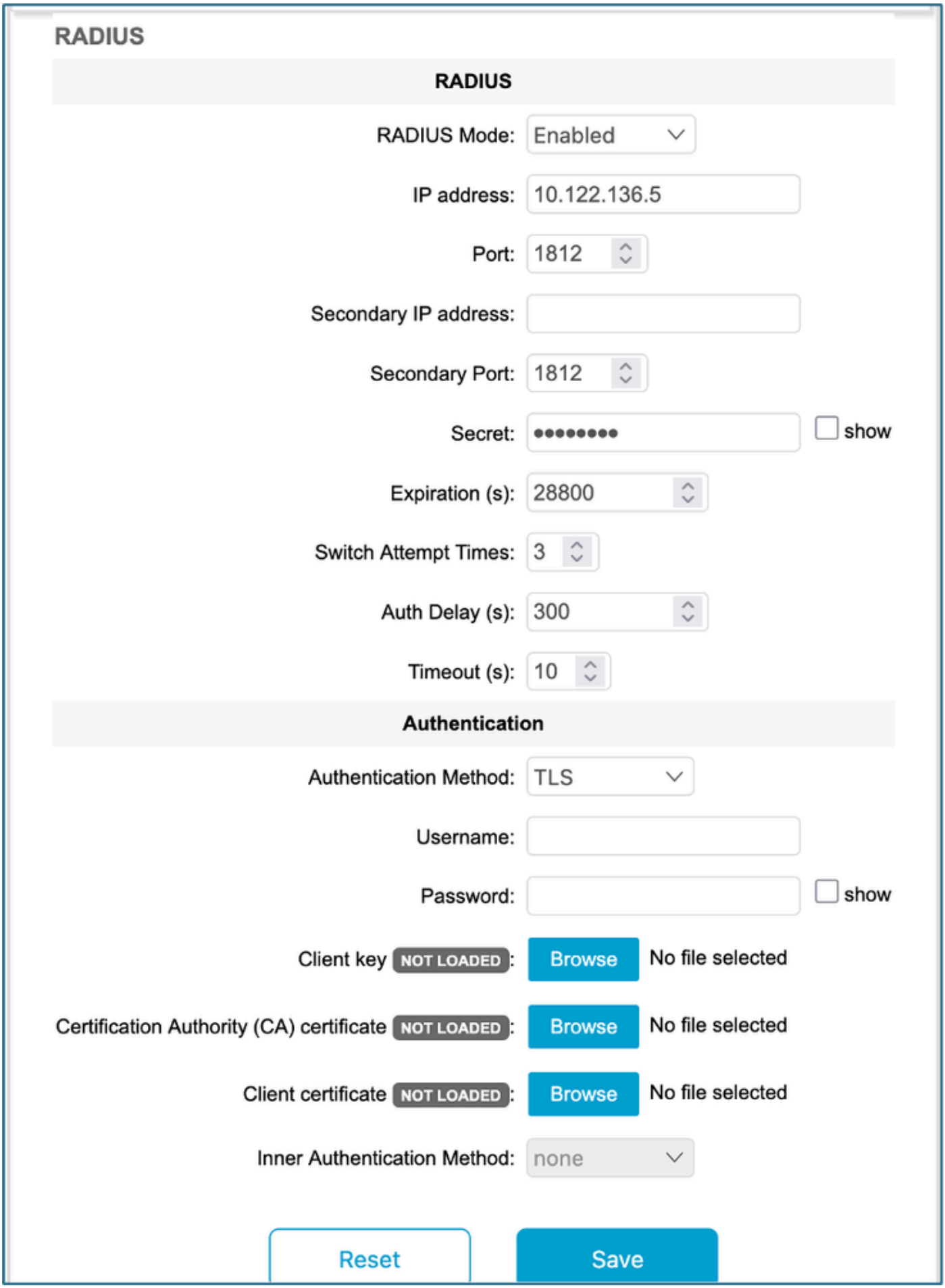
此参数用于向配置的主或辅助RADIUS服务器发起RADIUS身份验证请求。

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).
```

通过GUI以及在网页的“Radius”选项卡下，可以在URWB模式下的工业无线无线电上配置相同的参数。


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

显示命令：

当前的Radius配置可通过CLI使用show命令进行验证。

1.

#show radius

此show命令指示设备上是启用还是禁用Radius。

```
[ME_TRK_IW9167EH#show radius
```

2.

#show radius accounting

#show radius auth-method-tls

#show RADIUS身份验证

这些show命令将显示当前配置的radius记帐服务器、身份验证服务器和已配置的authentication method tls参数。

```
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身份验证序列

LNO或大型网络优化是建议在具有50个或更多基础设施无线电的大型网络上启用的功能，以优化网络中所有设备之间的伪线形成。它同时用于第2层和第3层网络。

在同时启用LNO和Radius的网络中，基础设施无线电按顺序进行身份验证（从最低的网状ID到最高网状ID）。 启用LNO将强制所有基础设施无线电仅建立到网状端的伪线，并且也会禁用BPDU转发。

本文将描述使用一个Mesh End无线电和4个Mesh Point Infrastructure无线电进行流动性设置时Radius身份验证的顺序。

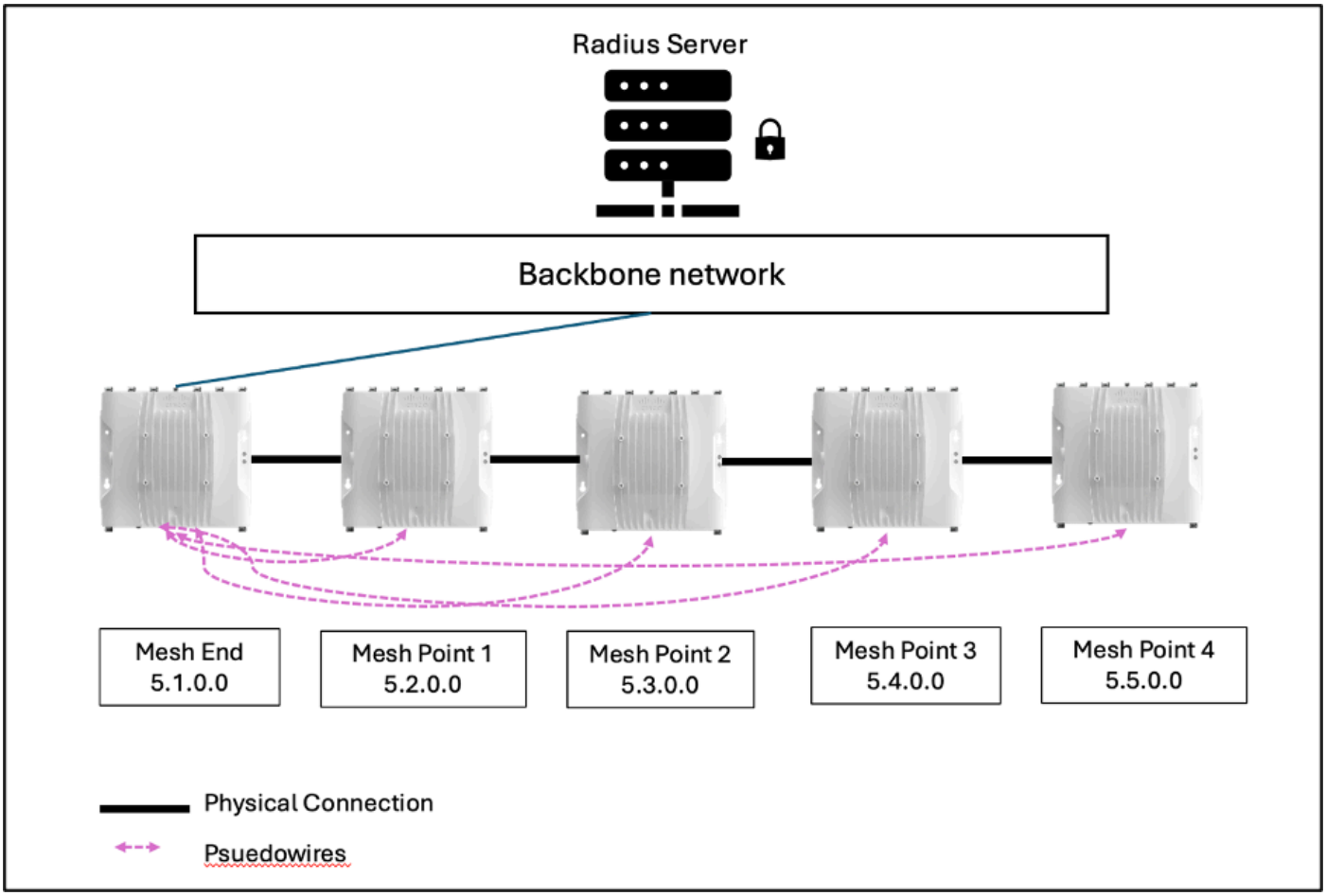
网状端无线电是流动性网络的默认“有线协调器”。也就是说，它具有autotap打开并充当网络的入口/出口点。

所有其他基础设施无线电都设置为网状点，并且它们都通过相互连接的交换机与网状端建立物理连接。

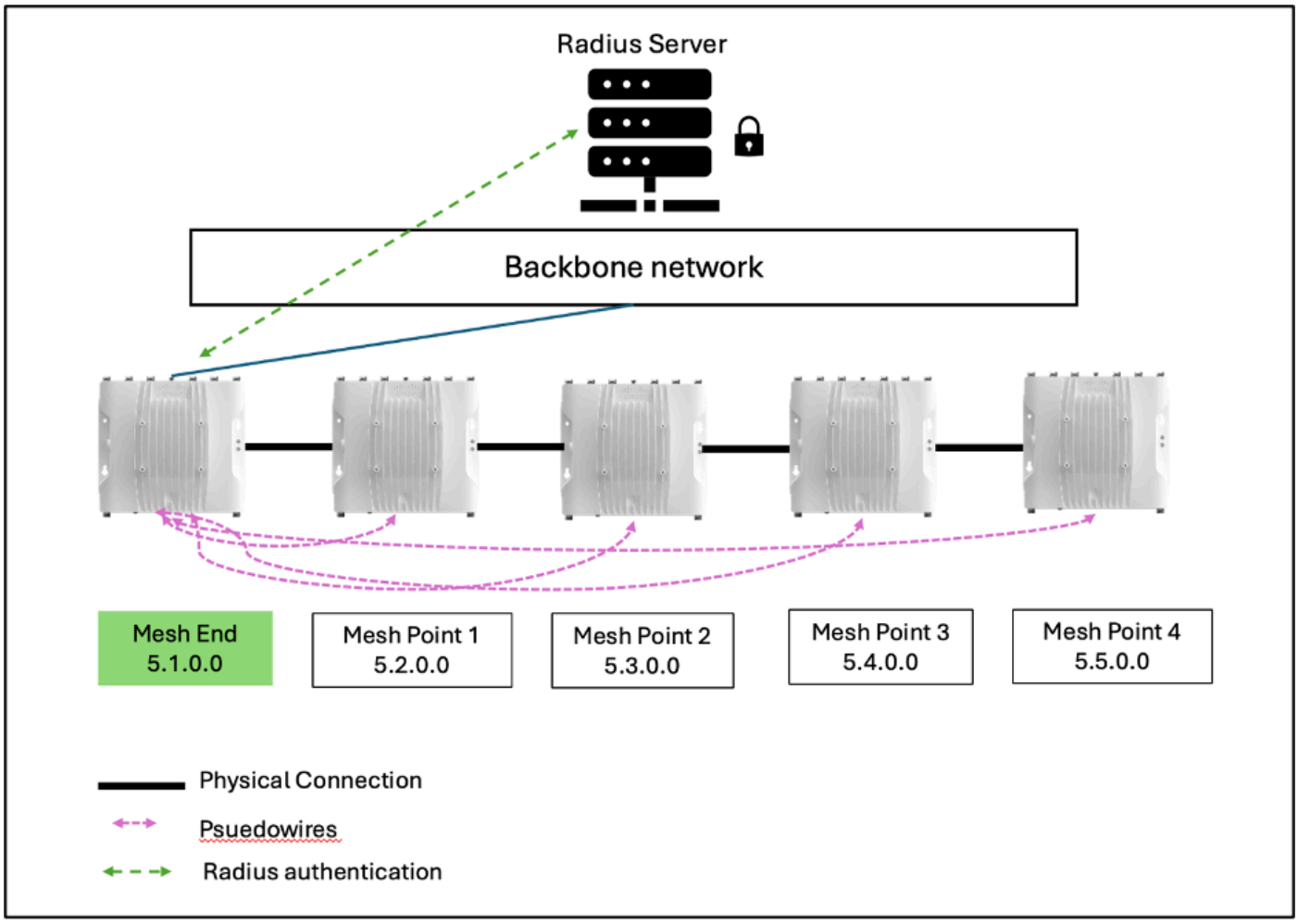
网状终端无线电通常通过光纤连接连接到主干网络，并通过主干网络，可以到达网络的Radius服务器。

只有满足以下条件时，任何设备才能访问Radius服务器：

1. 是有线协调器。
2. 它使用有线主设备（即网状端）构建伪线。



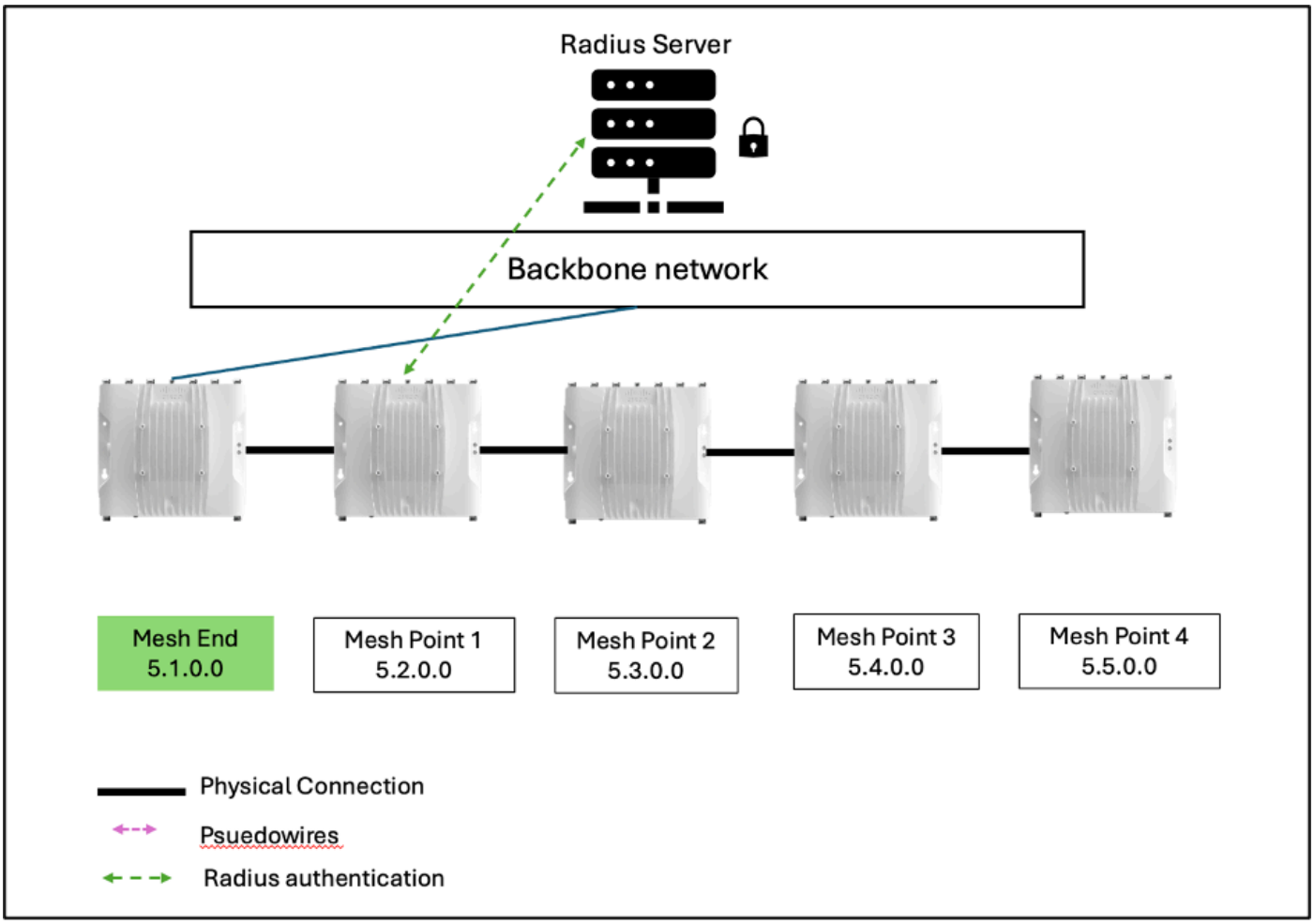
步骤 1：所有设备均未经身份验证。



开始时，所有单元（包括网状端）均未经身份验证。Autotap将仅在网状终端（整个网络的入口/出口点）无线电上打开。任何基础设施设备要到达Radius服务器进行自身身份验证，它必须是网状端或具有到网状端的伪线。

现在，网状端无线电5.1.0.0将通过主干网络向Radius服务器发出身份验证请求。收到回传的通信后，它将经过身份验证，然后对未经过身份验证的基础设施网状点的其余部分变得“不可见”，就像对具有Radius的AAA的要求一样。

步骤 2：网状终端5.1.0.0经过身份验证，其余部分未经身份验证。

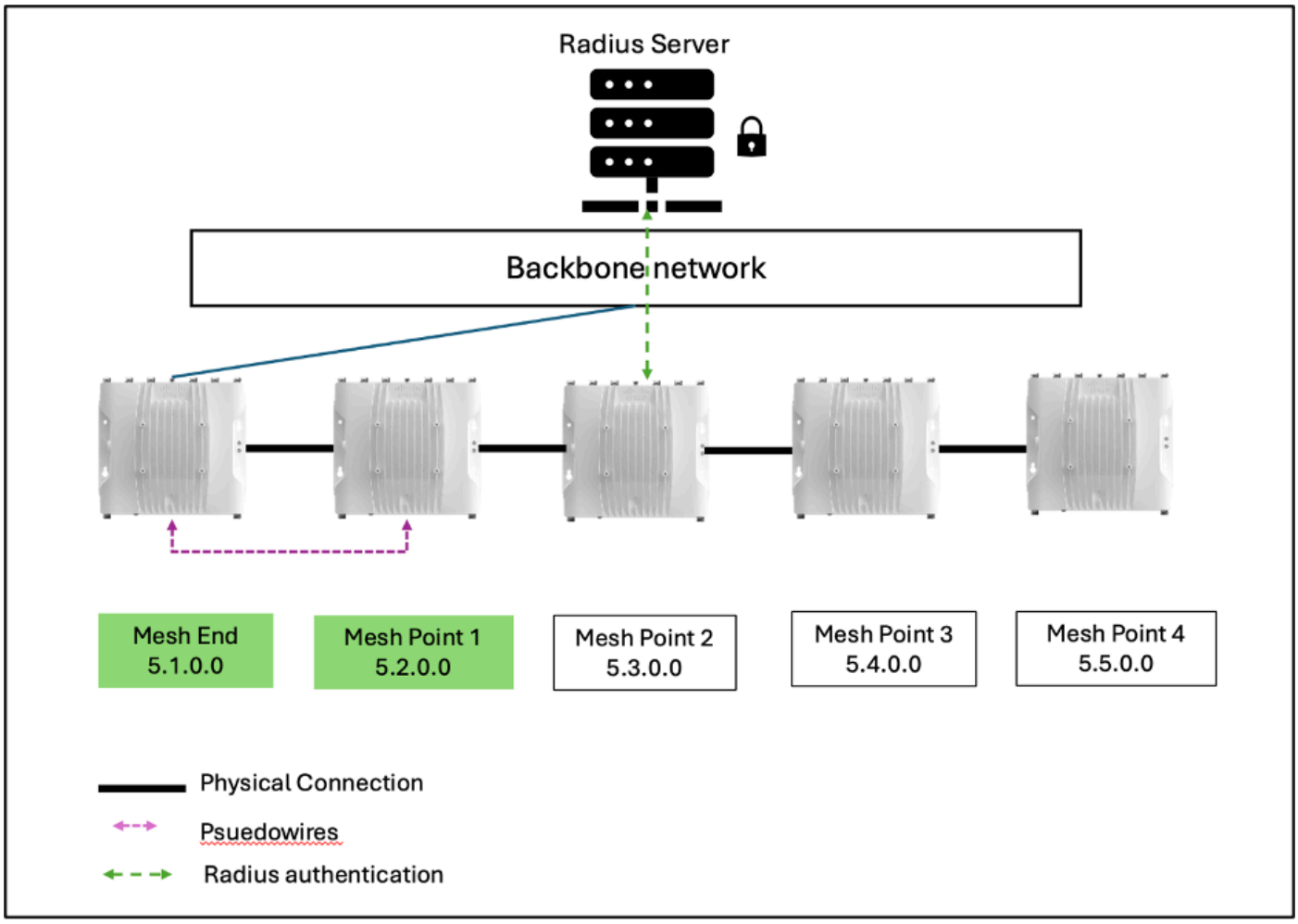


现在，网状终端5.1.0.0已经过身份验证且对网络的其余部分不可见，其余的网状点将运行选举并选择具有最低网状ID的设备作为下一个有线协调器。在本例中，该网状ID为5.2.0.0的网状点1。然后，将在网状点1上打开自动分路器。

由于启用了LNO，不会形成网状点1的伪线。所有剩余无线电设备在其自动分路打开时都必须按顺序进行身份验证。

现在，网状点1可以向Radius服务器发出身份验证请求并验证其自身。

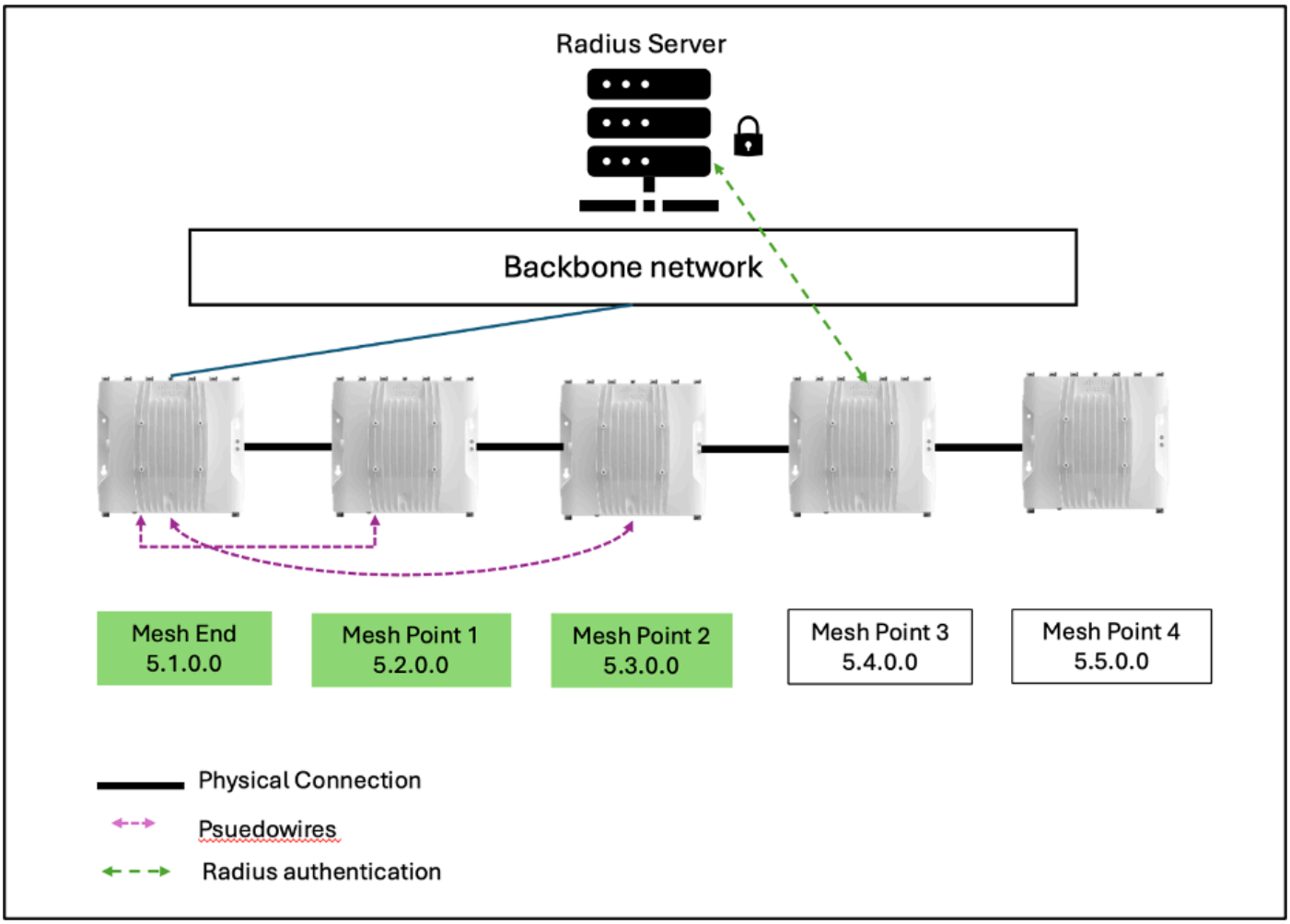
步骤 3：Mesh End、Mesh Point 1进行身份验证，而其他未经身份验证。



由于网状点1也经过身份验证，因此它将与经过身份验证的网状端形成一条虚线，并且对于未经身份验证的基础设施无线电的其余部分也是不可见的。

其余未经身份验证的无线电重新运行选举，并选择具有最低网状ID 5.3.0.0的网状点2作为新的有线协调器，该无线电在Autotap现在打开时向Radius服务器发出身份验证请求。

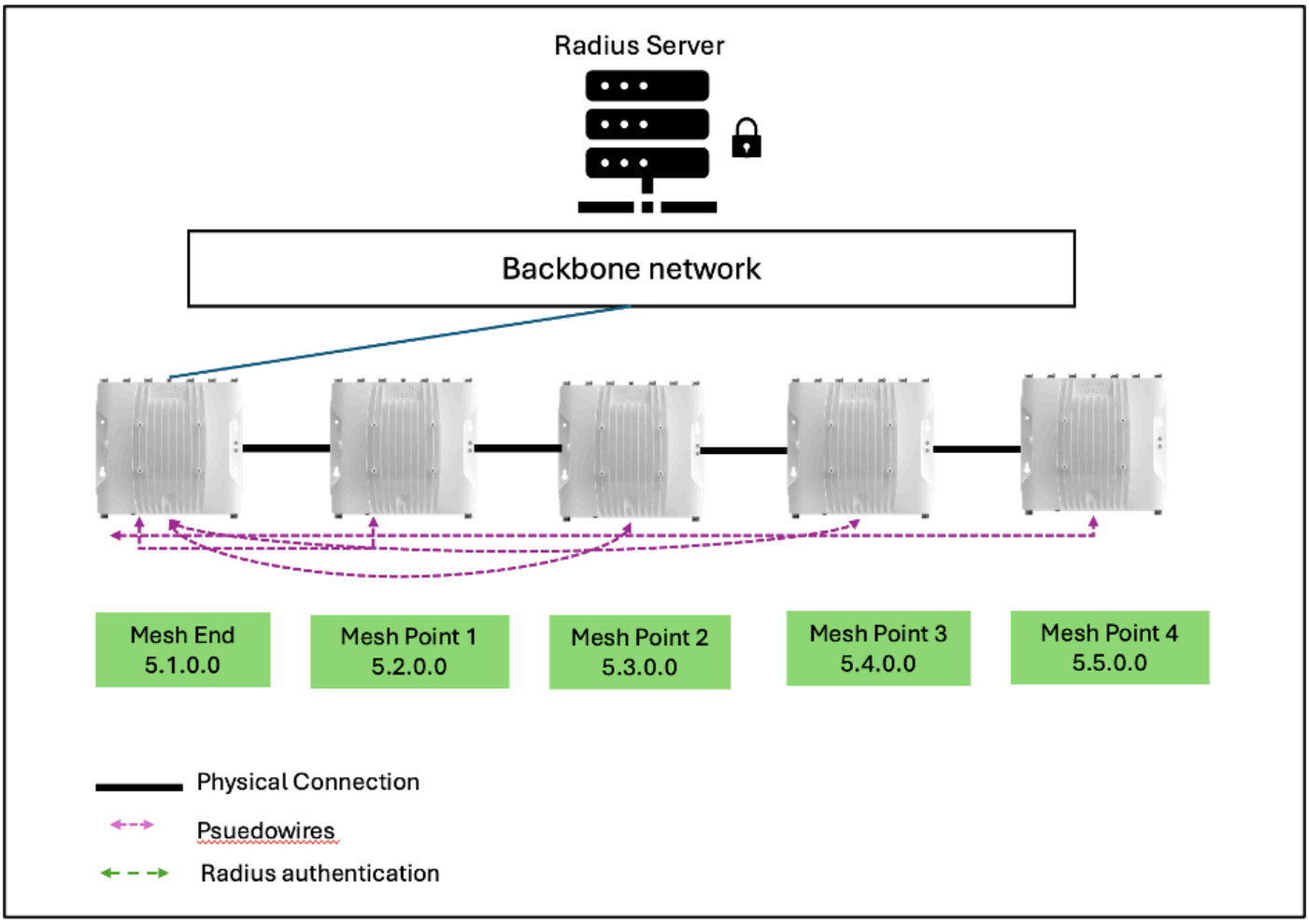
步骤 4：Mesh End、MP 1和MP 2进行身份验证。



然后重复此过程，网状点2通过身份验证并与网状终端设备形成伪线。

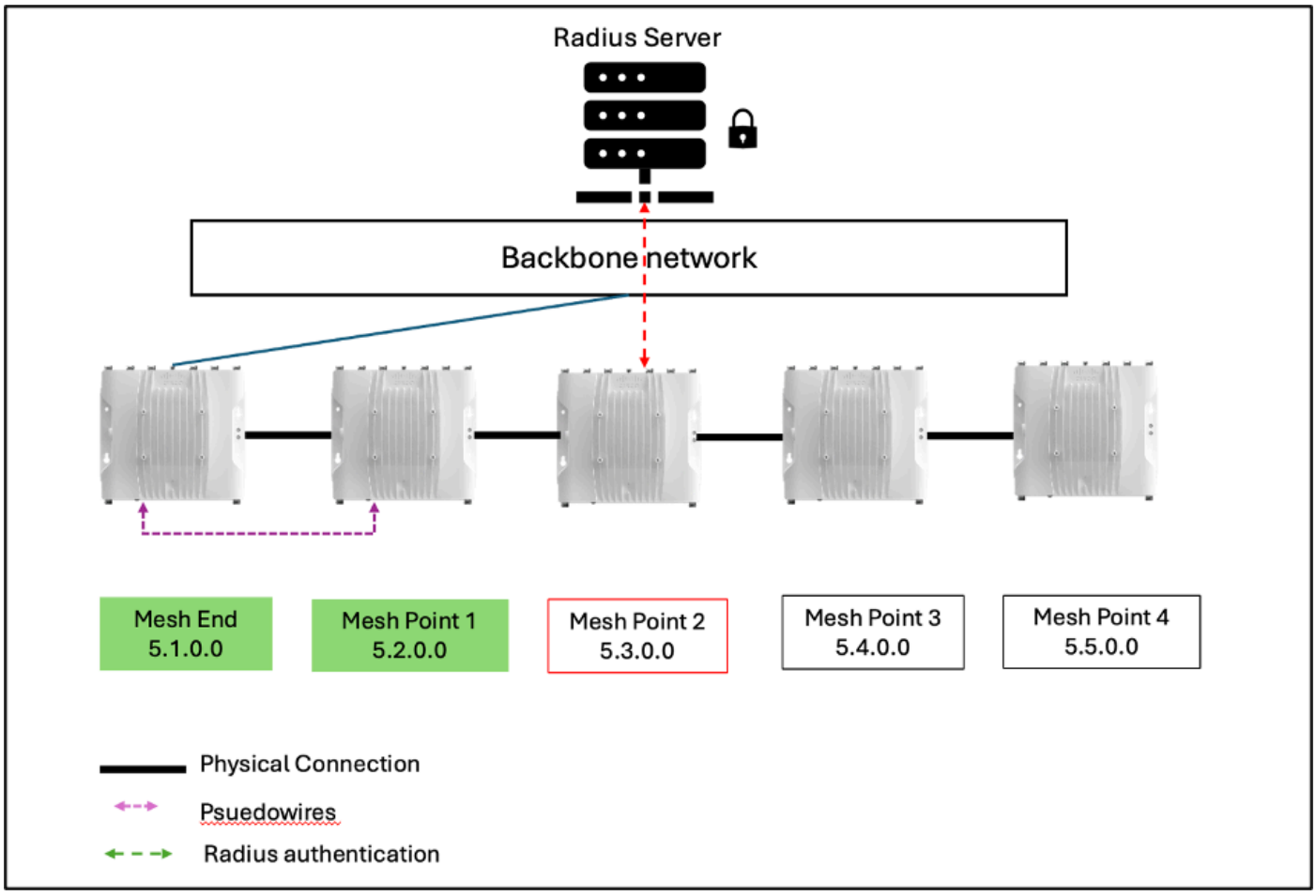
其余的基础设施无线电在打开自己的自动分路器时，会依次按最低到最高网状ID的顺序进行身份验证。

步骤 5：所有无线电都经过身份验证。



配置错误或问题案例：

如果任何基础设施网状点的凭证有误，或者错误地禁用了Radius，这将影响其他无线电进行身份验证。在将无线电部署到生产环境之前，始终确保检查凭证和设置。



在本示例中，如果网状点2的折线错误，它将保持未经身份验证的状态，并且网状点3和网状点4将永远不会有机会对自身进行身份验证，因为启用了LNO，所以没有从网状点2到网状点2形成伪线。

未进行身份验证的无线电取决于错误配置的无线电的Mesh ID。网状网标识高于当前有线协调器的任何无线电都保持未经身份验证的状态，并会导致问题。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。