SNMP auf Industrial Wireless Access Points im URWB-Modus konfigurieren

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration und Fehlerbehebung von SNMP Industrial Wireless Access Points, die im URWB-Modus betrieben werden.

SNMP-Grundlagen

Simple Network Management Protocol (SNMP) ist ein weit verbreitetes Protokoll zur Verwaltung und Überwachung von Geräten in IP-Netzwerken. Es ermöglicht Netzwerkadministratoren, Informationen über Geräte zu sammeln, um einen reibungslosen Betrieb sicherzustellen. SNMP nutzt den Nachrichtenaustausch zwischen einem SNMP-Manager, der die Netzwerküberwachung überwacht, und SNMP-Agenten, die sich auf verwalteten Geräten befinden. Das Protokoll verwendet eine Management Information Base (MIB), eine hierarchische Datenbank mit Variablen, um Informationen zu definieren und zu speichern, auf die zugegriffen werden kann oder die geändert werden können. Mithilfe verschiedener SNMP-Prozesse wie GET (zum Abrufen von Informationen), SET (zum Ändern der Konfiguration) und TRAP (zum Empfangen von Warnmeldungen) können Administratoren den Netzwerkzustand überwachen, die Leistung verfolgen, Fehler erkennen und Geräte remote konfigurieren.

Das Simple Network Management Protocol (SNMP)-Protokoll wird in der URWB-Software für Netzwerkverwaltungsfunktionen verwendet.

Der SNMP-Client (eine beliebige Überwachungsanwendung) sendet eine Anforderung an den SNMP-Agenten, der auf der CURWB-Funkeinheit ausgeführt wird. Der SNMP-Agent leitet die Anforderung an den Subagenten weiter. Der Subagent antwortet auf den SNMP-Agenten. Der SNMP-Agent erstellt ein SNMP-Antwortpaket und sendet es an die Remote-Netzwerkmanagementanwendung, die die Anforderung initiiert.

Versionen von SNMP

SNMP hat sich über mehrere Versionen hinweg entwickelt, von denen jede die Sicherheit und Funktionalität verbessert. SNMPv1, die ursprüngliche Version, bietet grundlegende Überwachungsfunktionen, bietet jedoch keine zuverlässige Sicherheit. Für die Zugriffskontrolle werden einfache Community-Strings verwendet. SNMPv2c verbesserte die Leistung und fügte neue Vorgänge hinzu, behielt jedoch das selbe eingeschränkte Sicherheitsmodell wie SNMPv1 bei. SNMPv3, die neueste Version, führte robuste Sicherheitsfunktionen wie Authentifizierung und Verschlüsselung ein und war damit die bevorzugte Wahl für die sichere Netzwerkverwaltung. Während SNMPv1 und SNMPv2c in Legacy-Systemen weiterhin häufig verwendet werden, wird SNMPv3 aufgrund der erweiterten Sicherheits- und Datenschutzfunktionen für die meisten Netzwerke empfohlen.

Konfiguration

V2-Konfiguration

SNMP mit diesem CLI-Befehl aktivieren:

```
Device#configure snmp enable
```

Verwenden Sie den folgenden CLI-Befehl, um die Version des SNMP-Protokolls anzugeben:

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

Verwenden Sie den folgenden CLI-Befehl, um die SNMP v2c Community ID-Nummer (nur SNMP v2c) anzugeben:

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

Beispiel:

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

V3-Konfiguration

Bei SNMP v3 müssen Authentifizierung und Verschlüsselung konfiguriert werden.

SNMP mit diesem CLI-Befehl aktivieren:

```
Device#configure snmp enable
```

Verwenden Sie den folgenden CLI-Befehl, um die Version des SNMP-Protokolls anzugeben:

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

Verwenden Sie den folgenden CLI-Befehl, um den SNMP v3-Benutzernamen (nur SNMP v3) anzugeben:

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

Verwenden Sie den folgenden CLI-Befehl, um das SNMP v3-Benutzerkennwort (nur SNMP v3) anzugeben:

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

Verwenden Sie den folgenden CLI-Befehl, um das SNMP v3-Authentifizierungsprotokoll (nur SNMP v3) anzugeben:

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

Verwenden Sie den folgenden CLI-Befehl, um das SNMP v3-Verschlüsselungsprotokoll (nur SNMP v3) anzugeben:

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

Traps aktivieren

SNMP-Traps sind asynchrone Benachrichtigungen, die von SNMP-Agenten (in diesem Fall IW Radios) an den SNMP-Manager (eine beliebige Überwachungsanwendung) gesendet werden, um ihn über signifikante Ereignisse oder Änderungen des Gerätestatus zu informieren, wie z. B. das Überschreiten von Fehlern, Neustarts oder Leistungsgrenzwerten. Anders als bei regulären Abfragen können Geräte mit Traps Probleme automatisch melden, sobald sie auftreten. Netzwerkprobleme werden so schneller erkannt und behoben.

Verwenden Sie den folgenden CLI-Befehl, um SNMP-Ereignis-Traps zu aktivieren oder zu deaktivieren:

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

Verwenden Sie den folgenden CLI-Befehl, um den Hostnamen oder die IP-Adresse des Netzwerküberwachungsservers anzugeben, auf dem die Anwendung ausgeführt wird:

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

Verwenden Sie den folgenden CLI-Befehl, um die Einstellungen für das periodische SNMP-Trap festzulegen:

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

Verwenden Sie den folgenden CLI-Befehl, um die Trap-Dauer für regelmäßige SNMP-Traps festzulegen:

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

Unterstützte MIBS

Hier sind die unterstützten MIBs für den IW9167E aufgeführt.

- UCD-SNMP-MIB (.1.3.6.14.1.2021 teilweise unterstützt)
- IF-MIB (.1.3.6.1.2.1.2 teilweise unterstützt)
- CISCO-URWB-MIB (.1.3.6.1.4.1.9.9.1056)

SNMP-Dienst überprüfen

Mit dem Befehl "show system status snmpd" kann überprüft werden, ob der SNMP-Agent auf dem Gerät ausgeführt wird (mit Version 17.9.x).

Wenn SNMPv2 aktiviert ist:

MP_TRK_Backhaul#show snmp

SNMP: aktiviert

Version: v2c

Community-ID: mytest123

Periodische Trap: disabled

Ereignis-Trap: disabled

Wenn SNMPv3 aktiviert ist:

MP_TRK_Backhaul#show snmp

SNMP: aktiviert

Version: V3

Benutzername: snmpadmin

Kennwort: Mytest12349

Authentifizierungsmethode: MD5

Verschlüsselung: AES

Verschlüsselungspasswort: Mytest12349

Modul-ID: 0x800000090368790989fa94

Periodische Trap: disabled

Ereignis-Trap: disabled

Die Konfiguration kann auch mit dem Befehl show run überprüft werden, wobei die SNMP-Konfiguration im Abschnitt Advanced Config (Erweiterte Konfiguration) angegeben wird.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.