

Configuring and Validating SNMP

• Configuring and Validating SNMP, on page 1

Configuring and Validating SNMP

Simple network management protocol (SNMP) applications are used in URWB software for network management functionalities.

The SNMP client sends a request to the SNMP agent. 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 station that initiates the request.

Figure 1: SNMP Process



Configuring SNMP from CLI

To configure SNMP, use the following CLI commands:



Note

- SNMP CLI logic modified for SNMP configuration, before enabling the SNMP feature using CLI, you
 must configure all SNMP parameters.
 - Disabling the SNMP feature automatically removes all related configurations.

To enable or disable SNMP functionality, use the following CLI command:

Device#configure snmp [enable | disable]

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

Device#configure snmp version {v2c | v3}

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

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

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

Device#configure snmp v3 username <length 32>

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

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

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

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

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

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

Possible encryption values are des or aes. Alternatively, enter none if a v3 encryption protocol is not needed.

To specify the SNMP v3 encryption passphrase (SNMP v3 only), use the following CLI command:

Device#configure snmp secret <length 8-64>

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

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

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

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

Notification value trap period measured in minutes.

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

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

To specify the SNMP NMS hostname or IP address, use the following CLI command:

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

To disable SNMP configuration, use the following CLI command:

Device#configure snmp disabled

Once you disable SNMP, it clears all the sensitive information including credentials. You have to re-specify all the valid values again to enable SNMP.

Example of SNMP configuration:

CLI for SNMP v2:

Device#configure snmp v2 community-id <length 1-64> Device#configure snmp nms-hostname hostname/Ip Address Device#configure snmp trap-period <1-2147483647> Device#configure snmp periodic-trap enable/disable Device#configure snmp event-trap enable/disable Device#configure snmp version v2c Device#configure snmp enabled

CLI for SNMP v3:

Device #configure snmp nms-hostname hostname/Ip Address Device#configure snmp trap-period <1-2147483647> Device#configure snmp v3 username <length 32> Device#configure snmp v3 password <length 8-64> Device#configure snmp auth-method <md5|sha> Device#configure snmp encryption <aes|des|none> Device#configure snmp secret <length 8-64> Device#configure snmp periodic-trap enable/disable Device#configure snmp event-trap enable/disable Device#configure snmp version v3 Device#configure snmp enabled L

Validating SNMP from CLI

To validate the SNMP, use the following show command:

Device# show snmp SNMP: enabled Version: v3 Username: username Password: password Authentication method: SHA Encryption: AES Encryption Passphrase: passphrase Engine ID: 0x8000000903c0f87fe5f314 Periodic Trap: enabled Notification Period (minutes): 5 Event Trap: enabled NMS hostname: 192.168.116.11 Device# show snmp SNMP: enabled Version: v2c Community ID: test Periodic Trap: enabled Notification Period (minutes): 5 Event Trap: enabled NMS hostname: 192.168.116.11 Device# show system status snmpd Service Status Service Name : snmpd Loaded : loaded Active : active (running) Main ProcessID : 6437 Running Since : Mon 2022-09-19 14:45:27 UTC; 3h 34min ago Service Restart : 0

Configuring SNMP Version v2c using GUI

By default, the access points are shipped from the factory with SNMP in disabled mode.

To change the access point's SNMP mode to version v2c and configure the access point, follow these steps:

Step 1Choose the version v2c from the SNMP mode drop-down list.
The SNMP window appears.

UTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 5.21.200.136 - MESH END MODE	
IOTOD IW Offline	SNMP	
IW-MONITOR Disabled	SNMP	
FM-QUADRO	SNMP mode:	v2c ~
GENERAL SETTINGS	Community ID:	test
- general mode - wireless radio	Enable SNMP periodic trap:	
- antenna alignment and stats	Enable SNMP event trap:	
NETWORK CONTROL	NMS hostname:	192.168.0.100
ADVANCED SETTINGS	Notification period (minutes);	1 0
- advanced radio settings - static routes		
- allowlist / blocklist	Reset	Sava
- multicast	Keset	Save
- snmp		
- nto		
- the met filter		
- 12to configuration		
- vlan settings		
- Fluidity		
- misc settings		
- smart license		
MANAGEMENT SETTINGS		
- remote access		
- firmware upgrade		
- status		
- configuration settings		
- reset factory default		
- reboot		
- logout		
	© 2023 Cisco and/or its affiliates. All rights reserved	d.

Step 2 Enter the community identity value in the **Community ID** field.

Important The same community identity value must be set for all the access points in the network.

Step 3 Check the **Enable SNMP event trap** check box to enable SNMP event traps for significant system-related events, and then enter the network management station (NMS) host name in the **NMS hostname** field.

Important The NMS host to which traps are sent must have an SNMP agent that is configured to collect SNMP v2c traps.

- **Step 4** Check the **Enable SNMP periodic trap** check box to enable periodic SNMP traps to send SNMP traps at defined periodic intervals and then enter the host name of NMS in the **NMS hostname** field. Enter the notification period (minutes) in the **Notification period**.
- Step 5 Click Save.

Configuring SNMP Version v3 using GUI

By default, the access points are shipped from the factory with SNMP in disabled mode.

To change the access point's SNMP mode to version **v3** and then configure the access point, follow these steps:

Step 1Choose the version v3 from the SNMP mode drop-down list.
The SNMP window appears.

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 5.21.200.136 - MESH END MODE		
TOD IW Offline	SNMP		
-MONITOR Disabled	SNMP		
M-QUADRO	SNMP mode: v3 V		
ENERAL SETTINGS	SNMP v3 username: user		
virelass radio	CNIND 12 meaning and another		
antenna alignment and stats	Sinime vo passivoro:		
ETWORK CONTROL	Show SNMP v3 password:		
advanced tools	SNMP v3 authentication proto: SHA		
DVANCED SETTINGS			
advanced radio settings	SNMP v3 encryption: AES V		
static routes			
allowlist / blocklist	SNMP v3 encryption passphrase:		
nulticast	Show SNMP v3 encryption passphrase:		
snmp	Enable SNMP periodic trap:		
adius			
ntp	Enable SNMP event trap:		
2th configuration	Engine ID: Currently Unavailable		
dan settings	NMS hostname: 192.168.0.100		
Fluidity			
nisc settings	Notification period (minutes): 1		
smart license			
ANAGEMENT SETTINGS			
remote access	Reset Save		
îrmware upgrade			
status			
configuration settings			
eset factory default			
reboot			
ogout			

Step 2 Enter the SNMP v3 username in the **SNMP v3 username** field.

Note The same SNMP v3 username must be set for all the access points in the network.

- Step 3 To change the current SNMP v3 password, enter the new password in the SNMP v3 password field.
- **Step 4** Choose the authentication type from the **SNMP v3 authentication proto** drop-down list. The available options are:
 - MD5
 - SHA

Important The same SNMP authentication protocol must be set for all the access points in the network.

- **Step 5** Choose the appropriate encryption protocol from the **SNMP v3 encryption** drop-down list. The available options are:
 - No Encryption
 - DES (Data Encryption Standard)
 - AES (Advanced Encryption Standard)
 - **Note** The same encryption protocol must be set for all the access points in the network.
- **Step 6** To change the encryption passphrase, enter a new passphrase in the **SNMP v3 encryption passphrase** field.
- **Step 7** Check the **Enable SNMP periodic trap** check box to enable the periodic SNMP traps to send SNMP traps at defined periodic intervals and then enter the host name of NMS in the **NMS hostname** field. Enter the notification period (minutes) in the **Notification period**.
- **Step 8** Check the **Enable SNMP event trap** check box to enable the SNMP event traps for significant system-related events and then enter the host name of NMS in the **NMS hostname** field.
 - **Note** The NMS host to which traps are sent must have an SNMP agent configured to collect v3 traps.

Step 9 Click Save.

If you disable the SNMP, the following pop-up appears:

