Dépannage des contrôleurs LAN sans fil Catalyst 9800

Table des matières

Introduction

Ce document décrit et fournit une vue d'ensemble de toutes les fonctionnalités de Cisco IOS® XE utilisées pour le dépannage de Catalyst 9800.

Conditions préalables

Exigences

- Connaissances de base des contrôleurs LAN sans fil (WLC).
- Connaissance de base des flux de cas d'utilisation impliqués dans l'utilisation d'un WLC.

Composants utilisés

Ce document couvre les contrôleurs 9800-CL, 9800-L, 9800-40 et 9800-80. Il est principalement basé sur la version 17.3 de Cisco IOS® XE.

Informations générales

Cisco IOS® XE exécuté sur les WLC 9800 est essentiellement constitué d'un noyau Linux (binOS)

avec Cisco IOS® et de tous les processus sans fil implémentés en tant que démons.

Tous les démons de processus peuvent être regroupés sous le terme générique Plan de contrôle (CP) et sont responsables du contrôle et de la mise en service des points d'accès (CAPWAP), de la mobilité et de la gestion des ressources radio (RRM). Gestion des systèmes non fiables, protocole NMSP (Network Mobility Service) destinés au WLC 9800 et provenant de celui-ci.

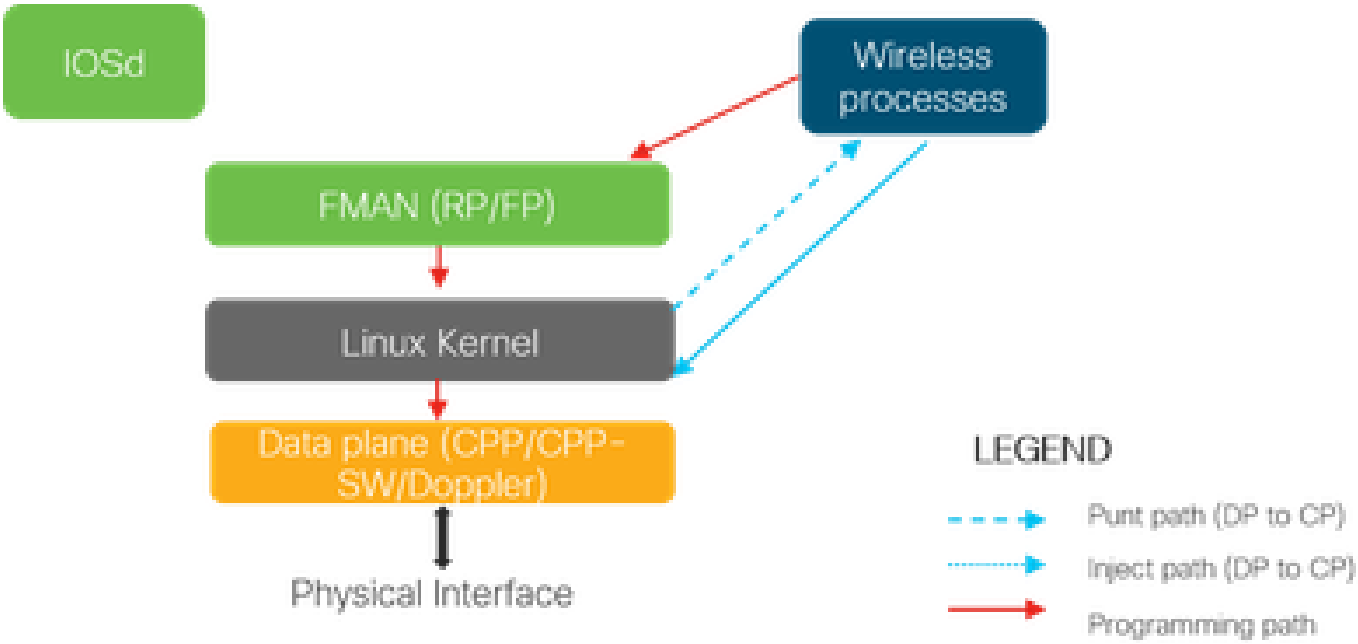
Le plan de données (DP) fait référence aux composants qui transfèrent les données sur le WLC 9800.

Sur toutes les itérations de 9800 (9800-40, 9800-80, 9800-CL, 9800-SW, 9800-L), le plan de contrôle reste assez commun.

Cependant, le plan de données varie avec les modèles 9800-40 et 9800-80 qui utilisent un complexe matériel de processeur Quantum Flow (QFP) similaire à ASR1k, tandis que les modèles 9800-CL et 9800-L utilisent la mise en oeuvre logicielle de Cisco Packet Processor (CPP).

Le 9800-SW exploite simplement le chipset Doppler sur les commutateurs de la gamme Catalyst 9k pour le transfert de données.

Flux de paquets dans le WLC 9800



Lorsqu'un paquet entre dans le WLC 9800 à partir de ports physiques, s'il est déterminé comme étant du trafic de contrôle, il est envoyé aux processus du plan de contrôle correspondants.

Pour une jointure AP, il s'agit de tous les échanges capwap et dtls provenant d'AP. Dans le cas d'une jointure client, il s'agit de tout le trafic provenant du client jusqu'à ce que le client passe à l'état d'exécution.

Au fur et à mesure que les différents démons traitent le trafic entrant, le trafic de retour résultant (réponse capwap, dot11, dot1x, réponse dcp) provenant du WLC 9800 à envoyer au client est réinjecté dans le plan de données pour être envoyé par le port physique.

Lorsque nous traitons des jointures AP, des jointures client, des échanges de mobilité, le plan de données doit être programmé pour pouvoir gérer le transfert du trafic de données.

Ceci se produit lorsque plusieurs composants sont programmés séquentiellement sur le chemin de programmation indiqué dans l'image.

Cisco IOS® XE fournit un ensemble d'outils polyvalent pour suivre le paquet à partir du moment où il entre dans le WLC 9800 jusqu'à ce que le trafic traité quitte la boîte.

La section suivante présente ces outils ainsi que les commandes utilisées pour les appeler à partir de l'interface de ligne de commande (CLI).

Suivi du plan de contrôle

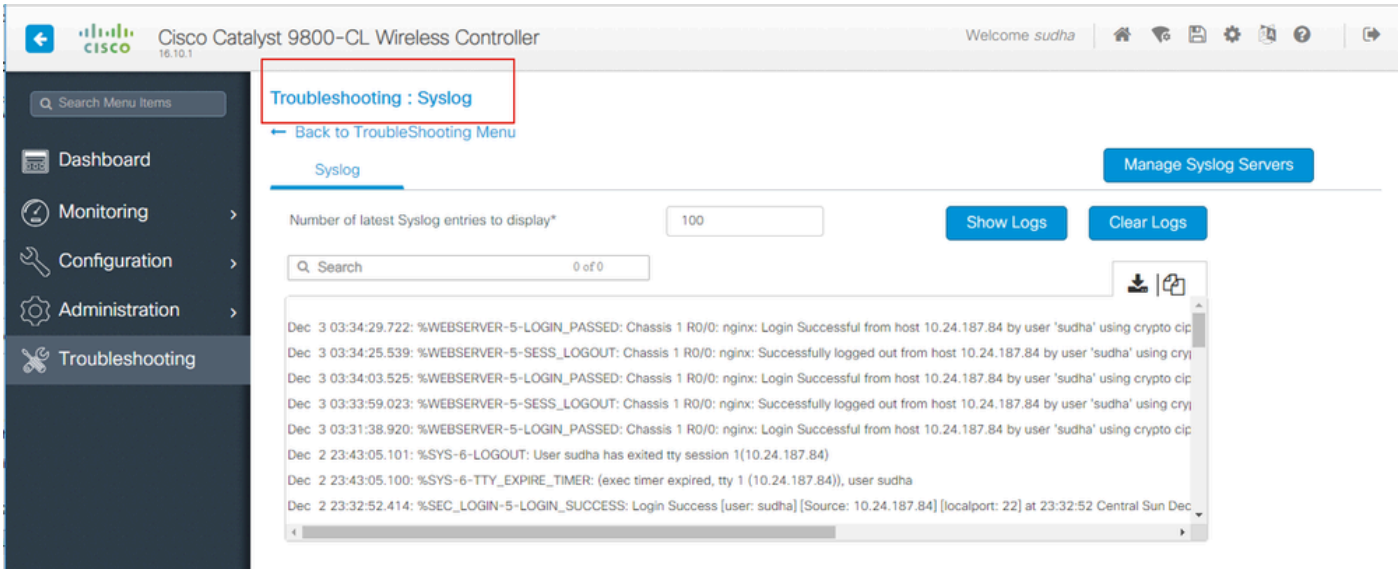
Cette section décrit les commandes et les outils disponibles pour visualiser le traitement effectué par les processus du plan de contrôle après que le paquet destiné au WLC 9800 a été envoyé du DP ou avant d'injecter le paquet de réponse provenant du WLC 9800 au DP pour envoyer l'interface physique

Syslog

Les journaux générés par le WLC 9800 constituent le premier moyen de vérifier l'état général du système.

Toute violation du seuil prédéfini pour les ressources système telles que le processeur, la mémoire et les tampons est signalée dans le journal.

En outre, toutes les erreurs générées par les sous-systèmes sont consignées dans les journaux. Pour afficher les journaux, accédez à Troubleshooting > Syslog



ou exécutez la commande CLI :

```
# show logging
```

Cette sortie affiche des journaux généraux ainsi que certains journaux spécifiques à la technologie sans fil. Cependant, contrairement à l'ancienne plate-forme logicielle Cisco IOS®, aucun débogage sans fil ne parvient généralement à cette sortie de journalisation.

Remarque : si le WLC9800 est configuré pour rediriger ces journaux vers un serveur syslog externe, vous devez également vérifier les journaux sur le serveur syslog externe.

Suivi permanent

Chaque processus de plan de contrôle sur le WLC9800 est constamment en train de se connecter au niveau de journalisation de Notice à sa propre mémoire tampon dédiée. C'est ce que l'on appelle le traçage permanent.

Il s'agit d'une fonctionnalité unique qui vous permet d'obtenir des données contextuelles sur une défaillance qui s'est produite sans exiger que la condition de défaillance soit reproduite.

Par exemple, si vous connaissez AireOS, pour tout dépannage de connectivité client, vous devez activer les débogages et reproduire l'état du problème de connectivité client afin d'identifier la cause première.

Avec le suivi toujours actif, vous pouvez revenir sur les traces déjà capturées et identifier s'il s'agit d'une cause racine commune. En fonction du volume de journaux générés, nous pouvons revenir en arrière de plusieurs heures à plusieurs jours.

Maintenant, alors que les traces sont enregistrées par processus individuel, il est possible de les afficher de manière holistique pour un contexte particulier d'intérêt comme mac client ou mac AP ou adresse ip AP. Pour ce faire, exécutez la commande

```
# show logging profile wireless filter mac  to-file bootflash:
```

Par défaut, cette commande ne remonte que 10 minutes en arrière pour générer et décoder les journaux. Vous pouvez choisir d'aller plus loin dans le temps avec :

```
# show logging profile wireless start last <number> [minutes|hours|days] filter mac  to-file bootflash:
```

Pour afficher les journaux par processus, exécutez la commande

```
# show logging process  to-file bootflash:
```

Remarque : ces CLI proposent plusieurs options de filtrage, notamment le module, le niveau de journalisation, l'horodatage de début, etc. Pour afficher et explorer ces options, exécutez la commande

```
# show logging profile wireless ?
# show logging process  ?
```

Débogage conditionnel et suivi RadioActive

Le débogage conditionnel permet d'activer la journalisation au niveau du débogage pour des fonctionnalités spécifiques pour les conditions d'intérêt.

Le traçage RadioActive va encore plus loin en ajoutant la possibilité d'imprimer conditionnellement des informations de débogage à travers des processus, des threads pour la condition d'intérêt.

Cela signifie que l'architecture sous-jacente est complètement abstraite.

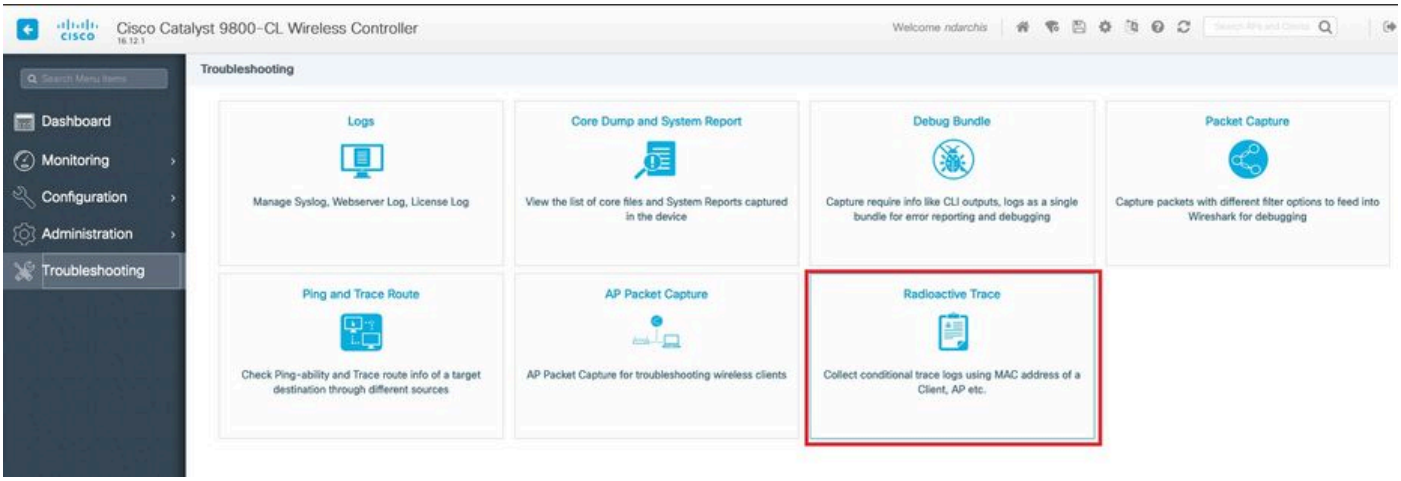
Remarque : sur la version 16.12, le suivi radioactif est uniquement mis en oeuvre pour le dépannage de la jonction AP avec les adresses MAC radio et Ethernet AP, de la jonction client avec l'adresse MAC client ainsi que des problèmes de mobilité avec la connectivité IP de l'homologue de mobilité et CMX avec l'adresse IP CMX comme conditions d'intérêt.

Remarque : la condition adresse MAC/adresse IP fournit des sorties différentes, car différents processus connaissent différents identificateurs pour la même entité réseau (point d'accès ou client ou homologue de mobilité).

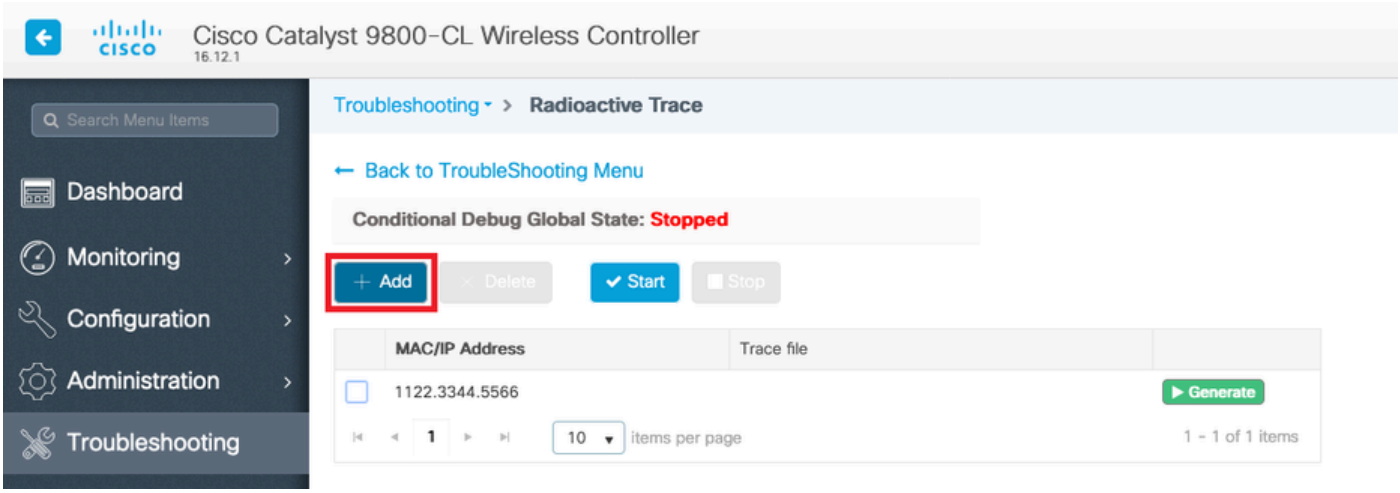
Avec la connectivité du client, comme exemple à dépanner, le débogage conditionnel s'exécute pour le client mac pour obtenir une vue de bout en bout au niveau du plan de contrôle.

Traces radioactives via l'interface utilisateur Web

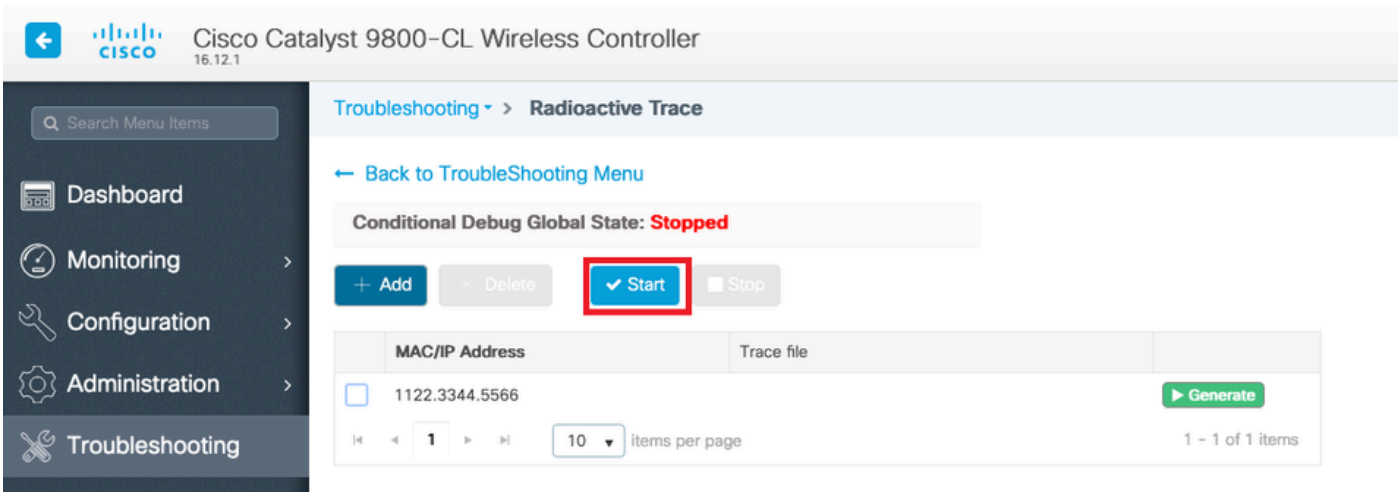
Accédez au menu de la page Dépannage et choisissez Suivi radioactif



Cliquez sur Add et entrez une adresse MAC de client ou d'AP que vous souhaitez dépanner. À partir de la version 16.12, seules les adresses MAC peuvent être ajoutées via l'interface utilisateur graphique. Vous pouvez ajouter une adresse IP via l'interface CLI.

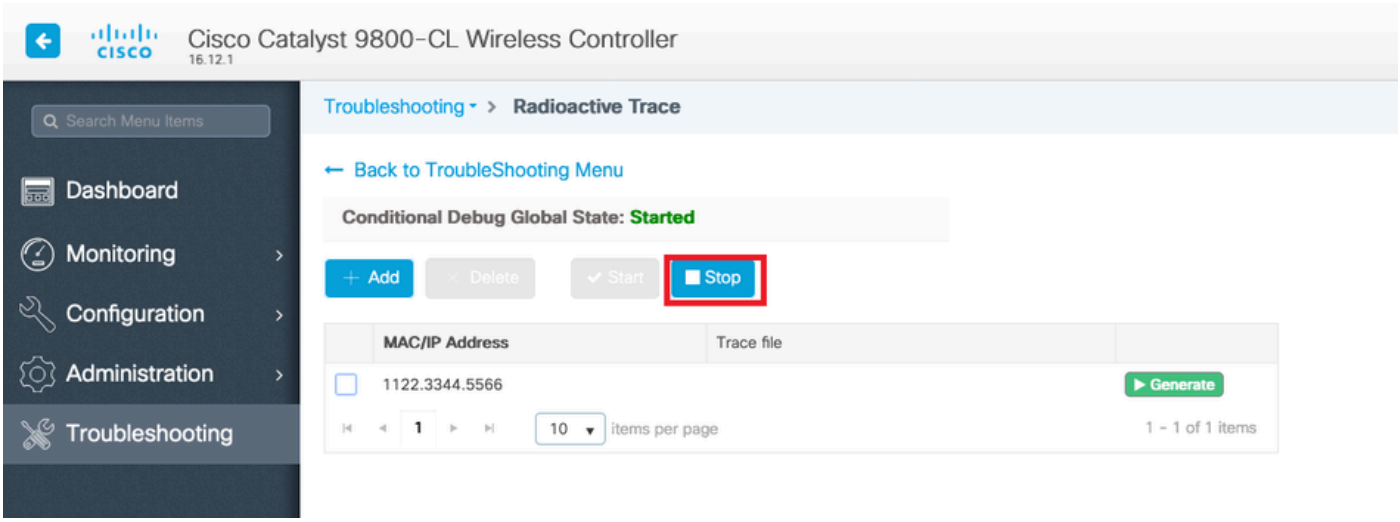


Vous pouvez ajouter plusieurs adresses MAC à suivre. Lorsque vous êtes prêt à démarrer le suivi radioactif, cliquez sur start.

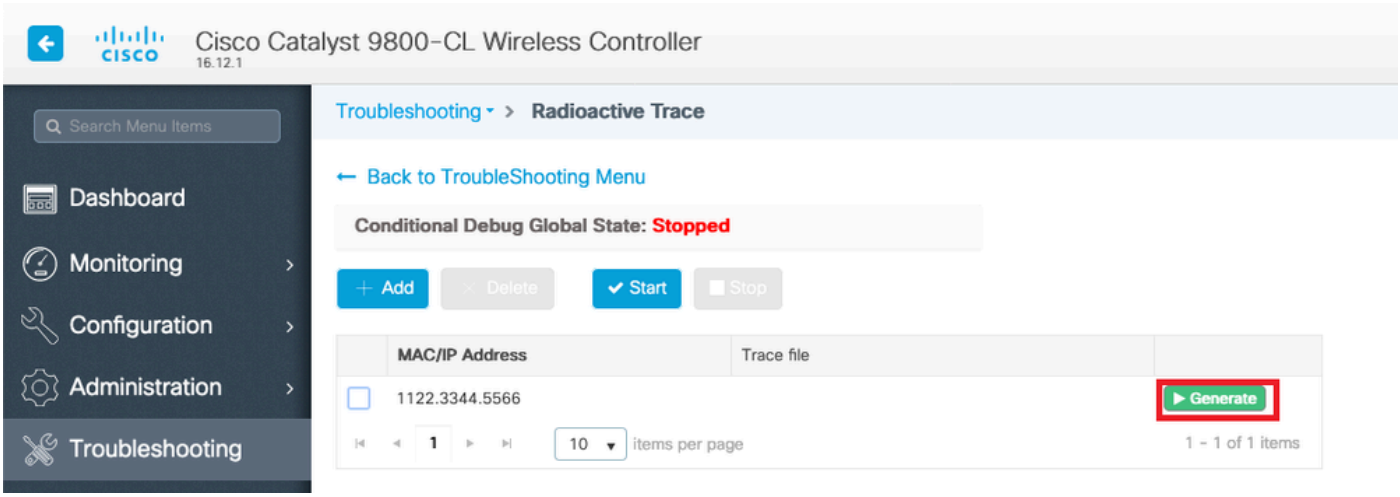


Une fois démarré, les journaux de débogage sont écrits sur le disque à propos de tout traitement du plan de contrôle lié aux adresses MAC suivies.

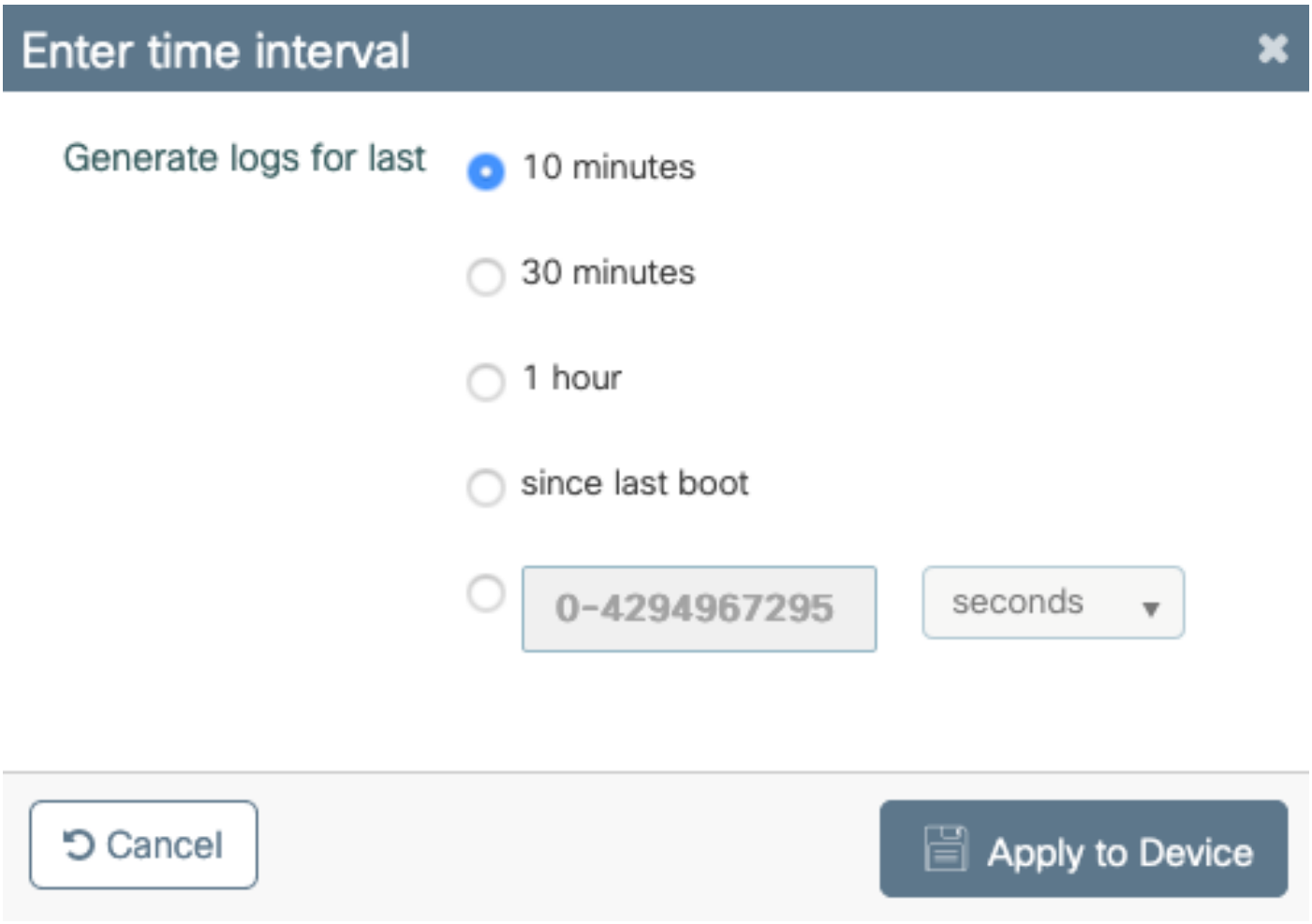
Lorsque vous avez reproduit le problème que vous souhaitez résoudre, cliquez sur Stop.



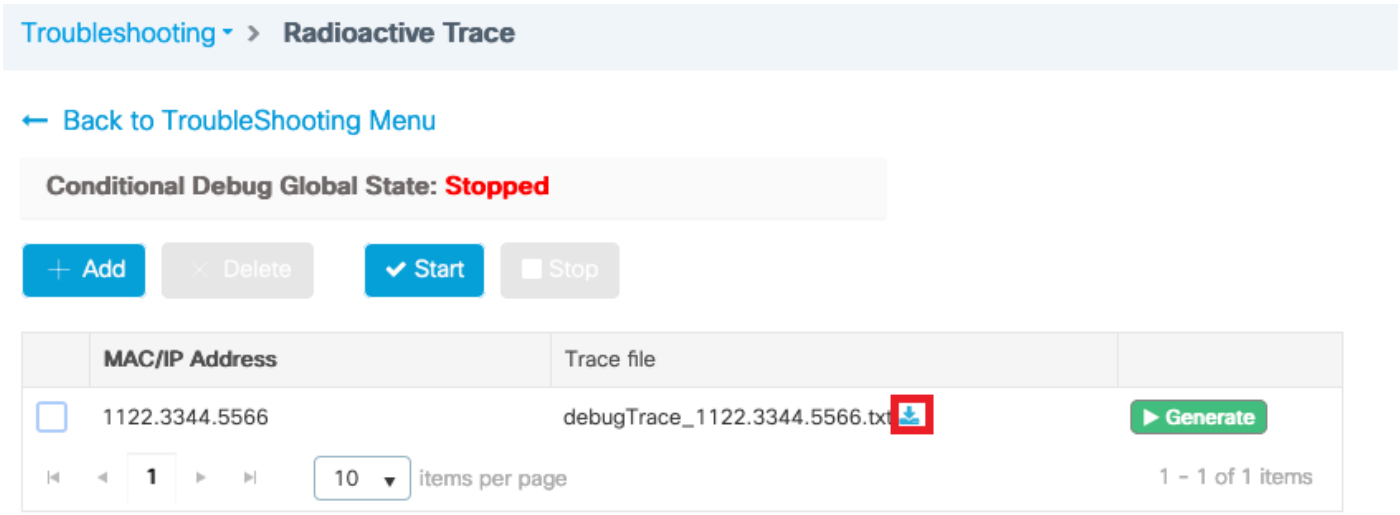
Pour chaque adresse mac déboguée, vous pouvez générer un fichier journal rassemblant tous les journaux appartenant à cette adresse mac en cliquant sur Générer.



Choisissez la durée d'attente avant laquelle vous souhaitez que votre fichier journal assemblé parte et cliquez sur Apply to Device (Appliquer au périphérique).



Vous pouvez maintenant télécharger le fichier en cliquant sur la petite icône située à côté du nom du fichier. Ce fichier est présent dans le lecteur bootflash du contrôleur et peut également être copié hors du boîtier via l'interface de ligne de commande.



Traces radioactives via CLI

Afin d'activer le débogage conditionnel, exécutez la commande

```
# debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds}
```

Pour afficher les conditions actuellement activées, exécutez la commande

```
# show debugging
```

Ces débogages n'impriment aucune sortie sur la session de terminal, mais stockent le fichier de sortie de débogage dans la mémoire flash pour être récupéré et analysé ultérieurement. Le fichier est enregistré avec la convention de dénomination ra_trace_*

Par exemple, pour l'adresse MAC aaaa.bbbb.cccc, le nom de fichier généré est ra_trace_MAC_aaabbbccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Un avantage est que la même commande peut être utilisée pour dépanner les problèmes de jonction AP (entrée AP radio mac et ethernet mac), les problèmes de connectivité client (entrée client mac), les problèmes de tunnel de mobilité (entrée peer ip), les problèmes d'itinérance client (entrée client mac).

En d'autres termes, vous n'avez pas à mémoriser plusieurs commandes comme debug capwap, debug client, debug mobility et ainsi de suite.

Remarque : debug wireless permet également de pointer vers un serveur FTP et d'exécuter une journalisation encore plus détaillée avec le mot clé internal. Nous ne les recommandons pas pour l'instant, car certains problèmes sont en cours de résolution.

Afin de déboguer le fichier de sortie sur la session de terminal, exécutez la commande

```
# more bootflash:ra_trace_MAC_*.log
```

Afin de rediriger la sortie de débogage vers un serveur externe pour l'analyse hors connexion, exécutez la commande

```
# copy bootflash:ra_trace_MAC_*.log ftp://username:password@FTPSERVERIP/path/RATRACE_FILENAME.txt
```

Il existe une vue beaucoup plus détaillée des mêmes niveaux de journal de débogage. pour afficher cette vue détaillée, exécutez la commande

```
# show logging profile wireless internal filter mac  to-file
```

Pour désactiver le débogage pour un contexte spécifique ou avant que le temps de surveillance configuré ou par défaut ne soit écoulé, exécutez la commande.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

⚠ Attention : le débogage conditionnel active la journalisation au niveau du débogage qui à son tour augmente le volume des journaux générés. Laisser cette opération en cours réduit le retard dans le temps à partir duquel vous pouvez afficher les journaux. Il est donc recommandé de toujours désactiver le débogage à la fin de la session de dépannage.

Afin de désactiver tout débogage, exécutez ces commandes

```
# clear platform condition all
# undebug all
```

Débogage non conditionnel par processus

Pour les cas d'utilisation et les processus, non implémentés pour le traçage radioactif, vous pouvez obtenir des traces de niveau de débogage. Pour définir le niveau de débogage sur un processus spécifique, utilisez la commande

```
# set platform software trace <PROCESS_NAME> wireless chassis active R0 { module_name | all-modules }
```

Pour vérifier les niveaux de suivi des différents modules, exécutez la commande

```
# show platform software trace level <PROCESS_NAME> chassis active R0
```

Pour afficher les traces collectées, exécutez la commande

```
# show logging process  to-file
```

Suivi des paquets du plan de données

Lorsqu'un paquet entre pour la première fois dans le WLC 9800, un certain traitement se produit au niveau du plan de données pour identifier si le trafic est un plan de contrôle ou un plan de données.

La fonction Packet-Trace fournit une vue détaillée de ce traitement Cisco IOS® XE effectué au niveau du plan de données et de la décision prise quant à l'envoi, la transmission, l'abandon ou la consommation du paquet.

Cette fonctionnalité sur le WLC 9800 fonctionne exactement de la même manière que l'implémentation sur ASR ! k.

Packet Tracer sur le WLC 9800 fournit trois niveaux d'inspection identiques à ASR1K.

- Statistiques : indique le nombre de paquets qui entrent dans le processeur réseau et en sortent
- Résumé-
  - Il est collecté pour un nombre fini de paquets qui correspondent à une condition d'intérêt spécifique.
  - Le résumé indique les interfaces d'entrée et de sortie, la décision de recherche prise par le plan de données et suit également les paquets de point, d'abandon et d'injection, le cas échéant.
  - Ce résultat fournit une vue succincte du traitement du plan de données
- Path Data : ce champ fournit la vue la plus détaillée de la gestion des paquets DP. Collecté pour un nombre fini de paquets, il inclut un ID de débogage conditionnel qui peut être utilisé pour corréler le paquet DP aux débogages du plan de contrôle, à l'horodatage ainsi qu'aux données de trace de chemin spécifiques aux fonctionnalités. Cette vue détaillée comporte deux fonctionnalités facultatives
  - La copie de paquets vous permet de copier des paquets entrants et sortants sur différentes couches du paquet (couche 2, couche 3 et couche 4)
  - Le tableau d'appel de fonction (FIA) est la liste séquentielle des fonctions qui sont exécutées sur le paquet par le plan de données. Ces fonctionnalités sont dérivées de la configuration par défaut et activée par l'utilisateur sur le WLC 9800

Pour une explication détaillée de la fonctionnalité et des sous-options, référez-vous à Fonctionnalité de trace de paquet de Datapath de Cisco IOS XE

Pour les workflows sans fil tels que la jonction AP, la connectivité client, etc., le suivi de la liaison ascendante bidirectionnel

---

⚠ Attention : le traceur de paquets du plan de données analyse uniquement l'en-tête CAPWAP externe. Par conséquent, des conditions telles que le mac client sans fil ne génèrent pas de résultats utiles.

Étape 1. Définissez la condition qui vous intéresse.

```
# debug platform condition { interface | mac | ingress | egress | both | ipv4 | ipv6 | mpls | match }
```

Avertissement : les commandes - debug platform condition feature ainsi que la commande debug platform condition mac aaaa.bbb.cccc sont destinées au suivi des paquets du plan de contrôle et ne renvoient aucune trace des paquets du plan de données.

Étape 2. Pour afficher les conditions actuellement activées, exécutez la commande

```
# show platform conditions
```

Étape 3. Activez packet-tracer pour un nombre fini de paquets. Ce numéro de paquet est défini comme une puissance de 2 comprise entre 16 et 8192. Par défaut, le résumé et les données de fonction sont capturés. Vous pouvez éventuellement choisir d'obtenir une vue récapitulative uniquement si vous utilisez une sous-option de synthèse uniquement. Vous avez également des sous-options disponibles pour obtenir la trace fia, définir la taille des paquets en octets, tracer punt, injecter ou abandonner des paquets, etc.

```
# debug platform packet-tracer packet <packet-number> {fia-trace}
```

Étape 4. (Facultatif) Vous pouvez copier et vider les paquets au fur et à mesure de leur suivi

```
# debug platform packet-trace copy packet both size 2048 { l2 | l3 | l4 }
```

Étape 5. Activez le débogage conditionnel.

```
# debug platform condition start
```

Étape 6. Afin de voir si le packet-trace collecte des informations, vérifiez les statistiques

```
# show platform packet-trace statistics
```

Étape 7. Pour afficher le résultat de la commande packet-trace, exécutez la commande

```
# show platform packet-tracer summary
```

Étape 8. (Facultatif) Vous pouvez exporter le vidage de paquets pour une analyse hors ligne par le TAC Cisco

```
# show platform packet-trace packet all | redirect { bootflash: | tftp: | ftp: } pactrac.txt
```

Capture de paquets intégrée

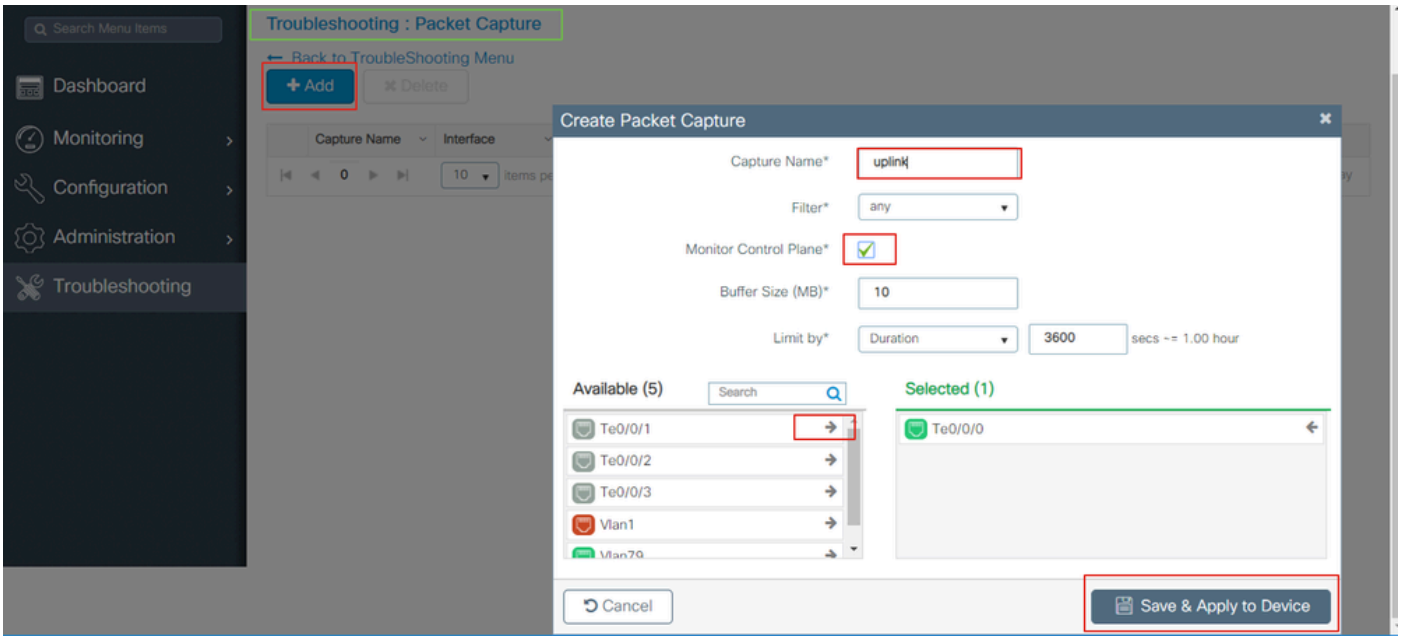
La capture de paquets intégrée (EPC) est une fonction de capture de paquets qui permet de visualiser les paquets destinés aux WLC Catalyst 9800, provenant de ceux-ci et transitant par ceux-ci. Ces captures peuvent être exportées pour une analyse hors ligne avec Wireshark.

Pour plus d'informations sur cette fonction, reportez-vous au Guide de configuration EPC

Comparé à AireOS, au lieu de s'appuyer sur les capacités de capture de paquets et de mise en miroir du trafic sur le commutateur de liaison ascendante, le WLC 9800 permet la capture de paquets sur le boîtier lui-même.

Sur le 9800, cette capture peut être configurée à la fois à partir de l'interface de ligne de commande (CLI) et de l'interface graphique utilisateur (GUI).

Pour configurer via l'interface graphique utilisateur, accédez à Troubleshooting > Packet Capture > +Add



Étape 1. Définissez le nom de la capture de paquets. Un maximum de 8 caractères est autorisé.

Étape 2. Définissez les filtres, le cas échéant

Étape 3. Cochez cette case pour surveiller le trafic de contrôle si vous voulez voir le trafic envoyé au CPU du système et réinjecté dans le plan de données

Étape 4. Définissez la taille du tampon. Un maximum de 100 Mo est autorisé

Étape 5. Définissez la limite, soit par la durée qui autorise une plage de 1 à 1000000 secondes, soit par le nombre de paquets qui autorise une plage de 1 à 100000 paquets, selon vos besoins

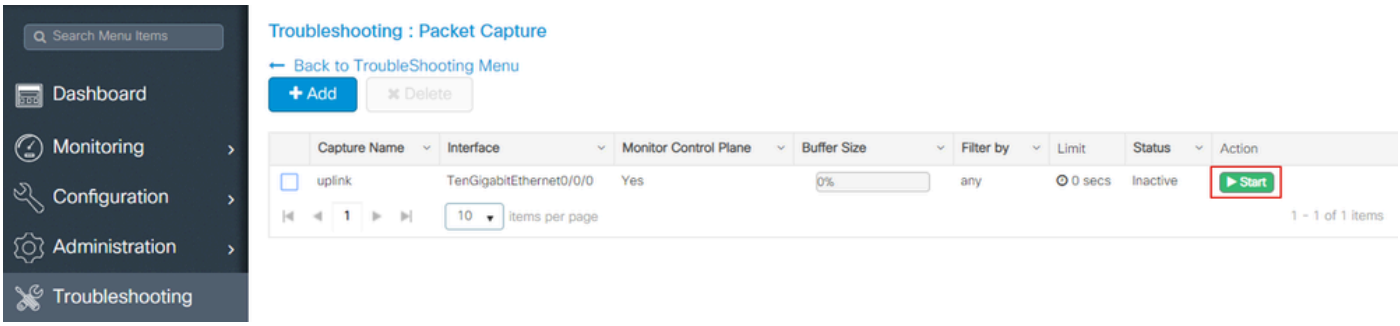
Étape 6. Choisissez l'interface dans la liste des interfaces de la colonne de gauche et sélectionnez la flèche pour la déplacer vers la colonne de droite

Étape 7. Enregistrer et appliquer au périphérique

Étape 8. Pour démarrer la capture, sélectionnez Démarrer

Étape 9. Vous pouvez laisser la capture s'exécuter jusqu'à la limite définie. Pour arrêter manuellement la capture, sélectionnez Arrêter.

Étape 10. Une fois arrêté, un bouton Export devient disponible pour cliquer avec l'option pour télécharger le fichier de capture (.pcap) sur le bureau local via https ou serveur TFTP ou serveur FTP ou disque dur du système local ou flash.



Remarque : l'interface de ligne de commande offre un peu plus de granularité pour les options telles que Limiter par. L'interface graphique utilisateur est suffisante pour capturer des paquets pour des cas d'utilisation courants.

Pour configurer via CLI :

Créez la capture de surveillance :

```
monitor capture uplink interface <uplink_of_the_9800> both
```

Associez un filtre. Le filtre peut être spécifié en ligne ou une liste de contrôle d'accès ou un mappage de classe peut être référencé.

Dans cet exemple, il s'agit de la liste de contrôle d'accès pour faire correspondre le trafic entre les 2 adresses IP du 9800 et d'un autre WLC 5520. Scénario type de dépannage de la mobilité :

```
conf t

ip access-list extended mobilitywlcs
permit ip host <5520_ip_address> host <9800_ip_address>
     permit ip host <9800_ip_address> host <5520_ip_address>
end

monitor capture uplink access-list mobilitywlcs
```

Si vous souhaitez que la capture s'exécute dans une mémoire tampon circulaire, vous disposez d'un certain temps pour remarquer le problème, puis arrêter la capture et l'enregistrer.

Si vous le définissez sur 50MB buffer par exemple. Il faut un maximum de 50 Mo de disque sur le 9800 et son assez grand pour capturer plusieurs minutes de données dans l'espoir que vous obtenez l'occurrence du problème.

```
monitor capture uplink buffer circular size 50
```

Démarrez la capture. Vous pouvez y accéder à partir de l'interface utilisateur graphique ou de la CLI :

```
monitor capture uplink start
```

La capture est maintenant active.

Laisser le client collecter les données nécessaires.

Arrêtez la capture. Vous pouvez le faire via l'interface utilisateur graphique ou CLI :

```
monitor capture uplink stop
```

Vous pouvez récupérer la capture à partir de la GUI > Troubleshooting > Packet Capture > Export.

Ou téléchargez vers un serveur à partir de l'interface CLI. Exemple via ftp :

```
monitor capture uplink export ftp://x.x.x.x/MobilityCAP.pcap
```

Une fois les données nécessaires collectées, supprimez la capture :

```
no monitor capture uplink
```

Voyant d'alarme et alarmes critiques de plate-forme

Tous les appareils 9800 (9800-L, 9800-40 et 9800-80) sont équipés d'un voyant ALM sur leur panneau avant. Si ce voyant devient rouge, cela signifie qu'il y a une alarme critique sur la plate-forme.

Vous pouvez vérifier les alarmes qui font passer le voyant au rouge avec la commande show facility-alarm status

```
WLC#show facility-alarm status
System Totals  Critical: 2  Major: 0  Minor: 0

Source                    Time                   Severity      Description [Index]
------                    ------                 --------      -------------------
TenGigabitEthernet0/1/0   Jul 26 2019 15:14:04   CRITICAL      Physical Port Link Down [1]
TenGigabitEthernet0/1/1   Jul 26 2019 15:14:04   CRITICAL      Physical Port Link Down [1]
```

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.