Configurazione di SNMP sui punti di accesso wireless industriali in modalità URWB

Sommario

Introduzione

In questo documento viene descritta la configurazione e la risoluzione dei problemi dei punti di accesso wireless industriali SNMP in modalità URWB.

Nozioni di base su SNMP

L'SNMP (Simple Network Management Protocol) è un protocollo ampiamente utilizzato per la gestione e il monitoraggio di dispositivi su reti IP. Consente agli amministratori di rete di raccogliere informazioni sui dispositivi per garantire un funzionamento senza problemi. Il protocollo SNMP funziona tramite lo scambio di messaggi tra un gestore SNMP, che controlla il monitoraggio della rete, e gli agenti SNMP, che risiedono su dispositivi gestiti. Il protocollo utilizza un MIB (Management Information Base), un database gerarchico di variabili, per definire e memorizzare le informazioni accessibili o modificabili. Tramite varie operazioni SNMP, quali GET (per recuperare le informazioni), SET (per modificare la configurazione) e TRAP (per ricevere gli avvisi), gli amministratori possono monitorare lo stato della rete, monitorare le prestazioni, rilevare gli errori e configurare i dispositivi in remoto.

Il protocollo SNMP (Simple Network Management Protocol) viene utilizzato nel software URWB per le funzionalità di gestione della rete.

Il client SNMP (qualsiasi applicazione di monitoraggio) invia una richiesta all'agente SNMP in esecuzione sulla radio CURWB. L'agente SNMP passa la richiesta al subagent. Il subagent risponde all'agente SNMP. L'agente SNMP crea un pacchetto di risposta SNMP e lo invia all'applicazione di gestione remota della rete che avvia la richiesta.

Versioni di SNMP

L'SNMP si è evoluto attraverso diverse versioni, ciascuna delle quali ha migliorato la sicurezza e la funzionalità. L'SNMPv1, la versione originale, fornisce funzionalità di monitoraggio di base ma non offre una protezione efficace, poiché si basa su semplici stringhe della community per il controllo degli accessi. SNMPv2c ha migliorato le prestazioni e ha aggiunto nuove operazioni, ma ha mantenuto lo stesso modello di sicurezza limitato di SNMPv1. SNMPv3, l'ultima versione, ha introdotto funzioni di sicurezza affidabili come l'autenticazione e la crittografia, rendendola la scelta preferita per la gestione sicura della rete. Mentre SNMPv1 e SNMPv2c sono ancora ampiamente utilizzati nei sistemi legacy, SNMPv3 è consigliato per la maggior parte delle reti grazie alle funzionalità avanzate di sicurezza e protezione dei dati.

Configurazione

Configurazione V2

Abilitare il protocollo SNMP utilizzando questo comando CLI:

```
Device#configure snmp enable
```

Per specificare la versione del protocollo SNMP, utilizzare questo comando CLI:

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

Per specificare il numero ID della community SNMP v2c (solo SNMP v2c), utilizzare questo comando CLI:

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

Esempio:

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

Configurazione V3

Con SNMP v3, è necessario configurare l'autenticazione e la crittografia.

Abilitare il protocollo SNMP utilizzando questo comando CLI:

```
Device#configure snmp enable
```

Per specificare la versione del protocollo SNMP, utilizzare questo comando CLI:

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

Per specificare il nome utente SNMP v3 (solo SNMP v3), utilizzare questo comando CLI:

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

Per specificare la password dell'utente SNMP v3 (solo SNMP v3), utilizzare questo comando CLI:

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

Per specificare il protocollo di autenticazione SNMP v3 (solo SNMP v3), utilizzare questo comando CLI:

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

Per specificare il protocollo di crittografia SNMP v3 (solo SNMP v3), utilizzare questo comando CLI:

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

Attivazione di trap

Le trap SNMP sono notifiche asincrone inviate dagli agenti SNMP (in questo caso Radio IW) al manager SNMP (qualsiasi applicazione di monitoraggio) per avvisarlo di eventi significativi o di modifiche nello stato di un dispositivo, come errori, riavvii o superamento delle soglie delle prestazioni. A differenza del polling regolare, le trap consentono ai dispositivi di segnalare automaticamente i problemi man mano che si verificano, consentendo un rilevamento e una risoluzione più rapida dei problemi di rete.

Per abilitare o disabilitare le trap degli eventi SNMP, utilizzare questo comando CLI:

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

Per specificare il nome host o l'indirizzo IP del server di monitoraggio della rete in cui è in esecuzione l'applicazione, utilizzare questo comando CLI:

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

Per specificare le impostazioni delle trap periodiche SNMP, utilizzare questo comando CLI:

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

Per specificare il periodo di trap delle notifiche per i trap SNMP periodici, utilizzare questo comando CLI:

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

MIB supportati

Elenca i MIB supportati per IW9167E

- UCD-SNMP-MIB (.1.3.6.14.1.2021 parzialmente supportato)
- IF-MIB (.1.3.6.1.2.1.2 parzialmente supportato)
- CISCO-URWB-MIB (.1.3.6.1.4.1.9.9.1056)

Convalida servizio SNMP

Il comando "show system status snmpd" può essere usato per verificare se l'agente SNMP sul dispositivo è in esecuzione o meno (con le versioni 17.9.x)

Quando SNMPv2 è abilitato:

MP_TRK_Backhaul#show snmp

SNMP: attivato

Version: v2c

ID community: test123!

Trap periodica: disabled

Trap evento: disabled

Quando SNMPv3 è abilitato:

MP_TRK_Backhaul#show snmp

SNMP: attivato

Version: v3

Username: snmpadmin

Password: Il mio test12349!

Metodo di autenticazione: MD5

Crittografia: AES

Passphrase di crittografia: Il mio test12349!

ID motore: 0x800000090368790989fa94

Trap periodica: disabled

Trap evento: disabled

La configurazione può essere verificata anche con il comando show run, dove si troverebbe la configurazione SNMP, nella sezione Advanced Config.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).