

URWB 모드에서 Industrial Wireless Access Points에 SNMP 구성

목차

- [소개](#)
 - [SNMP 기본 사항](#)
 - [SNMP 버전](#)
 - [설정](#)
 - [V2 컨피그레이션](#)
 - [V3 컨피그레이션](#)
 - [트랩 활성화](#)
 - [지원되는 MIB](#)
 - [SNMP 서비스 확인](#)
-

소개

이 문서에서는 URWB 모드에서 작동하는 SNMP Industrial Wireless Access Point의 컨피그레이션 및 문제 해결에 대해 설명합니다.

SNMP 기본 사항

SNMP(Simple Network Management Protocol)는 IP 네트워크에서 디바이스를 관리하고 모니터링 하는 데 널리 사용되는 프로토콜입니다. 또한 네트워크 관리자가 디바이스에 대한 정보를 수집하여 원활한 운영을 보장할 수 있습니다. SNMP는 네트워크 모니터링을 감독하는 SNMP 관리자와 관리 되는 디바이스에 상주하는 SNMP 에이전트 간에 메시지를 교환하여 작동합니다. 이 프로토콜은 변수의 계층적 데이터베이스인 MIB(Management Information Base)를 사용하여 액세스하거나 수정 할 수 있는 정보를 정의하고 저장합니다. 관리자는 GET(정보 검색), SET(컨피그레이션 변경), TRAP(알림 수신) 등 다양한 SNMP 작업을 통해 네트워크 상태를 모니터링하고 성능을 추적하고 결 함을 탐지하며 원격으로 디바이스를 구성할 수 있습니다.

SNMP(Simple Network Management Protocol) 프로토콜은 네트워크 관리 기능을 위해 URWB 소프트웨어에서 사용됩니다.

SNMP 클라이언트(모든 모니터링 애플리케이션)는 CURWB 라디오에서 실행 중인 SNMP 에이전 트에 요청을 보냅니다. SNMP 에이전트는 하위 에이전트에 요청을 전달합니다. 하위 에이전트는 SNMP 에이전트에 응답합니다. SNMP 에이전트는 SNMP 응답 패킷을 생성하여 요청을 시작하는 원격 네트워크 관리 애플리케이션에 전송합니다.

SNMP 버전

SNMP는 여러 버전을 통해 진화했으며, 각각 보안 및 기능을 향상시켰습니다. 원래 버전인

SNMPv1은 기본적인 모니터링 기능을 제공하지만 액세스 제어를 위해 간단한 커뮤니티 문자열에 의존하여 강력한 보안이 결여되어 있습니다. SNMPv2c는 성능을 개선하고 새로운 작업을 추가했지만 SNMPv1과 동일한 제한된 보안 모델을 유지했습니다. 최신 버전인 SNMPv3는 인증 및 암호화와 같은 강력한 보안 기능을 도입하여 보안 네트워크 관리를 위한 기본 옵션으로 채택되었습니다. SNMPv1 및 SNMPv2c는 레거시 시스템에서 여전히 널리 사용되고 있지만, SNMPv3는 보안 및 데이터 보호 기능이 향상되어 대부분의 네트워크에 권장됩니다.

설정

V2 컨피그레이션

다음 CLI 명령을 사용하여 SNMP를 활성화합니다.

```
Device#configure snmp enable
```

SNMP 프로토콜 버전을 지정하려면 다음 CLI 명령을 사용합니다.

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

SNMP v2c 커뮤니티 ID 번호(SNMP v2c에만 해당)를 지정하려면 다음 CLI 명령을 사용합니다.

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

예:

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

V3 컨피그레이션

SNMP v3에서는 인증 및 암호화를 구성해야 합니다.

다음 CLI 명령을 사용하여 SNMP를 활성화합니다.

```
Device#configure snmp enable
```

SNMP 프로토콜 버전을 지정하려면 다음 CLI 명령을 사용합니다.

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

SNMP v3 사용자 이름을 지정하려면(SNMP v3만 해당) 다음 CLI 명령을 사용합니다.

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

SNMP v3 사용자 비밀번호를 지정하려면(SNMP v3만 해당) 다음 CLI 명령을 사용합니다.

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

SNMP v3 인증 프로토콜(SNMP v3만 해당)을 지정하려면 다음 CLI 명령을 사용합니다.

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

SNMP v3 암호화 프로토콜(SNMP v3만 해당)을 지정하려면 다음 CLI 명령을 사용합니다.

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

트랩 활성화

SNMP 트랩은 SNMP 에이전트(이 경우 IW 무선)가 SNMP 관리자(모든 모니터링 애플리케이션)에 보내는 비동기 알림으로, 오류, 재부팅 또는 성능 임계값이 초과되는 등 디바이스 상태의 중요한 이벤트 또는 변경 사항을 알립니다. 일반 폴링과 달리 트랩을 사용하면 디바이스가 문제를 발생하면

자동으로 보고할 수 있으므로 네트워크 문제를 더 빠르게 탐지하고 해결할 수 있습니다.

SNMP 이벤트 트랩을 활성화하거나 비활성화하려면 다음 CLI 명령을 사용합니다.

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

애플리케이션이 실행 중인 네트워크 모니터링 서버의 호스트 이름 또는 IP 주소를 지정하려면 다음 CLI 명령을 사용합니다.

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

SNMP 주기적인 트랩 설정을 지정하려면 다음 CLI 명령을 사용합니다.

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

주기적인 SNMP 트랩에 대한 알림 트랩 기간을 지정하려면 다음 CLI 명령을 사용합니다.

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

지원되는 MIB

여기에는 IW9167E에 대해 지원되는 MIB가 나열됩니다

- UCD-SNMP-MIB(.1.3.6.14.1.2021 일부 지원됨)
- IF-MIB(.1.3.6.1.2.1.2 일부 지원됨)
- CISCO-URWB-MIB(.1.3.6.1.4.1.9.9.1056)

SNMP 서비스 확인

'show system status snmpd' 명령을 사용하여 디바이스에서 SNMP 에이전트가 실행 중인지 여부 (버전 17.9.x)를 확인할 수 있습니다

SNMPv2가 활성화된 경우:

```
MP_TRK_Backhaul#show snmp
```

SNMP: 활성화됨

버전: v2c

커뮤니티 ID: 마이테스트 123!

주기적인 트랩: 비활성화됨

이벤트 트랩: 비활성화됨

SNMPv3이 활성화된 경우:

MP_TRK_Backhaul#show snmp

SNMP: 활성화됨

버전: v3

사용자 이름: snmpadmin

암호: 내 12349!

인증 방법: MD5

암호화: AES

암호화 암호: 내 12349!

엔진 ID: 0x800000090368790989fa94

주기적인 트랩: 비활성화됨

이벤트 트랩: 비활성화됨

SNMP 컨피그레이션이 Advanced Config(고급 컨피그레이션) 섹션에 있는 show run 명령을 사용하여 컨피그레이션을 확인할 수도 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.