Configurar o SNMP em pontos de acesso sem fio industriais no modo URWB

Contents

Introdução

Conceitos básicos de SNMP

Versões do SNMP

Configuração

- Configuração V2
- Configuração V3
- Ativando armadilhas

MIBs suportados

Validar serviço SNMP

Introdução

Este documento descreve a configuração e a solução de problemas de pontos de acesso sem fio industriais SNMP operando no modo URWB.

Conceitos básicos de SNMP

O SNMP (Simple Network Management Protocol) é um protocolo amplamente usado para gerenciar e monitorar dispositivos em redes IP. Ele permite que os administradores de rede coletem informações sobre dispositivos para garantir uma operação tranquila. O SNMP opera através da troca de mensagens entre um gerenciador SNMP, que supervisiona o monitoramento de rede, e agentes SNMP, que residem em dispositivos gerenciados. O protocolo usa uma Base de Informações de Gerenciamento (MIB - Management Information Base), um banco de dados hierárquico de variáveis, para definir e armazenar informações que podem ser acessadas ou modificadas. Por meio de várias operações SNMP, como GET (para recuperar informações), SET (para alterar a configuração) e TRAP (para receber alertas), os administradores podem monitorar a integridade da rede, rastrear o desempenho, detectar falhas e configurar dispositivos remotamente.

O protocolo SNMP (Simple Network Management Protocol) é usado no software URWB para recursos de gerenciamento de rede.

O cliente SNMP (qualquer aplicativo de monitoramento) envia uma solicitação ao agente SNMP em execução no rádio CURWB. O agente SNMP passa a solicitação ao subagente. O subagente responde ao agente SNMP. O agente SNMP cria um pacote de resposta SNMP e o envia ao aplicativo de gerenciamento de rede remota que inicia a solicitação.

Versões do SNMP

O SNMP evoluiu através de várias versões, cada uma melhorando a segurança e a funcionalidade. O SNMPv1, a versão original, fornece recursos básicos de monitoramento, mas não possui uma segurança forte, dependendo de strings de comunidade simples para controle de acesso. O SNMPv2c melhorou o desempenho e adicionou novas operações, mas manteve o mesmo modelo de segurança limitado que o SNMPv1. O SNMPv3, a versão mais recente, introduziu recursos de segurança robustos como autenticação e criptografia, tornando-o a escolha preferencial para o gerenciamento de rede seguro. Embora o SNMPv1 e o SNMPv2c ainda sejam amplamente usados em sistemas legados, o SNMPv3 é recomendado para a maioria das redes devido a seus recursos aprimorados de segurança e proteção de dados.

Configuração

Configuração V2

Habilite o SNMP usando este comando CLI:

```
Device#configure snmp enable
```

Para especificar a versão do protocolo SNMP, use este comando CLI:

```
Device#configure snmp version v2c
```

Para especificar o número de ID da comunidade SNMP v2c (somente SNMP v2c), use este comando CLI:

```
Device#configure snmp v2c community-id
```

Exemplo:

Device#configure snmp v2c community-id MytestPa$$word!

Configuração V3

Com o SNMP v3, a autenticação e a criptografia precisariam ser configuradas.

Habilite o SNMP usando este comando CLI:

```
Device#configure snmp enable
```

Para especificar a versão do protocolo SNMP, use este comando CLI:

```
Device#configure snmp version v3
```

Para especificar o nome de usuário SNMP v3 (somente SNMP v3), use este comando CLI:

```
Device#configure snmp v3 username
```

Para especificar a senha de usuário SNMP v3 (somente SNMP v3), use este comando CLI:

```
Device#configure snmp v3 password
```

Para especificar o protocolo de autenticação SNMP v3 (somente SNMP v3), use este comando CLI:

```
Device#configure snmp auth-method
```

Para especificar o protocolo de criptografia SNMP v3 (somente SNMP v3), use este comando CLI:

```
Device#configure snmp encryption {des | aes | none}
```

Ativando armadilhas

As interceptações SNMP são notificações assíncronas enviadas pelos agentes SNMP (neste caso, rádios IW) para o gerenciador SNMP (qualquer aplicativo de monitoramento) para alertá-lo sobre eventos significativos ou alterações no status de um dispositivo, como erros, reinicializações ou limites de desempenho excedidos. Diferentemente do polling normal, as interceptações permitem que os dispositivos relatem automaticamente os problemas à medida que eles ocorrem, permitindo detecção e resolução mais rápidas dos problemas de rede.

Para habilitar ou desabilitar interceptações de eventos SNMP, use este comando CLI:

```
Device#configure snmp event-trap {enable | disable}
```

Para especificar o nome do host ou o endereço IP do servidor de monitoramento de rede onde o aplicativo está sendo executado, use este comando CLI:

```
Device#configure snmp nms-hostname {hostname |Ip Address}
```

Para especificar as configurações de armadilha periódica SNMP, use este comando CLI:

```
Device#configure snmp periodic-trap {enable | disable}
```

Para especificar o período de interceptação de notificação para interceptações SNMP periódicas, use este comando CLI:

```
Device#configure snmp trap-period <1-2147483647>
```

MIBs suportados

Lista as MIBs suportadas para o IW9167E

- UCD-SNMP-MIB (.1.3.6.14.1.2021 Parcialmente suportado)

- IF-MIB (.1.3.6.1.2.1.2 Parcialmente suportado)
- CISCO-URWB-MIB (.1.3.6.1.4.1.9.9.1056)

Validar serviço SNMP

O comando ‘show system status snmpd’ pode ser usado para validar se o agente SNMP no dispositivo está em execução ou não (com as versões 17.9.x)

Quando o SNMPv2 está habilitado:

MP_TRK_Backhaul#show snmp

SNMP: habilitado

Versão: v2c

ID da comunidade: meu teste123!

Interceptação periódica: Desabilitado

Interceptação de evento: Desabilitado

Quando o SNMPv3 está habilitado:

MP_TRK_Backhaul#show snmp

SNMP: habilitado

Versão: v3

Nome de usuário: snmpadmin

Senha: Meu teste12349!

Método de autenticação: MD5

Criptografia: AES

Senha de criptografia: Meu teste12349!

ID do mecanismo: 0 x 800000090368790989 fa 94

Interceptação periódica: Desabilitado

Interceptação de evento: Desabilitado

A configuração também pode ser verificada usando o comando show run, onde a configuração SNMP estaria na seção Advanced Config.

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.