

URWB 모드에서 Industrial Wireless Access Points에 RADIUS 및 LNO 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[LNO가 있는 RADIUS 인증 시퀀스](#)

소개

이 문서에서는 URWB 모드의 IW9165 및 IW9167 무선에서 RADIUS 인증 및 LNO(Large Network Optimization)의 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 CLI 탐색 및 명령
- IW URWB 모드 무선 송수신 장치 이해

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IW9165 및 IW9167 무선

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

RADIUS - Remote Authentication Dial-In User Service(원격 인증 전화 접속 사용자 서비스)는 네트워크 서비스에 연결하여 사용하는 사용자 또는 장치에 대해 중앙 집중식 AAA(Authentication, Authorization, and Accounting) 관리를 제공하는 데 사용되는 네트워킹 프로토콜입니다. URWB 모드의 산업용 무선 디바이스의 경우 네트워크에 참가하기 전에 디바이스를 인증하는 데 Radius를 사용할 수 있습니다.

Radius 컨피그레이션에 대한 매개변수는 GUI 또는 CLI 액세스에서 또는 IoT OD에서도 IW 디바이스에 구성할 수 있습니다.

Radius 매개변수의 CLI 컨피그레이션:

이러한 매개변수는 디바이스의 CLI에서 활성화 모드에서 구성할 수 있습니다.

1. Radius 인증 활성화:

이 매개변수는 디바이스에서 Radius 인증을 활성화할 수 있습니다. 이는 radius 인증에 필요한 다른 필수 매개변수를 추가한 후에 실행해야 합니다.

Radio1#configure radius enabled

```
ME_TRK_IW9167EH#configure radius enabled
```

2. Radius 인증을 사용하지 않도록 설정합니다.

이 매개변수는 디바이스에서 Radius 인증을 비활성화할 수 있습니다.

Radio1#configure radius disabled

```
[ME_TRK_IW9167EH#configure radius disabled
```

3. 통행권

이 매개변수는 인프라 무선에서만 구성됩니다. 패스스루 매개변수로 인프라 무선 장치를 구성하면 차량 무선 장치가 인프라 무선 장치를 통해 스스로를 인증할 수 있으며, 인증된 차량 무선 장치와 인증되지 않은 인프라 무선 장치 간의 통신도 허용합니다.

Radio1#configure radius passthrough

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

4. Radius 서버 추가:

이 매개변수는 디바이스가 통신할 Radius 서버의 IP 주소를 지정하는 데 사용됩니다.

Radio1#configure radius server

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

5. 반지름 포트

이 매개변수는 디바이스가 통신할 Radius 서버의 포트를 지정하는 데 사용됩니다. Radius 인증을 위한 기본 포트는 1812입니다.

Radio1#configure radius server

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

6. 반지름 암호

이 매개변수는 Radius 서버와 함께 사용할 사전 공유 키를 지정하는 데 사용됩니다.

Radio1#configure radius secret

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

7. 보조 서버 IP 및 포트:

이 매개변수는 디바이스가 기본 서버에 연결할 수 없는 경우에 사용할 두 번째 Radius 서버의 IP 주소 및 포트 번호를 지정하는 데 사용됩니다.

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. 반경 시간 초과:

이 매개변수는 클라이언트가 보조 서버에 연결하기 전에 기본 Radius 서버의 응답을 기다리는 시간 (초)을 지정하는 데 사용됩니다. 기본값은 10초로 설정됩니다.

Radio1#configure radius timeout

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

9. 인증 매개변수

이 매개변수는 Radius 인증 방법 및 전달할 해당 매개변수를 지정하는 데 사용됩니다. 몇 가지 옵션을 사용할 수 있습니다.

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
```

다음 방법을 사용하는 경우: GTC(Generic token card), MD5(Message-Digest Algorithm 5) 또는 MSCHAPV2(Microsoft Challenge Handshake Authentication Protocol 버전 2)는 다음 명령과 함께 사용자 이름과 비밀번호를 추가할 수 있습니다.

Radio1#configure radius authentication gtc

Radio1#configure radius authentication md5

Radio1#configure radius authentication mschapv2

다음 방법을 사용하는 경우: 인증을 위한 PEAP(Protected Extensible Authentication Protocol) 또는 EAP-TTLS(Extensible Authentication Protocol-Tunneled Transport Layer Security), 다른 내부 인증 방법도 제공해야 합니다. gtc, md5 또는 mschapv2일 수 있습니다.

Radio1#configure radius authentication peap

inner-auth-method

Radio1#configure radius authentication ttls

inner-auth-method

10. 스위치 시도 횟수:

이 매개변수는 클라이언트가 보조 서버로 전환되기 전에 기본 서버에 대해 허용되는 RADIUS 인증 시도 횟수를 지정합니다. 기본값은 3입니다.

Radio1#configure radius switch <1-6>

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

11. 백오프 시간

이 매개변수는 클라이언트가 최대 인증 시도 횟수를 초과한 후 대기할 시간(초)을 지정합니다.

Radio1#configure radius backoff-time

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

12. 유효기간

이 매개변수는 Radius 인증이 완료되지 않은 경우 인증 시도가 취소되는 시간(초)의 값을 지정합니다.

Radio1#configure radius expiration

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

13. 요청 보내기:

이 매개변수는 구성된 기본 또는 보조 Radius 서버에 대한 RADIUS 인증 요청을 시작하는 데 사용됩니다.

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).
```

GUI를 통해 URWB 모드의 산업용 무선 무선 라디오에서도 웹 페이지의 'Radius' 탭 아래에 동일한 매개변수를 구성할 수 있습니다.

RADIUS

RADIUS

RADIUS Mode: Enabled 

IP address:

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 No file selected

Certification Authority (CA) certificate NOT LOADED No file selected

Client certificate NOT LOADED No file selected

Inner Authentication Method: none 

Show 명령:

현재 Radius 컨피그레이션은 CLI를 통해 show 명령으로 확인할 수 있습니다.

1.

#show 반지름

이 show 명령은 디바이스에서 Radius가 활성화되었는지 또는 비활성화되었는지를 알려줍니다.

```
[ME_TRK_IW9167EH#show radius
```

2 .

#show 계정 관리

#show radius auth-method-tls

#show 인증

이러한 show 명령은 구성된 radius 계정 관리 서버, 인증 서버 및 인증 방법 tls 매개변수의 현재 컨피그레이션을 보여줍니다.

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

LNO가 있는 RADIUS 인증 시퀀스

LNO 또는 Large Network Optimization은 네트워크에 있는 모든 디바이스 간의 의사 전선 형성을 최적화하기 위해 50개 이상의 Infrastructure 무선 장치가 있는 대규모 네트워크에서 사용하도록 권장되는 기능입니다. 레이어 2 및 레이어 3 네트워크에서 모두 사용됩니다.

LNO와 Radius가 모두 활성화된 네트워크에서는 인프라 무선 장치가 순서대로(가장 낮은 메시 ID에서 가장 높은 메시 ID로) 인증됩니다. LNO를 활성화하면 모든 인프라 무선 장치가 Mesh End에 대한 의사 전선만 구축하게 되며 BPDU 전달도 비활성화됩니다.

이 문서에서는 하나의 메시 엔드와 4 메시 포인트 인프라 무선 장치를 사용하는 유동성 설정에 대한 Radius 인증 순서에 대해 설명합니다.

Mesh End 라디오는 Fluidity 네트워크의 기본 "유선 조정자"입니다. 즉, 자동 탭이 열려 있고 네트워크의 인그레스/이그레스 지점 역할을 합니다.

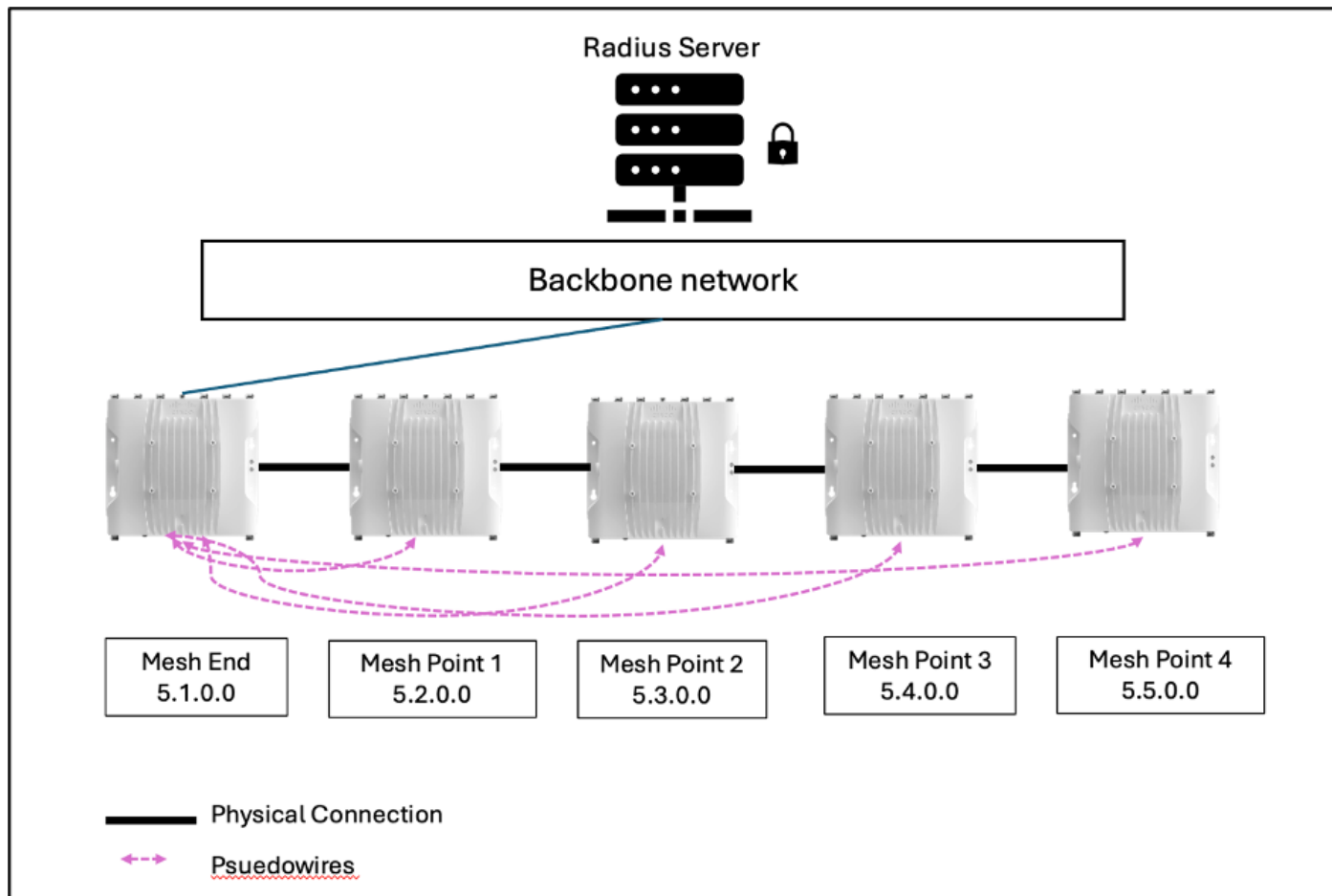
다른 모든 인프라 무선 장치는 메시 포인트로 설정되며 서로 연결된 스위치를 통해 메시 끝에 물리적으로 연결됩니다.

메시 엔드 라디오는 일반적으로 파이버 연결을 통해 백본 네트워크에 연결되며, 백본 네트워크를

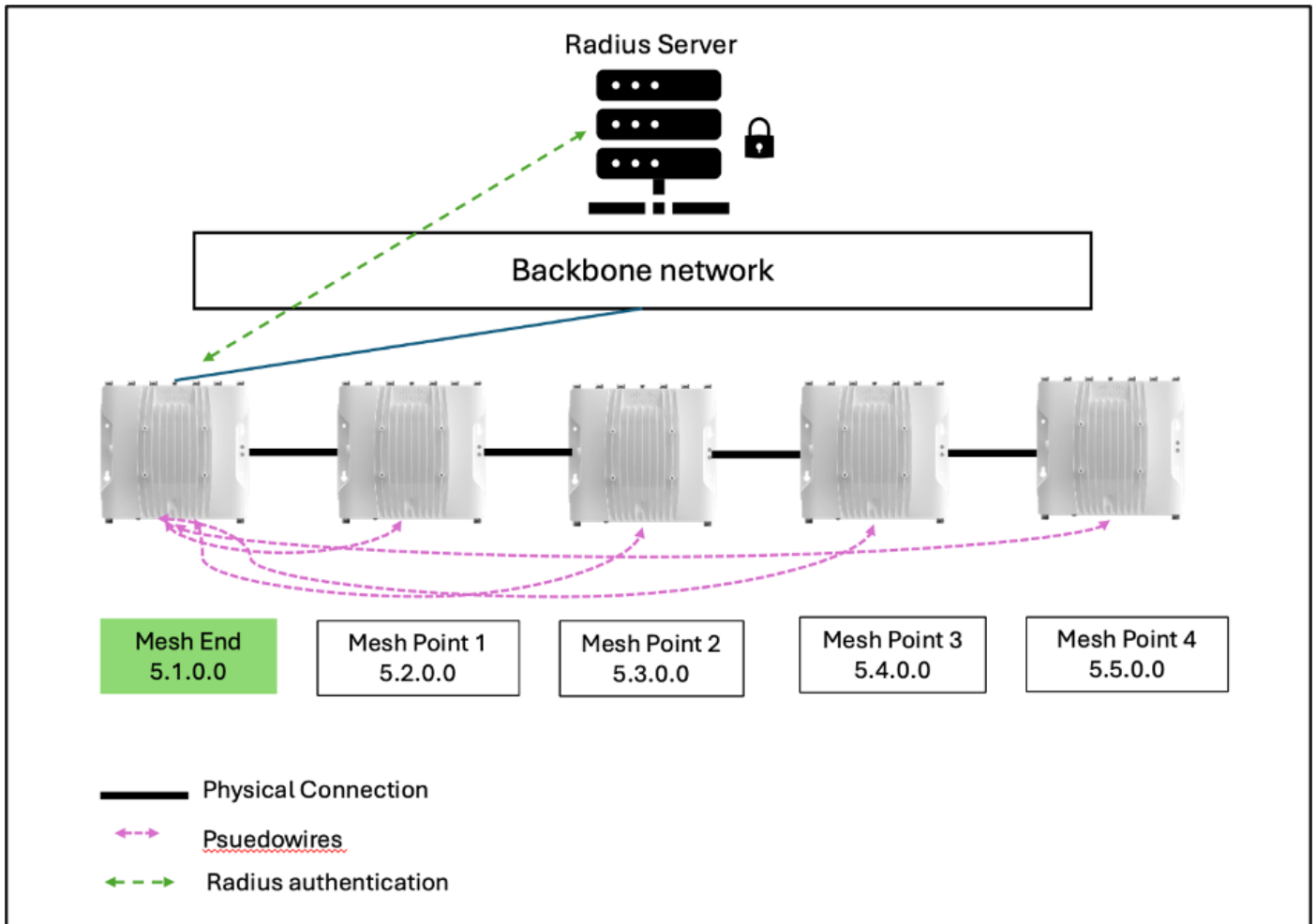
통해 네트워크의 Radius 서버에 연결할 수 있습니다.

다음과 같은 경우에만 모든 디바이스가 Radius 서버에 연결할 수 있습니다.

1. 유선 코디네이터입니다.
2. 유선 마스터, 즉 Mesh End로 구축된 의사 와이어가 있습니다.



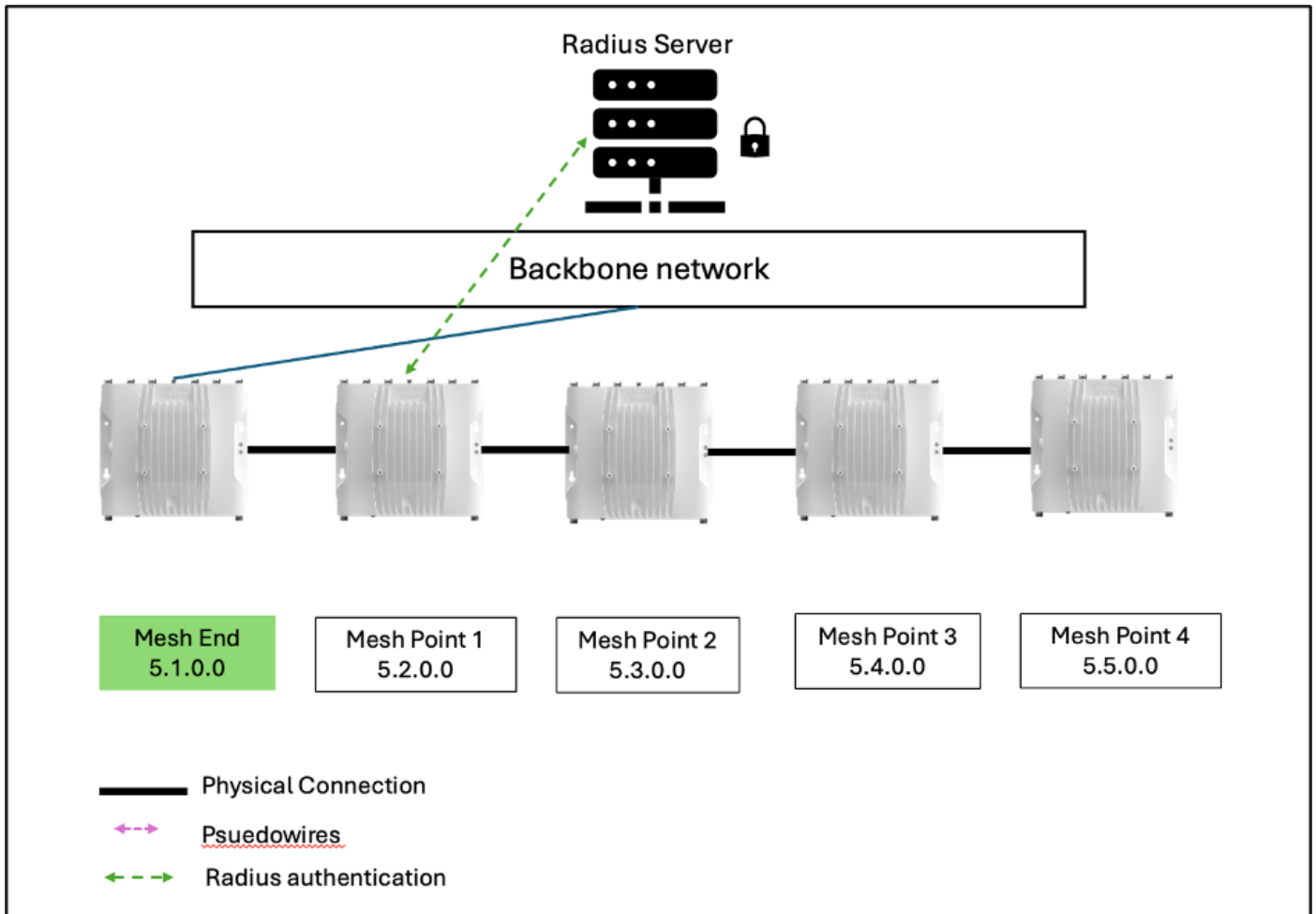
1단계: 모든 장치가 인증되지 않았습니다.



처음에는 메시 엔드를 포함한 모든 유닛이 인증되지 않습니다. 자동 탭은 전체 네트워크의 인그레스(Ingress)/이그레스(Egress) 지점인 메시 엔드(Mesh End) 라디오에서만 열립니다. 인프라 디바이스가 Radius 서버에 도달하여 자체 인증을 받으려면 메시 엔드이거나 메시 엔드에 대한 의사 와이어가 있어야 합니다.

이제 Mesh End 라디오 5.1.0.0은 백본 네트워크를 통해 Radius 서버에 인증 요청을 보냅니다. 통신을 다시 수신하면 인증이 완료되고 인증되지 않은 인프라 메시 포인트의 나머지는 '보이지 않음'이 됩니다. AAA with Radius의 요구 사항도 마찬가지입니다.

2단계: 메시 End 5.1.0.0. 는 인증되고 나머지는 인증되지 않습니다.

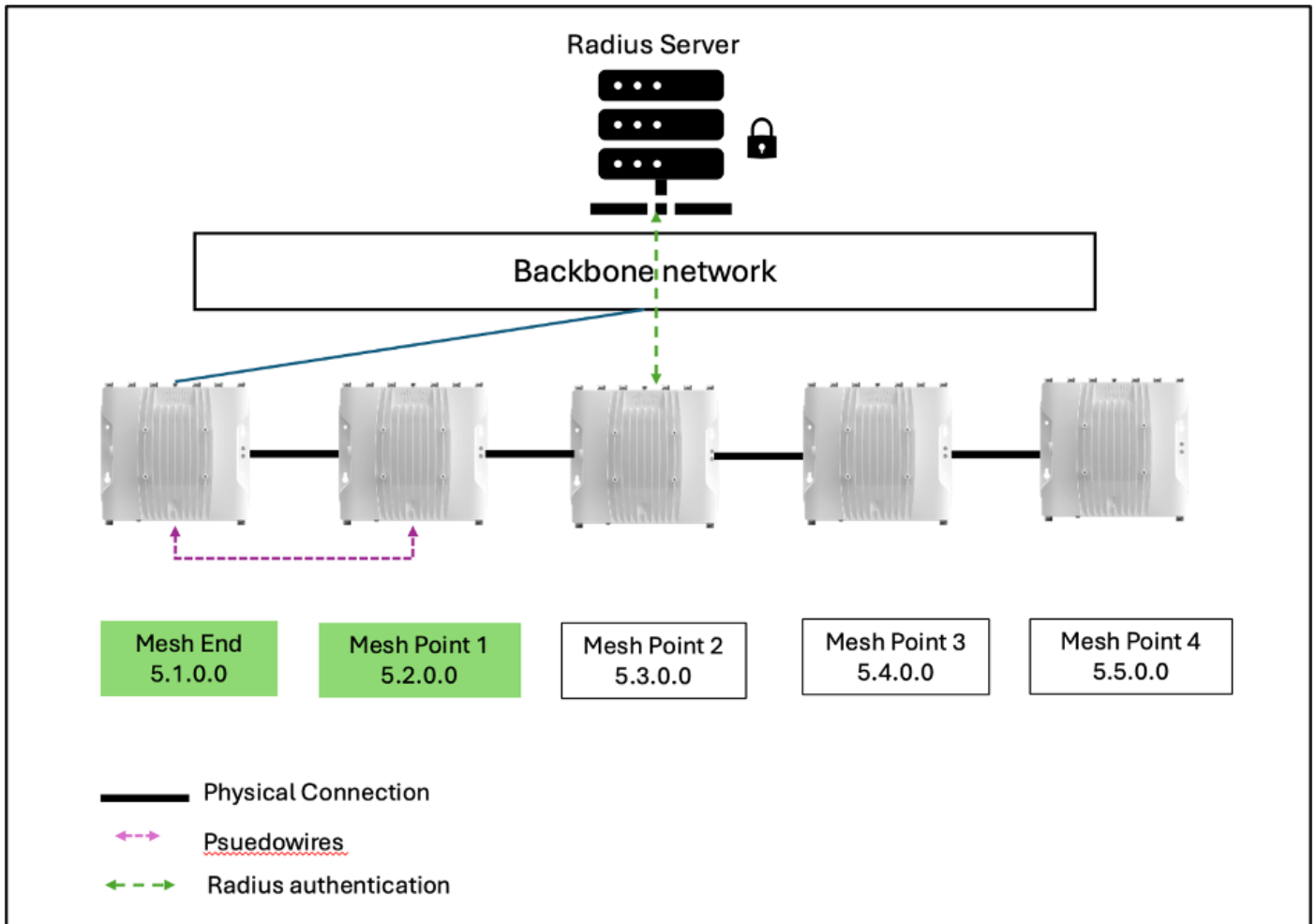


이제 Mesh End 5.1.0.0이 인증되어 네트워크의 나머지 부분에 표시되지 않으므로 나머지 Mesh Points는 선택을 실행하고 Mesh ID가 가장 낮은 디바이스를 다음 유선 코디네이터로 선택합니다. 이 예에서는 메시 ID가 5.2.0.0인 메시 포인트 1이 됩니다. 그러면 메시 포인트 1에서 자동 탭이 열립니다.

LNO가 활성화되어 있으므로 메시 포인트 1에 의사 와이어가 형성되지 않습니다. 나머지 모든 무선 장치는 Autotap이 열려 있을 때 순차적으로 인증해야 합니다.

이제 메시 포인트 1은 Radius 서버에 인증 요청을 보내고 스스로를 인증할 수 있습니다.

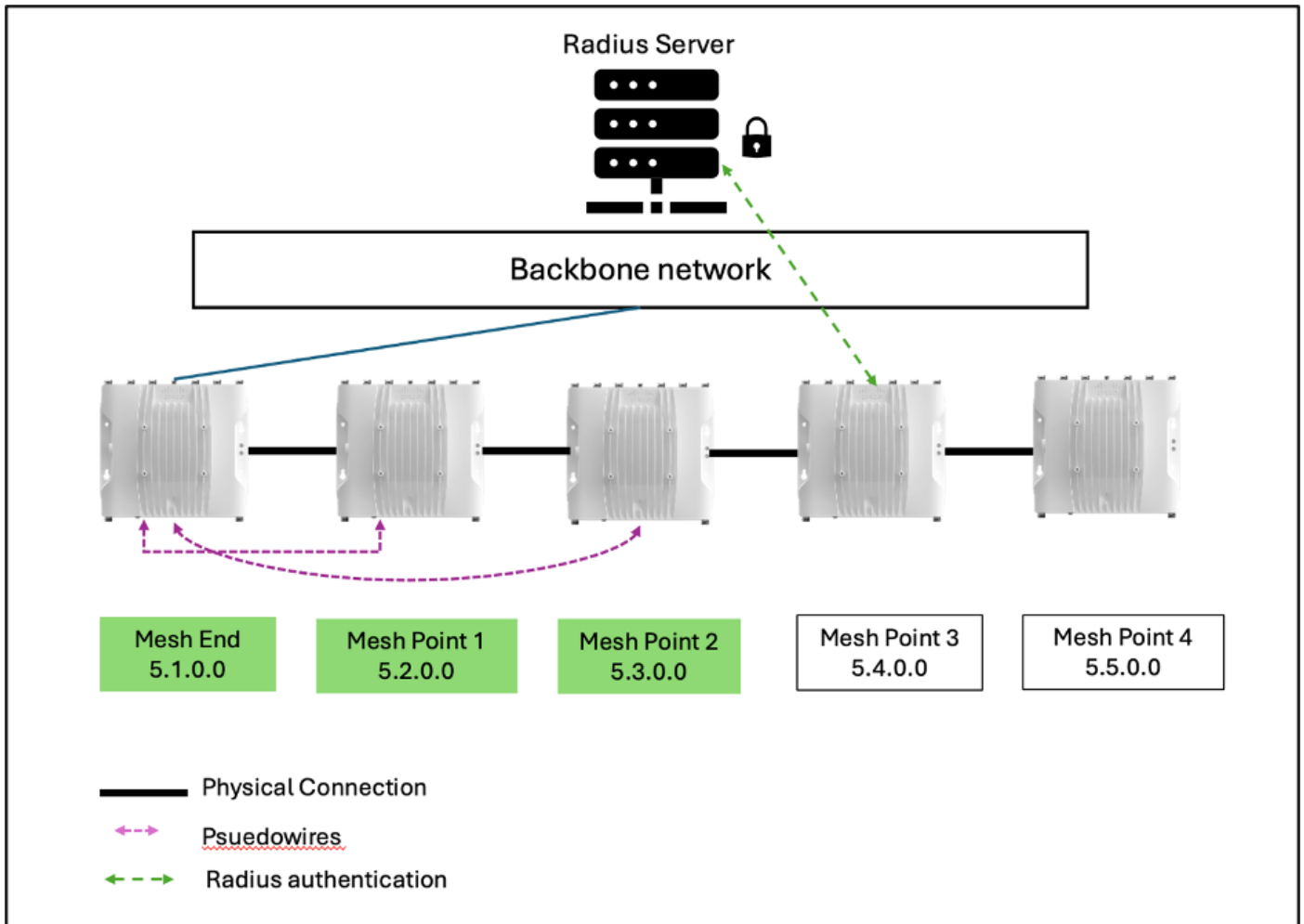
3단계: 메시 End, 메시 Point 1은 인증되고 나머지는 인증되지 않습니다.



이제 메시 포인트 1도 인증되었으므로 인증된 메시 엔드와 함께 회선을 형성하고 인증되지 않은 나머지 인프라 무선 장치에도 표시되지 않습니다.

나머지 인증되지 않은 무선 장치는 선택을 다시 실행하고 새 유선 조정자로 가장 낮은 메시 ID가 5.3.0.0인 메시 포인트 2를 선택합니다. 그러면 해당 무선 장치는 Autotap이 열려 있는 Radius 서버에 인증 요청을 보냅니다.

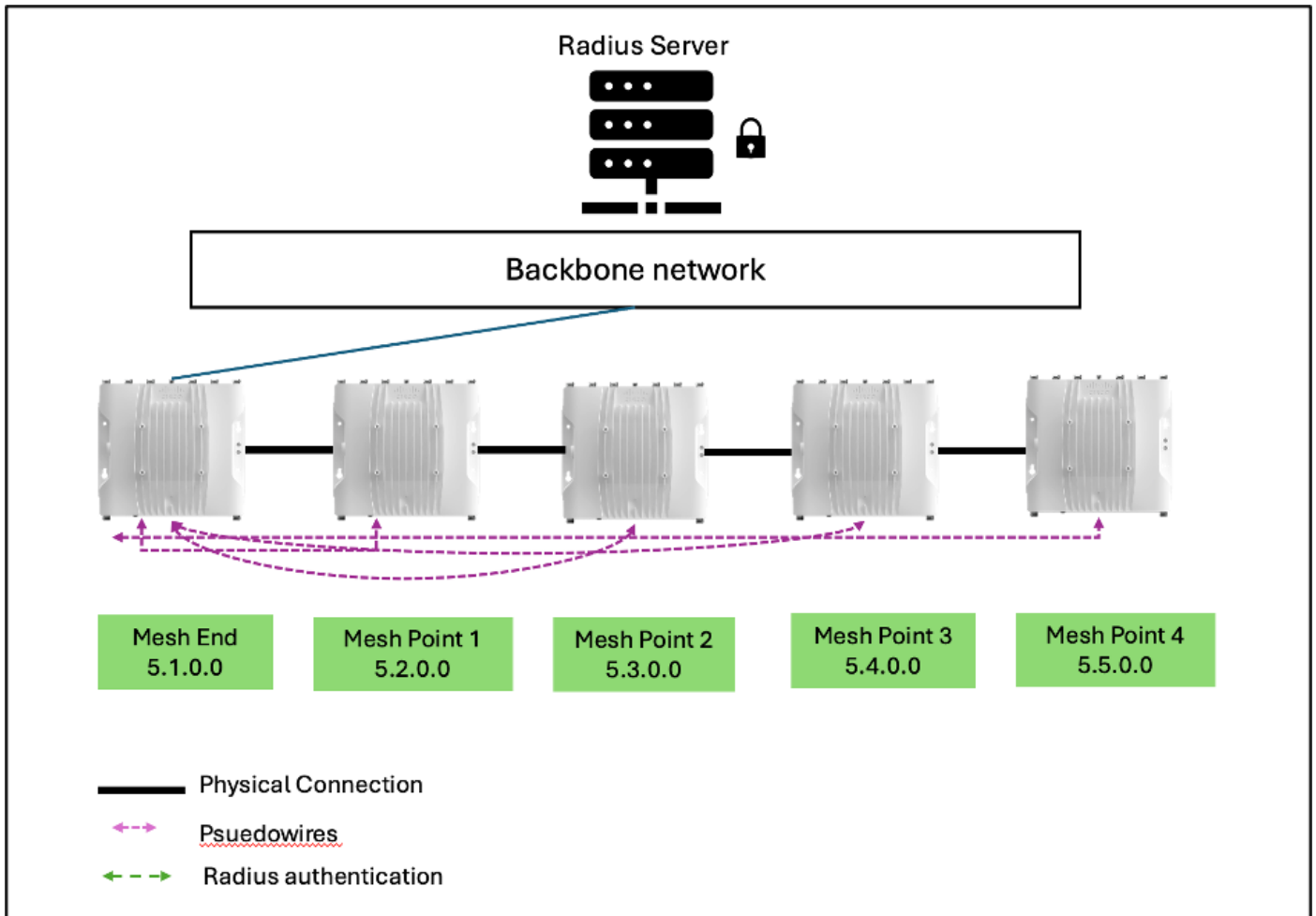
4단계: 메시 엔드, MP 1 및 MP 2가 인증됩니다.



그런 다음 메시 포인트 2가 인증되고 메시 엔드 디바이스와 의사 와이어가 형성되면서 프로세스가 반복됩니다.

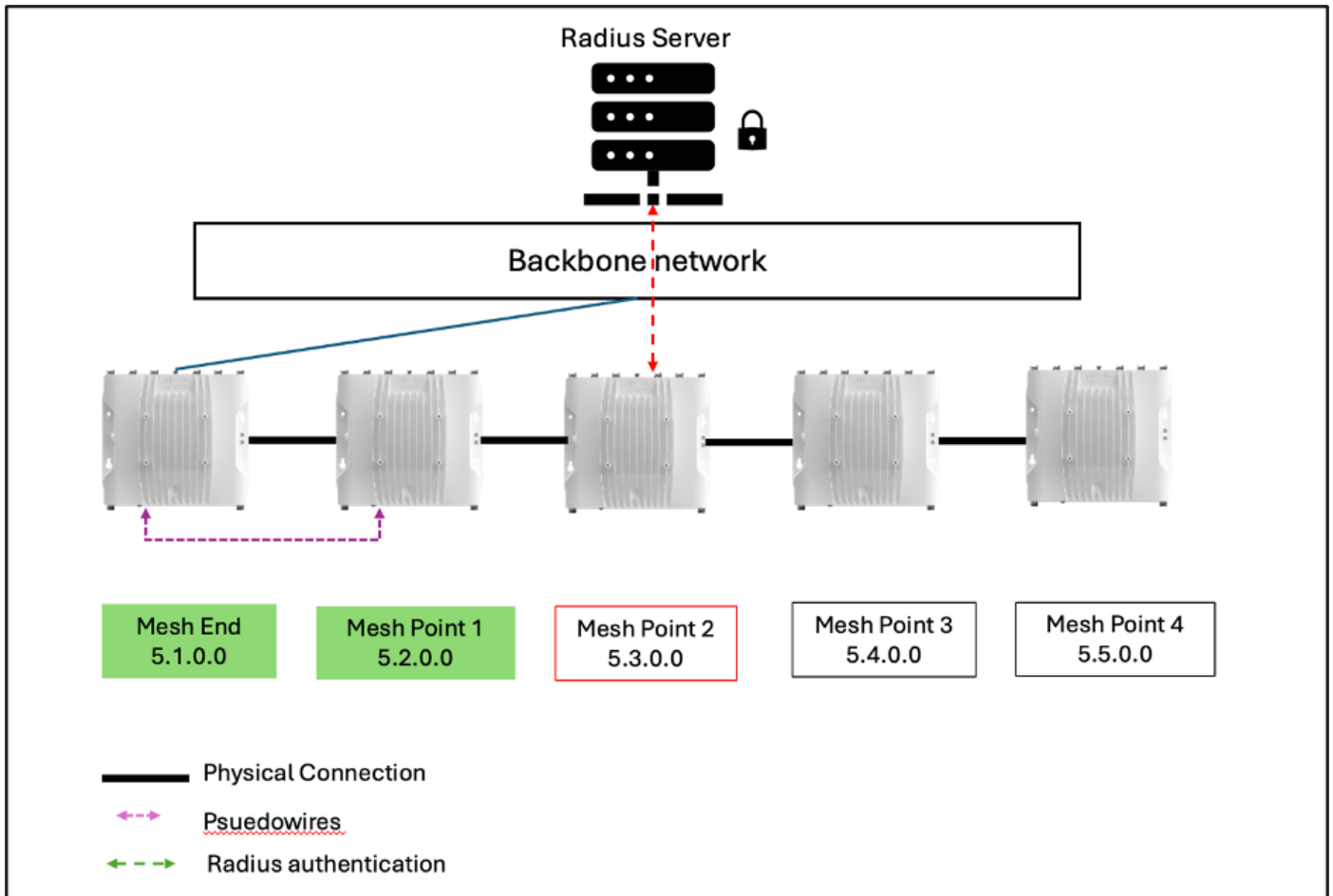
인프라 무선 통신 장치의 나머지 부분은 교대로 최저 메시 ID부터 최고 메시 ID의 순서로 자신을 인증하고 자체 자동 탭이 열리면 이를 인증합니다.

5단계: 모든 무선 장치가 인증됩니다.



잘못된 컨피그레이션 또는 문제 사례:

인프라 메시 포인트에 잘못된 자격 증명이 있거나 실수로 Radius가 비활성화된 경우, 이는 다른 무선 디바이스의 인증에 영향을 줍니다. 라디오를 프로덕션에 배포하기 전에 항상 자격 증명과 설정을 확인하십시오.



이 예에서 메시 포인트 2의 크레드가 잘못되면 인증되지 않은 상태로 유지되며, LNO가 활성화되어 있기 때문에 메시 포인트 3과 메시 포인트 4는 메시 포인트 2로 연결된 의사 와이어가 없으므로 스스로를 인증할 기회를 얻지 못합니다.

인증되지 않은 상태로 유지되는 무선 장치는 잘못 구성된 무선 장치의 메시 ID에 따라 달라집니다. 메시 ID가 현재 유선 코디네이터보다 높은 모든 라디오는 인증되지 않은 상태로 유지되며 문제가 발생합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.