Configuración de RADIUS y LNO en los puntos de acceso inalámbricos industriales en modo URWB

Contenido

Introducción

Este documento describe la configuración de la autenticación RADIUS y la optimización de red grande (LNO) en radios IW9165 e IW9167 en modo URWB.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Navegación y comandos básicos de CLI
- Comprensión de las radios de modo URWB de IW

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Radios IW9165 e IW9167

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

RADIUS: servicio de usuario de acceso telefónico de autenticación remota es un protocolo de red

que se utiliza para proporcionar administración centralizada de autenticación, autorización y cuentas (AAA) para los usuarios o dispositivos que se conectan y utilizan un servicio de red. Para dispositivos inalámbricos industriales en modo URWB, se puede utilizar Radius para autenticar los dispositivos antes de que puedan conectarse a una red.

Los parámetros para la configuración de Radius se pueden configurar en los dispositivos IW desde la GUI o desde el acceso CLI o desde IoT OD también.

Configuración CLI de los parámetros Radius:

Estos parámetros se pueden configurar desde el modo de habilitación en la CLI de los dispositivos.

1. Habilitación de la autenticación Radius:

Este parámetro permite habilitar la autenticación Radius en los dispositivos. Esto se debe ejecutar después de agregar otros parámetros obligatorios requeridos para la autenticación de RADIUS.

Radio1#configure radius enabled

2. Inhabilitación de la autenticación Radius:

Este parámetro permite inhabilitar la autenticación Radius en los dispositivos.

Radio1#configure radius disabled

3. Paso:

Este parámetro sólo se debe configurar en las radios de infraestructura. La configuración de radios de infraestructura con el parámetro passthrough permite que las radios del vehículo se autentiquen a través de las radios de infraestructura, lo que también permite la comunicación entre las radios del vehículo autenticadas y las radios de infraestructura no autenticadas.

Radio1#configure radius passthrough

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

4. Adición del servidor Radius:

Este parámetro se utiliza para especificar la dirección IP del servidor Radius con el que se comunicará el dispositivo.

Radio1#configure radius server

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

5. Puerto de radio:

Este parámetro se utiliza para especificar el puerto del servidor Radius con el que se comunicará el dispositivo. El puerto predeterminado para la autenticación Radius es 1812.

Radio1#configure radius server

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

6. Secreto de radio:

Este parámetro se utiliza para especificar la clave previamente compartida que se utilizará con el servidor Radius.

Radio1#configure radius secret

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

7. IP y puerto del servidor secundario:

Estos parámetros se utilizan para especificar la dirección IP y el número de puerto de un segundo servidor Radius, que se utilizará en caso de que el dispositivo no pueda alcanzar el servidor principal.

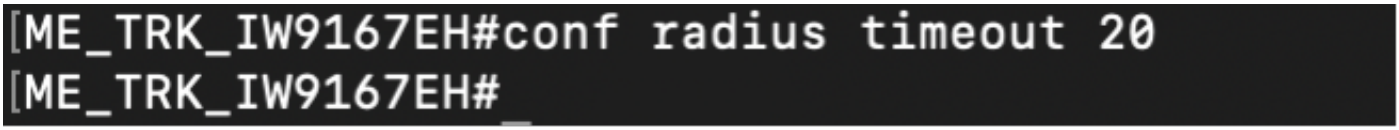
Radio1#configure radius secondary server

Radio1#configure radius secondary port

8. Tiempo de espera de RADIUS:

Este parámetro se utiliza para especificar la cantidad de tiempo en segundos que el cliente esperará una respuesta del servidor Radius principal, antes de intentar conectarse al servidor secundario. El valor predeterminado se establece en 10 segundos.

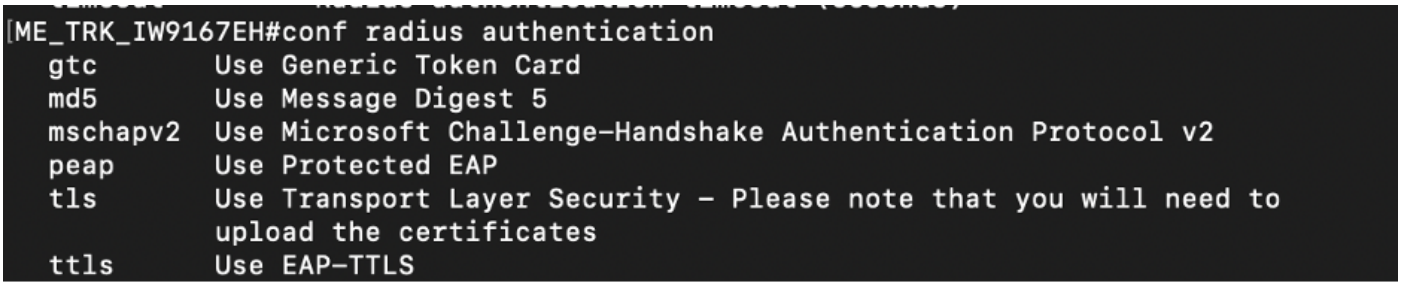
Radio1#configure radius timeout



9. Parámetros de autenticación:

Este parámetro se utiliza para especificar el método de autenticación Radius y los parámetros correspondientes que se van a pasar. Hay varias opciones para utilizar.

Radio1#configure radius authentication



Si utiliza estos métodos: GTC (Generic token card), MD5 (Message-Digest Algorithm 5) o MSCHAPV2 (Microsoft Challenge Handshake Authentication Protocol versión 2), tanto el nombre de usuario como la contraseña se pueden agregar con estos comandos:

Radio1#configure radius authentication gtc

Radio1#configure radius authentication md5

Radio1#configure radius authentication mschapv2

Si utiliza estos métodos: PEAP (protocolo de autenticación extensible protegido) o EAP-TTLS (protocolo de autenticación extensible-seguridad de capa de transporte en túnel) para la autenticación, también se debe proporcionar otro método de autenticación interna. Puede ser gtc, md5 o mschapv2.

Radio1#configure radius authentication peap

inner-auth-method

Radio1#configure radius authentication ttls

inner-auth-method

10. Intentos de cambio:

Este parámetro especifica el número de intentos de autenticación de RADIUS permitidos hacia el servidor primario antes de que el cliente cambie al servidor secundario. El valor predeterminado es 3.

Radio1#configure radius switch <1-6>

11. Tiempo de espera:

Este parámetro especifica el valor del tiempo en segundos que el cliente debe esperar, después de superar el número máximo de intentos de autenticación.

Radio1#configure radius backoff-time

12. Plazo de expiración:

Este parámetro especifica el valor de tiempo en segundos si durante el cual la autenticación Radius no está completa, el intento de autenticación se abandonará.

Radio1#configure radius expiration

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

13. Enviar solicitud:

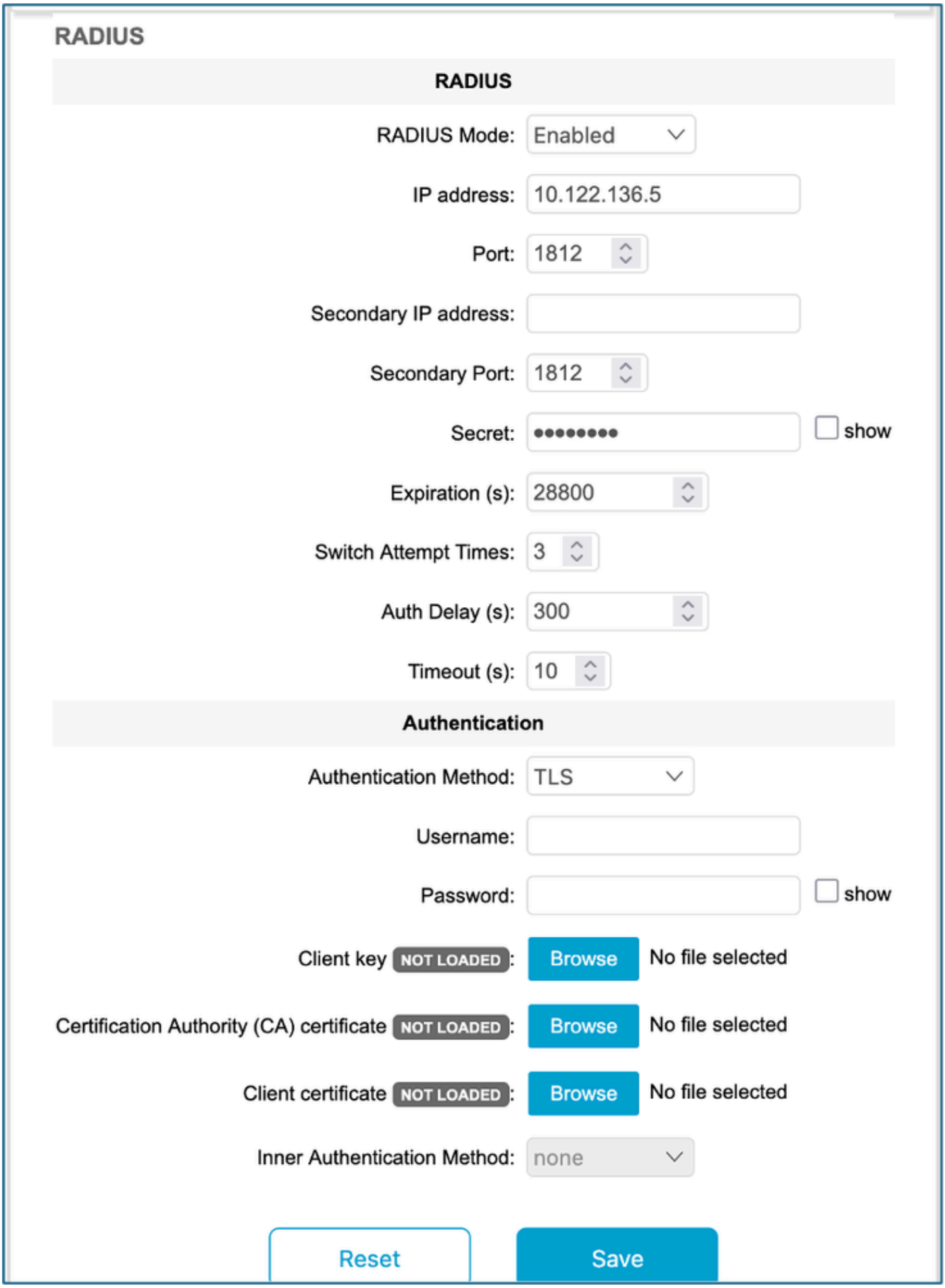
Este parámetro se utiliza para iniciar una solicitud de autenticación de RADIUS para el servidor Radius principal o secundario configurado.

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).
```

Los mismos parámetros se pueden configurar en las radios inalámbricas industriales en modo URWB mediante la GUI, así como en la ficha ‘Radius’ de la página web.



Comandos show:

La configuración actual de Radius se puede verificar a través de CLI con los comandos show.

1.

#show RADIUS

Este comando show indica si Radius está activado o desactivado en el dispositivo.

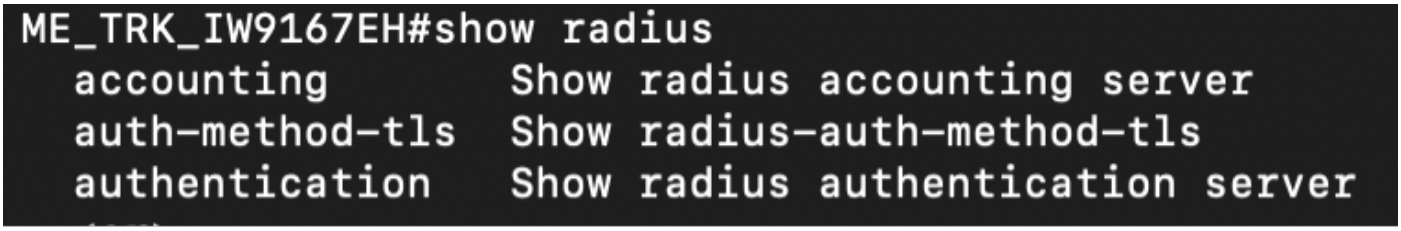
2.

#show radius accounting

#show radius auth-method-tls

Autenticación RADIUS #show

Estos comandos show mostrarán la configuración actual del servidor de contabilización de RADIUS, el servidor de autenticación y los parámetros tls del método de autenticación configurados.



Secuencia de autenticación de RADIUS con LNO

La optimización de redes grandes o LNO es una función que se recomienda habilitar en redes grandes con 50 o más radios de infraestructura para optimizar la formación de pseudowire entre todos los dispositivos de la red. Se utiliza tanto en redes de capa 2 como en redes de capa 3.

En las redes en las que se habilitan LNO y Radius, las radios de infraestructura se autentican a sí mismas secuencialmente (desde la ID de malla más baja a la ID de malla más alta). Al habilitar LNO, todas las radios de la infraestructura se verán obligadas a construir pseudowires SOLAMENTE en el extremo de la malla y también se desactivará el reenvío de BPDU.

En este artículo se describe la secuencia de autenticación Radius en una configuración de fluidez con un extremo de malla y 4 radios de infraestructura de punto de malla.

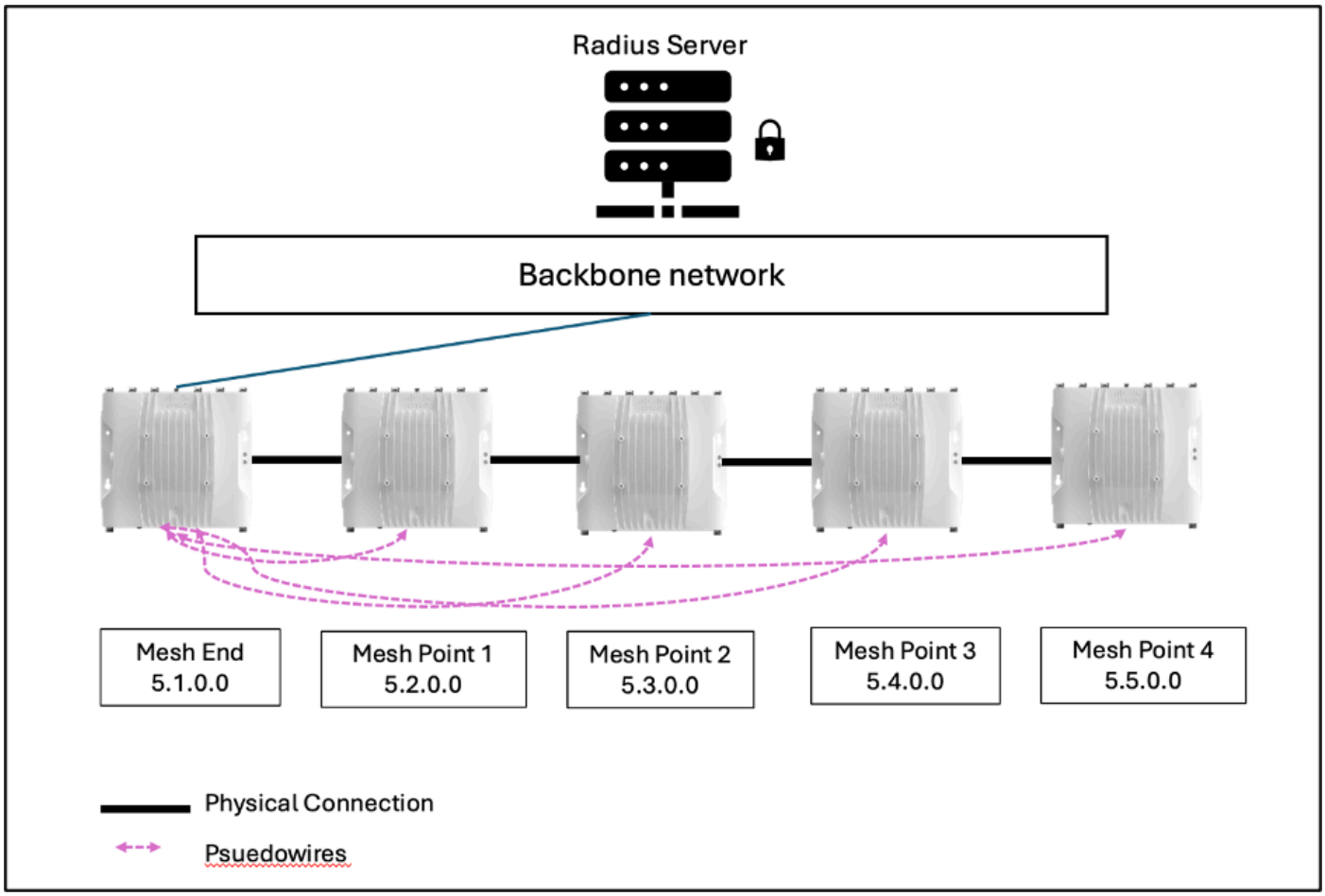
La radio Mesh End es el "coordinador con cables" predeterminado de la red Fluidity. Esto significa que tiene abierto su teclado automático y actúa como punto de entrada/salida de la red.

Todas las demás radios de infraestructura se configuran como puntos de malla y todas tienen conexión física con el extremo de malla a través de switches que están conectados entre sí.

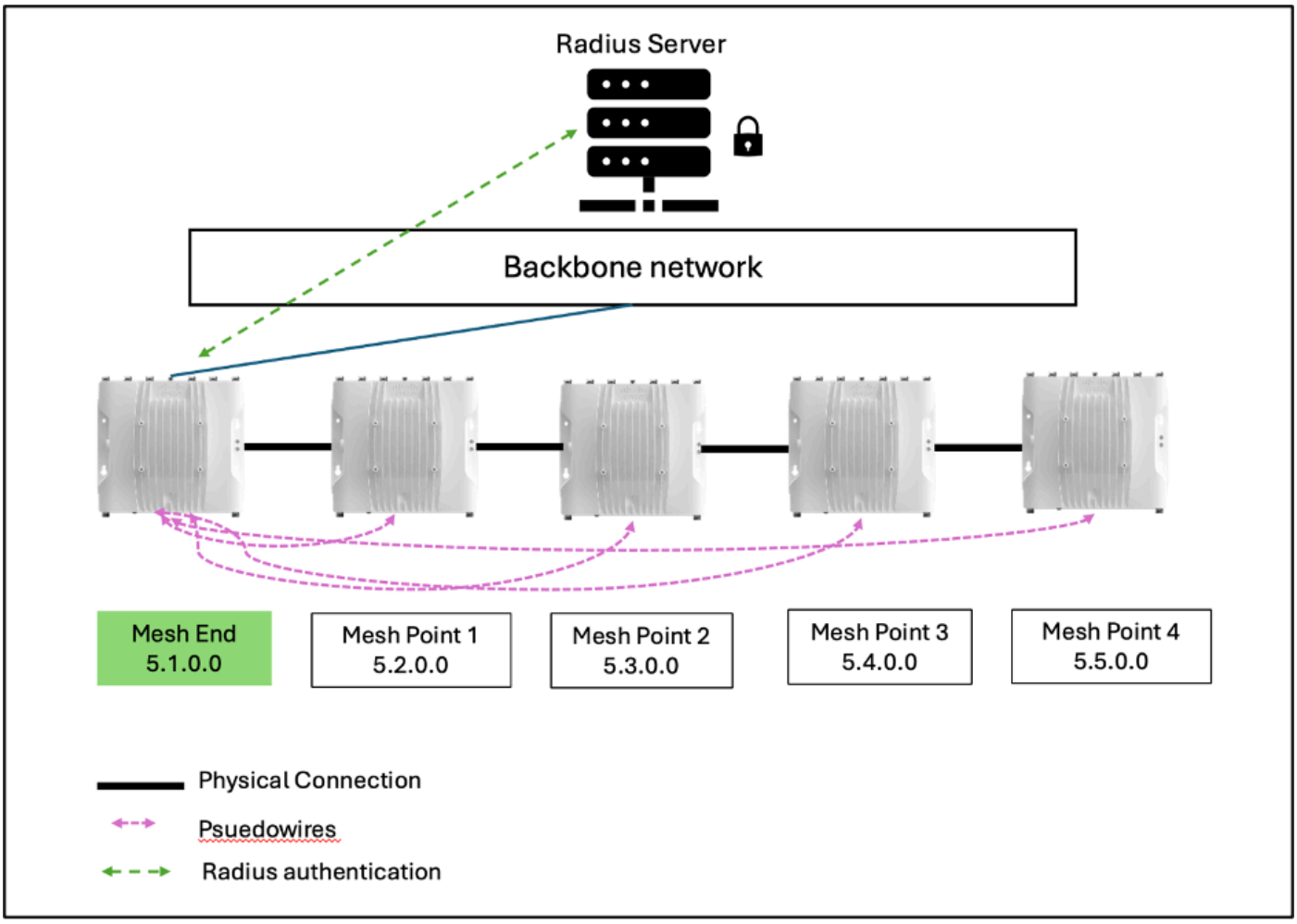
La radio de extremo de malla está conectada a la red de estructura básica generalmente a través de una conexión de fibra y a través de la red de estructura básica, puede alcanzar el servidor Radius de la red.

Cualquier dispositivo sólo puede alcanzar el servidor Radius si:

1. Se trata de un coordinador por cable.
2. Tiene un pseudowire construido con el cableado principal, es decir, el extremo de malla.



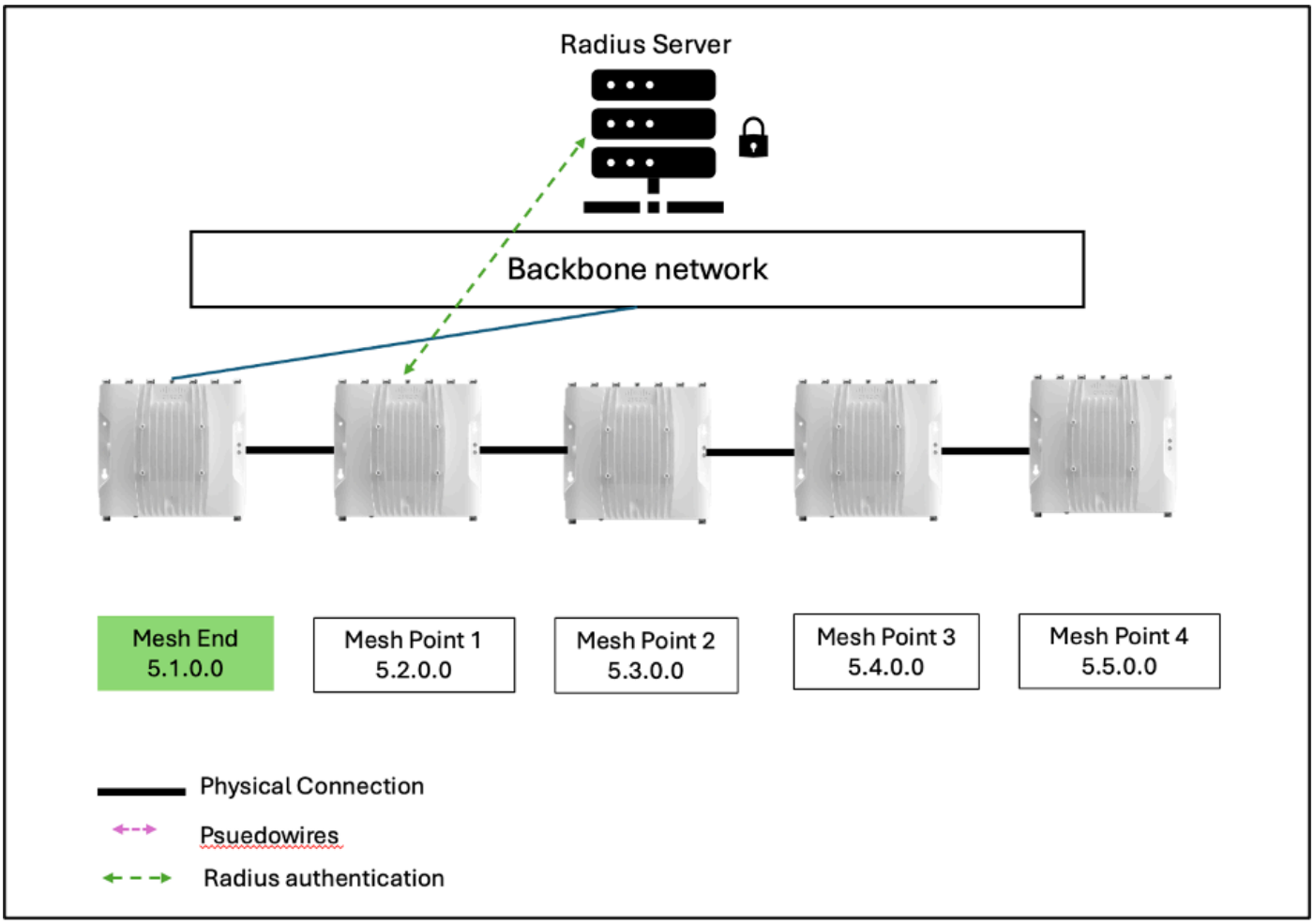
Paso 1: Todas las unidades no están autenticadas.



Al principio, todas las unidades, incluido el extremo de malla, no se autenticarán. El autotap se abrirá solamente en la radio de fin de malla que es el punto de ingreso/egreso de toda la red. Para que cualquier dispositivo de infraestructura llegue al servidor Radius para autenticarse, debe ser un extremo de malla o tener un pseudowire en el extremo de malla.

Ahora, la radio de extremo de malla 5.1.0.0 enviará una solicitud de autenticación al servidor Radius a través de la red troncal. Una vez que recibe la comunicación de vuelta, se autentica y luego se vuelve "invisible" para el resto de los puntos de malla de infraestructura no autenticados, como es el requisito para AAA con Radius.

Paso 2: El extremo de malla 5.1.0.0 está autenticado, el resto no está autenticado.

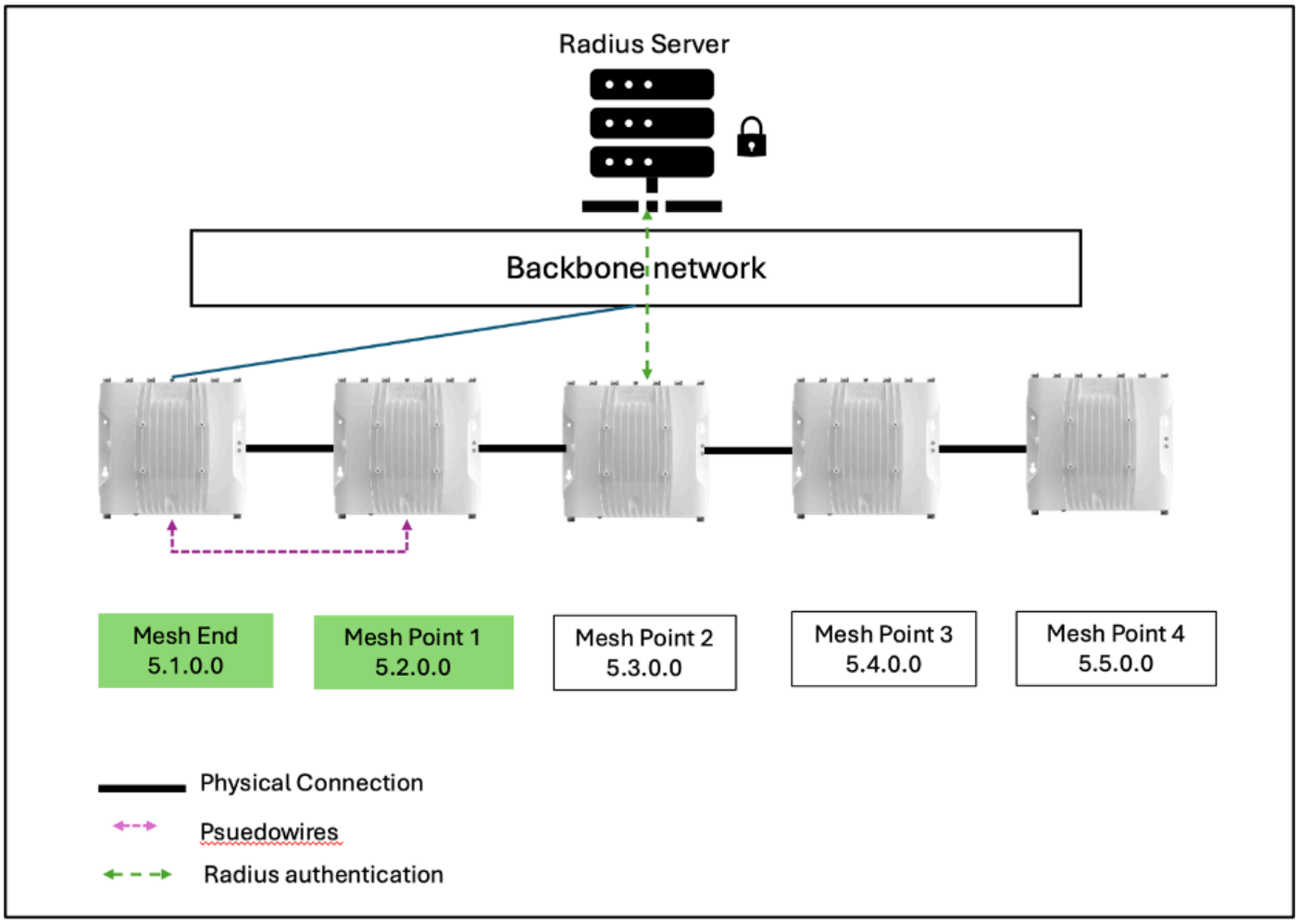


Ahora que el extremo de malla 5.1.0.0 está autenticado e invisible para el resto de la red, los puntos de malla restantes realizarán una elección y elegirán el dispositivo con el ID de malla más bajo para ser el siguiente coordinador cableado. En este ejemplo, sería Punto de malla 1 con ID de malla 5.2.0.0. El Ajuste automático se abrirá en el Punto de malla 1.

Debido a que LNO está habilitado, no se formará ningún Pseudowire en el Punto de malla 1. Todas las radios restantes tendrán que autenticarse secuencialmente cuando su Autotap esté abierto.

Ahora, el punto de malla 1 puede enviar una solicitud de autenticación al servidor Radius y autenticarse a sí mismo.

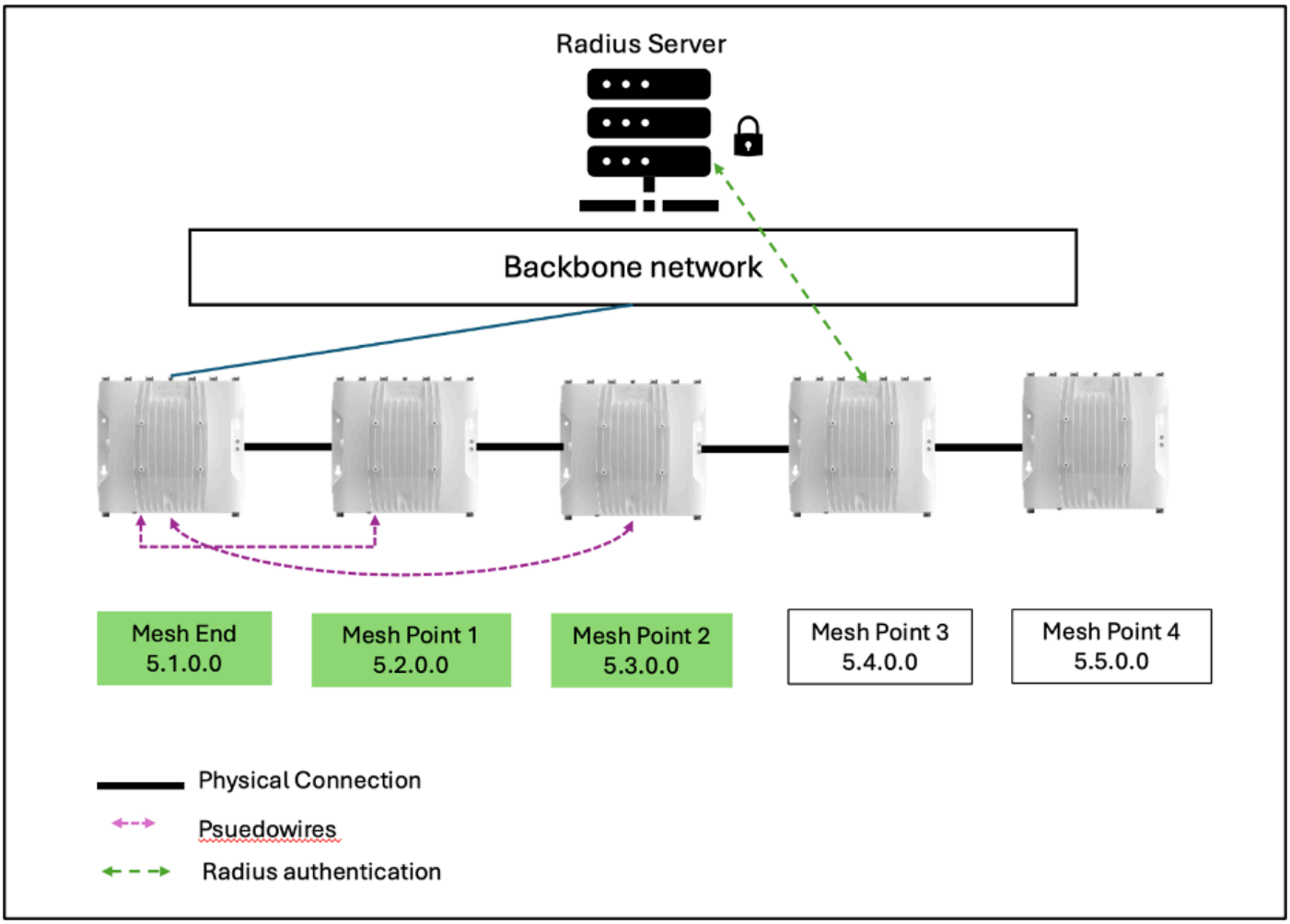
Paso 3: Extremo de malla, Punto de malla 1 se autentica y otros no se autentican.



Ahora que el punto de malla 1 también está autenticado, formará un psuedowire con el extremo de malla autenticado y también se volverá invisible para el resto de las radios de infraestructura no autenticadas.

El resto de las radios no autenticadas vuelven a ejecutar la elección y eligen el Punto de malla 2 con el ID de malla más bajo 5.3.0.0 como el nuevo coordinador con cable y esa radio envía una solicitud de autenticación al servidor Radius ya que su Autotap está ahora abierto.

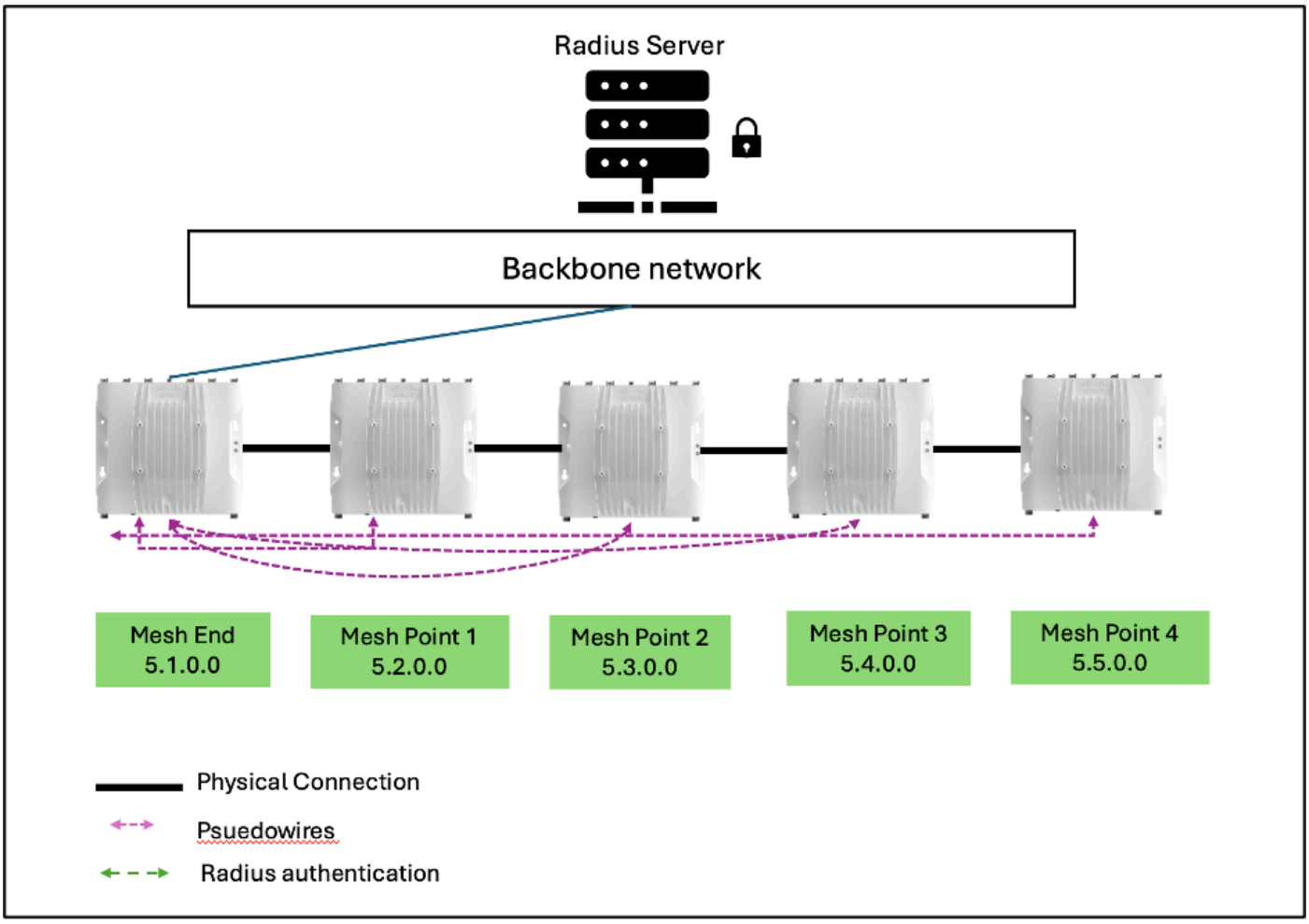
Paso 4: Fin de malla, MP 1 y MP 2 están autenticados.



A continuación, el proceso se repite con el punto de malla 2 que se autentica y forma Pseudowire con el dispositivo de extremo de malla.

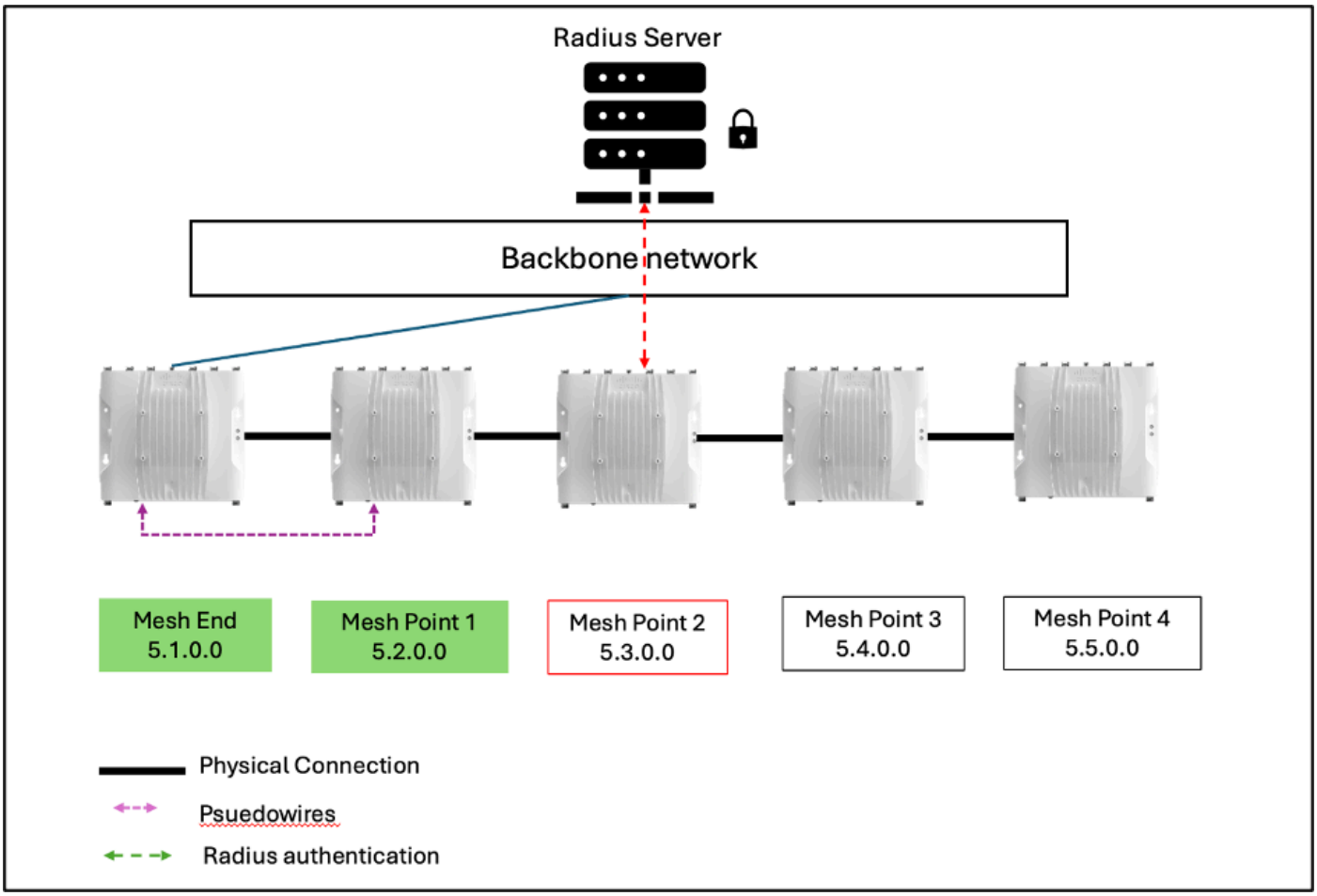
El resto de las radios de infraestructura se turnan para autenticarse, en el orden de ID de malla de menor a mayor, cuando se abre su propio autotap.

Paso 5: Todas las radios están autenticadas.



Configuración incorrecta o casos problemáticos:

Si alguno de los puntos de malla de infraestructura tiene credenciales erróneas o tiene Radius desactivado por error, esto afectará a otras radios de la autenticación. Asegúrese siempre de comprobar las credenciales y la configuración antes de implementar radios en producción.



En este ejemplo, si el punto de malla 2 tiene credenciales erróneas, permanecerá sin autenticar y, a su vez, el punto de malla 3 y el punto de malla 4 nunca tendrán la oportunidad de autenticarse a sí mismos, ya que no hay un Pseudowire formado a partir de ellos en el punto de malla 2 debido a la activación de LNO.

Las radios que permanecen sin autenticar dependen de la ID de malla de la radio configurada incorrectamente. Cualquier radio con ID de malla superior al coordinador con cable actual permanecerá sin autenticar y causará problemas.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).