Dépannage des AP COS

Table des matières

Introduction

Ce document décrit certains des outils de dépannage disponibles pour les AP exécutant le système d'exploitation COS (Cheetah OS, Click OS, simplement Cisco AP OS).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document se concentre sur les AP COS comme les modèles AP des séries 2800, 3800, 1560 et 4800, ainsi que les nouveaux AP 11ax Catalyst 91xx.

Ce document se concentre sur de nombreuses fonctionnalités disponibles dans AireOS 8.8 et versions ultérieures. Cisco IOS® XE 16.12.2s et versions ultérieures.

Il peut y avoir des commentaires sur la disponibilité de certaines fonctionnalités dans les versions précédentes.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Capturer les traces de paquets (traces de renifleur)

PCAP câblé sur le port AP

Il est possible (à partir de la version 8.7 avec le filtre disponible dans la version 8.8) de prendre un pcap sur le port Ethernet AP. Vous pouvez soit afficher le résultat en direct sur l'interface de ligne de commande (avec seulement des détails de paquet résumés) ou l'enregistrer en tant que pcap complet dans la mémoire flash de l'AP.

Le capuchon filaire capture tout ce qui se trouve sur le côté Ethernet (à la fois Rx/Tx) et le point de dérivation à l'intérieur du point d'accès est immédiatement avant que le paquet ne soit mis sur le câble.

Cependant, il ne capture que le trafic du plan CPU AP, ce qui signifie le trafic vers et depuis l'AP (AP DHCP, AP capwap control tunnel, ...) et n'affiche pas le trafic client.

Notez que la taille est très limitée (limite de taille maximale de 5 Mo), il peut donc être nécessaire de configurer des filtres pour capturer uniquement le trafic qui vous intéresse.

Assurez-vous d'arrêter la capture de trafic avec « no debug traffic wired ip capture » ou simplement « undebug all » avant d'essayer de la copier (sinon la copie ne se termine pas car les paquets sont toujours écrits).

Procédure

Étape 1. Démarrez le pcap ; sélectionnez le type de trafic avec « debug traffic wired ip capture » :

<#root>

```
AP70DB.98E1.3DEC#debug traffic wired ip capture
% Writing packets to "/tmp/pcap/
```

AP70DB.98E1.3DEC_capture.pcap0"

```
AP70DB.98E1.3DEC#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
```

Étape 2. Attendez que le trafic circule, puis arrêtez la capture avec la commande « no debug traffic wired ip capture » ou simplement « undebug all » :

```
AP70DB.98E1.3DEC#no debug traffic wired ip capture
```

Étape 3. Copiez le fichier sur le serveur tftp/scp :

<#root>

```
AP70DB.98E1.3DEC#copy pcap
```

AP70DB.98E1.3DEC_capture.pcap0

```
 tftp 192.168.1.100
##################################################################################################
AP70DB.98E1.3DEC#
```

Étape 4. Vous pouvez maintenant ouvrir le fichier dans wireshark. Le fichier est pcap0. Sélectionnez pcap pour qu'il s'associe automatiquement à wireshark.

Options de commande

La commande debug traffic wired comporte plusieurs options qui peuvent vous aider à capturer un trafic spécifique :

```
APC4F7.D54C.E77C#debug traffic wired
  <0-3>   wired debug interface number
  filter  filter packets with tcpdump  filter string
  ip      Enable wired ip traffic dump
  tcp     Enable wired tcp traffic dump
  udp     Enable wired udp traffic dum
```

Vous pouvez ajouter « verbose » à la fin de la commande debug pour voir le vidage hexadécimal du paquet. Sachez que cela peut submerger votre session CLI très rapidement si votre filtre n'est

pas assez étroit.

PCAP câblé grâce à l'utilisation du filtre

Le format de filtre correspond au format de filtre de capture tcpdump.

	Exemple de filtre	Description
Hôte	« hôte 192.168.2.5 »	Cette opération filtre la capture de paquets pour collecter uniquement les paquets qui arrivent ou arrivent de l'hôte 192.168.2.5.
	« src host 192.168.2.5 »	Cela filtre la capture de paquets pour collecter uniquement les paquets provenant de 192.168.2.5.
	« dst host 192.168.2.5 »	Cela filtre la capture de paquets pour collecter uniquement les paquets qui vont vers 192.168.2.5.
Port	« port 443 »	Cela filtre la capture de paquets pour collecter uniquement les paquets dont la source ou la destination est le port 443.
	« port src 1055 »	Il capture le trafic provenant du port 1055.
	« dst port 443 »	Il capture le trafic destiné au port 443.

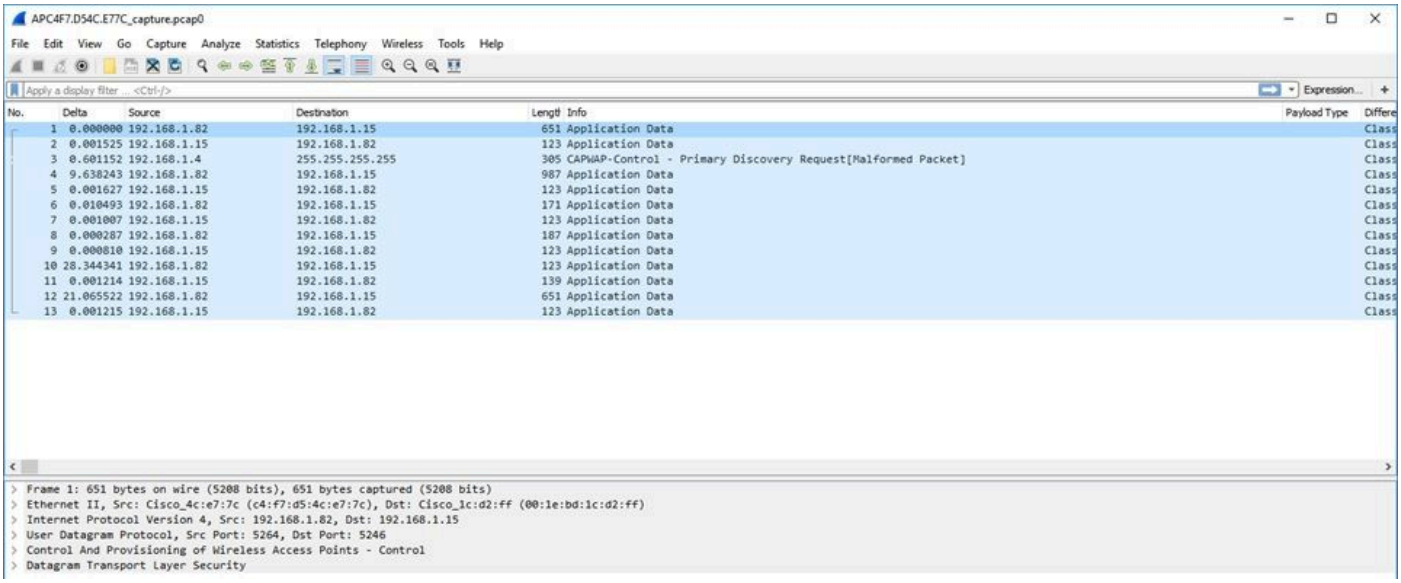
Voici un exemple où la sortie s'affiche sur la console mais également filtrée pour ne voir que les paquets de données CAPWAP :

```
APC4F7.D54C.E77C#debug traffic wired filter "port 5246"
APC4F7.D54C.E77C#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
12:20:50.483125 IP APC4F7-D54C-E77C.lan.5264 > 192.168.1.15.5246: UDP, length 81
12:20:50.484361 IP 192.168.1.15.5246 > APC4F7-D54C-E77C.lan.5264: UDP, length 97

APC4F7.D54C.E77C#no debug traffic wired filter "port 5246"
APC4F7.D54C.E77C#Killed
APC4F7.D54C.E77C#
```

Exemple de résultat sur le fichier :

```
APC4F7.D54C.E77C#debug traffic wired filter "port 5246" capture
% Writing packets to "/tmp/pcap/APC4F7.D54C.E77C_capture.pcap0"
APC4F7.D54C.E77C#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
APC4F7.D54C.E77C#no debug traffic wired filter "port 5246" capture
APC4F7.D54C.E77C#copy pcap APC4F7.D54C.E77C_capture.pcap0 tftp 192.168.1.100
##################################################################################################################
APC4F7.D54C.E77C#
```

Pour ouvrir la capture sur wireshark :



Capture radio

Il est possible d'activer la capture de paquets sur le plan de contrôle de la radio. En raison de l'impact sur les performances, il n'est pas possible d'effectuer une capture sur le plan de données radio.

Cela signifie que le flux d'association du client (sondes, authentification, association, paquets eap, arp, dhcp ainsi que les paquets de contrôle ipv6, icmp et NDP) est visible, mais pas les données que le client transmet après le passage à l'état connecté.

Procédure

Étape 1. Ajoutez l'adresse MAC du client suivi. Plusieurs adresses MAC peuvent être ajoutées. Il est également possible d'exécuter la commande pour tous les clients, mais cela n'est pas recommandé.

```
config ap client-trace address add < client-mac> --- Per client debugging. Allows multiple macs.
config ap client-trace all-clients <enable | disable>  -- All clients debugging. Not recommended.
```

Étape 2. Définissez un filtre pour enregistrer uniquement des protocoles spécifiques ou tous les

protocoles pris en charge :

```
config ap client-trace filter <all|arp|assoc|auth|dhcp|eap|icmp|ipv6|ndp|probe> <enable|disable>
```

Étape 3. Choisissez d'afficher la sortie sur la console (de manière asynchrone) :

```
configure ap client-trace output console-log enable
```

Étape 4. Démarrez le suivi.

```
config ap client-trace start
```

Exemple :

<#root>

```
APOCD0.F894.46E4#show dot11 clients

Total dot11 clients: 1
       Client MAC Slot ID WLAN ID AID    WLAN Name RSSI Maxrate WGB

A8:DB:03:08:4C:4A

       0       1   1 testewlcwlan  -41 MCS92SS  No

APOCD0.F894.46E4#config ap client-trace address add

A8:DB:03:08:4C:4A


APOCD0.F894.46E4#config ap client-trace filter
  all    Trace ALL filters
  arp    Trace arp Packets
  assoc  Trace assoc Packets
  auth   Trace auth Packets
  dhcp   Trace dhcp Packets
  eap    Trace eap Packets
  icmp   Trace icmp Packets
  ipv6   Trace IPv6 Packets
  ndp    Trace ndp Packets
  probe  Trace probe Packets
APOCD0.F894.46E4#config ap client-trace filter all enable
APOCD0.F894.46E4#configure ap client-trace output console-log enable
APOCD0.F894.46E4#configure ap client-trace start
APOCD0.F894.46E4#term mon
```

Pour arrêter la capture :

```
configure ap client-trace stop
configure ap client-trace clear
configure ap client-trace address clear
```

Vérifier

Vérifier le suivi client :

<#root>

AP70DB.98E1.3DEC#

show ap client-trace status

```
Client Trace Status         : Started

Client Trace ALL Clients    : disable

Client Trace Address        : a8:db:03:08:4c:4a

Remote/Dump Client Trace Address    : a8:db:03:08:4c:4a

Client Trace Filter         : probe
Client Trace Filter         : auth
Client Trace Filter         : assoc
Client Trace Filter         : eap
Client Trace Filter         : dhcp
Client Trace Filter         : dhcpv6
Client Trace Filter         : icmp
Client Trace Filter         : icmpv6
Client Trace Filter         : ndp
Client Trace Filter         : arp

Client Trace Output         : eventbuf
Client Trace Output         : console-log
Client Trace Output         : dump
Client Trace Output         : remote

Remote trace IP             : 192.168.1.100
Remote trace dest port      : 5688
NOTE - Only VIP packets are seen on remote if VIP is enabled

Dump packet length          : 10
Client Trace Inline Monitor            : disable
Client Trace Inline Monitor pkt-attach : disable
```

Exemple d'une connexion client réussie :

Les lettres entre crochets vous aident à comprendre où cette trame a été vue (E pour Ethernet, W pour Wireless, C pour le module Click lorsqu'il est interne au point d'accès) et dans quelle direction (Upload ou Download).

Voici un petit tableau de la signification de ces lettres :

U - paquet de liaison ascendante (du client)
D - paquet de liaison descendante (à cliquer)
W - Pilote de module sans fil
E - Pilote Ethernet de module
C - module Click

Autres options

Afficher le journal de manière asynchrone :

Les journaux peuvent alors être consultés avec la commande : "show ap client-trace events mac xx:xx:xx:xx:xx" (ou remplacez le mac par "all")

<#root>

```
AP0CD0.F894.46E4#
```

show ap client-trace events mac a8:db:03:08:4c:4a

```
[*04/06/2020 10:11:54.287675] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v1> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:11:54.288144] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:11:54.289870] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ASSOC_REQUEST
[*04/06/2020 10:11:54.317341] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ASSOC_RESPONS
[*04/06/2020 10:11:54.341370] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] EAPOL_KEY.M1 : Desc
[*04/06/2020 10:11:54.374500] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] EAPOL_KEY.M2 : Desc
```

```
[*04/06/2020 10:11:54.377237] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] EAPOL_KEY.M3 : Desc
[*04/06/2020 10:11:54.390255] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] EAPOL_KEY.M4 : Desc
[*04/06/2020 10:11:54.396855] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.416650] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.469089] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.469157] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:57.921877] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:57.921942] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:15:36.123119] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_DEAUTHENTICAT
[*04/06/2020 10:15:36.127731] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_DISASSOC : (.
[*04/06/2020 10:17:24.128751] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.128870] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v1> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.129303] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.133026] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ASSOC_REQUEST
[*04/06/2020 10:17:24.136095] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ASSOC_RESPONS
[*04/06/2020 10:17:24.138732] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M1 : Desc
[*04/06/2020 10:17:24.257295] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] EAPOL_KEY.M2 : Desc
[*04/06/2020 10:17:24.258105] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M3 : Desc
[*04/06/2020 10:17:24.278937] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] EAPOL_KEY.M4 : Desc
[*04/06/2020 10:17:24.287459] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.301344] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.327482] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.327517] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.430136] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.430202] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:19:08.075326] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_PROBE_REQUEST
[*04/06/2020 10:19:08.075392] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_PROBE_RESPONS
[*04/06/2020 10:19:08.075437] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v1> [U:W] DOT11_PROBE_REQUEST
```

Vider les paquets au format hexadécimal

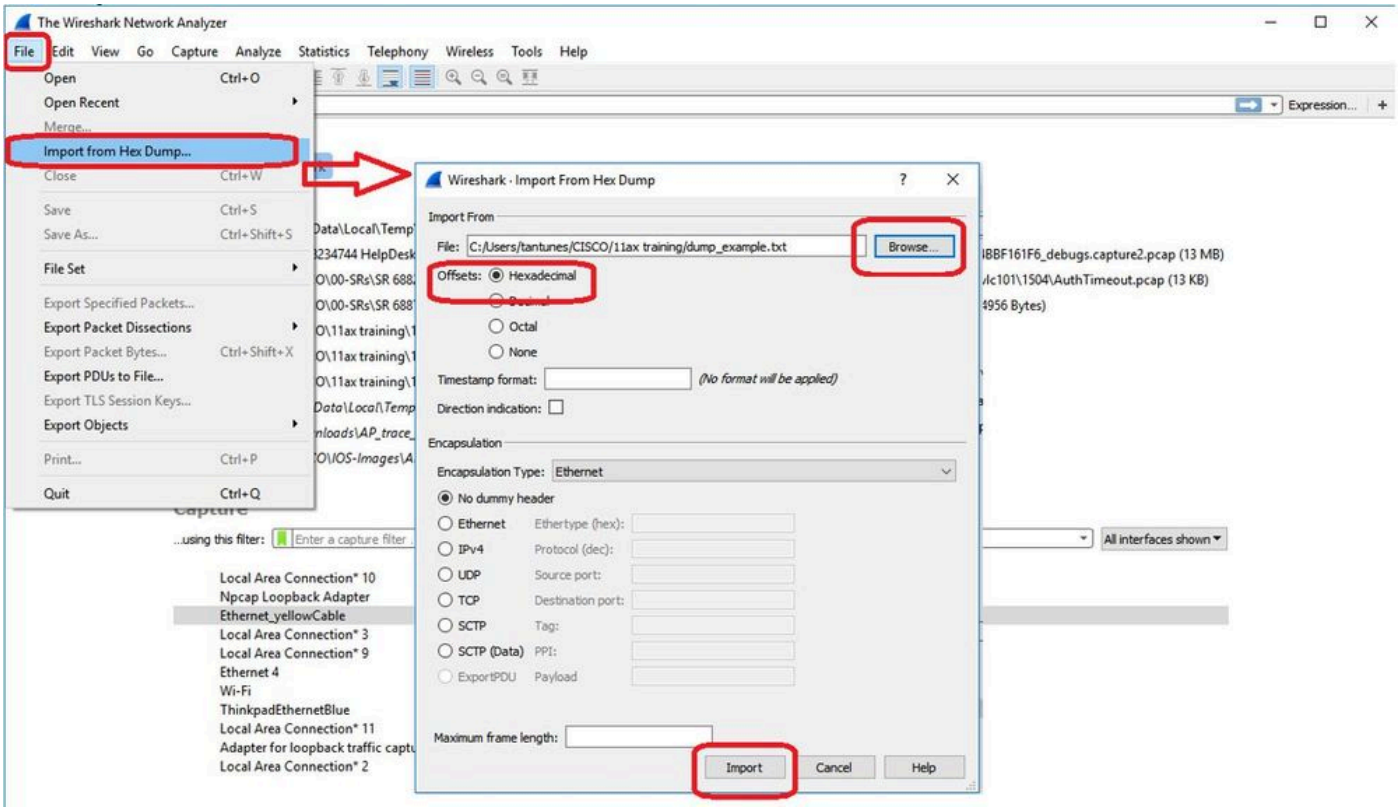
Vous pouvez vider les paquets au format hexadécimal dans l'interface de ligne de commande :

```
configure ap client-trace output dump address add xx:xx:xx:xx:xx:xx
configure ap client-trace output dump enable x -> Enter the packet dump length value
```

```
AP70DB.98E1.3DEC#configure ap client-trace start
Warning: To recover WLC pushed config, need CAPWAP restart or reload to re-apply the config from WLC
AP70DB.98E1.3DEC#Apr  6 13:28:53 kernel: [*04/06/2020 13:28:53.2837] systemd[1]: Starting Lighttpd Watcher...
Apr  6 13:28:53 kernel: [*04/06/2020 13:28:53.3269] systemd[1]: Started Lighttpd Watcher.
configure ap client-trace output dump address add a8:db:03:08:4c:4a
AP70DB.98E1.3DEC#Apr  6 13:29:02 kernel: [*04/06/2020 13:29:02.5997] MAC already exists: index 0
configure ap client-trace output dump
  address  Remote/Local dump Client Addresses
  enable   Enable Trace output for local dump
AP70DB.98E1.3DEC#configure ap client-trace output dump enable
  <6-5000>  Enter the packet dump length value
AP70DB.98E1.3DEC#configure ap client-trace output dump enable 100
  <cr>
AP70DB.98E1.3DEC#configure ap client-trace output dump enable 100
AP70DB.98E1.3DEC#Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4648]
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4648] Time:464876us Dir:Rx Rate:m7.2-2  Rssi:-43 Ch:1 Fc:188 Dur:30 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 54:7c:69:b7:3f:42 Seq:126(294) Info:ARP Retry:0 Len:121 Typesub:28 Tid:q0
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0020 00 00 13 88 15 b3 ff ff 00 00 00 ff ab cd 02 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0030 00 00 37 00 00 00 06 00 07 00 01 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0040 00 01 2c 00 00 49 31 21 0f d5 a8 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0050 00 00 00 00 3e 00 3e 00 00 5e 8b 2e b6 00 07 30
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0060 ed 88 01 30 00 00 27 e3 36 4d a0 a8 db 03 08 4c
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0070 4a 54 7c 69 b7 3f 42 40 12 00 00 aa aa 03 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4650] 0080 00 08 06 00 01 08 00 06 04 00 01 a8 db 03 08 4c
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4650] 0090 4a c0 a8 65
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4748]
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4748] Time:474888us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:288 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 54:7c:69:b7:3f:42 Seq:6(6) Info:ARP Retry:0 Len:104 Typesub:28 Tid:q0
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 50 00 50
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0030 00 00 5e 8b 2e b6 00 07 3f 50 02 01 00 00 88 02
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 54 7c
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0050 69 b7 3f 42 40 00 00 00 aa aa 03 00 00 00 08 06
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0060 00 01 08 00 06 04 00 02 54 7c 69 b7 3f 42 c0 a8
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0070 65 01 a8 db 03 08 4c 4a c0 a8 65 0d 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4750] 0090 00 00 6b 6b 6b 6b 6b 6b
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800]
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] Time:180019us Dir:Rx Rate:5 Rssi:-36 Ch:1 Fc:40 Dur:0 ff:ff:ff:ff:ff:ff a8:db:03:08:4c:4a ff:ff:ff:ff:ff:ff Seq:277(631) Info:DOT11_PROBE_REQUEST Retry:0 Len:197 Typesub:04
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0020 00 00 13 88 15 b3 ff ff 00 00 dc c8 00 ad 00 ad
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0030 00 00 5e 8b 2f 16 00 02 c2 75 0b 01 14 00 40 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0040 00 00 ff ff ff ff ff ff a8 db 03 08 4c 4a ff ff
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0050 ff ff ff ff 70 27 00 00 01 04 02 04 0b 16 32 08
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0060 0c 12 18 24 30 48 60 6c 03 01 01 2d 1a 2d 00 1b
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0070 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0080 00 00 00 00 00 00 00 7f 0a 00 00 48 00 00 40 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0090 40 00 21 ff
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000]
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] Time:200019us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:50 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:65e(1630) Info:DOT11_PROBE_RESPONSE Retry:0 Len:250 Typesub:05
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 e2 00 e2
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0030 00 00 5e 8b 2f 16 00 02 c2 94 02 01 00 00 b0 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 00 27
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0050 e3 36 4d a0 e0 65 96 0c 12 18 24 03 01 0d 64 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0060 11 11 00 0c 74 65 73 74 65 77 6c 63 77 6c 61 6e
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0070 01 08 82 84 8b 96 0c 12 18 24 03 01 01 07 06 49
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0080 4c 20 01 0d 12 20 01 00 2a 01 00 32 04 30 48 60
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0090 6c 30 14 01
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001]
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] Time:200161us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:50 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a1 00:27:e3:36:4d:a1 Seq:65f(1631) Info:DOT11_PROBE_RESPONSE Retry:0 Len:251 Typesub:05
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
```

Ensuite, vous pouvez nettoyer le vidage hexadécimal et l'enregistrer au format texte et l'importer dans wireshark :

```
Time:20010us Dir:Rx Rate:1 Rssi:-37 Ch:1 Fc:b0 Dur:13a 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 Seq:1(1) Info:DOT11_AUTHENTICATION Retry:0 Len:65 Typesub:0b
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 db c8 00 29 00 29
0030 00 00 5e 8b 2f 1f 00 00 57 36 02 01 13 00 b0 00
0040 3a 01 00 27 e3 36 4d a0 a8 db 03 08 4c 4a 00 27
0050 e3 36 4d a0 10 00 00 00 01 00 00 00 dd 09 00 10
0060 18 02 00 00 10 00 00 00 00 00 00 6b 6b 6b 6b 6b
0070 6b

Time:43054us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:d0 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:66c(1644) Info:DOT11_ACTION Retry:0 Len:54 Typesub:0d
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 1e 00 1e
0030 00 00 5e 8b 2f 1f 00 00 57 b2 02 01 00 00 d0 00
0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 00 27
0050 e3 36 4d a0 c0 66 03 02 00 08 01 00 00 00 00 00
0060 6b 6b 6b 6b 6b 6b

Time:43155us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:b0 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:66d(1645) Info:DOT11_AUTHENTICATION Retry:0 Len:65 Typesub:0b
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 29 00 29
0030 00 00 5e 8b 2f 1f 00 00 5d 06 02 01 00 00 b0 00
0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 00 27
0050 e3 36 4d a0 d0 66 00 00 02 00 00 00 dd 09 00 10
0060 18 02 00 00 10 00 00 00 00 00 00 6b 6b 6b 6b 6b
0070 6b

Time:43261us Dir:Rx Rate:1 Rssi:-34 Ch:1 Fc:800 Dur:13a 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 Seq:2(2) Info:DOT11_ASSOC_REQUEST Retry:1 Len:220 Typesub:00
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 de cc 00 c4 00 c4
0030 00 00 5e 8b 2f 1f 00 00 8a a1 02 01 12 00 00 08
0040 3a 01 00 27 e3 36 4d a0 a8 db 03 08 4c 4a 00 27
0050 e3 36 4d a0 20 00 31 15 0a 00 00 0c 74 65 73 74
0060 65 77 6c 63 77 6c 61 6e 01 08 82 84 8b 96 24 30
0070 48 6c 32 04 0c 12 18 60 21 02 05 13 24 02 01 0d
0080 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00
0090 00 0f ac 04
```



Étant donné que la sortie peut être très volumineuse et que la sortie ne mentionne que le type de trame qui est vu et non aucun détail interne, il peut être plus efficace de rediriger la capture de paquets vers un ordinateur portable qui exécute une application de capture (telle que wireshark).

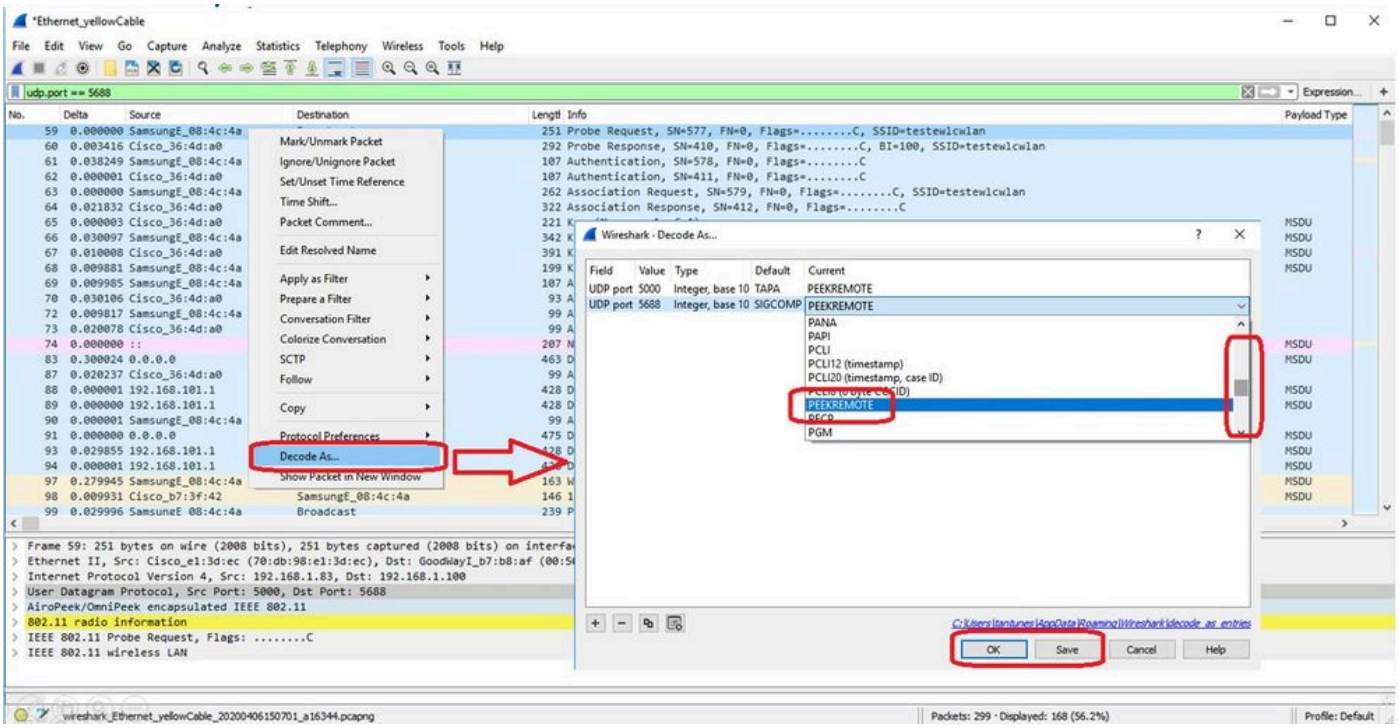
Activez la fonction de capture à distance pour envoyer les paquets au périphérique externe avec wireshark :

```
config ap client-trace output remote enable
```

La commande signifie que le point d'accès transfère chaque trame capturée par le filtre client-trace vers l'ordinateur portable à l'adresse 192.168.68.68 et utilise l'encapsulation PEEKREMOTE (tout comme les points d'accès en mode renifleur) sur le port 5000.

Une limitation est que l'ordinateur portable cible doit se trouver dans le même sous-réseau que l'AP sur lequel vous exécutez cette commande. Vous pouvez modifier le numéro de port pour prendre en compte les stratégies de sécurité en place sur votre réseau.

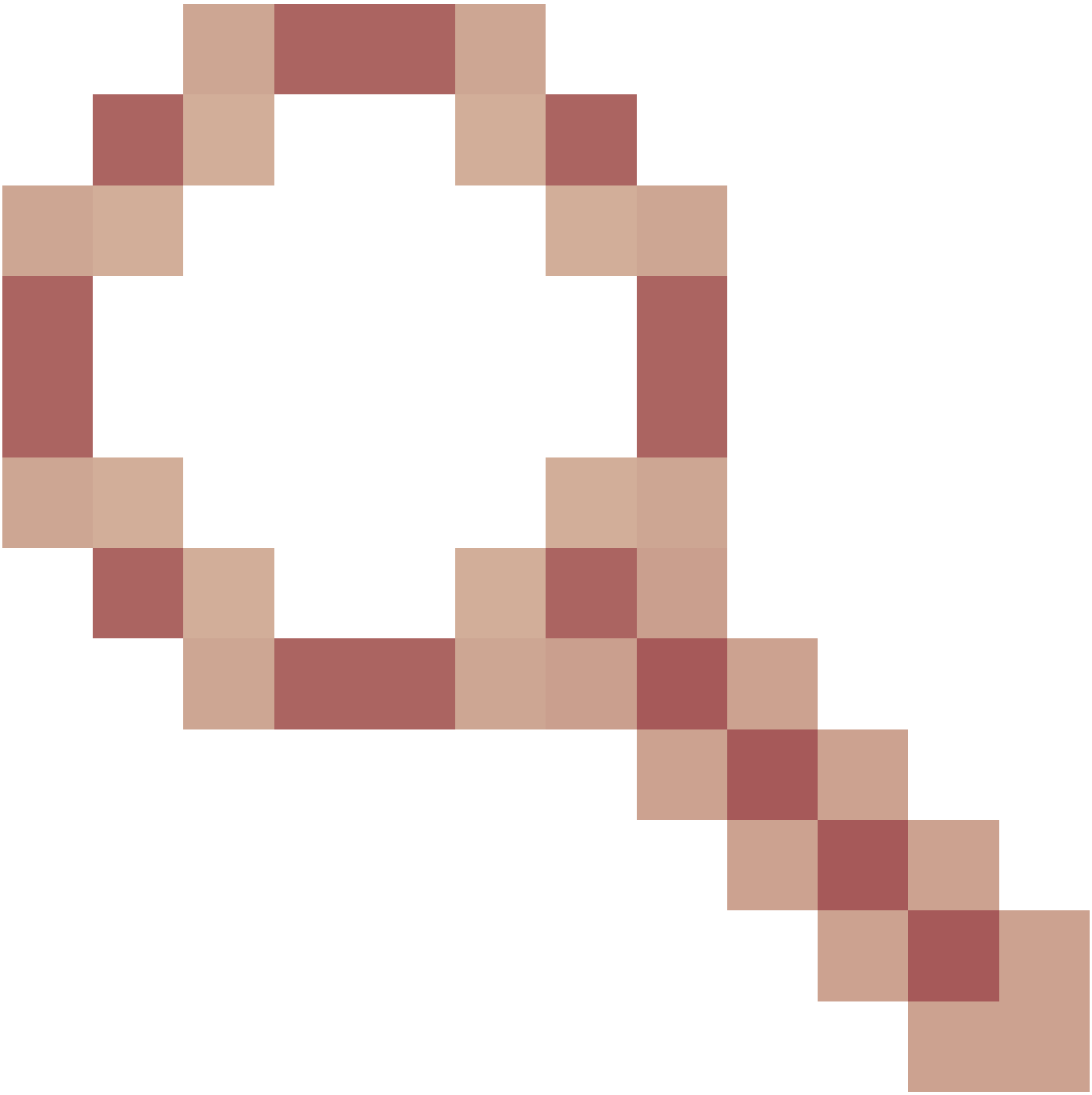
Une fois que vous avez reçu tous les paquets sur l'ordinateur portable qui exécute Wireshark, vous pouvez cliquer avec le bouton droit sur l'en-tête udp 5000 et choisir decode as et choisir PEEKREMOTE comme illustré dans cette figure :



Liste des bogues et des améliorations de cette fonctionnalité :

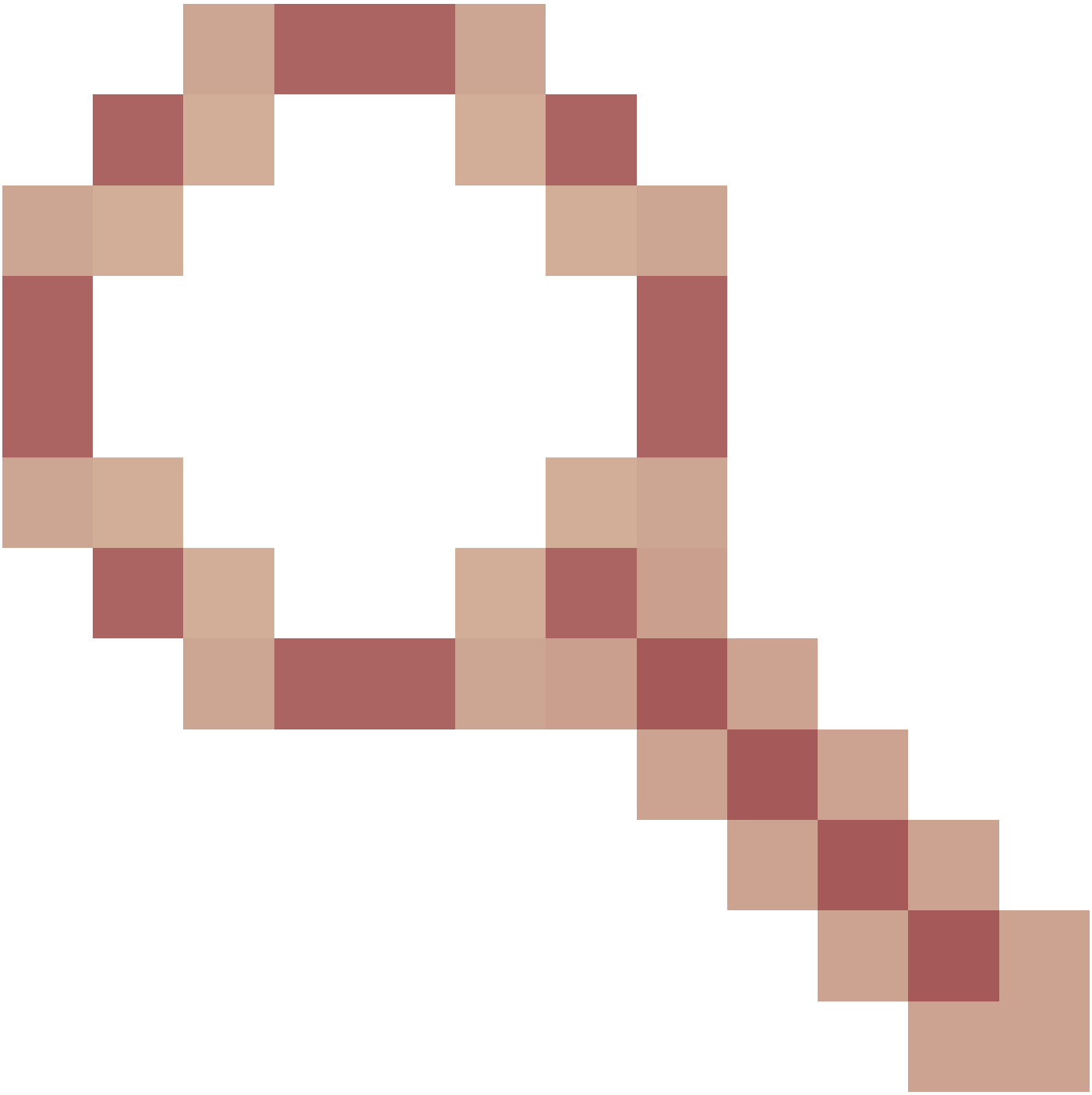
[ID de bogue Cisco CSCvm09020]
DNS n'est plus vu par la trace du client sur 8.8

[ID de bogue Cisco CSCvm09015]



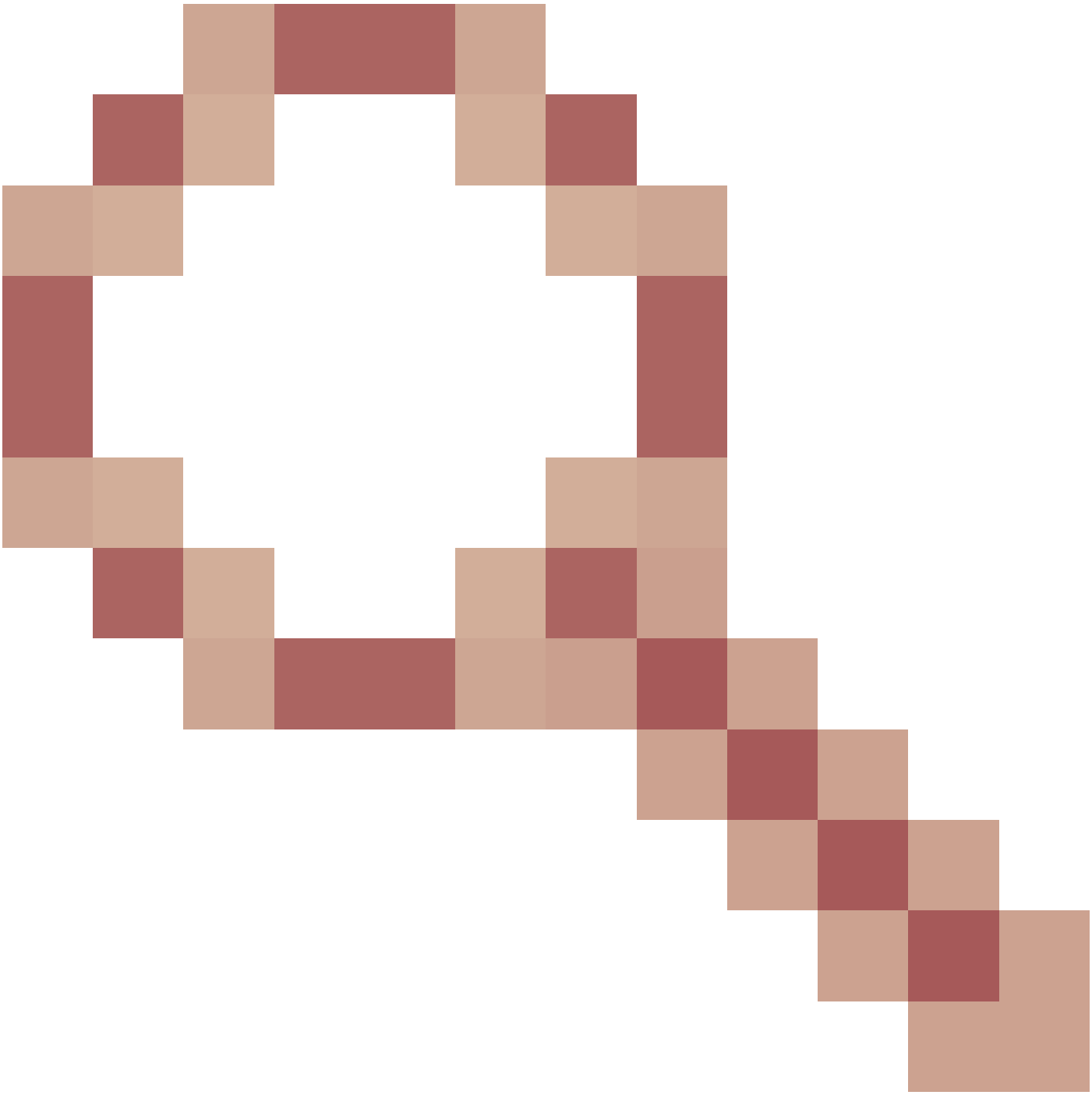
le suivi client affiche de nombreux ICMP_other avec un numéro de séquence nul

ID de bogue Cisco CSCvm02676



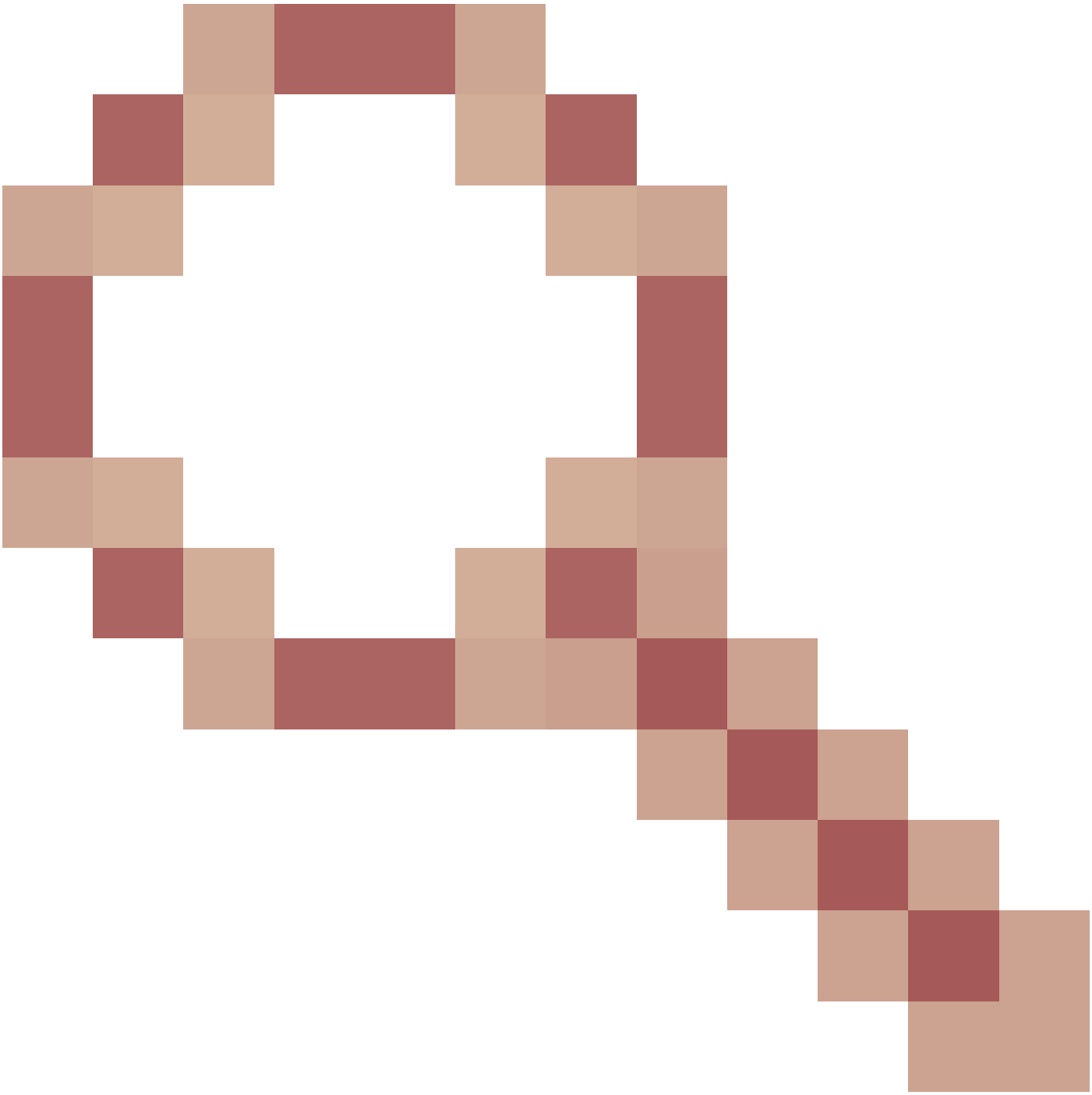
AP COS client-trace ne capture pas les paquets webauth

ID de bogue Cisco CSCvm02613



Le résultat de la commande AP COS client-trace remote ne fonctionne pas

ID de bogue Cisco CSCvm00855



Les numéros SEQ du client-trace sont incohérents

Contrôlez la trace du client AP à partir du WLC 9800

Vous pouvez configurer plusieurs points d'accès pour effectuer un suivi de client radio et le déclencher à partir de

Étape 1. Configurez un profil de suivi AP qui définit le trafic à capturer

```
config term
   wireless profile ap trace
```

```
filter all no filter probe output console-log
```

Étape 2 : ajout du profil de trace AP à un profil de jointure AP utilisé par les AP que vous ciblez

```
ap profile < ap join profile name>
    trace
```

Assurez-vous que ce profil de jointure de point d'accès est appliqué à une balise de site qui est utilisée par vos points d'accès cibles

Étape 4 - Déclenchez le démarrage/l'arrêt

```
ap trace client start ap
```

```
client all/
```

```
ap trace client stop ap
```

```
client all/
```

```
ap trace client start site
```

```
client all/
```

```
ap trace client stop site
```

```
client all/
```

Commandes de vérification :

```
show wireless profile ap trace summary
show wireless profile ap trace detailed PROF_NAME detail
sh ap trace client summary
show ap trace unsupported-ap summary
```

Bundle de débogage client sur l'AP

Plutôt que de collecter un débogage/capture radio, il peut être plus facile d'utiliser la fonctionnalité de groupe de débogage client si vous déboguez un ou plusieurs clients spécifiques.

Étape 1. Identifiez le client à dépanner.

```
9164#show dot11 clients

Total dot11 clients: 6
       Client MAC   Slot ID WLAN ID AID WLAN Name RSSI  Maxrate is_wgb_wired is_
mld_sta
52:1E:34:C9:D6:F3         1       2  35   MySSID  -62      M7            No
     No
80:A9:97:2C:DC:6E         1       2  34   MySSID  -47 MCS112SS          No
     No
E8:D8:D1:1F:71:F3         0       2  35   MySSID  -62      M7            No
     No
6A:E4:06:E7:AB:E1         1       2  33   MySSID  -44 MCS112SS          No
     No
00:1D:63:70:AC:23         0       2  33   MySSID  -56      M7            No
     No
68:72:C3:FD:17:F5         0       2  34   MySSID  -53     M15            No
     No
```

Étape 2. Démarrez le débogage pour une ou plusieurs adresses MAC client

```
9164#debug client-bundle start debug 80:A9:97:2C:DC:6E
  WORD
```

Par défaut, rien ne sera imprimé à l'écran. Vous pouvez activer terminal monitor et voir les débogages en cours d'impression en direct, mais sachez que cela rendra le terminal très difficile à utiliser. Il n'est pas nécessaire d'imprimer les débogages sur le terminal pour collecter le bundle.

Étape 3. Vous devez arrêter le bundle de débogage avant de pouvoir en télécharger le résultat :

```
debug client-bundle start debug 80:A9:97:2C:DC:6E
```

Étape 4. Téléchargez le bundle sur un serveur FTP ou SCP (pour rappel, le WLC peut agir comme serveur SCP)

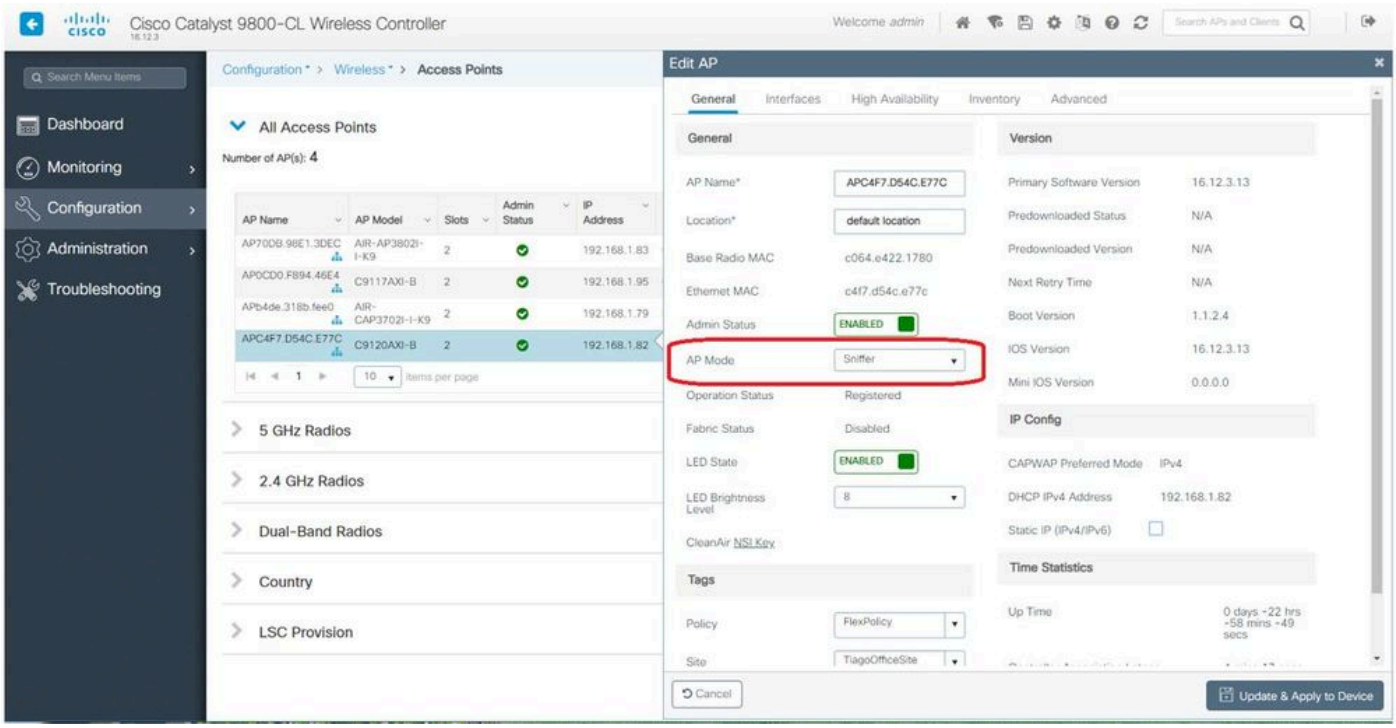
```
9164#debug client-bundle upload tftp 192.168.129.29 80:a9:97:2c:dc:6e
2024-09-04 11:58:48 Creating client bundle, please wait...

2024-09-04 11:59:01 Client bundle file 9164-_client_bundle.17.15.1.6.20240904.115848.tgz created.
2024-09-04 11:59:01 TFTP uploading...
Successful file transfer:
9164_client_bundle.17.15.1.6.20240904.115848.tgz

9164#
```

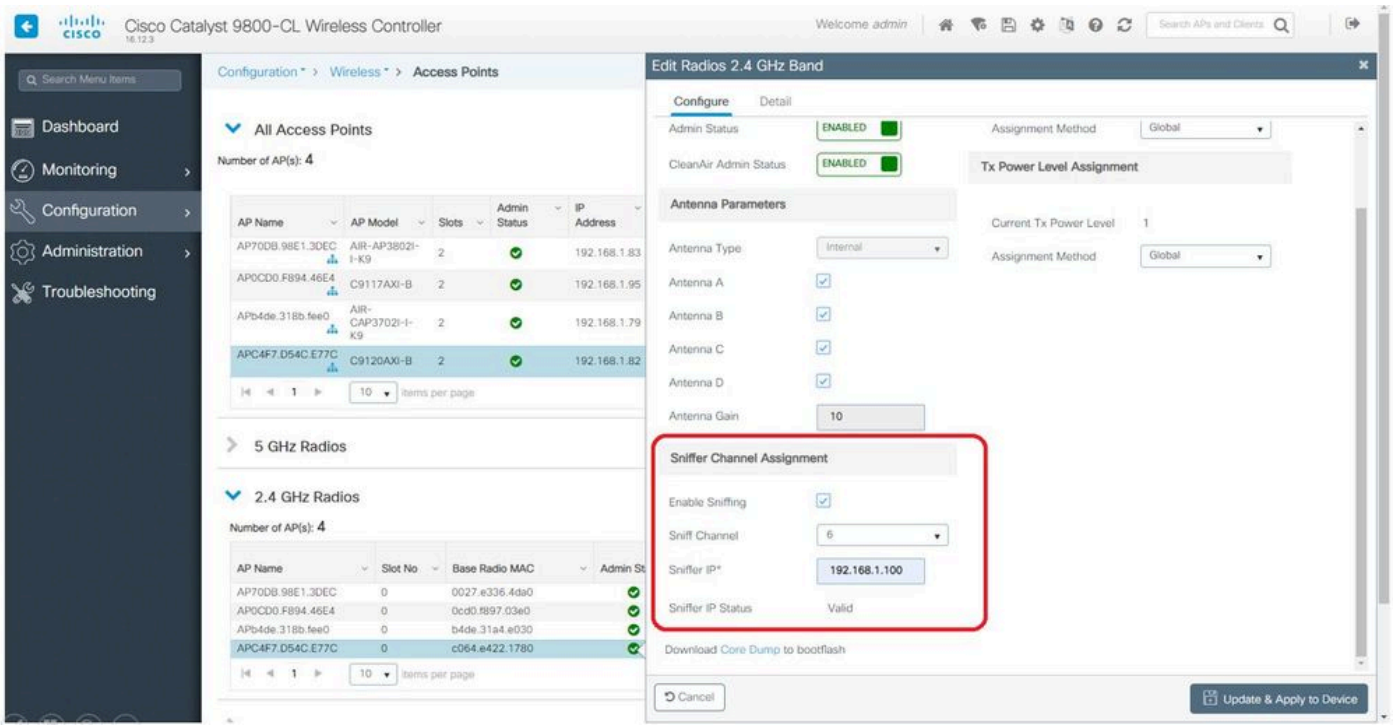
Le bundle TGZ contient 4 fichiers :

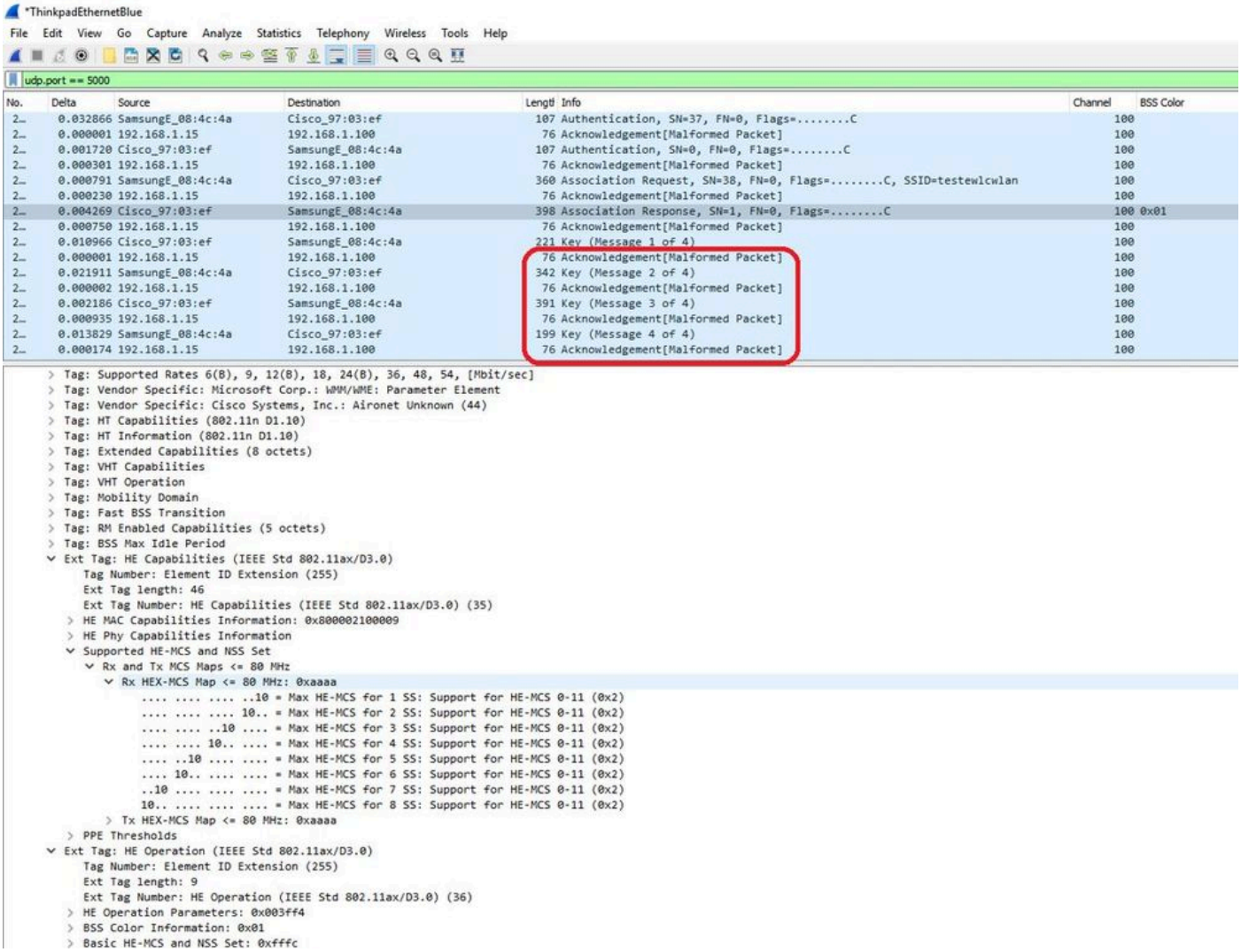
- 2 contenant les commandes show relatives aux radios et au client
- 1 à propos du débogage réel (qui est affiché sur le terminal si vous utilisez term mon)
- 1 contenant syslogs

Points d'accès Catalyst 91xx en mode renifleur

Les nouveaux Catalyst 9115, 9117, 9120 et 9130 peuvent être configurés en mode renifleur. La procédure est similaire aux modèles AP précédents.







Remarque : les trames de données envoyées aux débits WIFI 6 sont capturées, mais

comme peekremote n'est pas à jour sur Wireshark, elles sont de type phy 802.11ax à partir de maintenant. Le correctif est dans Wireshark 3.2.4 où Wireshark affiche le taux de phy wifi6 approprié.

Remarque : les points d'accès Cisco ne peuvent pas capturer les trames MU-OFDMA pour le moment, mais peuvent capturer les trames de déclenchement (envoyées au débit de données de gestion) qui annoncent une fenêtre MU-OFDMA. Vous pouvez déjà déduire que MU-OFDMA se produit (ou non) et avec quel client.

Conseils de dépannage

MTU du chemin

Bien que la détection de MTU de chemin trouve le MTU optimal pour l'AP, il est possible de remplacer ces paramètres manuellement.

Sur le WLC AireOS 8.10.130, la commande config ap pmtu disable <ap/all> définit une MTU statique pour un ou tous les AP plutôt que de s'appuyer sur le mécanisme de découverte dynamique.

Pour activer les débogages au démarrage

Vous pouvez exécuter la commande config boot debug capwap pour activer les débogages capwap, DTLS et DHCP au prochain démarrage, avant même que le système d'exploitation ait démarré et que l'invite ne s'affiche.

Vous avez également "config boot debug memory xxxx" pour plusieurs débogages de mémoire.

Vous pouvez voir si les débogages de démarrage sont activés ou non au prochain redémarrage avec « show boot ».

Ils peuvent être désactivés en ajoutant le mot clé disable à la fin, par exemple « config boot debug capwap disable ».

Mécanisme d'économie de puissance

L'économie d'énergie d'un client donné peut être dépanné en exécutant

debug client trace <adresse mac>

Qualité de service des clients

Pour vérifier que les balises QoS sont appliquées, vous pouvez exécuter "debug capwap client qos".

Elle affiche la valeur UP des paquets pour les clients sans fil.

Il n'est pas filtrable mac à partir de 8.8 ; demande d'amélioration bogue Cisco IDCSCvm08899 .

```
labAP#debug capwap client qos

[*08/20/2018 09:43:36.3171] chatter: set_qos_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:8
[*08/20/2018 09:43:45.0051] chatter: set_qos_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:8
[*08/20/2018 09:43:45.5463] chatter: set_qos_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:8
[*08/20/2018 09:43:46.5687] chatter: set_qos_up :: SetQosPriority: bridged packet dst: AC:81:12:C7:CD:3
[*08/20/2018 09:43:47.0982] chatter: set_qos_up :: SetQosPriority: bridged packet dst: AC:81:12:C7:CD:3
```

Vous pouvez également vérifier la table Qos UP à DSCP sur le point d'accès ainsi que la quantité totale de paquets marqués, mis en forme et abandonnés par Qos :

```
LabAP#show dot11 qos
Qos Policy Maps (UPSTREAM)

no policymap
Qos Stats (UPSTREAM)

total packets:   0
dropped packets: 0
marked packets:  0
shaped packets:  0
policed packets: 0
copied packets:  0

DSCP TO DOT1P (UPSTREAM)

Default dscp2dot1p Table Value:
[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48
Active dscp2dot1p Table Value:
[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48

Qos Policy Maps (DOWNSTREAM)

no policymap
Qos Stats (DOWNSTREAM)

total packets:   0
dropped packets: 0
marked packets:  0
shaped packets:  0
policed packets: 0
copied packets:  0

DSCP TO DOT1P (DOWNSTREAM)

Default dscp2dot1p Table Value:
[0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1
[8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1
[16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1
[24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1
[32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1
```

```
[40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1
[48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1
[56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1
Active dscp2dot1p Table Value:
[0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1
[8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1
[16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1
[24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1
[32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1
[40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1
[48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1
[56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1
LabAP#
```

Lorsque des stratégies Qos sont définies sur le WLC et téléchargées sur le point d'accès Flexconnect, vous pouvez les vérifier avec :

```
AP780C-F085-49E6#show policy-map
2 policymaps
Policy Map BWLimitAAAClients            type:qos client:default
    Class BWLimitAAAClients_AVC_UI_CLASS
      drop

    Class BWLimitAAAClients_ADV_UI_CLASS
      set dscp af41 (34)


    Class class-default
      police rate 5000000 bps (625000Bytes/s)
        conform-action
        exceed-action


Policy Map platinum-up          type:qos client:default
    Class cm-dscp-set1-for-up-4
      set dscp af41 (34)


    Class cm-dscp-set2-for-up-4
      set dscp af41 (34)


    Class cm-dscp-for-up-5
      set dscp af41 (34)


    Class cm-dscp-for-up-6
      set dscp ef (46)


    Class cm-dscp-for-up-7
      set dscp ef (46)


    Class class-default
      no actions
```

En cas de limitation du débit de QoS :

```
AP780C-F085-49E6#show rate-limit client
Config:
              mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in nrt_burs
A8:DB:03:6F:7A:46   2           0          0            0           0             0            0
Statistics:
            name    up  down
        Unshaped     0     0
  Client RT pass     0     0
 Client NRT pass     0     0
 Client RT drops     0     0
Client NRT drops     0 38621
               9 54922     0
```

analyse hors canal

Le débogage de l'analyse hors canal du point d'accès peut être utile lors du dépannage de la détection de voyous (pour valider si et quand le point d'accès va sur un canal spécifique pour effectuer une analyse), mais peut également être utile dans le dépannage vidéo où un flux en temps réel sensible obtient des interruptions constantes si la fonctionnalité « off channel scan defer » n'est pas utilisée.

```
debug rrm off-channel defer
debug rrm off-chanel dbg (starting 17.8.1)
debug rrm off-channel schedule
debug rrm off-channel voice (starting 17.8.1)
debug rrm schedule (starting 17.8.1, debug NDP packet tx)
show trace dot_11 channel enable

[*06/11/2020 09:45:38.9530] wcp/rrm_userspace_0/rrm_schedule :: RRMSchedule process_int_duration_timer_
[*06/11/2020 09:45:39.0550] noise measurement channel 5 noise 89
[*06/11/2020 09:45:43.5490] wcp/rrm_userspace_1/rrm_schedule :: RRMSchedule process_int_duration_timer_
[*06/11/2020 09:45:43.6570] noise measurement channel 140 noise 97
```

Connectivité client

Il est possible de répertorier les clients qui ont été désauthentifiés par le point d'accès avec le dernier horodatage d'événement :

```
LabAP#show dot11 clients deauth
               timestamp               mac vap reason_code
Mon Aug 20 09:50:59 2018 AC:BC:32:A4:2C:D3   9           4
Mon Aug 20 09:52:14 2018 00:AE:FA:78:36:89   9           4
Mon Aug 20 10:31:54 2018 00:AE:FA:78:36:89   9           4
```

Dans le résultat précédent, le code de raison est le code de raison de désauthentification comme détaillé dans ce lien :

https://community.cisco.com:443/t5/wireless-mobility-knowledge-base/802-11-association-status-802-11-deauth-reason-codes/ta-p/3148055

Le vap fait référence à l'identificateur du WLAN à l'intérieur du point d'accès (qui est différent de l'ID WLAN sur le WLC !!!).

Vous pouvez le croiser avec d'autres sorties détaillées par la suite qui mentionne toujours la vap des clients associés.

Vous pouvez voir la liste des ID de VAP avec "show controllers Dot11Radio 0/1 wlan".

Lorsque les clients sont toujours associés, vous pouvez obtenir des détails sur leur connexion avec :

```
LabAP#show dot11 clients

Total dot11 clients: 1
       Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate WGB
00:AE:FA:78:36:89       1      10   1   TestSSID -25 MCS82SS  No
```

Vous pouvez obtenir beaucoup plus de détails sur l'entrée client avec :

```
LabAP#show client summ

Radio Driver client Summary:
============================
wifi0
[*08/20/2018 11:54:59.5340]
[*08/20/2018 11:54:59.5340] Total STA List Count 0
[*08/20/2018 11:54:59.5340] | NO|              MAC|STATE|
[*08/20/2018 11:54:59.5340] ----------------------------
wifi1
[*08/20/2018 11:54:59.5357]
[*08/20/2018 11:54:59.5357] Total STA List Count 1
[*08/20/2018 11:54:59.5357] | NO|              MAC|STATE|
[*08/20/2018 11:54:59.5357] ----------------------------
[*08/20/2018 11:54:59.5357] |  1| 0:ffffffae:fffffffa:78:36:ffffff89|    8|

Radio Driver Client AID List:
============================
wifi0
[*08/20/2018 11:54:59.5415]
[*08/20/2018 11:54:59.5415] Total STA-ID List Count 0
[*08/20/2018 11:54:59.5415] | NO|              MAC|STA-ID|
[*08/20/2018 11:54:59.5415] ----------------------------
wifi1
[*08/20/2018 11:54:59.5431]
```

```
[*08/20/2018 11:54:59.5431] Total STA-ID List Count 1
[*08/20/2018 11:54:59.5431] | NO|             MAC|STA-ID|
[*08/20/2018 11:54:59.5432] ------------------------------
[*08/20/2018 11:54:59.5432] |  1| 0:ffffffae:ffffffa:78:36:ffffff89|     6|

WCP client Summary:
====================

              mac radio vap aid state       encr Maxrate is_wgb_wired      wgb_mac_addr
00:AE:FA:78:36:89     1   9   1   FWD AES_CCM128 MCS82SS        false 00:00:00:00:00:00


NSS client Summary:
====================
Current Count: 3
|       MAC       | OPAQUE |PRI POL|VLAN|BR|TN|QCF|BSS|RADID|MYMAC|
|F8:0B:CB:E4:7F:41|00000000|      3|   0| 1| 1|  0|  2|    3|    1|
|F8:0B:CB:E4:7F:40|00000000|      3|   0| 1| 1|  0|  2|    3|    1|
|00:AE:FA:78:36:89|00000003|      1|   0| 1| 1|  0|  9|    1|    0|

Datapath IPv4 client Summary:
================================
               id vap   port         node tunnel               mac        seen_ip     hashed_ip sniff_a
00:AE:FA:78:36:89   9 apr1v9 192.0.2.13      - 00:AE:FA:78:36:89 192.168.68.209 10.228.153.45  5.990000

Datapath IPv6 client Summary:
================================
client               mac                  seen_ip6 age      scope   port
     1 00:AE:FA:78:36:89 fe80::2ae:faff:fe78:3689  61 link-local apr1v9

Wired client Summary:
======================
mac port state local_client detect_ago associated_ago tx_pkts tx_bytes rx_pkts rx_bytes
```

Vous pouvez forcer la déconnexion d'un client spécifique avec :

```
test dot11 client deauthenticate
```

Les compteurs de trafic peuvent être obtenus par client avec :

```
LabAP#show client statistics wireless 00:AE:FA:78:36:89
Client MAC address: 00:AE:FA:78:36:89
Tx Packets                    : 621
Tx Management Packets         : 6
Tx Control Packets            : 153
Tx Data Packets               : 462
Tx Data Bytes                 : 145899
Tx Unicast Data Packets       : 600
Rx Packets                    : 2910
Rx Management Packets         : 13
Rx Control Packets            : 943
Rx Data Packets               : 1954
Rx Data Bytes                 : 145699
```

```
LabAP#
```

Plus sur le plan radio, beaucoup d'informations peuvent être obtenues dans le "show controllers". Lorsque vous ajoutez l'adresse MAC du client, les débits de données pris en charge, les débits de données actuels, les capacités PHY ainsi que le nombre de tentatives et d'échecs de transmission s'affichent :

<#root>

```
LabAP#show controllers dot11Radio 0 client 00:AE:FA:78:36:89
              mac radio vap aid state       encr Maxrate is_wgb_wired      wgb_mac_addr
00:AE:FA:78:36:89     0   9   1   FWD AES_CCM128    M15         false 00:00:00:00:00:00
Configured rates for client 00:AE:FA:78:36:89
Legacy Rates(Mbps): 11
HT Rates(MCS):M0 M1 M2 M3 M4 M5 M6 M7 M8 M9 M10 M11 M12 M13 M14 M15
VHT Rates: 1SS:M0-7 2SS:M0-7

HT:yes     VHT:yes     HE:no     40MHz:no     80MHz:no     80+80MHz:no     160MHz:no
11w:no     MFP:no     11h:no     encrypt_polocy: 4
_wmm_enabled:yes     qos_capable:yes     WME(11e):no     WMM_MIXED_MODE:no
short_preamble:yes     short_slot_time:no     short_hdr:yes     SM_dyn:yes
short_GI_20M:yes     short_GI_40M:no     short_GI_80M:yes     LDPC:yes     AMSDU:yes     AMSDU_long:no
su_mimo_capable:yes     mu_mimo_capable:no     is_wgb_wired:no     is_wgb:no

Additional info for client 00:AE:FA:78:36:89
RSSI: -90
PS  : Legacy (Sleeping)
Tx Rate: 0 Kbps
Rx Rate: 117000 Kbps
VHT_TXMAP: 0
CCX Ver: 4

Statistics for client 00:AE:FA:78:36:89
              mac   intf TxData TxMgmt TxUC TxBytes
```

TxFail

```
 TxDcrd TxCumRetries RxData RxMgmt RxBytes RxErr TxRt   RxRt idle_counter stats_ago expiration
00:AE:FA:78:36:89 apr0v9      8      1    6    1038      1      0            0     31      1    1599

Per TID packet statistics for client 00:AE:FA:78:36:89
Priority Rx Pkts Tx Pkts Rx(last 5 s) Tx (last 5 s) QID Tx Drops Tx Cur Qlimit
       0     899     460            1             1 144        0      0   1024
       1       0       0            0             0 145        0      0   1024
       2       0       0            0             0 146        0      0   1024
       3      59       0            0             0 147        0      0   1024
       4       0       0            0             0 148        0      0   1024
       5       0       0            0             0 149        0      0   1024
       6       0       0            0             0 150        0      0   1024
       7       0       0            0             0 151        0      0   1024

Legacy Rate Statistics:
  (Mbps :   Rx, Tx, Tx-Retries)
11 Mbps :    2,    0,    0
 6 Mbps :    0,    9,    0

HT/VHT Rate Statistics:
(Rate/SS/Width :   Rx, Rx-Ampdu, Tx, Tx-Ampdu, Tx-Retries)
```

```
        0/1/20 :    4,    4,    0,    0,    0
        6/2/20 :    4,    4,    0,    0,    0
        7/2/20 :    5,    5,    0,    0,    0

webauth done:
false
```

Afin de suivre constamment un débit de données client et/ou une valeur RSSI, vous pouvez exécuter "debug dot11 client rate address <mac> " et cela consigne ces informations toutes les secondes :

```
LabAP#debug dot11 client rate address 00:AE:FA:78:36:89
[*08/20/2018 14:17:28.0928]                MAC    Tx-Pkts    Rx-Pkts  Tx-Rate  Rx-Rate  RSSI   SNR Tx-R
[*08/20/2018 14:17:28.0928] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -45    53
[*08/20/2018 14:17:29.0931] 00:AE:FA:78:36:89          7         18       12  a8.2-2s   -45    53
[*08/20/2018 14:17:30.0934] 00:AE:FA:78:36:89          3         18       12  a8.2-2s   -45    53
[*08/20/2018 14:17:31.0937] 00:AE:FA:78:36:89          2         20       12  a8.2-2s   -45    53
[*08/20/2018 14:17:32.0939] 00:AE:FA:78:36:89          2         20       12  a8.2-2s   -45    53
[*08/20/2018 14:17:33.0942] 00:AE:FA:78:36:89          2         21       12  a8.2-2s   -46    52
[*08/20/2018 14:17:34.0988] 00:AE:FA:78:36:89          1          4       12  a8.2-2s   -46    52
[*08/20/2018 14:17:35.0990] 00:AE:FA:78:36:89          9         23       12  a8.2-2s   -46    52
[*08/20/2018 14:17:36.0993] 00:AE:FA:78:36:89          3          7       12  a8.2-2s   -46    52
[*08/20/2018 14:17:37.0996] 00:AE:FA:78:36:89          2          6       12  a8.2-2s   -46    52
[*08/20/2018 14:17:38.0999] 00:AE:FA:78:36:89          2         14       12  a8.2-2s   -46    52
[*08/20/2018 14:17:39.1002] 00:AE:FA:78:36:89          2         10       12  a8.2-2s   -46    52
[*08/20/2018 14:17:40.1004] 00:AE:FA:78:36:89          1          6       12  a8.2-2s   -46    52
[*08/20/2018 14:17:41.1007] 00:AE:FA:78:36:89          9         20       12  a8.2-2s   -46    52
[*08/20/2018 14:17:42.1010] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:43.1013] 00:AE:FA:78:36:89          2          8       12  a8.2-2s   -46    52
[*08/20/2018 14:17:44.1015] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:45.1018] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:46.1021] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:47.1024] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:48.1026] 00:AE:FA:78:36:89          7         15       12  a8.2-2s   -46    52
[*08/20/2018 14:17:49.1029] 00:AE:FA:78:36:89          0          6       12  a8.2-2s   -46    52
[*08/20/2018 14:17:50.1032] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:51.1035] 00:AE:FA:78:36:89          1          7       12  a8.2-2s   -46    52
[*08/20/2018 14:17:52.1037] 00:AE:FA:78:36:89          0         17       12  a8.2-2s   -46    52
[*08/20/2018 14:17:53.1040] 00:AE:FA:78:36:89          1         19       12  a8.2-2s   -46    52
[*08/20/2018 14:17:54.1043] 00:AE:FA:78:36:89          2         17       12  a8.2-2s   -46    52
[*08/20/2018 14:17:55.1046] 00:AE:FA:78:36:89          2         22       12  a8.2-2s   -45    53
[*08/20/2018 14:17:56.1048] 00:AE:FA:78:36:89          1         18       12  a8.2-2s   -45    53
[*08/20/2018 14:17:57.1053] 00:AE:FA:78:36:89          2         18       12  a8.2-2s   -45    53
[*08/20/2018 14:17:58.1055] 00:AE:FA:78:36:89         12         37       12  a8.2-2s   -45    53
```

Dans cette sortie, les compteurs de paquets Tx et Rx sont des paquets transmis dans le deuxième intervalle depuis sa dernière impression, la même chose pour les Tx Retries. Cependant, le RSSI, le SNR et le débit de données sont les valeurs du dernier paquet de cet intervalle (et non une moyenne pour tous les paquets de cet intervalle).

Scénarios Flexconnect

Vous pouvez vérifier quelles listes de contrôle d'accès sont actuellement appliquées à un client dans un scénario de pré-authentification (CWA par exemple) ou de post-authentification :

```
AP#show client access-lists pre-auth all f48c.507a.b9ad
Pre-Auth URL ACLs for Client: F4:8C:50:7A:B9:AD
IPv4 ACL: IPv6 ACL:
ACTION URL-LIST

Resolved IPs for Client: F4:8C:50:7A:B9:AD
HIT-COUNT URL ACTION IP-LIST

REDIRECT
rule 0: allow true and ip proto 17 and src port 53
rule 1: allow true and ip proto 17 and dst port 53
rule 2: allow true and src 10.48.39.161mask 255.255.255.255
rule 3: allow true and dst 10.48.39.161mask 255.255.255.255
rule 4: deny true
No IPv6 ACL found


AP#show client access-lists post-auth all f48c.507a.b9ad
Post-Auth URL ACLs for Client: F4:8C:50:7A:B9:AD
IPv4 ACL: IPv6 ACL:
ACTION URL-LIST

Resolved IPs for Client: F4:8C:50:7A:B9:AD
HIT-COUNT URL ACTION IP-LIST

post-auth
rule 0: deny true and dst 192.0.0.0mask 255.0.0.0
rule 1: deny true and src 192.0.0.0mask 255.0.0.0
rule 2: allow true
No IPv6 ACL found
```

Vous pouvez voir les compteurs d'accès sur les ACL Flexconnect en activant debug flexconnect access-list counter client <client MAC>

Les exécutions suivantes de la commande show client access-list pre-auth/post-auth all <MAC> ajoutent ensuite des compteurs d'accès pour chaque entrée de liste de contrôle d'accès. Cela fonctionne pour tous les types de listes de contrôle d'accès flexibles à partir de Cisco IOS® XE 17.13. Dans les versions antérieures, les mêmes commandes existent, mais seuls les ACL VLAN ont leurs compteurs d'accès mis à jour.

Vous pouvez réinitialiser les compteurs d'accès de la liste de contrôle d'accès avec clear counters access-list client <mac>

AP Filesystem

Les points d'accès COS ne permettent pas de répertorier tout le contenu du système de fichiers comme sur les plates-formes Unix.

La commande "show filesystems" donne un détail de l'utilisation et de la distribution de l'espace

sur la partition actuelle :

```
2802#show filesystems
Filesystem                Size      Used Available Use% Mounted on
/dev/ubivol/storage      57.5M    364.0K     54.1M   1% /storage
2802#
```

La commande "show flash" répertorie les fichiers principaux sur la mémoire flash AP. Vous pouvez également ajouter le mot-clé syslog ou core pour répertorier ces dossiers spécifiques.

```
ap_2802#show flash
Directory of /storage/
total 84
-rw-r--r--    1 root     root             0 May 21  2018 1111
-rw-r--r--    1 root     root             6 Apr 15 11:09 BOOT_COUNT
-rw-r--r--    1 root     root             6 Apr 15 11:09 BOOT_COUNT.reserve
-rw-r--r--    1 root     root            29 Apr 15 11:09 RELOADED_AT_UTC
drwxr-xr-x    2 root     root           160 Mar 27 13:53 ap-images
drwxr-xr-x    4 5        root          2016 Apr 15 11:10 application
-rw-r--r--    1 root     root          6383 Apr 26 09:32 base_capwap_cfg_info
-rw-r--r--    1 root     root            20 Apr 26 10:31 bigacl
-rw-r--r--    1 root     root          1230 Mar 27 13:53 bootloader.log
-rw-r--r--    1 root     root             5 Apr 26 09:29 bootloader_verify.shadow
-rw-r--r--    1 root     root            18 Jun 30  2017 config
-rw-r--r--    1 root     root          8116 Apr 26 09:32 config.flex
-rw-r--r--    1 root     root            21 Apr 26 09:32 config.flex.mgroup
-rw-r--r--    1 root     root             0 Apr 15 11:09 config.local
-rw-r--r--    1 root     root             0 Jul 26  2018 config.mesh.dhcp
-rw-r--r--    1 root     root           180 Apr 15 11:10 config.mobexp
-rw-r--r--    1 root     root             0 Jun  5  2018 config.oeap
-rw-r--r--    1 root     root          2253 Apr 26 09:43 config.wireless
drwxr-xr-x    2 root     root           160 Jun 30  2017 cores
drwxr-xr-x    2 root     root           320 Jun 30  2017 dropbear
drwxr-xr-x    2 root     root           160 Jun 30  2017 images
-rw-r--r--    1 root     root           222 Jan  2  2000 last_good_uplink_config
drwxr-xr-x    2 root     root           160 Jun 30  2017 lists
-rw-r--r--    1 root     root           215 Apr 16 11:01 part1_info.ver
-rw-r--r--    1 root     root           215 Apr 26 09:29 part2_info.ver
-rw-r--r--    1 root     root          4096 Apr 26 09:36 random_seed
-rw-r--r--    1 root     root             3 Jun 30  2017 rxtx_mode
-rw-r--r--    1 root     root            64 Apr 15 11:11 sensord_CSPRNG0
-rw-r--r--    1 root     root            64 Apr 15 11:11 sensord_CSPRNG1
drwxr-xr-x    3 support  root           224 Jun 30  2017 support
drwxr-xr-x    2 root     root          2176 Apr 15 11:10 syslogs
---------------------------------------------------------------------------
Filesystem                Size      Used Available Use% Mounted on
flash                    57.5M    372.0K     54.1M   1% /storage
```

Stocker et envoyer des syslogs

Le dossier syslog stocke la sortie syslog des redémarrages précédents. La commande « show log

» affiche uniquement syslog depuis le dernier redémarrage.

À chaque cycle de redémarrage, les journaux système sont écrits sur des fichiers incrémentiels.

```
artaki# show flash syslogs
Directory of /storage/syslogs/
total 128
-rw-r--r--    1 root     root         11963 Jul  6 15:23 1
-rw-r--r--    1 root     root         20406 Jan  1  2000 1.0
-rw-r--r--    1 root     root           313 Jul  6 15:23 1.last_write
-rw-r--r--    1 root     root         20364 Jan  1  2000 1.start
-rw-r--r--    1 root     root            33 Jul  6 15:23 1.watchdog_status
-rw-r--r--    1 root     root         19788 Jul  6 16:46 2
-rw-r--r--    1 root     root         20481 Jul  6 15:23 2.0
-rw-r--r--    1 root     root           313 Jul  6 16:46 2.last_write
-rw-r--r--    1 root     root         20422 Jul  6 15:23 2.start
---------------------------------------------------------------------------
Filesystem                Size      Used Available Use% Mounted on
flash                    57.6M     88.0K     54.5M   0% /storage

artaki# show flash cores
Directory of /storage/cores/
total 0
---------------------------------------------------------------------------
Filesystem                Size      Used Available Use% Mounted on
flash                    57.6M     88.0K     54.5M   0% /storage
```

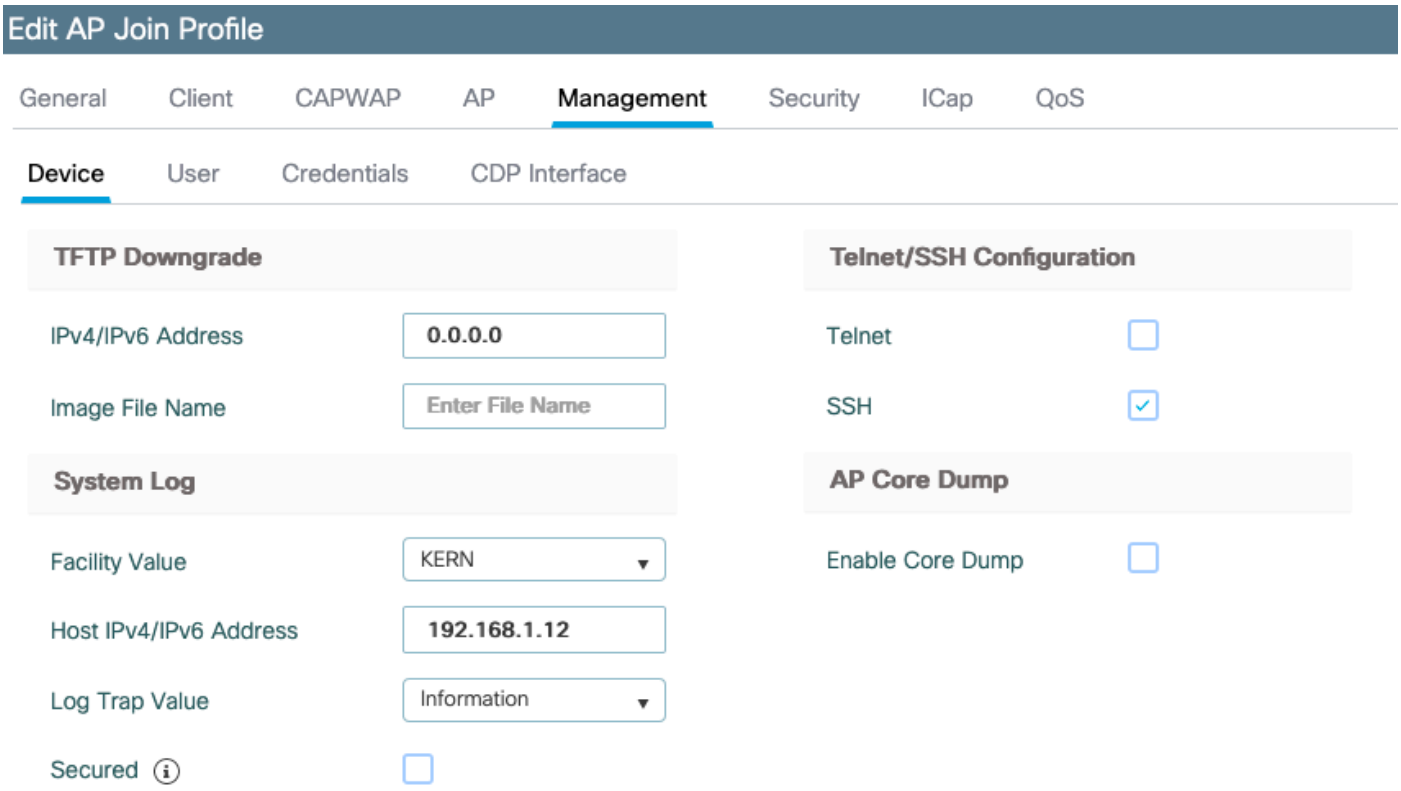
La première sortie après le démarrage initial est le fichier 1.0 et un fichier 1.1 est créé si 1.0 devient trop long. Après le redémarrage, un nouveau fichier 2.0 est créé, etc.

À partir du WLC, vous pouvez configurer la destination Syslog si vous voulez que vos AP envoient leurs messages syslog unicast à un serveur spécifique.

Par défaut, les AP envoient leurs syslog à une adresse de diffusion qui peut provoquer une tempête de diffusion, alors assurez-vous de configurer un serveur syslog.

Le point d'accès envoie par défaut via syslog tout ce qui est imprimé sur la sortie de sa console.

Sur le contrôleur 9800, vous pouvez modifier ces paramètres dans le profil Configuration -> AP Join, sous Management.



Vous pouvez modifier la valeur de déroutement de journal pour envoyer également des débogages via syslog. Vous pouvez ensuite activer les débogages sur l'interface de ligne de commande de l'AP et les résultats de ceux-ci sont envoyés via des messages syslog à votre serveur configuré .

En raison de l'ID de bogue Cisco CSCvu75017
, c'est seulement quand vous définissez l'utilitaire syslog sur KERN (la valeur par défaut) que l'AP envoie des messages syslog.

Si vous dépannez des problèmes où un AP peut perdre la connectivité réseau (ou sur un WGB par exemple), syslog n'est pas aussi fiable qu'aucun message n'est envoyé si l'AP perd sa connectivité de liaison ascendante.

Par conséquent, l'utilisation des fichiers syslog stockés dans la mémoire flash est un excellent moyen de déboguer et de stocker la sortie sur l'AP lui-même, puis de la télécharger périodiquement par la suite.

Offre groupée de support AP

Certaines informations de diagnostic de différents types, généralement collectées, peuvent être mises à disposition dans un seul bundle que vous pouvez télécharger à partir des points d'accès.

Les informations de diagnostic que vous pouvez inclure dans l'offre groupée sont les suivantes :

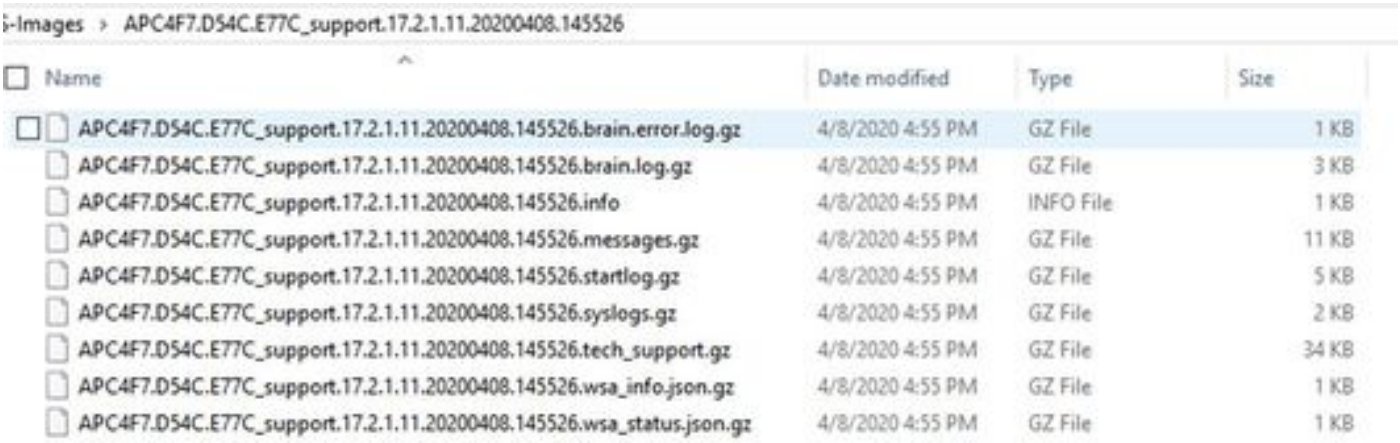
- AP show tech
- Syslog AP
- AP Capwapd Brain logs
- Journaux de démarrage et de messages AP
- Fichiers AP Coredump

Pour obtenir le bundle de support AP, vous pouvez accéder à l'interface de ligne de commande AP et entrer la commande "copy support-bundle tftp: x.x.x.x".

Après cela, vous pouvez vérifier le fichier nommé avec le nom AP ajouté avec le support.apversion.date.time.tgz comme montré par la suite :

```
APC4F7.D54C.E77C#copy support-bundle tftp: 192.168.1.100
  <cr>
APC4F7.D54C.E77C#copy support-bundle tftp: 192.168.1.100
Creating support bundle, please wait...ifconfig: wired1: error fetching interface information: Device not found
Unit systemd-journald.socket could not be found.
tar: ./*.tgz: No such file or directory
tar: error exit delayed from previous errors
tar: *.tgz: No such file or directory
tar: error exit delayed from previous errors
+=== Support file APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.tgz created ===+
################################################################################################################################################ 100.0%
Successful file transfer:
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.tgz
APC4F7.D54C.E77C#
```

Lorsque vous "untar" le fichier, vous pouvez afficher les différents fichiers collectés :



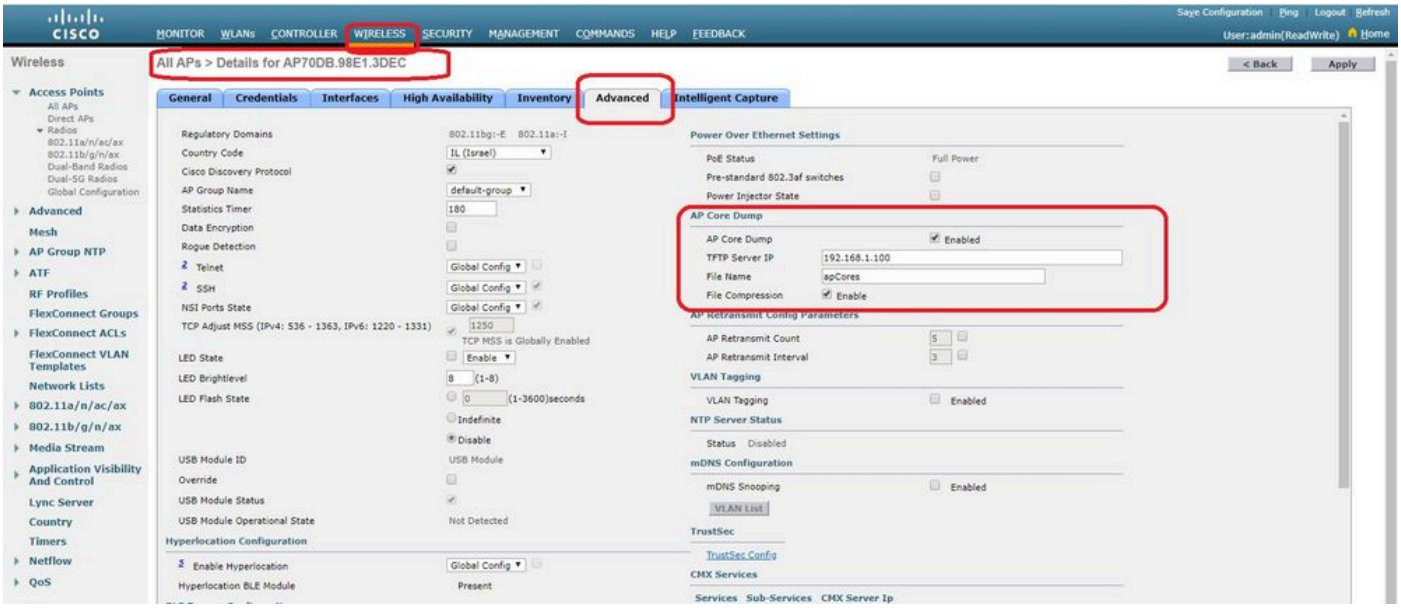
Collecter les fichiers principaux AP à distance

Pour collecter les fichiers de base AP à distance, veuillez activer le core dump pour être inclus dans le bundle de support, puis télécharger le bundle de support à partir de l'AP, ou envoyer directement au serveur tftp. Les exemples suivants utilisent le serveur TFTP 192.168.1.100.

ILC AireOS

```
(c3504-01) >config ap core-dump enable 192.168.1.100 apCores uncompress ?

<Cisco AP>     Enter the name of the Cisco AP.

all            Applies the configuration to all connected APs.
```

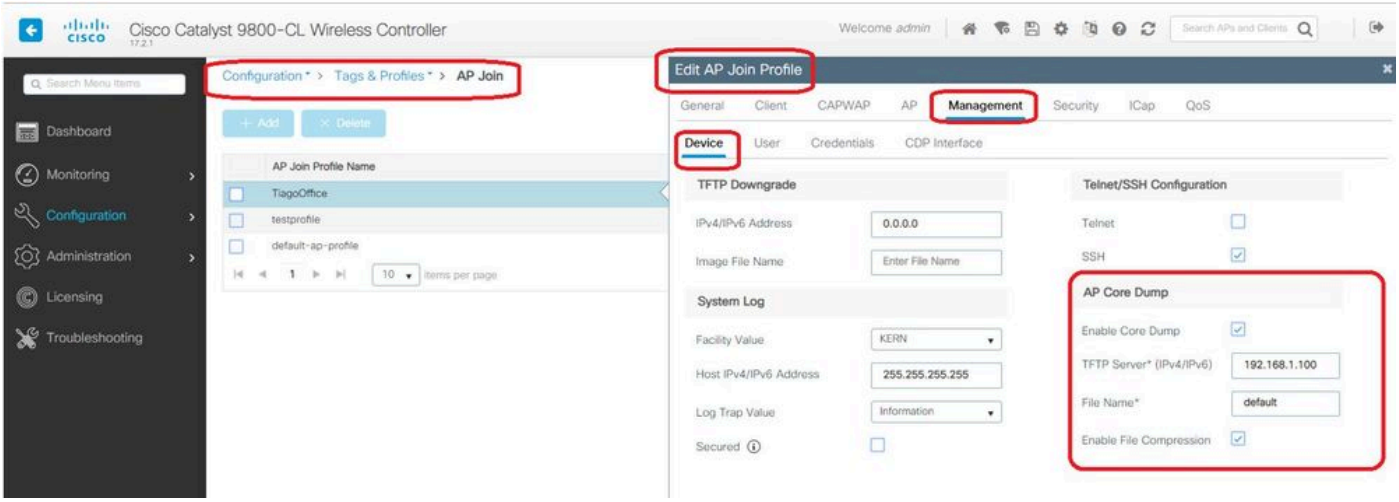
Interface graphique AireOS



CLI Cisco IOS®

```
<#root>

eWLC-9800-01(

config

)#ap profile TiagoOffice
eWLC-9800-01(

config-

ap

-profile

)#core-dump tftp-server 192.168.1.100 file apCores uncompress
```

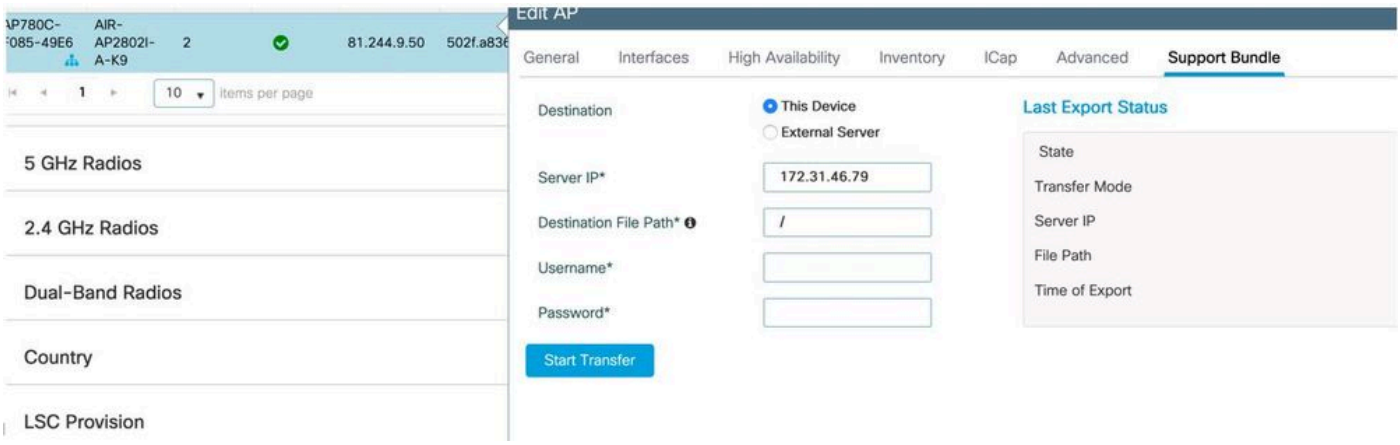
Interface graphique utilisateur Cisco IOS®



À partir de Cisco IOS® XE 17.3.1, vous disposez d'un onglet Support Bundle et pouvez télécharger AP SB à partir de l'interface graphique WLC.

Tout ce qu'il fait est d'exécuter la commande «copy support-bundle» sur l'AP et l'envoie via SCP au WLC (parce que WLC peut être un serveur SCP).

Vous pouvez ensuite le télécharger à partir de votre navigateur :



Cela signifie que vous pouvez faire manuellement la même astuce dans les versions d'eWLC antérieures à 17.3.1 :

Copiez le bundle de support de l'AP via SCP vers l'IP eWLC si vous n'avez pas de serveur TFTP accessible à l'AP.

Le eWLC est généralement accessible via SSH à partir de l'AP, c'est donc une bonne astuce pour les versions antérieures à 17.3.

Étape 1. Activer SSH sur 9800 v17.2.1

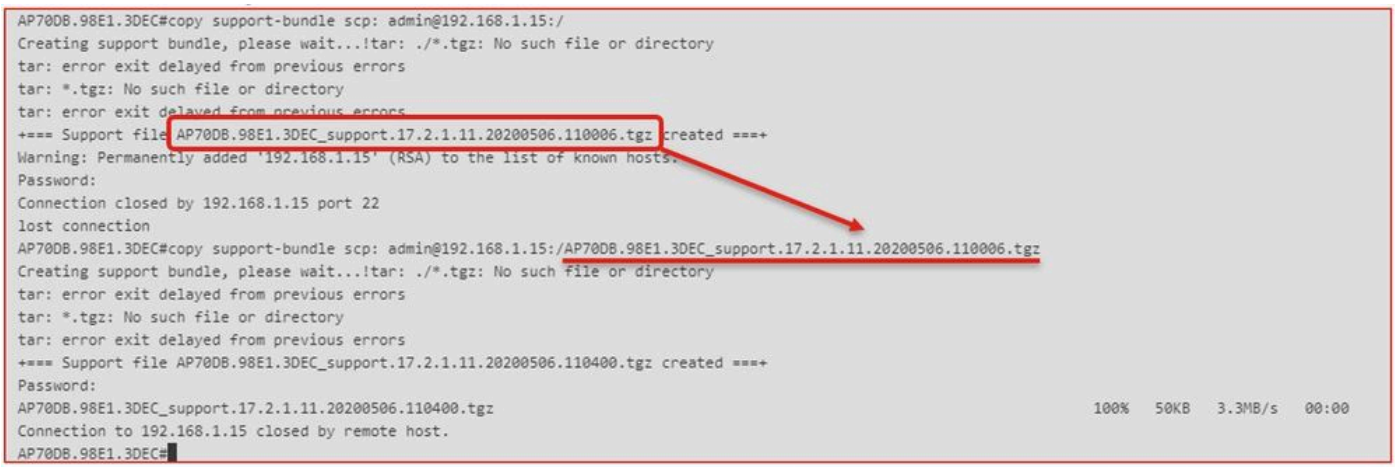
Étape 2. Activer SCP sur Cisco IOS® XE v17.2.1

Cet exemple montre comment configurer la fonctionnalité côté serveur de SCP. Cet exemple utilise un nom d'utilisateur et un mot de passe définis localement :

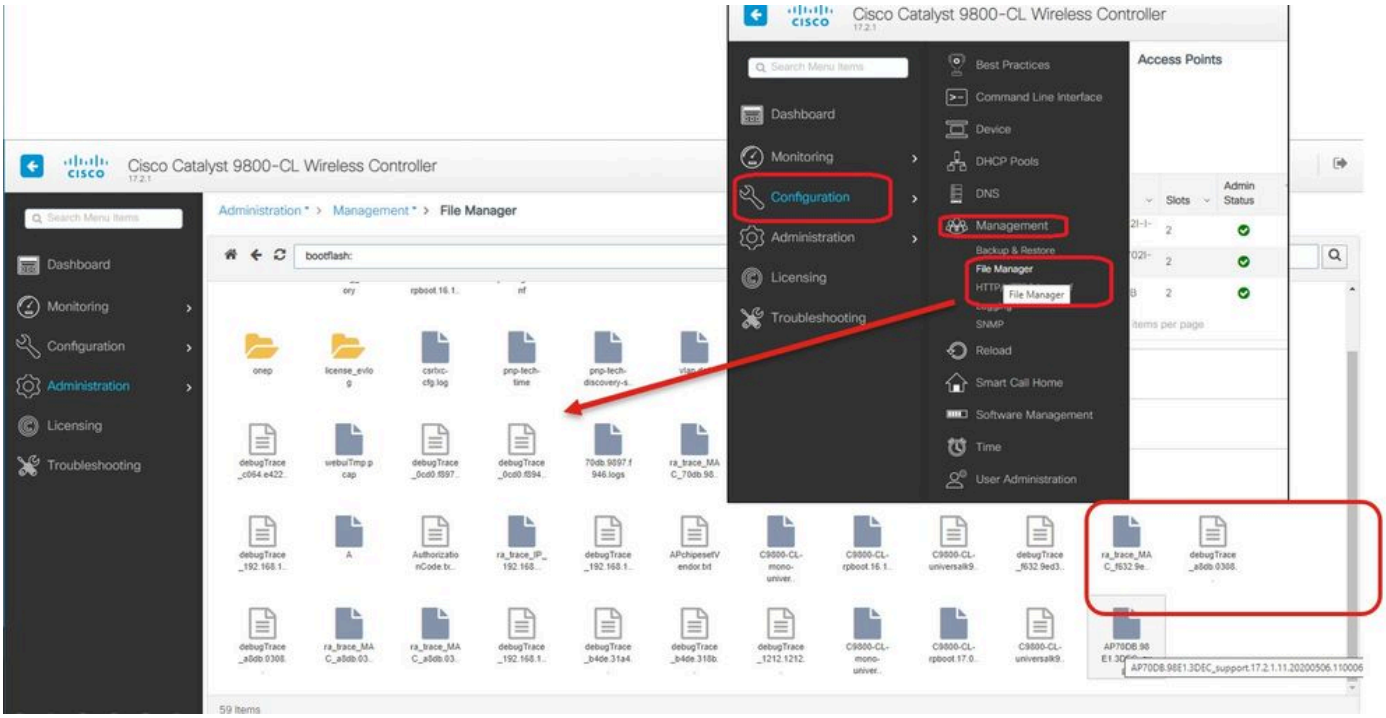
```
! AAA authentication and authorization must be configured properly in order for SCP to work.
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authorization exec default local
Device(config)# username user1 privilege 15 password 0 lab
! SSH must be configured and functioning properly.
Device(config)# ip scp server enable
Device(config)# end
```

Étape 3. Utilisez la commande «copy support-bundle» et nous devons spécifier le nom de fichier à créer dans le serveur SCP.

Conseil : vous pouvez exécuter la commande une fois pour obtenir un nom de fichier significatif, puis copier/coller ce nom de fichier dans la commande :



Étape 4. Ensuite, vous pouvez aller dans l'interface graphique utilisateur d'eWLC et obtenir le fichier sous : Administration > Management > File Manager :



IoT et Bluetooth

Les journaux du serveur gRPC peuvent être vérifiés sur l'AP avec :

```
AP# show grpc server log
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] spaces conn url 10.22.243.33:8000"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] entering stopDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] exiting stopDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] entering startDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] launching token request cycle"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] exiting startDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] spaces token expiration time 2020-04-02 01:36:52 +00
time="2020-04-01T01:36:52Z" level=info msg=" Calling startDNASpacesConn routine "
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Receive Success status"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Connection not in ready state sleeping for 10 second
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Setup Stream for the gRPC connection"
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Connect RPC Succeeded."
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] RX  routine got enabled "
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] TX routine got enabled "
```

La connectivité au connecteur Cisco DNA Spaces peut être vérifiée à l'aide de :

```
AP# show cloud connector key access
Token Valid : Yes
Token Stats :
        Number of Attempts  : 44
        Number of Failures  : 27
        Last Failure on     : 2020-03-28 02:02:15.649556818 +0000 UTC m=+5753.097022576
        Last Failure reason : curl: SSL connect error
        Last Success on     : 2020-04-01 00:48:37.313511596 +0000 UTC m=+346934.760976625
        Expiration time     : 2020-04-02 00:48:37 +0000 UTC
```

```
Connection Retry Interval : 30
```

```
AP# show cloud connector connection detail
Connection State           : READY
Connection Url             :  10.22.243.33:8000
Certificate Available      :  true
Controller Ip              :  10.22.243.31
Stream Setup Interval      :  30
Keepalive Interval         :  30
Last Keepalive Rcvd On     :  2020-04-01 00:32:47.891433113 +0000 UTC m=+345985.338898246
Number of Dials               :  2
Number of Tx Pkts             :  2788175
Number of Rx Pkts             :  11341
Number of Dropped Pkts        :  0
Number of Rx Keepalive        :  11341
Number of Tx Keepalive        :  11341
Number of Rx Cfg Request      :  0
Number of Tx AP Cfg Resp      :  0
Number of Tx APP Cfg Resp     :  0
Number of Tx APP state pkts   :  5
Number of Tx APP data pkts    :  2776829
```

Pour afficher la configuration de diffusion BLE actuelle du point d'accès :

```
AP# show controllers ioTRadio ble 0 broadcast

BLE Profile Config
-------------------
Active profile           : v-iBeacon
Profile 0 (iBeacon)
UUID                     : 00001000000000000000000000000000
Interval (ms)            : 100
Power (dBm)              : -21
Advertised Power (dBm)   : -65
Minor                    : 0
Major                    : 0
TxPower byte             : bfbfbfbfbfbfbfbfbfbfbfbfbf

Profile 1 (Eddystone UID)
Namespace (hex)          : 0000000000005446089c
Instance-ID (hex)        : 7f0000001f00

Profile 2 (Eddystone URL)
URL                      : http://www.
```

Pour afficher les résultats analysés :

```
AP# show controllers ioTRadio ble 0 scan brief
      Profile               MAC  RSSI(-dBm)  RSSI@1meter(-dBm)        Last-heard
```

```
      Unknown 3C:1D:AF:62:EC:EC          88                  0 0000D:00H:00M:01S
      iBeacon 18:04:ED:04:1C:5F          86                 65 0000D:00H:00M:01S
      Unknown 18:04:ED:04:1C:5F          78                 65 0000D:00H:00M:01S
      Unknown 04:45:E5:28:8E:E7          85                 65 0000D:00H:00M:01S
      Unknown 2D:97:FA:0F:92:9A          91                 65 0000D:00H:00M:01S
      iBeacon E0:7D:EA:16:35:35          68                 65 0000D:00H:00M:01S
      Unknown E0:7D:EA:16:35:35          68                 65 0000D:00H:00M:01S
      iBeacon 04:EE:03:53:74:22          45                256 0000D:00H:00M:01S
      Unknown 04:EE:03:53:74:22          45                256 0000D:00H:00M:01S
              04:EE:03:53:6A:3A          72                N/A 0000D:00H:00M:01S
      Unknown 04:EE:03:53:6A:3A          72                 65 0000D:00H:00M:01S
      iBeacon E0:7D:EA:16:35:35          68                 65 0000D:00H:00M:01S
      Unknown E0:7D:EA:16:35:35          67                 65 0000D:00H:00M:01S
      iBeacon 04:EE:03:53:74:22          60                256 0000D:00H:00M:01S
      Unknown 04:EE:03:53:74:22          60                256 0000D:00H:00M:01S
Eddystone URL 04:EE:03:53:6A:3A          72                N/A 0000D:00H:00M:01S
```

Lorsque l'AP agit en mode de passerelle BLE avancé où une application est déployée, vous pouvez vérifier l'état de l'application IoX avec :

```
AP#show iox applications
Total Number of Apps : 1
--------------------------
App Name                      : cisco_dnas_ble_iox_app
   App Ip                     : 192.168.11.2
   App State                  : RUNNING
   App Token                  : 02fb3e98-ac02-4356-95ba-c43e8a1f4217
   App Protocol               : ble
   App Grpc Connection        : Up
   Rx Pkts From App           : 3878345
   Tx Pkts To App             : 6460
   Tx Pkts To Wlc             : 0
   Tx Data Pkts To DNASpaces  : 3866864
   Tx Cfg Resp To DNASpaces   : 1
   Rx KeepAlive from App      : 11480
   Dropped Pkts               : 0
   App keepAlive Received On  : Mar 24 05:56:49
```

Vous pouvez vous connecter à l'application IOX à l'aide de ces commandes, puis surveiller les journaux pendant la configuration de la balise de sol :

```
AP#connect iox application
/ #

/# tail -F /tmp/dnas_ble.log
Tue Mar 24 06:55:21 2020 [INFO]: Starting DNA Spaces BLE IOx Application
Tue Mar 24 06:55:21 2020 [INFO]: Auth token file contents: db26a8ab-e800-4fe9-a128-80683ea17b12
Tue Mar 24 06:55:21 2020 [INFO]: Setting gRPC endpoint to: 1.1.7.101:57777
Tue Mar 24 06:55:21 2020 [INFO]: Auth with token: db26a8ab-e800-4fe9-a128-80683ea17b12
Tue Mar 24 06:55:21 2020 [INFO]: Attempt to connect to DNAS Channel
Tue Mar 24 06:55:21 2020 [INFO]: Starting to run metrics
Tue Mar 24 06:55:21 2020 [INFO]: Starting to run Channel Keepalive
Tue Mar 24 06:55:21 2020 [INFO]: Initialize DNAS Reader Channel
```

```
Tue Mar 24 06:55:21 2020 [INFO]: Start listener for messages
Tue Mar 24 06:55:21 2020 [INFO]: Running BLE scan thread
```

Conclusion

De nombreux outils de dépannage sont disponibles pour nous aider à résoudre les problèmes liés aux points d'accès COS.

Ce document répertorie les plus couramment utilisés et est régulièrement mis à jour.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.