Intelligent Capture Hardening

Feature History for Cisco Intelligent Capture Hardening

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature History for Cisco Intelligent Capture Hardening

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.12.1	Cisco Intelligent Capture (iCAP) Hardening	The following enhancements are made to the iCAP feature: • Anomaly Detection • RF Statistics

Information About Cisco Intelligent Capture Hardening

The Cisco Intelligent Capture (iCAP) feature aims at making troubleshooting for wireless clients and APs easier. When there are onboarding issues for wireless clients or AP transmission issues, network operators can find out the cause by using the Cisco Catalyst CenterGUI. The Cisco Catalyst Center gathers data from the wireless controller and APs, and displays an aggregated view.

The following enhancements are made to the iCAP feature:

- Anomaly Detection
- RF Statistics

Anomaly Detection

Anomaly Detection is the capability of Cisco APs to detect possible anomalies in the lifecycle of wireless clients and APs.

This functionality is crucial as it allows you to determine if there is an issue in the network, to identify what happened, and avoid the same problem in the future.

APs send individual anomalies to Cisco Catalyst Center every time an anomaly is detected. To prevent Cisco Catalyst Center from getting bombarded with anomaly events of the same type and from the same client, enhancements are made to collapse repeated events, and multiple events are aggregated for the same client if the events occur within a certain time frame.

Anomaly-detection configurations are enhanced on the controller to provision and display the iCAP status.

RF Statistics

The Cisco Catalyst Center receives RF statistics of connected APs. Until Cisco IOS XE Dublin 17.11.1, the data received was basic statistical information. However, from Cisco IOS XE Dublin 17.12.1 onwards, per AP statistical information is directly sent from the wireless controller through iCAP subscription to specific APs.

Configuring Anomaly Detection in AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# onfigure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**icap subscription client anomaly-detection report-individual enable** **Example:** `Device(config-ap-profile)# icap subscription client anomaly-detection report-individual enable`	Enables individual reports for client anomaly-detection subscription.
Step 4	**icap subscription client anomaly-detection report-individual enable aggregate** **Example:** `Device(config-ap-profile)# icap subscription client anomaly-detection report-individual enable aggregate`	Enables individual reports aggregation for client anomaly-detection subscription. This command is disabled by default.

	Command or Action	Purpose
Step 5	**icap subscription client anomaly-detection report-individual per-client throttle** *number-of-event-reports* **Example:** `Device(config-ap-profile)# icap subscription client anomaly-detection report-individual per-client throttle 20`	Configures event reports per client, every five minutes. The value of an event report ranges from 0 to 50 reports. The default value is five reports.
Step 6	**icap subscription client anomaly-detection report-individual per-type throttle** *number-of-event-reports* **Example:** `Device(config-ap-profile)# icap subscription client anomaly-detection report-individual per-type throttle 50`	Configures event reports per type, every five minutes. The value of an event report ranges from 0 to 100 reports. The default value is five reports.

Configuring Anomaly Detection in an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **icap subscription client anomaly-detection report-individual enable** **Example:** `Device# ap name ap1 icap subscription client anomaly-detection report-individual enable`	Enables individual reports for client anomaly-detection subscription for a single AP.
Step 3	**ap name** *ap-name* **icap subscription client anomaly-detection report-individual enable aggregate** **Example:** `Device# ap name ap1 icap subscription client anomaly-detection report-individual enable`	Enables individual reports aggregation for client anomaly-detection subscription, for a single AP.
Step 4	**ap name** *ap-name* **icap subscription client anomaly-detection report-individual per-client throttle** *number-of-event-reports* **Example:**	Configures event reports per client, every five minutes, for a single AP. The value of an event report ranges from 0 to 50 reports.

	Command or Action	Purpose
	`Device# ap name ap1 icap subscription client anomaly-detection report-individual per-client throttle 20`	
Step 5	**ap name** *ap-name* **icap subscription client anomaly-detection report-individual per-type throttle** *number-of-event-reports* **Example:** `Device# ap name ap1 icap subscription client anomaly-detection report-individual per-type throttle 50`	Configures event reports per type, every five minutes, for a single AP. The value of an event report ranges from 0 to 100 reports.

Verifying Anomaly Detection and RF Statistics

To verify the current status of the anomaly-detection subscription of an AP, use the following command:

```
Device# show ap name cisco-AP icap subscription client anomaly-detection chassis active R0
Per-AP ICap configuration

Anomaly detection subscription
  State                     : enabled
  Client filter             : 006b.f107.a520
  Client filter             : 006b.f107.a521
  DHCP timeout (seconds)    : 5
  Trigger AP packet trace   : enabled
  Report Individual         : enabled
  Report Individual aggregate : enabled
  Report Individual throttled events (per 5 minute) : 5
  Report Individual per type throttled events (per 5 minute) : 14
  Report Individual per client throttled events (per 5 minute) : 15
  Report Summary            : disabled
  Report Summary frequency (minutes) : 5
```

To verify RF statistics, use the following command:

Note The controller **show** command is enhanced to display data from the **txTotalDrops** counter.

```
Device# show wireless client mac-address 00XX.ecXX.7aXX detail
.
.
.
Client Statistics:
  Number of Bytes Received from Client : 62861
  Number of Bytes Sent to Client : 6754
  Number of Packets Received from Client : 455
  Number of Packets Sent to Client : 65
  Number of Data Retries : 0
  Number of RTS Retries : 0
  Number of Tx Total Dropped Packets: x
  Number of Duplicate Received Packets : 0
  Number of Decrypt Failed Packets : 0
  Number of Mic Failured Packets : 0
  Number of Mic Missing Packets : 0
  Number of Policy Errors : 0
```

```
  Radio Signal Strength Indicator : -21 dBm
  Signal to Noise Ratio : 73 dB
.
.
.
```