SNMP op industriële draadloze access points configureren in URWB-modus

Inhoud

Inleiding

Dit document beschrijft de configuratie en probleemoplossing van SNMP industriële draadloze access points die in de URWB-modus werken.

SNMP-basisbeginselen

Simple Network Management Protocol (SNMP) is een veelgebruikt protocol voor het beheer en de bewaking van apparaten op IP-netwerken. Hiermee kunnen netwerkbeheerders informatie over apparaten verzamelen om een soepele werking te waarborgen. SNMP werkt door berichten uit te wisselen tussen een SNMP-beheerder, die toezicht houdt op netwerkbewaking, en SNMP-agents, die zich op beheerde apparaten bevinden. Het protocol gebruikt een Management Information Base (MIB), een hiërarchische database van variabelen, om informatie te definiëren en op te slaan die kan worden benaderd of aangepast. Via verschillende SNMP-bewerkingen zoals GET (om informatie op te halen), SET (om configuratie te wijzigen) en TRAP (om meldingen te ontvangen) kunnen beheerders de netwerkstatus bewaken, prestaties volgen, fouten detecteren en apparaten op afstand configureren.

Simple Network Management Protocol (SNMP) wordt gebruikt in URWB-software voor netwerkbeheerfuncties.

De SNMP-client (elke bewakingsapplicatie) stuurt een verzoek naar de SNMP-agent die op de CURWB-radio actief is. De SNMP-agent geeft de aanvraag door aan de subagent. De subagent reageert op de SNMP-agent. De SNMP-agent maakt een SNMP-responspakket en stuurt het naar de externe netwerkbeheertoepassing die het verzoek initieert.

Versies van SNMP

SNMP is geëvolueerd door verscheidene versies, elk die veiligheid en functionaliteit verbeteren. SNMPv1, de oorspronkelijke versie, biedt eenvoudige controlefuncties maar niet voldoende beveiliging; voor toegangscontrole is het gebruik van eenvoudige communautaire strings vereist. SNMPv2c verbeterde prestaties en voegde nieuwe bewerkingen toe, maar behield hetzelfde beperkte beveiligingsmodel als SNMPv1. SNMPv3, de nieuwste versie, introduceerde robuuste beveiligingsfuncties zoals verificatie en codering, waardoor het de voorkeurskeuze was voor veilig netwerkbeheer. Hoewel SNMPv1 en SNMPv2c nog steeds op grote schaal worden gebruikt in oudere systemen, wordt SNMPv3 voor de meeste netwerken aanbevolen vanwege de verbeterde beveiliging en mogelijkheden voor gegevensbescherming.

Configuratie

V2-configuratie

SNMP met deze CLI-opdracht inschakelen:

```
Device#configure snmp enable
```

Om de SNMP-protocolversie te specificeren, gebruikt u deze CLI-opdracht:

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

Om het SNMP v2c community-ID-nummer te specificeren (alleen SNMP v2c), gebruikt u deze CLI-opdracht:

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

Voorbeeld:

Apparaat#configureer snmp v2c community-id MytestPa$$word!

V3-configuratie

Met SNMP v3 zouden verificatie en codering moeten worden geconfigureerd.

SNMP met deze CLI-opdracht inschakelen:

```
Device#configure snmp enable
```

Om de SNMP-protocolversie te specificeren, gebruikt u deze CLI-opdracht:

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

Om de SNMP v3-gebruikersnaam te specificeren (alleen SNMP v3), gebruikt u deze CLI-opdracht:

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

Om het SNMP v3 gebruikerswachtwoord te specificeren (alleen SNMP v3), gebruikt u deze CLI-opdracht:

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

Gebruik deze CLI-opdracht om het SNMP v3-verificatieprotocol te specificeren (alleen SNMP v3):

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

Om het SNMP v3-encryptieprotocol te specificeren (alleen SNMP v3), gebruikt u deze CLI-opdracht:

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

Traps inschakelen

SNMP-traps zijn asynchrone meldingen die door SNMP-agents (in dit geval IW Radios) naar de SNMP-beheerder (elke monitoringtoepassing) worden gestuurd om hem te waarschuwen voor belangrijke gebeurtenissen of veranderingen in de status van een apparaat, zoals fouten, herstart, of prestatiedrempels die worden overschreden. In tegenstelling tot regelmatige opiniepeilingen, staan de vallen apparaten toe om automatisch kwesties te melden aangezien zij gebeuren, toelatend snellere opsporing en resolutie van netwerkproblemen.

Gebruik deze CLI-opdracht om SNMP-gebeurtenisvallen in- of uit te schakelen:

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

Gebruik deze CLI-opdracht om de hostnaam of het IP-adres op te geven van de netwerkbewakingsserver waarop de toepassing wordt uitgevoerd:

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

Als u de instellingen voor de SNMP-periodieke overvulling wilt opgeven, gebruikt u deze CLI-opdracht:

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

Gebruik deze CLI-opdracht om de kennisgevingstrap voor periodieke SNMP-traps te specificeren:

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

Ondersteunde MIBS

Dit geeft de ondersteunde MIB's voor de IW9167E aan

- UCD-SNMP-MIB (gedeeltelijk ondersteunde versie 1.3.6.14.1.2021)
- IF-MIB (.1.3.6.1.2.1.2 gedeeltelijk ondersteund)
- CISCO-URWB-MIB (.1.3.6.1.4.1.9.9.1056)

SNMP-service valideren

De opdracht "show system status snmpd" kan worden gebruikt om te valideren of de SNMP-agent op het apparaat al dan niet actief is (met versies 17.9.x)

Als SNMPv2 is ingeschakeld:

MP_TRK_Backhaul#show snmp

SNMP: ingeschakeld

Versie: v2c

Community-id: Mijn test123!

Periodieke trap: uitgeschakeld

Event Trap: uitgeschakeld

Als SNMPv3 is ingeschakeld:

MP_TRK_Backhaul#show snmp

SNMP: ingeschakeld

Versie: v3

Username: mompadmin

Password (Wachtwoord): Mijn test12349!

Verificatiemethode: MD5

Versleuteling: AES

Wachtwoord voor encryptie: Mijn test12349!

Motor-ID: 0x800000090368790989fa

Periodieke trap: uitgeschakeld

Event Trap: uitgeschakeld

De configuratie kan ook worden geverifieerd met behulp van de opdracht show run, waar de SNMP-configuratie zich zou bevinden in de sectie Advanced Config.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.