Configuración de SNMP en puntos de acceso inalámbricos industriales en modo URWB

Contenido

Introducción

Este documento describe la configuración y la resolución de problemas de los puntos de acceso inalámbricos industriales SNMP que funcionan en el modo URWB.

Fundamentos de SNMP

El protocolo simple de administración de red (SNMP) es un protocolo ampliamente utilizado para administrar y supervisar dispositivos en redes IP. Permite a los administradores de red recopilar información sobre los dispositivos para garantizar un funcionamiento sin problemas. SNMP funciona intercambiando mensajes entre un administrador SNMP, que supervisa la supervisión de la red, y agentes SNMP, que residen en dispositivos administrados. El protocolo utiliza una Base de información de administración (MIB), una base de datos jerárquica de variables, para definir y almacenar información a la que se puede acceder o modificar. A través de varias operaciones SNMP, como GET (para recuperar información), SET (para cambiar la configuración) y TRAP (para recibir alertas), los administradores pueden supervisar el estado de la red, realizar un seguimiento del rendimiento, detectar fallos y configurar dispositivos de forma remota.

El protocolo simple de administración de red (SNMP) se utiliza en el software URWB para las capacidades de administración de red.

El cliente SNMP (cualquier aplicación de monitoreo) envía una solicitud al agente SNMP que se ejecuta en el radio CURWB. El agente SNMP pasa la solicitud al subagente. El subagente responde al agente SNMP. El agente SNMP crea un paquete de respuesta SNMP y lo envía a la aplicación de administración de red remota que inicia la solicitud.

Versiones de SNMP

SNMP ha evolucionado a través de varias versiones, cada una mejorando la seguridad y la funcionalidad. SNMPv1, la versión original, proporciona funciones básicas de supervisión, pero carece de una seguridad sólida, ya que se basa en cadenas de comunidad sencillas para el control de acceso. SNMPv2c mejoró el rendimiento y agregó nuevas operaciones, pero conservó el mismo modelo de seguridad limitada que SNMPv1. SNMPv3, la versión más reciente, introdujo sólidas funciones de seguridad, como la autenticación y el cifrado, lo que lo convierte en la opción preferida para la administración de redes seguras. Aunque SNMPv1 y SNMPv2c siguen siendo muy utilizados en los sistemas heredados, SNMPv3 se recomienda para la mayoría de las redes debido a su seguridad mejorada y a las capacidades de protección de datos.

Configuración

Configuración V2

Habilite SNMP con este comando de CLI:

```
Device#configure snmp enable
```

Para especificar la versión del protocolo SNMP, utilice este comando CLI:

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

Para especificar el número de ID de comunidad SNMP v2c (sólo SNMP v2c), utilice este comando de CLI:

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

Ejemplo:

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

Configuración V3

Con SNMP v3, se tendría que configurar la autenticación y el cifrado.

Habilite SNMP con este comando de CLI:

```
Device#configure snmp enable
```

Para especificar la versión del protocolo SNMP, utilice este comando CLI:

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

Para especificar el nombre de usuario SNMP v3 (sólo SNMP v3), utilice este comando de CLI:

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

Para especificar la contraseña de usuario de SNMP v3 (sólo SNMP v3), utilice este comando de CLI:

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

Para especificar el protocolo de autenticación SNMP v3 (sólo SNMP v3), utilice este comando de CLI:

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

Para especificar el protocolo de cifrado SNMP v3 (sólo SNMP v3), utilice este comando de CLI:

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

Habilitación de Trampas

Las trampas SNMP son notificaciones asíncronas que envían los agentes SNMP (radios IW en este caso) al administrador SNMP (cualquier aplicación de supervisión) para alertarle de eventos significativos o cambios en el estado de un dispositivo, como errores, reinicios o superación de umbrales de rendimiento. A diferencia de los sondeos regulares, las trampas permiten que los dispositivos notifiquen automáticamente los problemas a medida que suceden, lo que permite una detección y resolución más rápidas de los problemas de la red.

Para habilitar o inhabilitar las trampas de eventos SNMP, utilice este comando CLI:

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

Para especificar el nombre de host o la dirección IP del servidor de supervisión de red donde se ejecuta la aplicación, utilice este comando de CLI:

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

Para especificar la configuración de capturas periódicas SNMP, utilice este comando CLI:

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

Para especificar el período de trampa de notificación para trampas SNMP periódicas, utilice este comando CLI:

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

MIB compatibles

Muestra los MIB compatibles con el IW9167E

- UCD-SNMP-MIB (.1.3.6.14.1.2021 Parcialmente compatible)
- IF-MIB (.1.3.6.1.2.1.2 Parcialmente compatible)
- CISCO-URWB-MIB (.1.3.6.1.4.1.9.9.1056)

Validar servicio SNMP

El comando "show system status snmpd" puede utilizarse para validar si el agente SNMP del dispositivo se está ejecutando o no (con las versiones 17.9.x)

Cuando SNMPv2 está habilitado:

MP_TRK_Backhaul#show snmp

SNMP (Protocolo de administración de red simple): habilitado

Versión: v2c

ID de comunidad: ¡mytest123!

Interrupción periódica: inhabilitado

Captura de evento: inhabilitado

Cuando SNMPv3 está habilitado:

MP_TRK_Backhaul#show snmp

SNMP (Protocolo de administración de red simple): habilitado

Versión: v3

Nombre de usuario: snmpadmin

Contraseña ¡Mytest12349!

Método de autentificación: MD5

Cifrado: AES

Frase de contraseña de cifrado: ¡Mytest12349!

ID del motor: 0x800000090368790989fa94

Interrupción periódica: inhabilitado

Captura de evento: inhabilitado

La configuración también se puede verificar mediante el comando show run, donde la configuración SNMP estaría en la sección Advanced Config.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).