CAPWAP Message Aggregation

Feature History for CAPWAP Message Aggregation

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 CAPWAP Message Aggregation

Release	Feature	Feature Information
Cisco IOS XE 17.14.1	CAPWAP Message Aggregation	The CAPWAP Message Aggregation feature aggregates the CAPWAP control messages of the same type waiting in the queue to be transmitted to the AP.

Information About CAPWAP Message Aggregation

The CAPWAP Message Aggregation feature aggregates the CAPWAP control messages to be sent to APs. When APs are busy processing packets, the messages to be sent to the APs are stored in the controller. When you enable the feature, if the last message type in the queue and the current message type are the same, the CAPWAP messages are aggregated and capped at Maximum Transmission Unit (MTU). This improves the performance of the system.

Guidelines

- Applicable to all AP modes.
- The CAPWAP Message Aggregation feature is disabled by default.

Use Case

Flex deployment use case: You can expect a round-trip delay when packets are sent over wide area network (WAN) in Flex deployments. With the CAPWAP message aggregation, the round-trip time reduces significantly. Also, the client join and client roam are faster.

Configuring CAPWAP Message Aggregation (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile default-ap-profile`	Configures an AP profile and enters the AP profile configuration mode.
Step 3	**capwap aggregation** **Example:** `Device(config-ap-profile)# capwap aggregation`	Enables CAPWAP message aggregation. This feature is disabled by default.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verifying CAPWAP Message Aggregation

To view the total number of aggregated CAPWAP control packets for the controller, use the following command:

```
Device# show wireless stats ap packet

Packet stats

Capwap Control Packets Received* : 11183016
Capwap Data Keep Alive Packets Received : 160399
Capwap Data DOT1X EAP Packets Received: 549
Capwap Data DOT1X Mgmt Packets Received: 6003
Capwap Data DOT1X Key Type Packets Received: 0
Capwap Data DOT1X Control Packets Received: 0
Capwap Data ARP Packets Received: 0
Capwap Data IP Packets Received: 0
Capwap Data IPV6 Packets Received: 0
Capwap Data RRM Packets Received: 0
Capwap Data DHCP Packets Received: 0
```

```
Capwap Data RFID Packets Received: 0
Capwap Data IAPP Packets Received: 2531939
Capwap Dgram Input Errors : 0
Capwap Discovery Packets Received : 22299
Capwap Discovery Dgram Input Errors : 0
Aggregated Capwap Control Packets Sent: 119337
**** Note: Capwap control packets exclude discovery/primary discovery packets ****
```

To verify the status of the CAPWAP message aggregation feature, use the following command:

```
Device# show ap profile name default-ap-profile detailed
AP Profile Name               : default-ap-profile
Description                   : default custom profile
Country code                  : Not configured
Stats Timer                   : 180
Link Latency                  : ENABLED
Data Encryption               : DISABLED
LED State                     : ENABLED
NTP server                    : 0.0.0.0
NTP Authentication            : DISABLED
Jumbo MTU                     : ENABLED
24ghz Report Interval         : 90
5ghz Report Interval          : 90
bssid stats status            : ENABLED
bssid stats frqncy interval   : 120
bssid neighbor stats status   : ENABLED
bssid neighbor stats interval : 120
CAPWAP Control Aggregation    : ENABLED
```