Configure SNMP on Industrial Wireless Access Points in URWB Mode

Contents

Introduction

SNMP Basics

Versions of SNMP

Configuration

- V2 configuration
- V3 configuration
- Enabling Traps

Supported MIBS

Validate SNMP service

Introduction

This document describes the configuration and troubleshooting of SNMP Industrial Wireless Access Points operating on URWB mode.

SNMP Basics

Simple Network Management Protocol (SNMP) is a widely used protocol for managing and monitoring devices on IP networks. It enables network administrators to collect information about devices to ensure smooth operation. SNMP operates by exchanging messages between an SNMP manager, which oversees network monitoring, and SNMP agents, which reside on managed devices. The protocol uses a Management Information Base (MIB), a hierarchical database of variables, to define and store information that can be accessed or modified. Through various SNMP operations like GET (to retrieve information), SET (to change configuration), and TRAP (to receive alerts), administrators can monitor network health, track performance, detect faults, and configure devices remotely.

Simple network management protocol (SNMP) protocol is used in URWB software for network management capabilities.

The SNMP client (any monitoring application) sends a request to the SNMP agent running on the CURWB radio. The SNMP agent passes the request to the subagent. The subagent responds to the SNMP agent. The SNMP agent creates an SNMP response packet and sends it to the remote network management application that initiates the request.

Versions of SNMP

SNMP has evolved through several versions, each enhancing security and functionality. SNMPv1, the original version, provides basic monitoring capabilities but lacks strong security, relying on simple community strings for access control. SNMPv2c improved performance and added new operations but retained the same limited security model as SNMPv1. SNMPv3, the latest version, introduced robust security features like authentication and encryption, making it the preferred choice for secure network management. While SNMPv1 and SNMPv2c are still widely used in legacy systems, SNMPv3 is

recommended for most networks due to its enhanced security and data protection capabilities.

Configuration

V2 configuration

Enable SNMP using this CLI command:

```
Device#configure snmp enable
```

To specify the SNMP protocol version, use this CLI command:

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

To specify the SNMP v2c community ID number (SNMP v2c only), use this CLI command:

```
Device#configure snmp v2c community-id <length 1-64>
```

Example:

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

V3 configuration

With SNMP v3, authentication and encryption would need to be configured.

Enable SNMP using this CLI command:

```
Device#configure snmp enable
```

To specify the SNMP protocol version, use this CLI command:

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

To specify the SNMP v3 username (SNMP v3 only), use this CLI command:

```
Device#configure snmp v3 username <length 32>
```

To specify the SNMP v3 user password (SNMP v3 only), use this CLI command:

```
Device#configure snmp v3 password <length 8-64>
```

To specify the SNMP v3 authentication protocol (SNMP v3 only), use this CLI command:

```
Device#configure snmp auth-method <md5|sha>
```

To specify the SNMP v3 encryption protocol (SNMP v3 only), use this CLI command:

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

Enabling Traps

SNMP traps are asynchronous notifications sent by SNMP agents (IW Radios in this case) to the SNMP manager (any monitoring application) to alert it of significant events or changes in a device's status, such as errors, reboots, or performance thresholds being exceeded. Unlike regular polling, traps allow devices to automatically report issues as they happen, enabling faster detection and resolution of network problems.

To enable or disable SNMP event traps, use this CLI command:

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

To specify the hostname or IP address of the network monitoring server where the application is running, use this CLI command:

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

To specify the SNMP periodic trap settings, use this CLI command:

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

To specify the notification trap period for periodic SNMP traps, use this CLI command:

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

Supported MIBS

This lists the supported MIBs for the IW9167E

- UCD-SNMP-MIB (.1.3.6.14.1.2021 Partly Supported)
- IF-MIB (.1.3.6.1.2.1.2 Partly Supported)
- CISCO-URWB-MIB (.1.3.6.1.4.1.9.9.1056)

Validate SNMP service

The command ‘show system status snmpd’ can be used to validate if the SNMP agent on the device is running or not (with versions 17.9.x)

When SNMPv2 is enabled:

MP_TRK_Backhaul#show snmp

SNMP: enabled

Version: v2c

Community ID: mytest123!

Periodic Trap: disabled

Event Trap: disabled

When SNMPv3 is enabled:

MP_TRK_Backhaul#show snmp

SNMP: enabled

Version: v3

Username: snmpadmin

Password: Mytest12349!

Authentication method: MD5

Encryption: AES

Encryption Passphrase: Mytest12349!

Engine ID: 0x800000090368790989fa94

Periodic Trap: disabled

Event Trap: disabled

The configuration can also be verified using the **show run** command where the SNMP configuration would

be under the **Advanced Config** section.