SNMP Traps

Information About Configuring SNMP Traps

Simple Network Management Protocol (SNMP) Traps are alert messages sent from a remote SNMP-enabled device such as the controller, to an SNMP manager. Traps are unreliable because the receiver does not send acknowledgments when the device receives traps. Hence, the sender cannot determine if the traps were received.

In order to configure the controller to send SNMP notifications, you must enter at least one **snmp-server host** command. If you do not enter an **snmp-server host** command, no notifications are sent.

In order to enable multiple hosts, you must specify separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host. When multiple **snmp-server host** commands are given for the same host and notification of either trap or inform, each command overwrites the previous command. Only the last **snmp-server host** command is taken into account. For example, if you enter an **snmp-server host** inform command for a host and then enter another **snmp-server host** inform command for the same host, the second command replaces the first.

Specify the **snmp-server enable traps wireless <TrapName>** command in order to specify which SNMP notifications are sent globally. In order for a host to receive wireless notifications, at least one **snmp-server enable traps wireless <TrapName>** command and the **snmp-server host** command for that host must be enabled. However, some notification types cannot be controlled with the **snmp-server enable** command. And some notification types are enabled by default . For example, few AP related traps **crash**, **register**, and **noradiocards** are enabled by default.

Configuring SNMP Traps (GUI)

Procedure

Step 1 Choose **Administration** > **Management** > **SNMP**.
The SNMP page is displayed. By default, the SNMP mode is disabled. To enable or disable SMNP, click the **SNMP Mode** toggle button.

Step 2 Choose the **Wireless Traps** tab.
By default, all SNMP wireless traps are disabled except the **Access Point** trap. To enable all the wireless traps, click **Enable All**.

Step 3 Select the wireless SNMP trap that you wish to enable. Click the **Select All** check box to enable all the trapflags present in the trap. For example, to enable all the trapflags in the **Mesh** trap section, check the **Select All** check box present at the right-hand corner of the section. Uncheck the **Select All** check box to remove selection.

Note In the **Access Point** trap, **Crash**, **No Radio Cards**, and **Register** trapflags are enabled by default. Select **Broken Antenna** trapflag to detect broken antenna. Select **AP Stats** trapflag to enable a trap for AP statistics.

Step 4 Click **Apply**.

Enabling Access Points Traps (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**snmp-server enable traps wireless AP** **Example:** `Device# snmp-server enable traps wireless AP`	Enables wireless SNMP traps for access points.
Step 3	**trapflags ap** { **authorization** | **broken-antenna** | **crash** | **interfaceup** | **ipaddrfallback** | **mfp** | **mode** | **noradiocards** | **register** } **Example:** `Device# trapflags ap authorization`	Enables or disables sending AP related trapflags. The **crash**, **noradiocards**, and **register** trapflags are enabled by default.

Enabling Wireless Client Traps (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**snmp-server enable traps wireless bsnMobileStation** **Example:** `Device# snmp-server enable traps wireless bsnMobileStation`	Enables wireless client traps.
Step 3	**trapflags client dot11** {**assocfail** | **associate** | **authenticate** | **authfail** | **deauthenticate** | **disassociate** } **Example:** `Device# trapflags client dot11 assocfail`	Enables or disables dot11 related trapflags for clients.
Step 4	**trapflags client excluded** **Example:** `Device# trapflags client excluded`	Enables the excluded trapflags for clients.

Enabling Mesh Traps (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**snmp-server enable traps wireless MESH** **Example:** `Device# snmp-server enable traps wireless MESH`	Enables wireless mesh traps.
Step 3	**trapflags mesh** {**abate-snr** | **authentication-failure** | **child-moved** |	Enables or disables mesh trapflags.

	Command or Action	Purpose
	excessive-children | **excessive-hopcount** | **onset-snr** | **parent-change** } **Example:** `Device# trapflags mesh abate-snr`	

Enabling RF Traps (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**snmp-server enable traps wireless bsnAutoRF** **Example:** `Device# snmp-server enable traps wireless bsnAutoRF`	Enables wireless RF related traps.
Step 3	**trapflags rrm-params** { **channels** | **tx-power** } **Example:** `Device# trapflags rrm-params channels`	Enables or disables sending RRM parameter update related traps.
Step 4	**trapflags rrm-profile** { **coverage** | **interference** | **load** | **noise** } **Example:** `Device# trapflags rrm-profile coverage`	Enables or disables RRM profile related traps.

Enabling Rogue, Mobility, RRM, and General Traps (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**snmp-server enable traps wireless rogue** **Example:** `Device# snmp-server enable traps wireless rogue`	Enables traps for wireless rogue.
Step 3	**trapflags rogue-ap** **Example:** `Device# trapflags rogue-ap`	Enables rogue AP detection trapflag.
Step 4	**trapflags rogue-client** **Example:** `Device# trapflags rogue-client`	Enables rogue client detection trapflag.
Step 5	**snmp-server enable traps wireless wireless_mobility** **Example:** `Device# snmp-server enable traps wireless wireless_mobility`	Enables traps for wireless mobility.
Step 6	**trapflags anchor** **Example:** `Device# trapflags anchor`	Enables anchor trapflags.
Step 7	**snmp-server enable traps wireless RRM** **Example:** `Device# snmp-server enable traps wireless RRM`	Enables traps for wireless RRM.
Step 8	**trapflags rrm-params group** **Example:** `Device# trapflags rrm-params group`	Enables or disables the RRM parameter related traps, when the RF manager group changes.
Step 9	**snmp-server enable traps wireless bsnGeneral** **Example:** `Device# snmp-server enable traps wireless bsnGeneral`	Enables general controller traps.

Verifying SNMP Wireless Traps

To verify the various SNMP traps enabled, use the following command:

```
Device# show run | sec trapflag
trapflags ap crash
trapflags ap noradiocards
```

```
trapflags ap register
trapflags rogue-client
```