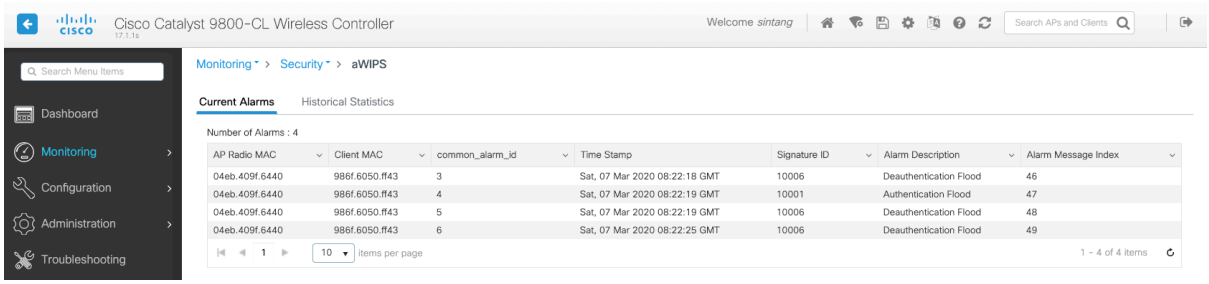
Adaptive WIPS Telemetry Monitor Deployment Guide

Starting from Catalyst 9800 IOS-XE 17.1, adaptive WIPS signatures are supported locally on the controller. 16x signatures will be supported on the controller by 17.3 release. The remaining signatures will be supported by DNA Center.

DNA Center is required to provide aWIPS logging and monitoring capabilities. Catalyst 9800 is able to detect wireless attacks using its internal 16x signatures, but it is not able to store the alarm beyond 5 minutes.

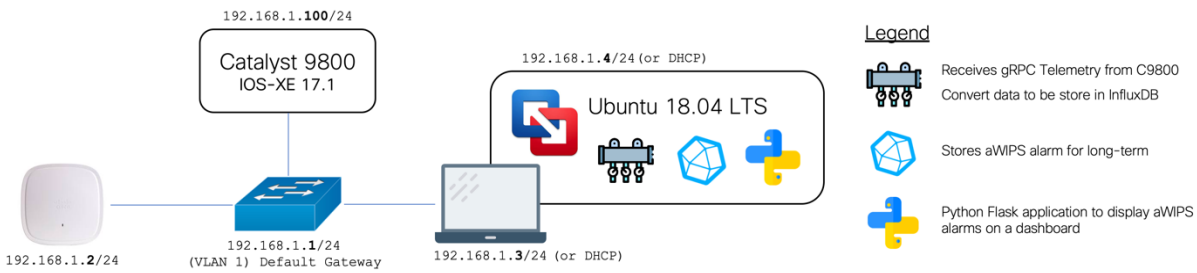


(Alarms will be available on the Catalyst 9800 for 5 minutes)

The purpose of this ad-hoc solution is to provide an external aWIPS logging and monitoring system that do not rely on DNA Center.

The use case is to provide a quick setup to troubleshoot a Proof-of-Concept (POC) environment that have complex RF characteristics. You may have suspicion that the Rogue APs and the legitimately placed APs may be degrading the performance of your POC RF environment. Having a quick-to-deploy aWIPS detection and monitoring system will help to identify the root cause of the issue.

Solution Overview



Tang Sing Yuen
Technical Solutions Specialist, Cisco Systems
sintang@cisco.com

Catalyst 9800 will be configured to stream aWIPS Telemetry at a pre-determined interval (E.G 1 min) to the Pipeline application which resides as an Ubuntu VM in the MacOS laptop.

Pipeline receives the gRPC Telemetry from C9800 and converts the data into an InfluxDB acceptable format. InfluxDB will store the aWIPS alarm history even when the C9800 deletes them after 5 minutes.

For visualization, the Python Flask application will provide a web dashboard that pulls aWIPS alarm data from InfluxDB.

Required Components

Layer 2 Switch

Cisco Access Point
- Tested with C9120AXI

Catalyst 9800 IOS-XE 17.1 and above (EWC not tested)

MacOS Laptop with VMware Fusion
- Tested with 11.1.0

Ubuntu Virtual Machine

Ubuntu Virtual Machine

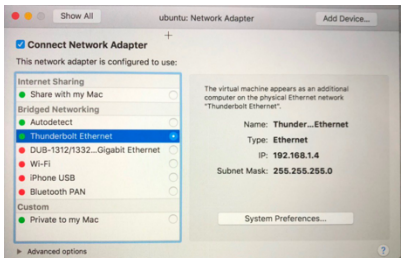
The Ubuntu VM is pre-installed with the necessary packages and software components to operate the following applications:
- Pipeline
- InfluxDB
- aWIPS Web Dashboard (Python Flask)

Request the Ubuntu VM from sintang@cisco.com

Ubuntu VM Setup

Setup VM Network

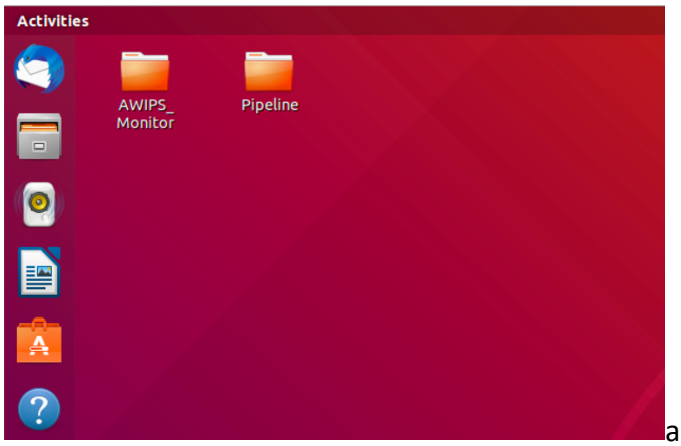
Ensure that the LAN connection is selected. Do not select “Share with my Mac” *(Internal NAT)*



Tang Sing Yuen
Technical Solutions Specialist, Cisco Systems
sintang@cisco.com

Start Ubuntu

Start the Ubuntu machine with the username **ubuntu** password **cisco,123**



a

The “AWIPS_Monitor” is the Python Web Dashboard for aWIPS monitoring.

The “Pipeline” is the application for receiving Telemetry sent by Catalyst 9800.

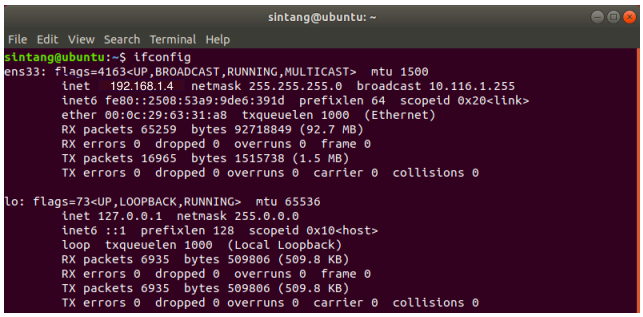
InfluxDB is installed natively into the operating system.

Verify Network IP Address

Open terminal and run the command:

```
ifconfig
```

Verify the IP Address (or configure as STATIC if DHCP is not available)



Ensure that the Ubuntu VM can ping the default gateway and Catalyst 9800.

Verify InfluxDB Database

Open up the terminal and enter the commands:

```
influx
show databases
```

```
sintang@ubuntu: ~
File  Edit  View  Search  Terminal  Help
sintang@ubuntu:~$ influx
Connected to http://localhost:8086 version 1.7.10
InfluxDB shell version: 1.7.10
> show databases
name: databases
name
----
_internal
mdt_db
```

Verify that the database “mdt_db” exist. This will be the database that Pipeline will push the aWIPS alarm data into.

Verify Pipeline Configuration

The main configuration files are “9800.conf” and “metrics.json”

Start Pipeline

Open up the terminal **in Pipeline folder** and enter the commands:

```
./bin/pipeline -config=9800.conf -log= --debug
```

You will need to <u>respond to the prompt</u> by providing any random username and password.

```
INFO[2020-03-12 07:12:32.563682] Metamonitoring: not enabled                    tag=pipeline
INFO[2020-03-12 07:12:32.565907] Starting up tap                                countonly=false filename="dump_script.json" name=inspector streamSpec=&{3 <nil>
} tag=pipeline

CRYPT Client [metrics_influx],[http://localhost:8086]
 Enter username: sintang
 Enter password:
INFO[2020-03-12 07:12:41.838980] setup authentication                           authenticator="http://localhost:8086" name="metrics_influx" pem= tag=pipeline u
sername=sintang
INFO[2020-03-12 07:12:41.839164] setup metrics collection                       basepath="Cisco-IOS-XE-wireless-awips-oper:awips-oper-data/awips-per-ap-info" n
ame="metrics_influx" tag=pipeline
INFO[2020-03-12 07:12:41.839235] setup metrics collection                       basepath="Cisco-IOS-XE-wireless-awips-oper:awips-oper-data/awips-alarm" name="m
etrics_influx" tag=pipeline
DEBU[2020-03-12 07:12:41.839248] metrics export configured                      file=metrics.json metricSpec={[{Cisco-IOS-XE-wireless-awips-oper:awips-oper-dat
a/awips-per-ap-info 0xc4202f63c0} {Cisco-IOS-XE-wireless-awips-oper:awips-oper-data/awips-alarm 0xc4202f66e0}] map[Cisco-IOS-XE-wireless-awips-oper:awips-oper
-data/awips-per-ap-info:0xc4202f63c0 Cisco-IOS-XE-wireless-awips-oper:awips-oper-data/awips-alarm:0xc4202f66e0] 0xc4202b4e40} name="metrics_influx" output=inf
lux tag=pipeline
DEBU[2020-03-12 07:12:41.839330] Conductor processing section...                name=conductor section=grpcdialout tag=pipeline
DEBU[2020-03-12 07:12:41.839387] Conductor processing section, type...          name=conductor section=grpcdialout tag=pipeline type=grpc
INFO[2020-03-12 07:12:41.839413] Conductor starting up section                  name=conductor section=grpcdialout stage="xport_input" tag=pipeline
INFO[2020-03-12 07:12:41.839676] Setting up workers                             database="mdt_db" influx="http://localhost:8086" name="metrics_influx" tag=pipe
line workers=2 xport_type=influx
DEBU[2020-03-12 07:12:41.839763] Conductor watching for shutdown...             config=9800.conf debug=true logfile= tag=pipeline
INFO[2020-03-12 07:12:41.839857] gRPC starting block                            encap=gpb name=grpcdialout server=:58000 tag=pipeline type="pipeline is SERVER"
INFO[2020-03-12 07:12:41.841638] gRPC: Start accepting dialout sessions         encap=gpb name=grpcdialout server=:58000 tag=pipeline type="pipeline is SERVER"
DEBU[2020-03-12 07:12:41.842358] dataMsg router running                         database="mdt_db" influx="http://localhost:8086" name="metrics_influx" tag=pipe
line workers=2 xport_type=influx
DEBU[2020-03-12 07:12:41.842541] Run worker                                     database="mdt_db" influx="http://localhost:8086" name="metrics_influx" tag=pipe
line wkid=1 workers=2 xport_type=influx
DEBU[2020-03-12 07:12:41.843076] Connected to influx node                       database="mdt_db" influx="http://localhost:8086" name="metrics_influx" tag=pipe
line wkid=1 workers=2 xport_type=influx
DEBU[2020-03-12 07:12:41.842480] Run worker                                     database="mdt_db" influx="http://localhost:8086" name="metrics_influx" tag=pipe
line wkid=0 workers=2 xport_type=influx
DEBU[2020-03-12 07:12:41.844287] Connected to influx node                       database="mdt_db" influx="http://localhost:8086" name="metrics_influx" tag=pipe
line wkid=0 workers=2 xport_type=influx
```

You will notice CLI output in this terminal when it receives the telemetry from the C9800.

***Measurements in InfluxDB will be created if the Pipeline is successful in receiving and pushing data into InfluxDB.*

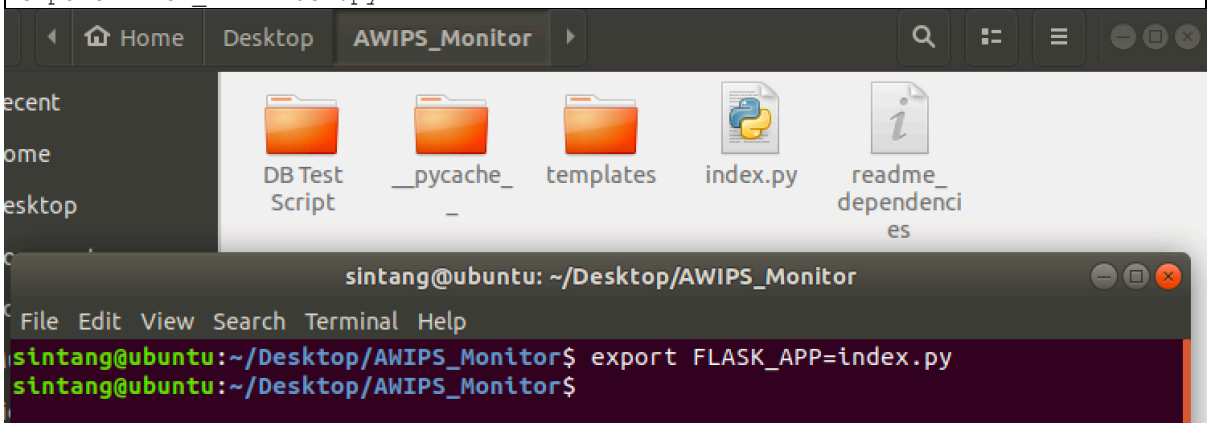
Tang Sing Yuen
Technical Solutions Specialist, Cisco Systems
sintang@cisco.com

Prepare Python Flask

Open up terminal and navigate into the “AWIPS_Monitor” folder.

Enter the following command:

```
export FLASK_APP=index.py
```

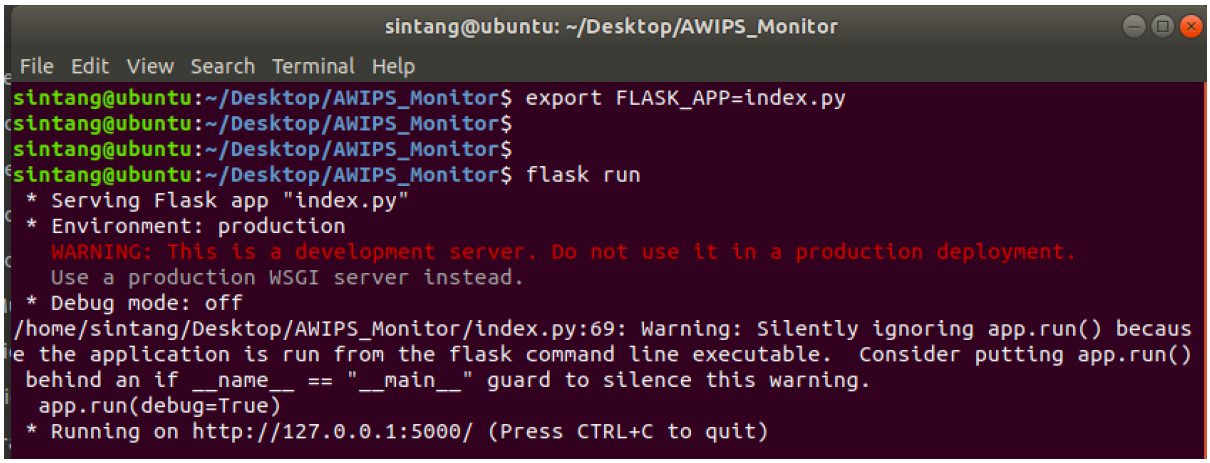


This command sets the environmental variable in order for the Flask application to know which Web page to spin up.

Start Web Dashboard

On the terminal, run the following command.

```
Flask run
```

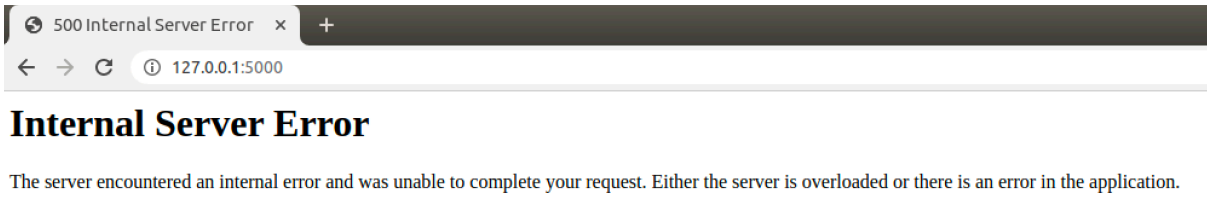


On the Ubuntu Virtual Machine, open up a web browser and put in the URL http://127.0.0.1:5000

**Take note that the server will return an error if the InfluxDB do not have data or if the measurement is not created.

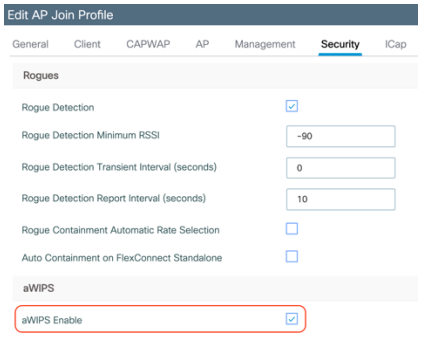
**Need to configure Streaming Telemetry on the Catalyst 9800 before the solution is ready.

Tang Sing Yuen
Technical Solutions Specialist, Cisco Systems
sintang@cisco.com



Catalyst 9800 Configuration

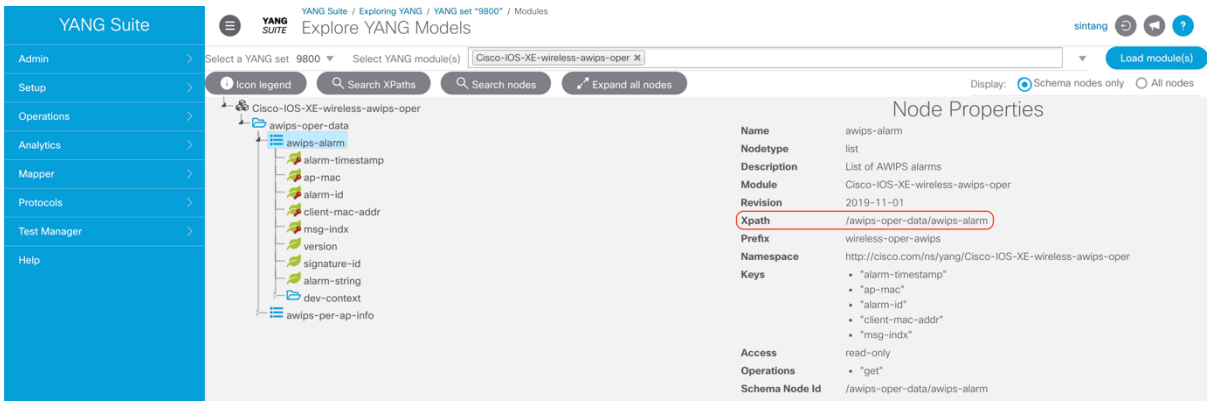
Enable aWIPS



https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/config-guide/b_wl_17_11_cg/b_wl_17_11_cg_chapter_010001100.html

Configure Streaming Telemetry

Using YANG Suite, we can explore the YANG model (Cisco-IOS-XE-wireless-awips-oper).



(Take note of the Xpath)

X-Path

```
/awips-oper-data/awips-alarm
```

Establish a Telnet/SSH session with C9800.

Enter the commands to configure Telemetry on C9800.

Tang Sing Yuen
Technical Solutions Specialist, Cisco Systems
sintang@cisco.com

```
telemetry ietf subscription 100
    encoding encode-kvgpb
    filter xpath /awips-oper-data/awips-alarm #Datapath
    source-address 192.168.1.100 #WLC's IP
    stream yang-push
    update-policy periodic 6000 #1min interval - Configurable
    receiver ip address 192.168.1.4 58000 protocol grpc-tcp #Ubuntu's IP Pipeline
```

Verify Streaming Telemetry

Enter the commands to verify that Streaming Telemetry is configured and connected.

```
Show telemetry ietf subscription 100 detail #verify configuration

Show telemetry ietf subscription 100 receiver #verify connection
```

```
9800-SY#Show telemetry ietf subscription 101 detail
Telemetry subscription detail:

  Subscription ID: 101
  Type: Configured
  State: Valid
  Stream: yang-push
  Filter:
    Filter type: xpath
    XPath: /awips-oper-data/awips-alarm
  Update policy:
    Update Trigger: periodic
    Period: 6000
  Encoding: encode-kvgpb
  Source VRF:
  Source Address: 10.68.34.85
  Notes:

  Receivers:
    Address                                    Port     Protocol         Protocol Profile
    ------------------------------------------------------------------------------------------
    10.68.34.87                                58000    grpc-tcp
```

```
9800-SY#Show telemetry ietf subscription 101 receiver
Telemetry subscription receivers detail:

  Subscription ID: 101
  Address: 10.68.34.87
  Port: 58000
  Protocol: grpc-tcp
  Profile:
  State: Connected
  Explanation:
```

*(Example with **different** IP Address)*

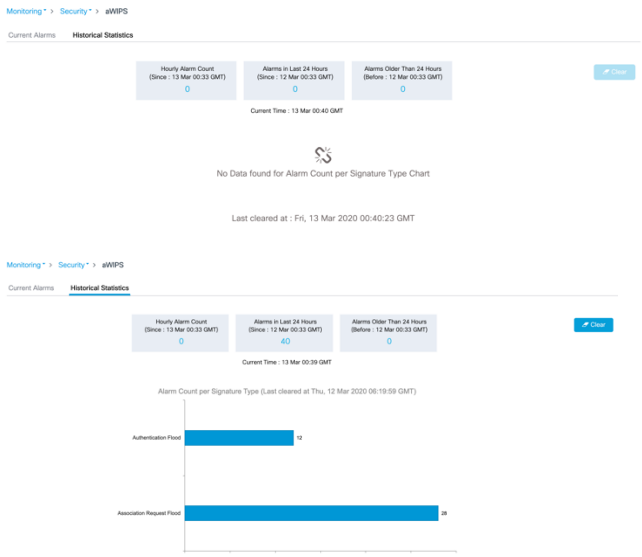
**Take note that the state will be connected only if the Pipeline application in the Ubuntu VM is running.

Tang Sing Yuen
Technical Solutions Specialist, Cisco Systems
sintang@cisco.com

Operating the Solution

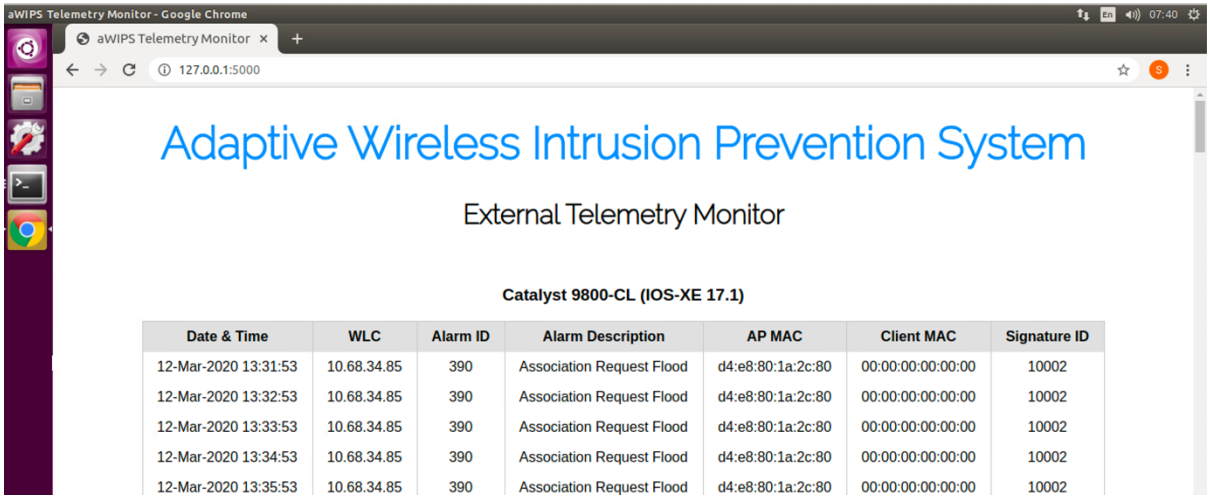
Observe the 9800 aWIPS Internal Dashboard

Wait for an alarm to appear in the statistics.



View aWIPS Web Dashboard in Ubuntu VM

http://127.0.0.1:5000



Date & Time	WLC	Alarm ID	Alarm Description	AP MAC	Client MAC	Signature ID
12-Mar-2020 13:31:53	10.68.34.85	390	Association Request Flood	d4:e8:80:1a:2c:80	00:00:00:00:00:00	10002
12-Mar-2020 13:32:53	10.68.34.85	390	Association Request Flood	d4:e8:80:1a:2c:80	00:00:00:00:00:00	10002
12-Mar-2020 13:33:53	10.68.34.85	390	Association Request Flood	d4:e8:80:1a:2c:80	00:00:00:00:00:00	10002
12-Mar-2020 13:34:53	10.68.34.85	390	Association Request Flood	d4:e8:80:1a:2c:80	00:00:00:00:00:00	10002
12-Mar-2020 13:35:53	10.68.34.85	390	Association Request Flood	d4:e8:80:1a:2c:80	00:00:00:00:00:00	10002

Tang Sing Yuen
Technical Solutions Specialist, Cisco Systems
sintang@cisco.com

EWC Support

Unable to verify if EWC is supported for streaming telemetry. YangSuite is unable to connect to EWC, and verification command on the EWC does not produce any output.

```
9800-EWC#
9800-EWC#show telemetry ietf sub all
The process for the command is not responding or is otherwise unavailable

9800-EWC#
```

Tang Sing Yuen
Technical Solutions Specialist, Cisco Systems
sintang@cisco.com