Configurar o RADIUS e o LNO em pontos de acesso sem fio industriais no modo URWB

Contents

[Introdução](#)

[Pré-requisitos](#)

- [Requisitos](#)
- [Componentes Utilizados](#)

[Informações de Apoio](#)

[Sequência de autenticação Radius com LNO](#)

Introdução

Este documento descreve a configuração da autenticação RADIUS e da otimização de rede de grande porte (LNO) nos rádios IW9165 e IW9167 no modo URWB.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Navegação e comandos CLI básicos
- Compreensão dos rádios do modo IW URWB

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Rádios IW9165 e IW9167

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

RADIUS - Remote Authentication Dial-In User Service é um protocolo de rede usado para fornecer gerenciamento centralizado de autenticação, autorização e tarifação (AAA - Authentication Dial-In User Service) para usuários ou dispositivos que se conectam e usam um serviço de rede. Para dispositivos sem fio industriais no modo URWB, o Radius pode ser usado

para autenticar dispositivos antes que eles possam se unir a uma rede.

Os parâmetros para a configuração do Radius podem ser configurados nos dispositivos de IW a partir da GUI ou do acesso à CLI ou também a partir do IoT OD.

Configuração CLI dos parâmetros Radius:

Esses parâmetros podem ser configurados no modo de ativação (enable mode) no CLI dos dispositivos.

1. Ativação da autenticação Radius:

Esse parâmetro permite ativar a autenticação Radius nos dispositivos. Isso deve ser executado após a adição de outros parâmetros obrigatórios necessários para a autenticação radius.

Radio1#configure radius enabled

2. Desativando a autenticação Radius:

Este parâmetro permite desativar a autenticação Radius nos dispositivos.

Radio1#configure radius disabled

3. Passagem:

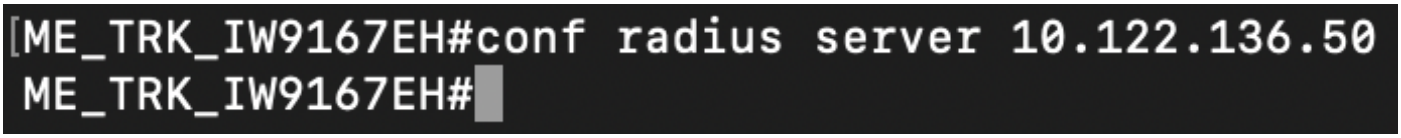
Esse parâmetro deve ser configurado somente nos rádios de infraestrutura. A configuração de rádios de infraestrutura com parâmetro de passagem permite que os rádios de veículo se autentiquem através dos rádios de infraestrutura, permitindo também a comunicação entre os rádios de veículo autenticados e os rádios de infraestrutura não autenticados.

Radio1#configure radius passthrough

4. Adicionando Servidor Radius:

Esse parâmetro é usado para especificar o endereço IP do servidor Radius com o qual o dispositivo deve se comunicar.

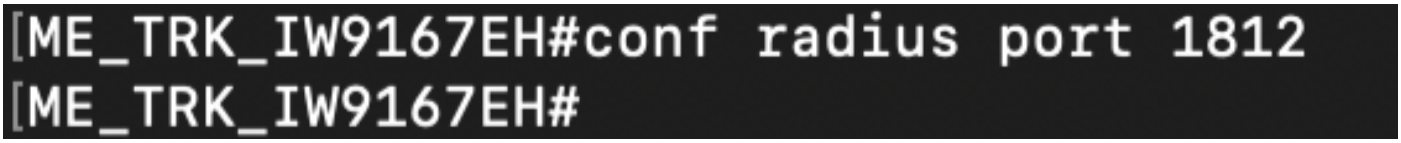
Radio1#configure radius server



5. Porta de raio:

Esse parâmetro é usado para especificar a porta do servidor Radius com a qual o dispositivo deve se comunicar. A porta padrão para autenticação Radius é 1812.

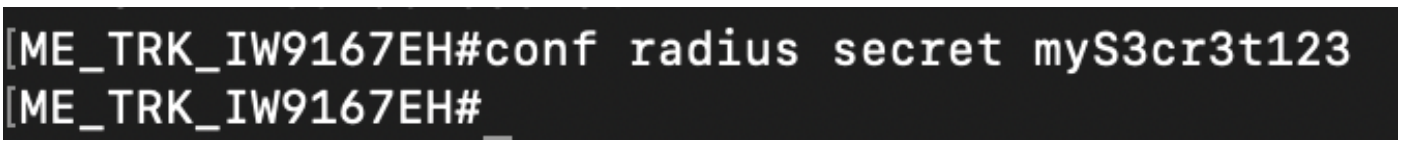
Radio1#configure radius server



6. Radius Secret:

Esse parâmetro é usado para especificar a chave pré-compartilhada a ser usada com o servidor Radius.

Radio1#configure radius secret



7. IP e porta do servidor secundário:

Esses parâmetros são usados para especificar o endereço IP e o número de porta de um segundo servidor Radius, a ser usado caso o dispositivo não consiga acessar o servidor primário.

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. Tempo limite do raio:

Este parâmetro é usado para especificar o tempo em segundos que o cliente aguardará por uma resposta do servidor Radius primário antes de tentar se conectar ao servidor secundário. O valor padrão é definido como 10 segundos.

Radio1#configure radius timeout

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

9. Parâmetros de autenticação:

Este parâmetro é usado para especificar o método de autenticação Radius e os parâmetros correspondentes a serem passados. Há várias opções para usar.

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
```

Se estiver usando estes métodos: GTC (Generic token card), MD5 (Message-Digest Algorithm 5) ou MSCHAPV2 (Microsoft Challenge Handshake Authentication Protocol version 2), o nome de usuário e a senha podem ser adicionados com estes comandos:

Radio1#configure radius authentication gtc

Radio1#configure radius authentication md5

Radio1#configure radius authentication mschapv2

Se estiver usando estes métodos: PEAP (Protected Extensible Authentication Protocol) ou EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) para a autenticação, então outro método de autenticação interna também deve ser fornecido. Pode ser gtc, md5 ou mschapv2.

Radio1#configure radius authentication peap

inner-auth-method

Radio1#configure radius authentication ttls

inner-auth-method

10. Tentativas de comutação:

Esse parâmetro especifica o número de tentativas de autenticação radius permitidas em direção ao servidor primário antes que o cliente alterne para o servidor secundário. O valor padrão é 3.

Radio1#configure radius switch <1-6>

11. Tempo de recuo:

Esse parâmetro especifica o valor de tempo em segundos para o cliente aguardar, depois de exceder o número máximo de tentativas de autenticação.

Radio1#configure radius backoff-time

12. Tempo de expiração:

Este parâmetro especifica o valor de tempo em segundos se, durante o qual a autenticação Radius não for concluída, a tentativa de autenticação será abandonada.

Radio1#configure radius expiration

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

13. Enviar solicitação:

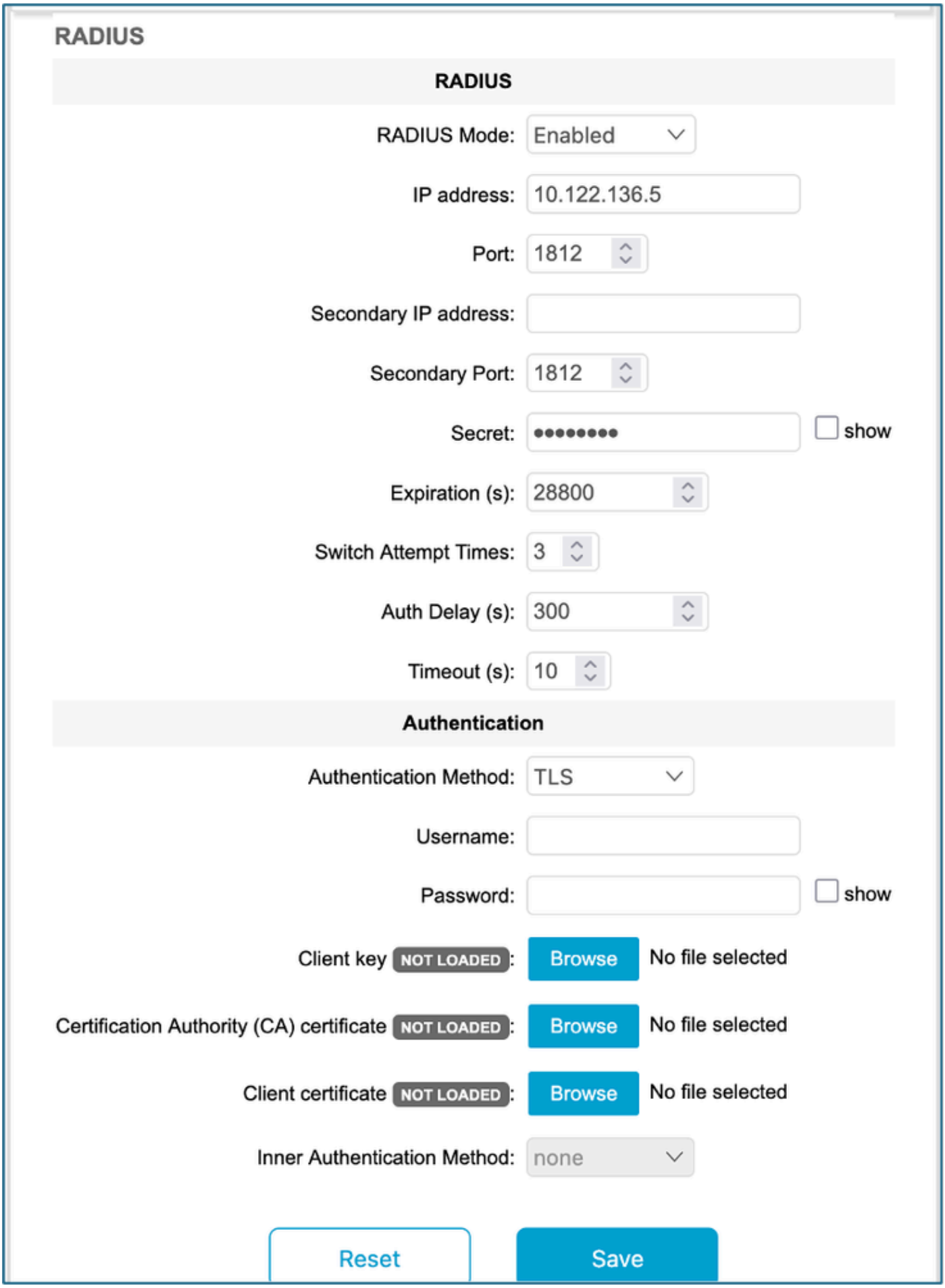
Este parâmetro é usado para iniciar uma solicitação de autenticação radius para o servidor Radius primário ou secundário configurado.

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).
```

Os mesmos parâmetros podem ser configurados nos rádios sem fio industriais no modo URWB via GUI, bem como na guia "Radius" na página Web.



Comandos show:

A configuração atual do Radius pode ser verificada via CLI com comandos show.

1.

raio de #show

Este comando show informa se o Radius está ativado ou desativado no dispositivo.

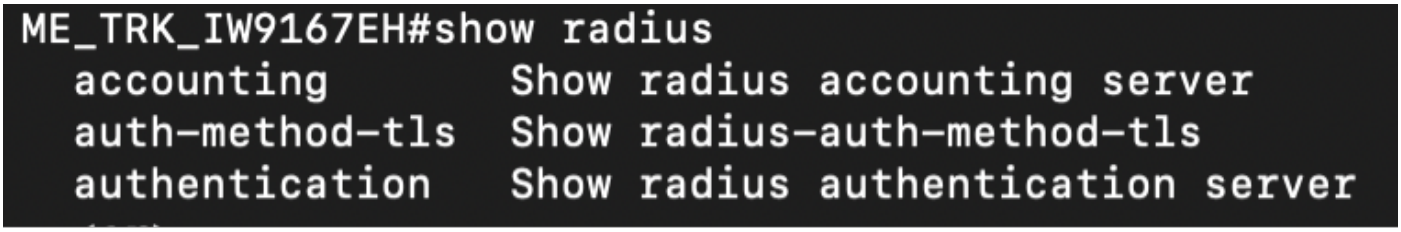
2.

contabilidade de raio de #show

#show radius auth-method-tls

autenticação #show radius

Esses comandos show mostrarão a configuração atual do servidor de contabilização radius, do servidor de autenticação e os parâmetros tls do método de autenticação configurados.



Sequência de autenticação Radius com LNO

LNO ou Otimização de Rede Grande é um recurso sugerido para ser habilitado em redes grandes com 50 ou mais rádios de Infraestrutura para otimizar a formação de pseudofios entre todos os dispositivos na rede. É usado em redes de Camada 2 e Camada 3.

Em redes onde LNO e Radius estão ativados, os rádios de infraestrutura autenticam-se sequencialmente (do menor ID de malha para o maior ID de malha). Habilitar o LNO forçará todos os rádios de infraestrutura a criarem pseudofios SOMENTE para a extremidade da malha e desabilitará também o encaminhamento de BPDU.

Este artigo descreverá a sequência de autenticação Radius em uma configuração de fluidez com rádios de infraestrutura de extremidade de malha e ponto de malha 4.

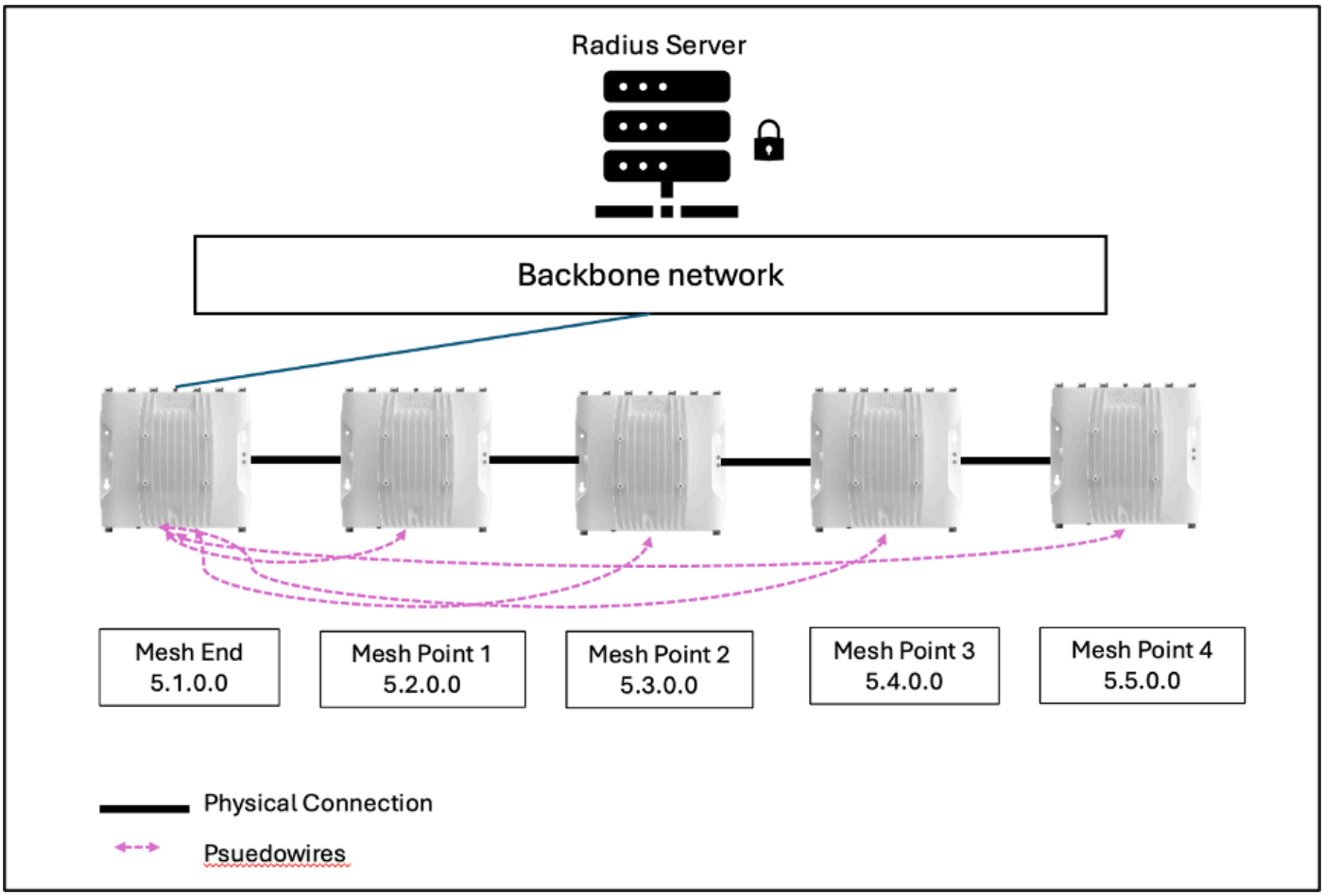
O rádio Mesh End é o "coordenador com fio" padrão da rede Fluidity. Isso significa que ele tem o toque automático aberto e atua como o ponto de entrada/saída da rede.

Todos os outros rádios de infraestrutura são configurados como pontos de malha e todos têm conexão física com a extremidade de malha por meio de switches conectados entre si.

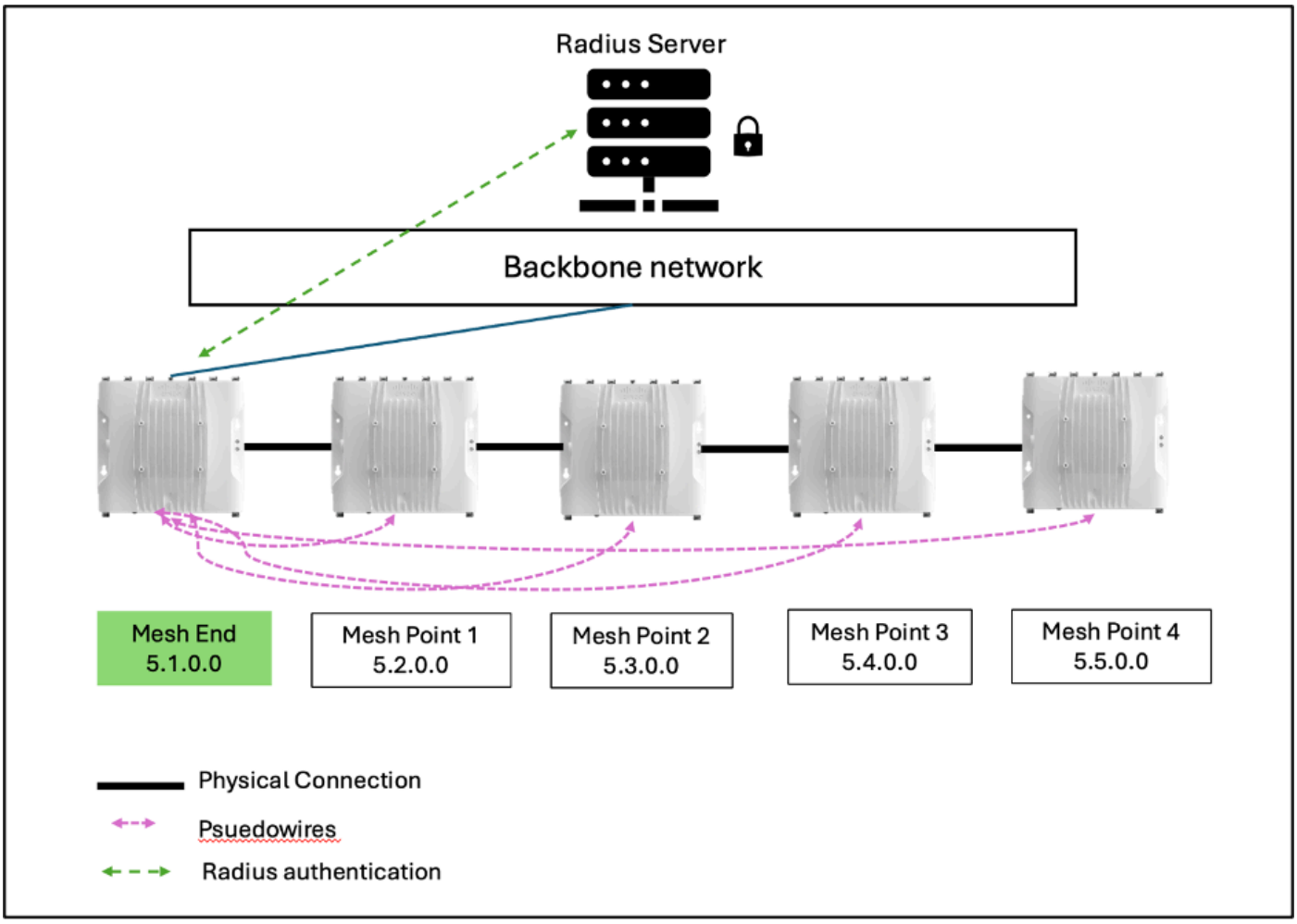
O rádio da extremidade da malha é conectado à rede de backbone geralmente através de conexão de fibra e através da rede de backbone, ele pode alcançar o servidor Radius da rede.

Qualquer dispositivo pode acessar o servidor Radius somente se:

1. É um coordenador com fio.
2. Ele tem um pseudofio construído com o mestre com fio, ou seja, Mesh End.



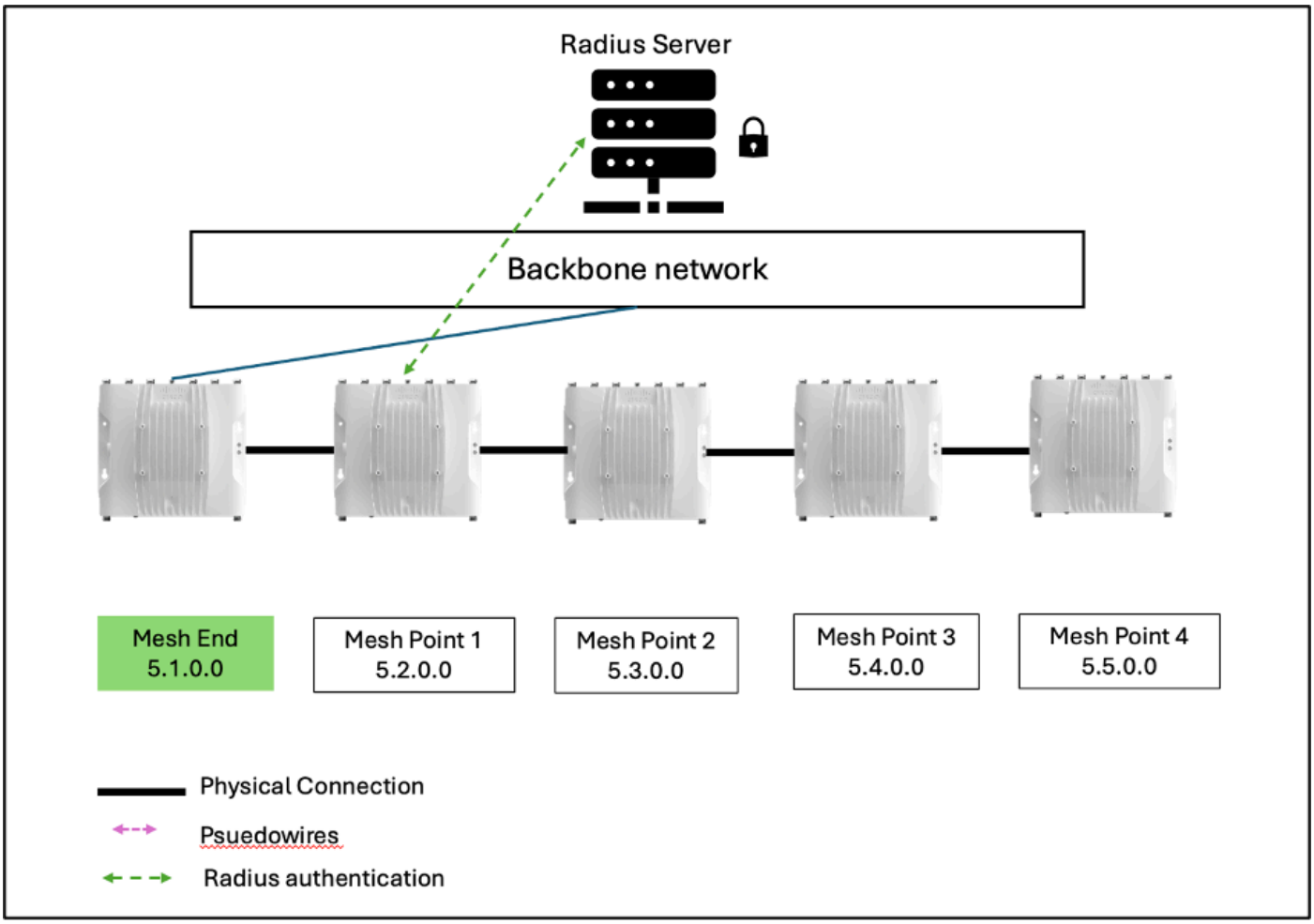
Passo 1: Todas as unidades não são autenticadas.



No início, todas as unidades, incluindo a extremidade da malha, não serão autenticadas. O toque automático será aberto apenas no rádio Mesh End, que é o ponto de entrada/saída de toda a rede. Para que qualquer dispositivo de infraestrutura acesse o servidor Radius para se autenticar, ele deve ser uma extremidade de malha ou ter um pseudofio para a extremidade de malha.

Agora, o rádio Mesh End 5.1.0.0 enviará uma solicitação de autenticação ao servidor Radius através da rede de backbone. Quando recebe a comunicação de volta, ele é autenticado e torna-se "invisível" para o restante dos pontos de malha de infraestrutura não autenticados, como é o requisito para AAA com Radius.

Passo 2: A extremidade da malha 5.1.0.0. é autenticada, o restante não é autenticado.

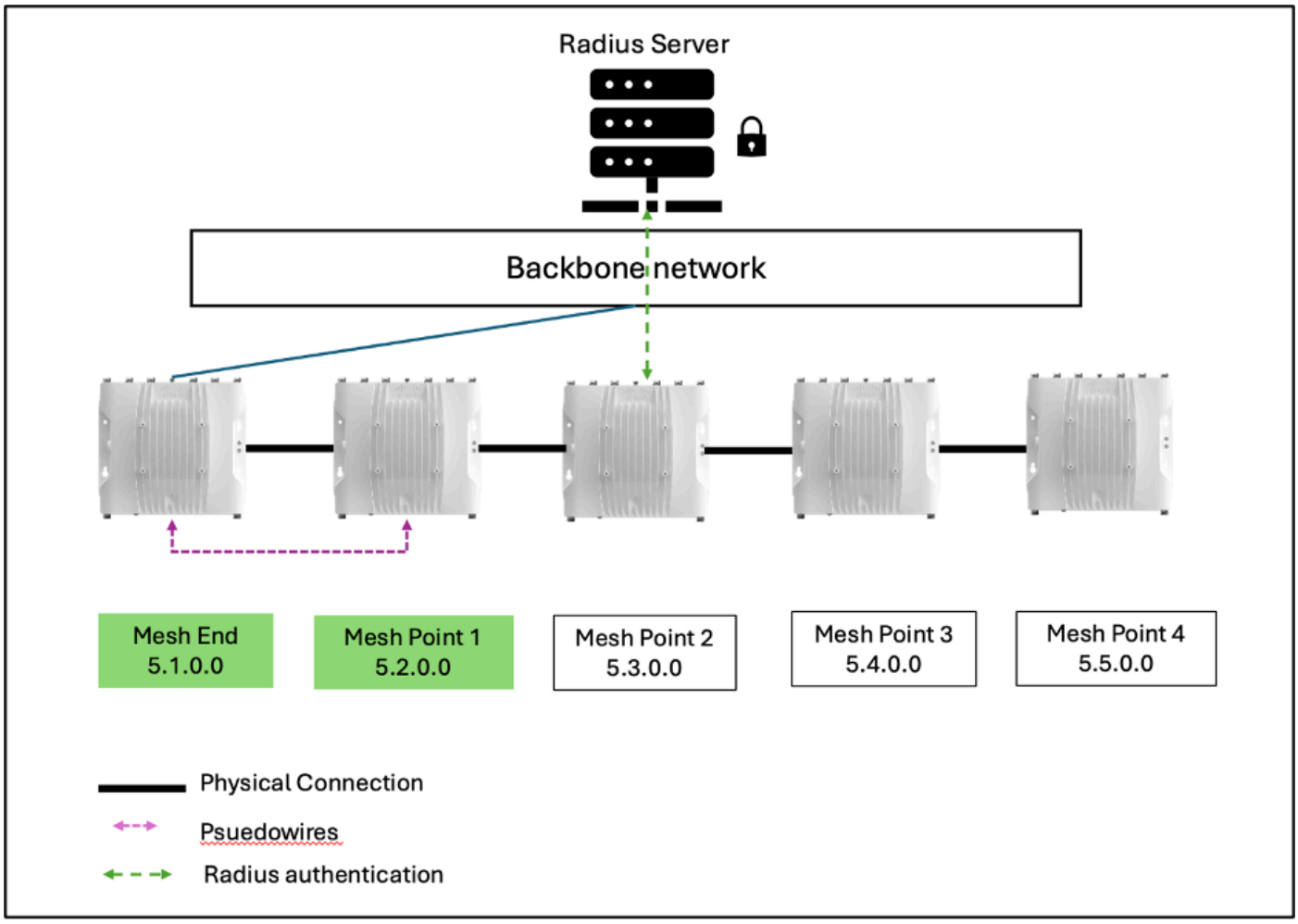


Agora que a extremidade da malha 5.1.0.0 é autenticada e invisível para o resto da rede, os pontos de malha restantes executarão uma eleição e escolherão o dispositivo com menor ID de malha como o próximo coordenador com fio. Neste exemplo, seria Mesh Point 1 com Mesh ID 5.2.0.0. Autotap será então aberto em Mesh Point 1.

Devido ao LNO estar habilitado, nenhum Pseudofio se formará no Ponto de Malha 1. Todos os rádios restantes terão que se autenticar sequencialmente quando seu Autotap estiver aberto.

Agora, o Mesh Point 1 pode enviar uma solicitação de autenticação ao servidor Radius e se autenticar.

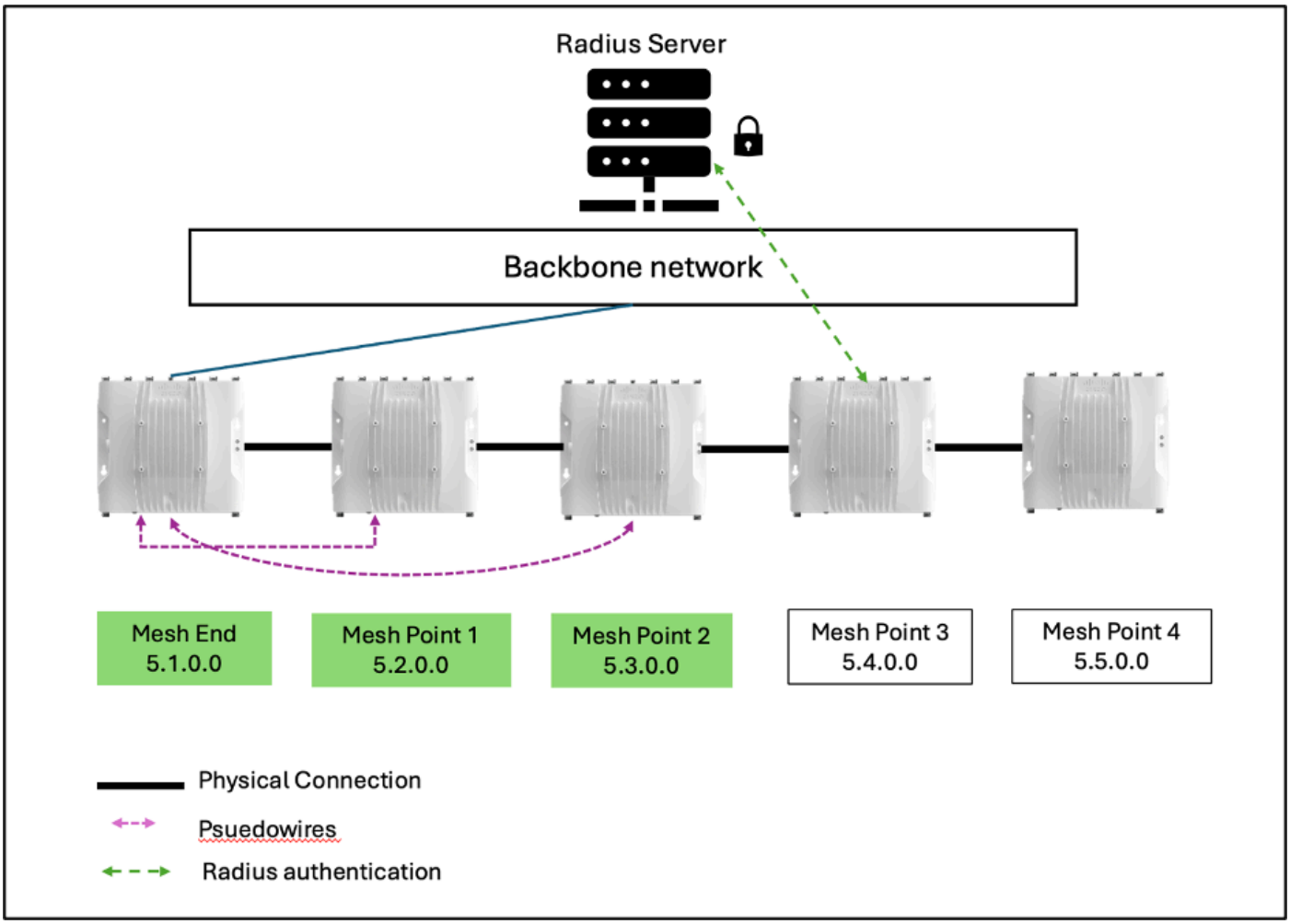
Passo 3: A extremidade da malha, o ponto de malha 1 é autenticado e outros não são autenticados.



Agora que o Ponto de malha 1 também está autenticado, ele formará um psuedowire com a Extremidade de malha autenticada e também se tornará invisível para o restante dos rádios de infraestrutura não autenticados.

O restante dos rádios não autenticados executa novamente a eleição e seleciona Ponto de malha 2 com o ID de malha mais baixo 5.3.0.0 como o novo coordenador com fio e esse rádio envia uma solicitação de autenticação ao servidor Radius, pois seu Autotap está agora aberto.

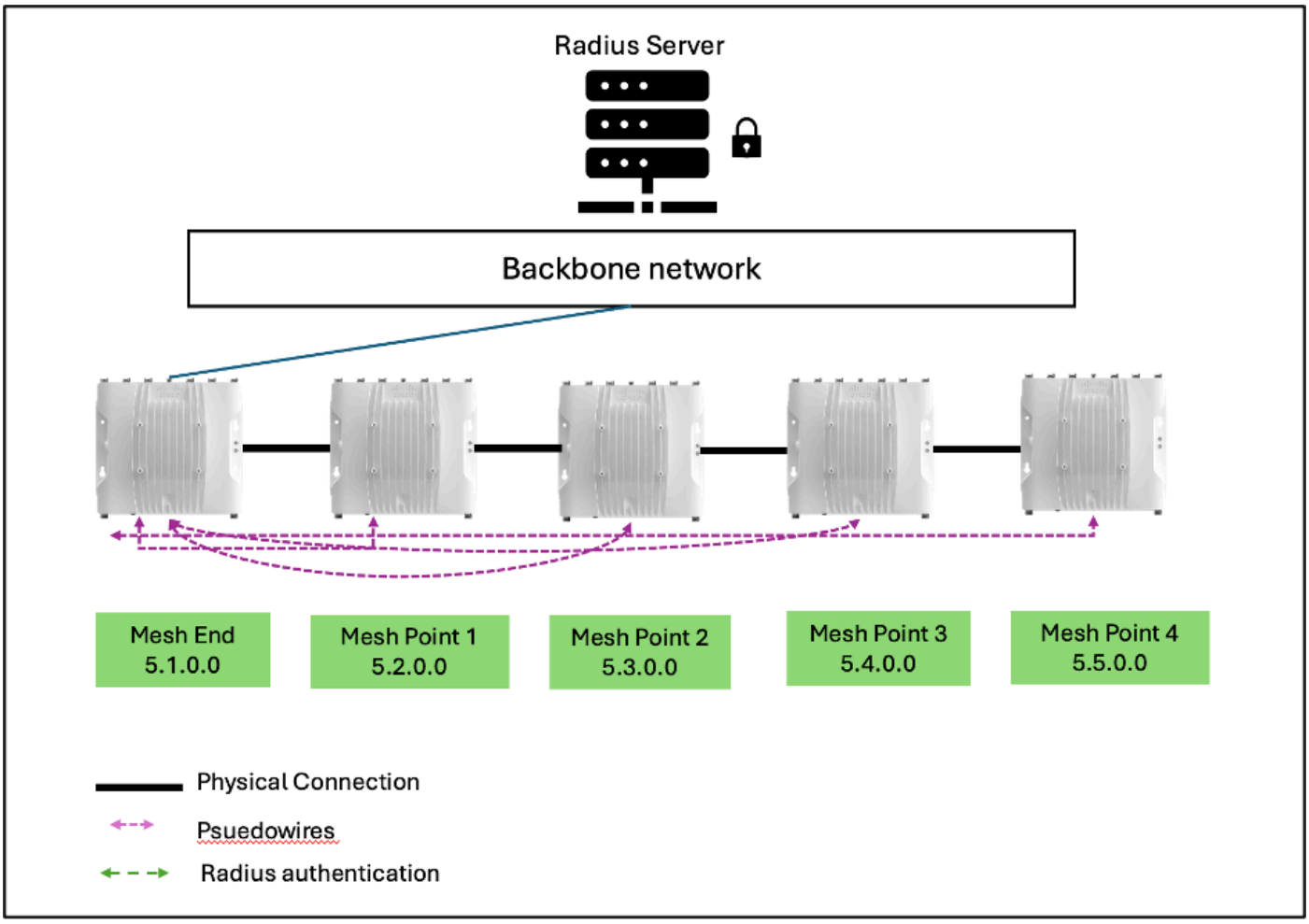
Passo 4: Fim de malha, MP 1 e MP 2 são autenticados.



O processo então se repete com o Ponto de malha 2 tornando-se autenticado e formando Pseudowire com o dispositivo final de malha.

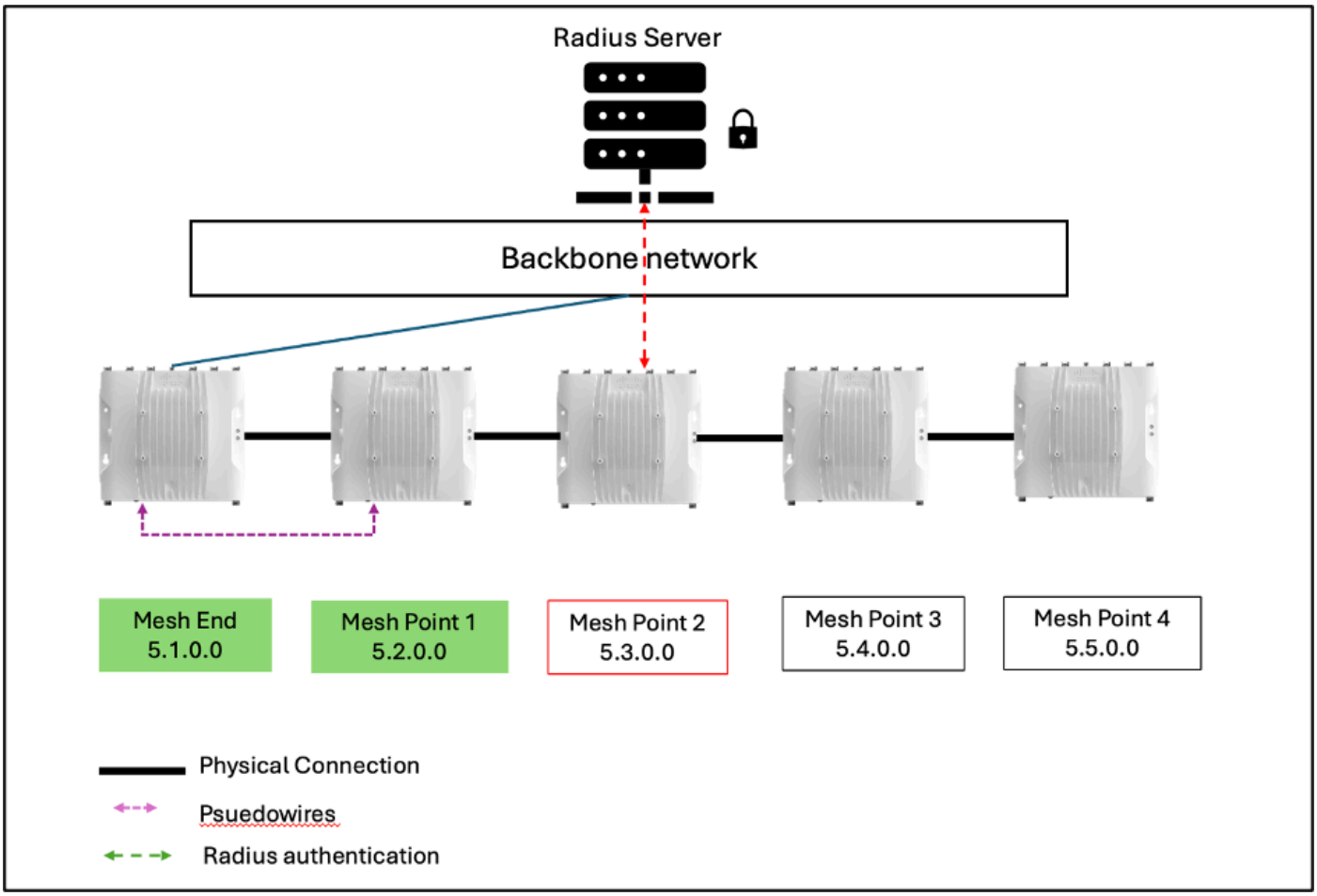
O restante dos rádios de infraestrutura se revezam para se autenticar, na ordem de IDs de malha do mais baixo para o mais alto, quando seu próprio toque automático é aberto.

Passo 5: Todos os rádios são autenticados.



Configuração incorreta ou casos de problema:

Se algum dos pontos da malha da infraestrutura tiver credenciais incorretas ou tiver o Radius desativado por engano, isso afetará a autenticação de outros rádios. Sempre verifique as credenciais e configurações antes de implantar rádios na produção.



Neste exemplo, se o Ponto de Malha 2 tiver credos errados, ele permanecerá não autenticado e, por sua vez, o Ponto de Malha 3 e o Ponto de Malha 4 nunca terão a chance de se autenticar, pois não há nenhum Pseudofio formado a partir deles para o Ponto de Malha 2 por causa do LNO estar habilitado.

Os rádios que permanecem não autenticados dependem da ID de malha do rádio configurada incorretamente. Qualquer rádio com ID de malha maior que o coordenador com fio atual permanecerá não autenticado e causará problemas.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.