Hewlett Packard Enterprise

HPE aruba networking

AOS-CX 10.13 Update: IP Flow Manager

Matt Fern, Technical Marketing Engineer

November 2023

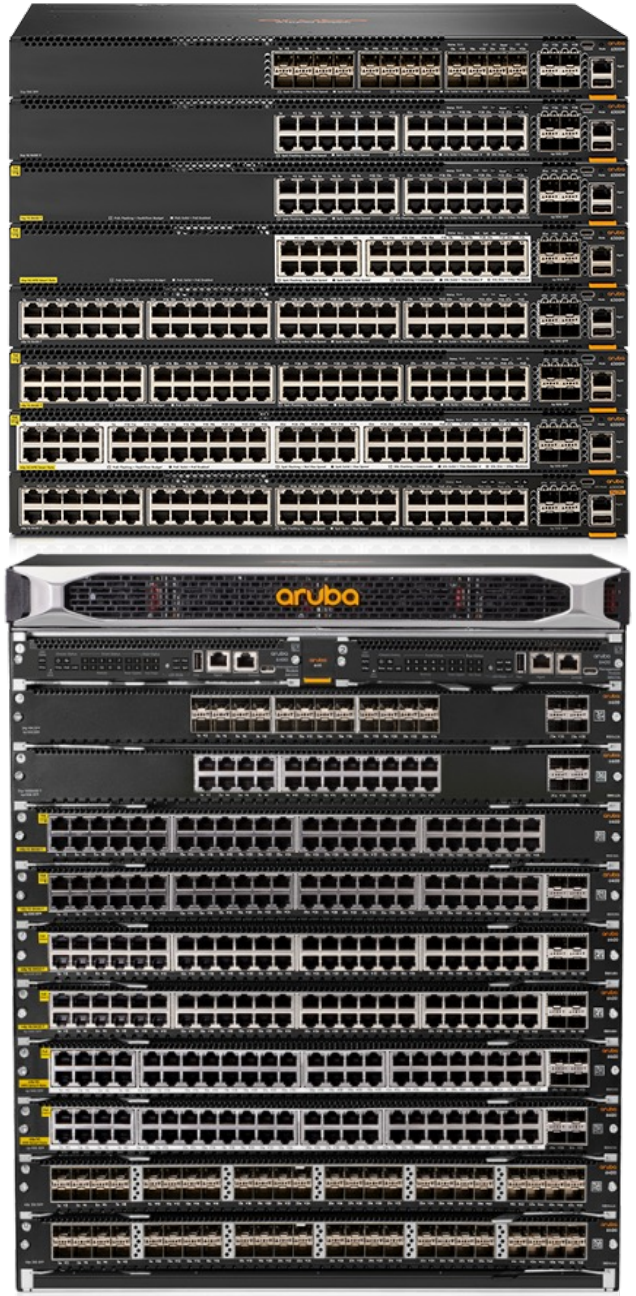
Agenda

1	Overview
2	Details
3	Configuration
4	Troubleshooting
5	Additional Resources

Overview

IP Flow Manager (IPFM)

- The **AOS-CX IP Flow Manager (IPFM)** was originally developed as part of the Application Recognition and Control (ARC) feature in AOS-CX 10.11.
- As originally implemented, flow tracking was used by AOS-CX to identify specific traffic flows initiated by connected users and devices for classification by ARC, and to apply actions defined by Application-Based Policy (ABP).
- In AOS-CX 10.13, flow tracking has been decoupled from ARC and implemented as a common framework known as the IP Flow Manager that is utilized by the following features:
  - Application Recognition and Control
  - Application-Based Policy
  - Reflexive Policy



IP Flow Manager

More information

For more details on AOS-CX flow tracking, review the **AOS-CX 10.11 Application Recognition** update:
https://www.youtube.com/watch?v=C1kogaM07l8&list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS

Details

IP Flow Manager
Platform support

Feature	4100i	6000	6100	6200	6300	6400	8100	8320	8325	8360	8400	9300	10000	OVA
IP Flow Manager	No	No	No	No	**Yes**	**Yes (v2 only)**	No	No	No	No	No	No	No	No

- **6300:** All supported 6300F and 6300M models (standalone and VSF stacks)
- **6400:** v2 line cards only (R0X__**C** part numbers)

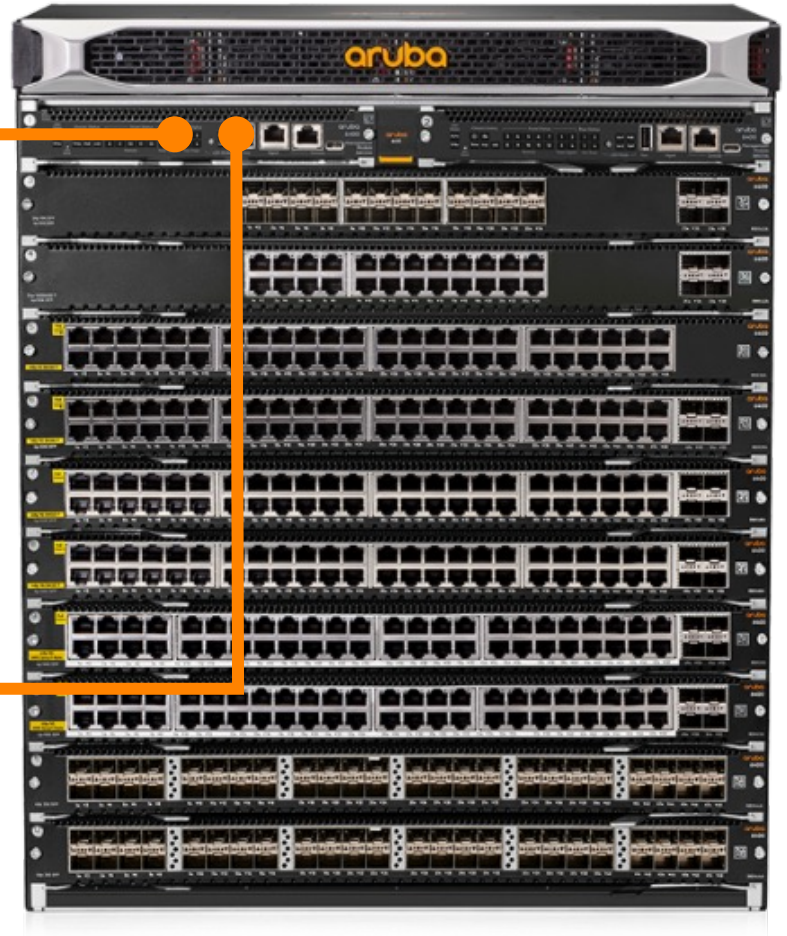
IP Flow Manager
Components

IP Flow Manager Daemon (ipfmd)

Responsible for overall control of flow tracking, maintains flow cache, communicates with IPFM agent running on line cards/VSF members

Message Queuing Telemetry Transport (MQTT) Broker[1]

Facilitates data exchange between daemon running on MM/Conductor and agents running on LCs/VSF members



[1] https://www.hivemq.com/blog/mqtt-essentials-part-3-client-broker-connection-establishment/
[2] https://www.hivemq.com/blog/mqtt-essentials-part-5-mqtt-topics-best-practices/

IP Flow Manager
Components

DPI Engine

Classifies flows on IPFM-enabled ports, provides application ID, name, category, URL information to IPFM once classification is complete

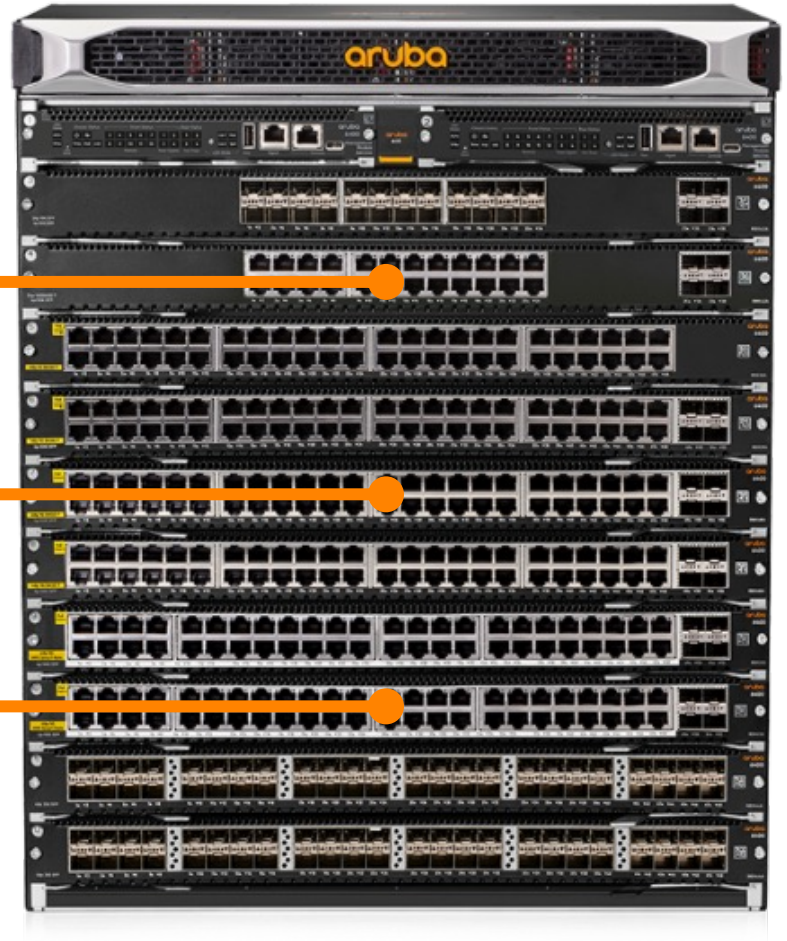
IP Flow Manager Agent

Receives flow packets, extracts 5-tuple information and VRF, builds LC flow cache

Publishes flow data via MQTT broker to other LCs and MM daemon

IPFIX Agent

Receives application parameters from IPFM agent, forwards to IPFIX MM daemon via MQTT, which exports to internal or external collectors as configured



IP Flow Manager

Global configuration context

- Global settings for the IP Flow Manager feature are contained within the **`flow-tracking`** context.
- From this context, flow tracking can be enabled or disabled globally.
  - Flow tracking is **disabled by default**.
  - IP Source Lockdown extended mode must be disabled before flow tracking can be enabled.
  - Flow tracking must be globally enabled in order to utilize ARC, ABP, or Reflexive Policy.
- The TCP and UDP inactive flow age-out timers can also be configured from this context.

```
switch(config)# flow-tracking
switch(config-flow-tracking)# ?
  enable                 Enable flow tracking
  end                    End current mode and change to enable mode.
  exit                   Exit current mode and change to previous mode
  interface-flow-limit   Configure global concurrent flow limit for flow
                         tracking enabled interfaces
  list                   Print command list
  no                     Negate a command or set its defaults
  show                   Show running system information
  tcp-ageout             Configure age-out time for established TCP flows
  udp-ageout             Configure age-out time for established UDP flows
```

IP Flow Manager

Per-interface flow limit

- The maximum number of concurrent flows per interface is a global setting defined from the global flow-tracking context.
- The interface flow limit is **disabled by default**.
- The limit can be configured to a value between 64 and 25,000, and applies to all enabled interfaces.
  - To disable the interface flow limit, use the command **`no interface-flow-limit`** from the **`flow-tracking`** context.

```
switch(config-flow-tracking)# interface-flow-limit ?
  <64-25000>  Set the number of concurrent flows allowed on flow tracking
              enabled interfaces (Default: None)
```

IP Flow Manager

TCP age-out timer

- The age-out time for established but inactive TCP flows is configurable from the global flow-tracking context.
  - TCP flows are normally removed when a FIN/RESET packet is received as part of a monitored flow.
- When an inactive TCP flow ages out, it will be marked for removal from the LC's flow cache during the next scheduled processing batch.
- The TCP age-out timer is configurable to a value between **120** and **86,400 seconds** (1 day).
  - The default TCP age-out time is **600 seconds** (10 minutes).

```
switch(config-flow-tracking)# tcp-ageout ?
  <120-86400>  Set the TCP flow age-out time in seconds (Default: 600 seconds)
```

IP Flow Manager

UDP age-out timer

- The age-out time for established UDP flows is configurable from the global flow-tracking context.
- As with inactive TCP flows, a UDP flow that ages out will be marked for removal from the LC's flow cache during the next scheduled processing batch.
- The UDP age-out timer is configurable to a value between **30** and **86,400 seconds** (1 day).
  - The default UDP age-out time is **30 seconds**.

```
switch(config-flow-tracking)# udp-ageout ?
  <30-86400>  Set the UDP flow age-out time in seconds (Default: 30 seconds)
```

IP Flow Manager

Platform scale

	6300	6400v2[1]	6400v2 (R0X44C/R0X45C)
Total flows[2] per system/LC/member	24576	24576	61440
Flow packets per second (ingress)	3500	3500	3500
Flow packets per second (egress)	3500	3500	3500
New connections per second[3] per system/LC/member	500	500	500

[1] Except R0X44C, R0X45C
[2] IPv4 and IPv6 combined
[3] 1 connection per second = 1 ingress flow + 1 egress flow

Configuration

IPFM configuration

Global flow-tracking configuration

- Disable IP source lockdown extended mode, if currently enabled.
- Enter the global **`flow-tracking`** context.
- Use the **`enable`** command to enable flow-tracking globally.
- *Optionally*:
  - Enable and configure a global per-interface concurrent flow limit for all flow-tracking enabled interfaces.
  - Specify desired non-default TCP and/or UDP age-out times for inactive flows.

```
switch(config)# no ip source-lockdown resource-extended
switch(config)# flow-tracking
switch(config-flow-tracking)# enable
```

```
switch(config-flow-tracking)# interface-flow-limit 1024
switch(config-flow-tracking)# tcp-ageout 300
switch(config-flow-tracking)# udp-ageout 60
```

IPFM configuration – REST API

Enable IPFM globally

PATCH /system/flow_tracking

Parameters

Cancel

No parameters

Request body

application/json

```
{
  "enable": true
}
```

Execute

IPFM configuration – REST API

Configure per-interface flow limit

PATCH /system/flow_tracking

Parameters

Cancel

No parameters

Request body

application/json

```
{
  "interface_flow_limit": 256
}
```

Execute

IPFM configuration – REST API

Configure TCP/UDP age-out timers

PATCH /system/flow_tracking

Parameters Cancel

No parameters

Request body application/json

```
{
  "tcp_ageout": 120,
  "udp_ageout": 60
}
```

Execute

IPFM configuration – REST API

Get current IPFM configuration

GET /system/flow_tracking

Parameters Cancel

Name	Description
attributes array[string] *(query)*	Columns to display. -- enable failure_reason tcp_ageout
depth integer *(query)*	Depth to traverse. depth - Depth to traverse.
selector string *(query)*	Select configuration, status and/or statistics. Default is all categories. --
filter array[string] *(query)*	Filter rows by attribute values. Format: attribute:value Add item
count string *(query)*	Count the number of rows found. --
If-None-Match string *(header)*	Entity-tag value for representation comparison (see RFC 7232 - Conditional Requests - section 3.2) If-None-Match - Entity-tag value for represen

Execute

Server response

Code	Details
200	Response body


```
{
  "enable": true,
  "failure_reason": null,
  "interface_flow_limit": null,
  "oper_status_enabled": true,
  "tcp_ageout": 600,
  "udp_ageout": 30
}
```


Download

Troubleshooting

Troubleshooting – general

Show commands

- The main show command is **`show flow-tracking`**, which displays global and per-port configuration.
- Each row in the port configuration table displays the interface number and status of App Recognition, Reflexive ACL, and flow tracking itself.
- The status of one or more interfaces can be displayed by adding an individual interface or a range of interfaces as a parameter.

```
switch# show flow-tracking ?
  IFNAME   Show flow tracking information for an interface
  IFRANGE  Show flow tracking information for a specified range of interfaces
  <cr>

switch# show flow-tracking

  Flow Tracking Global Configuration
     Configuration status            : Enabled
     Operational status              : Enabled
     Failure Reason                  : NA
     UDP Ageout                      : 30  (Seconds)
     TCP Ageout                      : 600 (Seconds)
     Interface Flow limit            : None

  Flow Tracking Port Configuration

    Interface       App Recognition    Reflexive ACL         Operation Status
    -----------     -----------       -------------------      ----------
   1/3/1              Enabled             Disabled            Enabled
   1/3/2              Disabled            Disabled            Disabled
   1/3/3              Disabled            Disabled            Disabled
   1/3/4              Disabled            Disabled            Disabled
   1/3/5              Disabled            Disabled            Disabled
   1/3/6              Disabled            Disabled            Disabled
   1/3/7              Disabled            Disabled            Disabled
   1/3/8              Disabled            Disabled            Disabled

switch# show flow-tracking 1/3/1

  Flow Tracking Port Configuration

    Interface       App Recognition    Reflexive ACL         Operation Status
    -----------     -----------       -------------------      ----------
   1/3/1              Enabled             Disabled            Enabled
```

Additional Resources

Additional Resources

- User Guides
  - AOS-CX 10.13 Security Guide (6200, 6300, 6400 Switch Series)
    - Chapter 16: **Application Recognition and Control**
    - Chapter 17: **IP Flow Information Export**
  - AOS-CX 10.13 Monitoring Guide (6300, 6400 Switch Series)
    - Chapter 3: **IP Flow Information Export**

Thank you!