Configurez la Multidiffusion Sans fil sur des gammes 5760 et 3850 WLCs

Contenu

Introduction

Ce document décrit comment configurer la Multidiffusion Sans fil sur les contrôleurs LAN Sans fil de gammes Cisco 5760 et 3850 (WLCs), qui prennent en charge la *Multidiffusion avec l'unicast* et la *Multidiffusion avec des* mécanismes de mise en oeuvre de *Multidiffusion*.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de base de l'implémentation de Multidiffusion sur les gammes Cisco 5760 et 3850 WLCs.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gamme Cisco 5760 WLC
- Gamme Cisco 3850 WLC
- Point d'accès de gamme Cisco 3602 (AP).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Terminez-vous ces étapes afin d'activer la Multidiffusion sur les Plateformes de l'armoire de câblage de nouvelle génération (NWGC) :

1. Sélectionnez la commande **Sans fil de Multidiffusion** afin d'activer la Multidiffusion sur le contrôleur :
   `ish_5760(config)#`**`wireless multicast`**Remarque: Cette commande par défaut active la *Multidiffusion avec le* mécanisme de mise en oeuvre d'*unicast*.
2. Si vous devez changer le mécanisme de mise en oeuvre à la *Multidiffusion avec la Multidiffusion*, alors sélectionnez cette commande :
   `ish_5760(config)#`**`ap capwap multicast 239.255.255.249`**Remarque: Cette commande configure le groupe de multidiffusion auquel tous les contrôle et ravitaillement des points d'accès sans fil (CAPWAP) des aps se joignent, qui optimise le commutateur de sorte qu'il envoie un message de la Multidiffusion CAPWAP qui atteint tous les aps. Ce processus est différent quand le mode d'unicast est utilisé, car le commutateur serait alors exigé pour envoyer des messages d'unicast à tout les CAPWAP aps. Ceci aide à réduire la charge du système sur le contrôleur.Sur option, vous pouvez naviguer vers la **configuration > le contrôleur du** GUI afin de configurer ces informations, comme affiché ici :

3. Sélectionnez ces commandes afin d'activer le Protocole IGMP (Internet Group Management Protocol) pillant sur le contrôleur (activé par défaut) :
   `ip igmp snooping`

   `ip igmp snooping querier`

   Remarque: La commande d'**ip igmp snooping querier** configure le contrôleur de sorte qu'elle vérifie périodiquement si un client écoute toujours le trafic de multidiffusion.

Écoulement de Multidiffusion sur NGWC

Ces étapes tracent les grandes lignes de l'écoulement du trafic de multidiffusion sur le NGWCs quand la configuration précédente est mise en application :

1. Le contrôleur intercepte les paquets IGMP qui sont envoyés par les clients sans fil.

2. Si l'entrée de client pour cette combinaison de groupe-VLAN-*source de* Multidiffusion existe, alors le contrôleur met à jour les temporisateurs IGMP.

   Si c'est une nouvelle entrée, alors le WLC crée un identifiant de groupe de multidiffusion

(MGID) basé sur (source, groupe, VLAN) le tuple, avec la plage entre 1 et 4,095 pour la couche 2 (L2) ou entre 4,160 et 8,191 pour la couche 3 (L3).

3. Le paquet IGMP est expédié l'en amont.

4. L'entrée MGID est envoyée à AP, avec les informations d'association de client de sorte que le client puisse recevoir le trafic de multidiffusion.

5. Basé sur le mécanisme de mise en oeuvre (Multidiffusion avec l'unicast/Multidiffusion), le contrôleur en avant le trafic à AP convenablement.Remarque: Si le mécanisme de mise en oeuvre est multidiffusé, alors le cryptage du Transport Layer Security de datagramme (DTLS) et le repérage de Qualité de service (QoS) ne sont pas appliqués.
6. AP puis en avant le trafic à chaque client, au besoin.

Vérifiez

Terminez-vous ces étapes afin de vérifier que votre configuration fonctionne correctement :

1. Sélectionnez la commande **Sans fil de Multidiffusion d'exposition** afin de vérifier si la Multidiffusion a été activée correctement :
```
ish_5760#show wireless multicast

Multicast : Enabled
AP Capwap Multicast : Multicast
AP Capwap Multicast group Address : 239.255.255.249
AP Capwap Multicast QoS Policy Name : unknown
AP Capwap Multicast QoS Policy State : None
Wireless Broadcast : Disabled
Wireless Multicast non-ip-mcast : Disabled

Vlan Non-ip-mcast Broadcast MGID
--------------------------------
1 Enabled Enabled Disabled
10 Enabled Enabled Enabled
24 Enabled Enabled Enabled
25 Enabled Enabled Enabled
26 Enabled Enabled Enabled
32 Enabled Enabled Enabled
```
2. Sélectionnez la commande de **somme de capwap d'exposition** afin de vérifier les informations CAPWAP :
```
ish_5760#show capwap sum

Name Src Src Dest Dst Dtls MTU Xact
IP Port IP Port En
---- ----------- ---- ------------ ----- ---- ----- ---
Ca1 172.16.15.1 5247 239.10.10.11 5247 No 1449 1
Ca19 172.16.15.1 5247 172.17.1.54 52451 Yes 1380  3
```
Remarque: Suivant les indications de la sortie, l'interface **Ca1** est utilisée pour le mode de Multidiffusion AP. L'interface **Ca1** a une valeur *DTLS* sans, alors que l'interface **Ca19** a une valeur *DTLS d'***oui**.
3. Écrivez le **détail de capwap d'exposition** ou le **résumé de capwap d'exposition** afin de vérifier le nombre d'aps qui ont joint le groupe de multidiffusion :
```
CAPWAP Tunnels General Statistics:
Number of Capwap Data Tunnels = 2
Number of Capwap Mobility Tunnels = 0
```

```
Number of Capwap Multicast Tunnels = 1


Name APName Type PhyPortIf Mode McastIf
------ --------------------------------
Ca2 ish_3502_lw_2 data  -  multicast Ca0
Ca1 ish_ap       data  - multicast Ca0
Ca0 -     mcas - unicast     -


Name SrcIP               SrcPort     DestIP DstPort DtlsEn MTU
--- ---------------     -------     ------  ------- ------ ---
Ca2 10.105.132.138 5247 10.106.55.133   39237   No     1464
Ca1 10.105.132.138 5247 10.106.15.135   38899   No     1464
Ca0 10.105.132.138 5247 239.255.255.249 5247    No     1464


Name IfId               McastRef
---   ------------------ --------
Ca2   0x0098BA0000000041 0
Ca1   0x00BC2C800000003D 0
Ca0   0x008B53C000000001 2
```

Remarque: La dernière ligne de cette sortie indique l'interface de tunnel CAPWAP qui a été créée pour le trafic de multidiffusion, et le **McastRef** affiche le nombre d'aps qui ont joint le groupe. Ces informations sont utiles quand vous devez vérifier si AP qui ne reçoit pas le trafic de multidiffusion a joint le groupe de multidiffusion.

4. Sélectionnez la commande du **capwap 0 de l'exposition international** afin de vérifier que l'interface de tunnel affiche l'adresse de destination comme adresse de groupe de multidiffusion :

```
ish_5760#show int capwap 0
Capwap0 is up, line protocol is up
Hardware is Capwap
MTU 1464 bytes, BW 10000000 Kbit/sec, DLY 0 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation UNKNOWN, loopback not set
Keepalive set (10 sec)
Carrier delay is 0 msec
Tunnel iifid 39217105861607425, Tunnel MTU 1464
Tunnel source 10.105.132.138:5247, destination 239.255.255.249:5247
```

5. Sélectionnez la commande **récapitulative de groupe de multidiffusion Sans fil d'exposition** afin de vérifier si une entrée MGID est créée pour le groupe de multidiffusion que le client tente de joindre (**239.255.255.250** est utilisé dans cet exemple) :

```
ish_5760#show wireless multicast group summary
IPv4 groups
-------------
MGID   Source   Group             Vlan
---------------------------------------
4160   0.0.0.0 239.255.255.250   32
```

6. Sélectionnez cette commande afin de vérifier si le client en question a été ajouté à la table MGID :

```
ish_5760#show wireless multicast group 239.255.255.250 vlan 32
Source : 0.0.0.0
Group : 239.255.255.250
Vlan : 32
MGID : 4160


Number of Active Clients : 1
Client List
-------------
```

```
Client MAC     Client IP      Status
---------------------------------------
1410.9fef.272c 192.168.24.50 MC_ONLY
```

7. Sélectionnez cette commande afin de vérifier si l'entrée MGID a été ajoutée sur AP pour ce client :

```
ish_ap#show capwap mcast mgid id 4160
L3 MGID = 4160 WLAN bitmap = 0x0001
Slot map/tx-cnt: R0:0x0000/0 R1:0x0001/1499
Clients per Wlan
Wlan : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

!! This shows the number of clients per slot, per Service Set
Identification (SSID) on the AP.

Normal Mcast Clients R0: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Normal Mcast Clients R1: 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
rx pkts = 1499 drp pkts = 0
tx packets:
wlan : 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
slots0 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
slots1 : 1499 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0


Normal Mcast Clients:
Client: 1410.9fef.272c --- Qos User Priority: 0
```

Remarque: Considérez les compteurs sur les paquets reçus et transmis. Ces informations sont utiles quand vous tentez de déterminer si AP correctement en avant les paquets au client.

8. Sélectionnez la commande du **show ip igmp snooping igmpv2-tracking** afin de visualiser tous les mappages de groupe de client-Multidiffusion. Ceci fournit un instantané des clients qui sont connectés et les groupes qu'elles ont joints. Voici un exemple de sortie :

```
ish_5760#show ip igmp snooping igmpv2-tracking

Client to SGV mappings
----------------------

Client: 192.168.24.50 Port: Ca1
Group: 239.255.255.250 Vlan: 32 Source: 0.0.0.0 blacklisted: no

!! If the client has joined more than one multicast group, all the group entries
will be shown here one after the other.


SGV to Client mappings
----------------------

Group: 239.255.255.250 Source: 0.0.0.0 Vlan: 32
Client: 192.168.24.50 Port: Ca1 Blacklisted: no

!! If there is more than one client entry, these will be shown here.
```

9. Sélectionnez cette commande afin de vérifier le MGID du contrôleur :

```
ish_5760#show ip igmp snoop wireless mgid
Total number of L2-MGIDs = 33

Total number of MCAST MGIDs = 0

Wireless multicast is Enabled in the system
Vlan bcast nonip-mcast mcast mDNS-br mgid Stdby Flags
1 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
100 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
115 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
```

```
517 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
518 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
519 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
520 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
521 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
522 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
523 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
524 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
525 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
526 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
527 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
528 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
529 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
530 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
531 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
1002 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1003 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1004 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1005 Enabled Enabled Enabled Enabled Disabled 0:0:1:0


Index MGID (S, G, V)
-------------------------------------------------------
```

Dépannez

Voici une liste de commandes de **débogage** que vous pouvez employer afin de dépanner des questions de configuration du contrôleur :

- **debug ip igmp snooping**
- **debug ip igmp snooping 239.255.255.250**
- **debug ip igmp snooping querier**
- **mettez au point le client-cheminement IOS de radio de fureteur d'igmp d'IP**
- **mettez au point les événements Sans fil IOS de fureteur d'igmp d'IP**
- **mettez au point l'erreur Sans fil IOS de fureteur d'igmp d'IP**
- **mettez au point le petit groupe Sans fil du fureteur AP d'igmp d'IP**
- **mettez au point l'erreur Sans fil du fureteur AP d'igmp d'IP**
- **mettez au point l'événement Sans fil du fureteur AP d'igmp d'IP**
- **mettez au point le message Sans fil du fureteur AP d'igmp d'IP**
- **mettez au point la Multidiffusion de plate-forme**
- **mettez au point l'erreur de Multidiffusion de plate-forme**

- **mettez au point l'événement de Multidiffusion de plate-forme**
- **mettez au point la plate-forme l2m-igmp/l2m-mld/l2multicast/l3multicast**
- **mettez au point l'erreur Sans fil IOS l2mcast**
- **mettez au point le mgid Sans fil IOS l2mcast**
- **mettez au point le spi Sans fil IOS l2mcast**

  Remarque: Assurez-vous que vous employez seulement les commandes de **débogage** appropriées de Multidiffusion afin d'éviter des problèmes de performance.

Voici une sortie de commande de **show debug d'**exemple :

```
show debug
NG3K Wireless:
NG3K WIRELESS Error DEBUG debugging is on
L3 Multicast platform:
NGWC L3 Multicast Platform debugs debugging is on
L2M IGMP platform debug:
NGWC L2M IGMP Platform debugs debugging is on
NGWC L2M IGMP SPI debugs debugging is on
NGWC L2M IGMP Error debugs debugging is on
IP multicast:
IGMP debugging is on for 239.10.10.11
IGMP tracking:
igmpv2 tracking debugging is on
L2MC Wireless:
L2MC WIRELESS SPI EVENTS debugging is on
L2MC WIRELESS REDUNDANCY EVENTS debugging is on
L2MC WIRELESS ERROR debugging is on
IGMP Wireless:
IGMP SNOOP wireless IOS Errors debugging is on
IGMP SNOOP wireless IOS Events debugging is on

Nova Platform:
igmp/snooping/wireless/ap/event debugging is on
multicast/event debugging is on
igmp/snooping/wireless/ap/message/rx debugging is on
igmp/snooping/wireless/ap/message/tx debugging is on
wireless/log debugging is on
l2multicast/error debugging is on
igmp/snooping/wireless/ap/error debugging is on
multicast/error debugging is on
multicast debugging is on
l2multicast/event debugging is on
wireless/platform debugging is on
igmp/snooping/wireless/ap/detail debugging is on
```

Voici un exemple de sortie qui affiche la création MGID sur le contrôleur :

```
*Sep 7 00:12:11.029: IGMPSN: Received IGMPv2 Report for group 239.255.255.250 received
on Vlan 32, port Ca1
*Sep 7 00:12:11.029: IGMPSN: group: Received IGMPv2 report for group 239.255.255.250
from Client 192.168.24.50 received on Vlan 32, port Ca1
*Sep 7 00:12:11.029: (l2mcast_tracking_is_client_blacklisted) Client: 192.168.24.50
Group: 239.255.255.250 Source: 0.0.0.0 Vlan: 32 Port: Ca1
*Sep 7 00:12:11.029: (l2mcsn_process_report) Allocating MGID for Vlan: 32 (S,G):
:239.255.255.250
```

```
*Sep 7 00:12:11.029: (l2mcast_wireless_alloc_mcast_mgid) Vlan: 32 Source: 0.0.0.0
Group: 239.255.255.250
*Sep 7 00:12:11.030: (l2mcast_wireless_alloc_mcast_mgid) Hash entry added!
*Sep 7 00:12:11.030: (l2mcast_wireless_track_and_inform_client) Protocol: IGMPSN
Client-address: 192.168.24.50 (S,G,V): 0.0.0.0 239.255.255.250 32 Port: Ca1, MGID:
4160 Add: Add
*Sep 7 00:12:11.030: (l2mcast_get_client_params) Client Addr: 192.168.24.50 Client-id:
40512055681220617 Mcast-vlan: 32(l2mcast_wireless_inform_client) Protocol: IGMPSN
Client-address: 192.168.24.50 (S,G,V): 0.0.0.0 239.255.255.250 32 Port: Ca1, iifid =
0x9667C000000004 MGID: 4160 Add: Add
*Sep 7 00:12:11.030: (l2mcast_wireless_inform_client) Sent INFORM CLIENT SPI
*Sep 7 00:12:11.030: (l2mcast_wireless_track_and_inform_client)
l2mcast_wireless_inform_client passed
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: IGMP has sent the
WCM_INFORM_CLIENT with ^I client_id = 40512055681220617/8fed8000000009 ^I capwap id =
42335320837980164 ^I mac_addr = 1410.9fef.272c ^I num_entry = 1
```

Une fois que l'entrée est créée du côté de Cisco IOS®, ceci est passé au processus du module de Wireless Control (WCM), qui vérifie avant qu'il ajoute l'entrée :

```
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: i = 0, source = 0.0.0.0 group =
239.255.255.250 client_ip = 192.168.24.50 vlan = 32, mgid = 4160 add = 1
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: in igmp_wcm_client_join_callback
source = 0.0.0.0 group = 239.255.255.250 client_ip = 192.168.24.50 vlan = 32
client_mac = 1410.9fef.272c mgid = 4160
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: apfMswtp_iifid = 9667c000000004
capwap_if_id = 9667c000000004
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: rrc_manual_mode = 0
rrc_status = 2
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: locking mgid Tree in file
bcast_process.c line 491
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: allocateL3mgid: mgid entry AVL
search key dump:
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: 00000000: 00 00 00 00 ef 01 01
01 00 08 ff ff ff ff ff ff .................^M 00000010: ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff .................^M 00000020: ff ff ..^M
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: mcast_group_client_lookup:
Lookup failed for client with mac 1410.9fef.272c
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: unlocking mgid Tree in file
bcast_process.c line 624
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: spamLradSendMgidInfo: ap =
0C85.25C7.9AD0 slotId = 1, apVapId = 1, numOfMgid = 1 join = 1 isL2Mgid = 0,
mc2ucflag = 0, qos = 0
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: mscbApMac = 0c85.25c7.9ad0
client_mac_addr = 1410.9fef.272c slotId = 1 vapId = 1 mgid = 4160 numOfSGs = 2,
rrc_status = 2
```

Voici une liste de commandes de **débogage** que vous pouvez employer afin de dépanner des questions de configuration d'AP :

- **mettez au point le Trans. de mcast de capwap**
- **mettez au point la requête de mcast de capwap**

Voici un exemple **mettent au point la** sortie de commande :

```
*Sep 7 06:00:38.099: CAPWAP MCAST: capwapDecodeMgidPayload: mgidTypeStr L3 IGMP MGID
ADD,mgidType 53,mgid=4160,mgid operation=1
*Sep 7 06:00:38.099: CAPWAP MCAST: capwapAddMgidEntry: slotId= 1, client_mac=
1410.9fef.272c, mgid= 4160, wlanid= 0, mc2ucflag= 0, priority= 0, downpriority= 0
L3 mgid flag = L3 IGMP MGID .
*Sep 7 06:00:38.099: CAPWAP MCAST: allocateMgidEntry: mgid = 4160,isL3Mgid=1
*Sep 7 06:00:38.099: CAPWAP MCAST: capwap_bss_mgid_enable:MGID 4160 enable -
Slot=1 WLAN=1
```

```
*Sep 7 06:00:38.099: CAPWAP MCAST: L3 IGMP MGID ADD MGID = 4160 SUCCESSFUL .!!
```

Remarque: Tandis que l'entrée MGID est ajoutée, l'ID DE VLAN affiche en tant que **0** dans la sortie précédente. Cependant, quoique l'entrée soit supprimée, il affiche le mappage correct VLAN.

Voici une liste de **commandes show** que vous pouvez utiliser l'analyse approfondie du contrôleur :

- **affichez le résumé de client sans fil**
- **affichez la base de données toute de wcdb**
- **affichez le résumé Sans fil de groupe de multidiffusion**
- **affichez le <id> Sans fil de VLAN de <ip> de groupe de multidiffusion**
- **affichez le <id> Sans fil de VLAN de <ip> de groupe de <ip> de source multicast**
- **mgid de radio de show ip igmp snooping**
- **show ip igmp snooping igmpv2-tracking**

Voici une liste de **commandes show** que vous pouvez utiliser l'analyse approfondie d'AP :

- **affichez le mgid tout de mcast de capwap**
- **affichez le <id> d'id de mgid de mcast de capwap**

Importantes considérations

Voici quelques importantes considérations et limites en vue de la configuration qui est décrite dans ce document :

- Le nombre de groupes de multidiffusion lesquels chaque client peut écouter est limité à 16. Une fois que le client envoie la *demande de jonction* avec le 17ème groupe, la création se produit du côté de Cisco IOS, mais le côté WCM envoie un message de *refuser au* Cisco IOS. Ce dernier supprime alors ce groupe.
- Actuellement, seulement l'IGMP version 2 (V2) est pris en charge. Si un client utilise l'IGMP version 3 (V3), alors la création MGID ne se produit pas sur le contrôleur. Pour cette raison, dans la source, le groupe, et le VLAN, l'adresse source est toujours **0.0.0.0**.
- Le nombre de L3 MGIDs qui sont pris en charge sur la plage NGWC de 4,160 à 8,191. Puisqu'une entrée MGID est une combinaison de l'adresse de multidiffusion et du VLAN, il peut y avoir seulement 4,000 telles combinaisons. Ceci pourrait être une limite dans de grands environnements.
- La caractéristique de *Bonjour* à travers des VLAN n'est pas prise en charge. C'est parce que l'adresse IP 224.0.0.251 est une adresse de multidiffusion de lien-gens du pays. Les gammes

Cisco 5760 et 3850 WLCs, comme aucun autre commutateur de Catalyst, pas snoop des adresses locales à la liaison. Pour cette raison, vous verrez ce message d'erreur apparaître :

```
IGMPSN: group: Received IGMPv2 report for group 224.0.0.251 from Client 192.168.24.94
received on Vlan 32, port Ca93 with invalid group address.
```