Configuration du protocole SNMP sur les points d'accès sans fil industriels en mode URWB

Table des matières

Introduction

Ce document décrit la configuration et le dépannage des points d'accès sans fil industriels SNMP fonctionnant en mode URWB.

Notions de base SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole largement utilisé pour la gestion et la surveillance des périphériques sur les réseaux IP. Il permet aux administrateurs réseau de collecter des informations sur les périphériques afin de garantir un fonctionnement sans heurts. Le protocole SNMP fonctionne en échangeant des messages entre un gestionnaire SNMP, qui supervise la surveillance du réseau, et des agents SNMP, qui résident sur des périphériques gérés. Le protocole utilise une base d'informations de gestion (MIB), une base de données hiérarchique de variables, pour définir et stocker des informations accessibles ou modifiables. Grâce à diverses opérations SNMP telles que GET (pour récupérer des informations), SET (pour modifier la configuration) et TRAP (pour recevoir des alertes), les administrateurs peuvent surveiller l'état du réseau, suivre les performances, détecter les pannes et configurer les périphériques à distance.

Le protocole SNMP (Simple Network Management Protocol) est utilisé dans le logiciel URWB pour les fonctions de gestion de réseau.

Le client SNMP (n'importe quelle application de surveillance) envoie une requête à l'agent SNMP s'exécutant sur l'émetteur-récepteur CURWB. L'agent SNMP transmet la requête au sous-agent. Le sous-agent répond à l'agent SNMP. L'agent SNMP crée un paquet de réponse SNMP et l'envoie à l'application d'administration de réseau distante qui initie la requête.

Versions de SNMP

Le protocole SNMP a évolué en plusieurs versions, chacune améliorant la sécurité et les fonctionnalités. SNMPv1, la version d'origine, fournit des fonctionnalités de surveillance de base, mais manque de sécurité renforcée, en s'appuyant sur des chaînes de communauté simples pour le contrôle d'accès. SNMPv2c a amélioré les performances et ajouté de nouvelles opérations, mais a conservé le même modèle de sécurité limité que SNMPv1. SNMPv3, la dernière version, a introduit des fonctionnalités de sécurité robustes telles que l'authentification et le cryptage, ce qui en fait le choix privilégié pour la gestion sécurisée du réseau. Bien que SNMPv1 et SNMPv2c soient encore largement utilisés dans les systèmes existants, SNMPv3 est recommandé pour la plupart des réseaux en raison de ses capacités de sécurité et de protection des données améliorées.

Configuration

configuration V2

Activez SNMP à l'aide de cette commande CLI :

```
Device#configure snmp enable
```

Pour spécifier la version du protocole SNMP, utilisez la commande CLI suivante :

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

Pour spécifier l'ID de communauté SNMP v2c (SNMP v2c uniquement), utilisez la commande CLI suivante :

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

Exemple :

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

configuration V3

Avec SNMP v3, l'authentification et le chiffrement doivent être configurés.

Activez SNMP à l'aide de cette commande CLI :

```
Device#configure snmp enable
```

Pour spécifier la version du protocole SNMP, utilisez la commande CLI suivante :

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

Pour spécifier le nom d'utilisateur SNMP v3 (SNMP v3 uniquement), utilisez la commande CLI suivante :

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

Pour spécifier le mot de passe utilisateur SNMP v3 (SNMP v3 uniquement), utilisez la commande CLI suivante :

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

Pour spécifier le protocole d'authentification SNMP v3 (SNMP v3 uniquement), utilisez la commande CLI suivante :

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

Pour spécifier le protocole de cryptage SNMP v3 (SNMP v3 uniquement), utilisez la commande CLI suivante :

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

Activation des déroutements

Les déroutements SNMP sont des notifications asynchrones envoyées par les agents SNMP (dans ce cas, des IW Radios) au gestionnaire SNMP (n'importe quelle application de surveillance) pour l'avertir d'événements importants ou de changements dans l'état d'un périphérique, tels que des erreurs, des redémarrages ou des dépassements de seuils de performances. Contrairement aux interrogations régulières, les déroutements permettent aux périphériques de signaler automatiquement les problèmes lorsqu'ils se produisent, ce qui accélère la détection et la résolution des problèmes réseau.

Pour activer ou désactiver les déroutements d'événements SNMP, utilisez la commande CLI suivante :

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

Pour spécifier le nom d'hôte ou l'adresse IP du serveur de surveillance du réseau sur lequel l'application est exécutée, utilisez la commande CLI suivante :

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

Pour spécifier les paramètres de déroutement périodique SNMP, utilisez la commande CLI suivante :

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

Pour spécifier la période de notification des déroutements SNMP périodiques, utilisez la commande CLI suivante :

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

MIBS pris en charge

Liste des MIB prises en charge pour l'IW9167E

- UCD-SNMP-MIB (.1.3.6.14.1.2021 partiellement pris en charge)
- IF-MIB (.1.3.6.1.2.1.2 Partiellement pris en charge)
- CISCO-URWB-MIB (.1.3.6.1.4.1.9.9.1056)

Valider le service SNMP

La commande « show system status snmpd » peut être utilisée pour valider si l'agent SNMP sur le périphérique est en cours d'exécution ou non (avec les versions 17.9.x)

Lorsque SNMPv2 est activé :

MP_TRK_Backhaul#show snmp

SNMP : activée

Version : v2c

ID de la communauté : mytest123 !

Interruption périodique : désactivé

Interruption d'événement : désactivé

Lorsque SNMPv3 est activé :

MP_TRK_Backhaul#show snmp

SNMP : activée

Version : v3

username (nom d’utilisateur) : snmpadmin

Mot de passe : Mytest12349 !

Méthode d'authentification : MD5

Chiffrement : AES

Phrase de passe de chiffrement : Mytest12349 !

ID du moteur : 0x800000090368790989fa94

Interruption périodique : désactivé

Interruption d'événement : désactivé

La configuration peut également être vérifiée à l'aide de la commande show run où la configuration SNMP serait sous la section Advanced Config.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.