

Dépannage du programme matériel de multidiffusion sur les périphériques 6500/7600

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Dépannage](#)

[Vérification](#)

Introduction

Ce document décrit comment dépanner et vérifier la programmation matérielle multidiffusion sur les plates-formes 6500 et 7600.

Conditions préalables

Conditions requises

Cisco vous recommande d'avoir des connaissances en multidiffusion.

Components Used

Les informations de ce document sont basées sur 7600 avec SUP720 12.2(33)SXJ6 ou supérieur.

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Sur les périphériques 6500 et 7600, les valeurs de transfert multidiffusion sont programmées dans le matériel pour une transmission plus rapide et la préservation du processeur.

Deux types de réplication multidiffusion sont possibles sur ces périphériques :

- Réplication entrante
- Réplication de sortie

La réplication de sortie est la méthode préférée car la réplication est effectuée sur les cartes de ligne qui quittent et qui enregistrent l'utilisation du fabric.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Vérifiez d'abord l'état de la route pour vous assurer que l'état (S, G) est créé.

```
R1#show ip mroute 239.1.1.5
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - URD, I - Received Source Specific Host Report,
Z - Multicast Tunnel, z - MDT-data group sender,
Y - Joined MDT-data group, y - Sending to MDT-data group,
V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.5), 7w0d/stopped, RP 10.1.1.1, flags: SJC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Vlan102, Forward/Sparse, 1y33w/00:02:48

(192.168.1.1, 239.1.1.5), 6d00h/00:02:50, flags: MT
Incoming interface: GigabitEthernet6/2, RPF nbr 172.16.2.2
Outgoing interface list:
Vlan102, Forward/Sparse, 6d00h/00:02:48
```

Assurez-vous que l'état S, G est créé avec le trafic entrant sur Gig6/2 et demandé sur le VLAN 102.

Vous pouvez également utiliser la version count de la commande précédente pour voir que les compteurs de paquets augmentent.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vérifiez que vlan 102 est une interface sortante commutée par matériel, vous pouvez également voir le nombre de paquets commutés et le nombre total de flux commutés par matériel.

```
R1#show platform software multicast ip group 239.1.1.5
Multicast hardware switched flows:

(192.168.1.1, 239.1.1.5) Incoming interface: GigabitEthernet6/2, Packets Switched: 4076111744
Hardware switched outgoing interfaces:
Vlan102
Total hardware switched flows: 25
```

Vérifiez maintenant l'utilisation interne du VLAN pour savoir quel VLAN interne a été attribué à l'interface entrante Gig6/2.

```
R1#show vlan internal usage
```

VLAN Usage

```
-----  
1006 online diag vlan0  
1007 online diag vlan1  
1008 online diag vlan2  
1009 online diag vlan3  
1010 online diag vlan4  
1011 online diag vlan5  
1012 PM vlan process (trunk tagging)  
1013 Control Plane Protection  
1014 vrf_0_vlan  
1015 Container0  
1016 IPv6-mpls RSVD VLAN  
1017 IPv4 VPN 0 Egress multicast  
1018 IP Multicast Partial SC vpn(0)  
1019 Multicast VPN 0 QOS Vlan  
1020 GigabitEthernet6/2  
1021 GigabitEthernet5/2
```

Vous pouvez voir que le VLAN interne 1020 a été attribué à l'interface GigabitEthernet6/2.

Passez à la vérification du programme CEF dans le superviseur.

```
R1#remote command switch show mls cef ip multicast source 192.168.1.1 group 239.1.1.5
```

```
Multicast CEF Entries for VPN#0
```

```
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial, E - Encapsulation, D -  
Decapsulation, M - MAC rewrite, T - Forwarding  
c - Central Rewrite, p - Primary Input, r - Recirculation, h - Entry sitting on Encap/Decap VRF  
layer
```

```
Source/mask Destination/mask RPF/DF Flags #packets #bytes rwindex Output Vlans/Info
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+  
+-----+  
192.168.1.1/32 239.1.1.5/32 V11020 CTp 4077289327 104637396418 0x7FFA V1102 [1 oifs]  
192.168.1.1/32 239.1.1.5/32 V11017 Tc 0 0 0x7FFA V1102 [1 oifs]
```

```
Found 1 entries. 1 are mfd entries
```

```
R1#remote command switch show mls cef ip multicast source 192.168.1.1 group 239.1.1.5
```

```
Multicast CEF Entries for VPN#0
```

```
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial, E - Encapsulation, D -  
Decapsulation, M - MAC rewrite, T - Forwarding  
c - Central Rewrite, p - Primary Input, r - Recirculation, h - Entry sitting on Encap/Decap VRF  
layer
```

```
Source/mask Destination/mask RPF/DF Flags #packets #bytes rwindex Output Vlans/Info
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+  
+-----+  
192.168.1.1/32 239.1.1.5/32 V11020 CTp 4077354094 104726386276 0x7FFA V1102 [1 oifs]  
192.168.1.1/32 239.1.1.5/32 V11017 Tc 0 0 0x7FFA V1102 [1 oifs]
```

```
Found 1 entries. 1 are mfd entries
```

À partir de cette sortie, vérifiez dans la colonne Reverse Path Forwarding (RPF)/ Don't Fragment (DF) le VLAN entrant sur lequel il reçoit.

Vous pouvez voir le V11020 qui correspond à ce qui a été vu dans l'utilisation interne du VLAN pour Gig6/2.

Voir V11017 dans la liste, c'est-à-dire le VLAN utilisé pour la réplication de sortie, et est également inclus dans la commande interne vlan usage.

En tant que Vlan de sortie, vous pouvez voir le VLAN 102 qui est votre interface sortante, dans le

cas où l'interface sortante est un port L3, vous devez voir un vlan interne répertorié qui peut ensuite être corrélé avec la commande d'utilisation interne du vlan pour voir s'il correspond.

Notez également la colonne rwindex avec la valeur 0x7FFA, utilisez cette option pour afficher les interfaces de destination.

```
R1#remote command switch mcast ltl-info index 7ffa
index 0x7FFA contain ports 1/T1,T2, 2/T1,T2, 3/T1,T2, 4/T1,T2, 5/T1, 6/T1
```

Le résultat affiche le trafic de multidiffusion envoyé aux modules de réplication sur les cartes de ligne. Il a cette nomenclature 1/T1, T2. Le numéro 1 correspond au module 1, tandis que T1 et T2 sont les deux modules de réplication de la carte de ligne 1. Assurez-vous que le paquet est envoyé aux modules de réplication sur les cartes de ligne 1, 2, 3, 4, 5 et 6.

Vérifiez les détails de la programmation CEF :

```
R1#remote command switch show mls cef ip multicast source 192.168.1.1 group 239.1.1.5 detail
```

```
Multicast CEF Entries for VPN#0
(172.16.5.51, 239.250.250.2)
IOSVPN:0 (1) PI:1 (1) CR:0 (1) Recirc:0 (1)
Vlan:1020 AdjPtr:475138 FibRpfNf:1 FibRpfDf:1 FibAddr:0x30090
rwvlans:1020 rwindex:0x7FFA adjmac:0alb.0ddd.bbbb rdt:1 E:0 CAP1:0
fmt:Mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L2&L3 met2:0x8427 met3:0x8405
packets:0004079198240 bytes:000000107260242880
Starting Offset: 0x8427
V E L0 C:1017 I:0x02028
Starting Offset: 0x8405
V E C: 102 I:0x02013
```

```
IOSVPN:0 (1) PI:0 (1) CR:1 (1) Recirc:0 (1)
Vlan:1017 AdjPtr:475139 FibRpfNf:0 FibRpfDf:1 FibAddr:0x30092
rwvlans:1017 rwindex:0x7FFA adjmac:0alb.0ddd.bbbb rdt:1 E:0 CAP1:0
fmt:Mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x8405
packets:00000000000000 bytes:000000000000000000
Starting Offset: 0x8405
V E C: 102 I:0x02013
```

```
Annotation-data: [0x14B455F0]
A-vlan: 1020 NS-vlan: 0 RP-rpf-vlan: 0
Anntn flags: [0x10] H
MTU: 1500 Retry-count: 0
Sec-entries count: 1
Met-handle: 0x455BA08 New-Met-handle: 0x0
Met2-handle: 0x10C07ED0
```

```
HAL L3-data : [0x5F954E8]
Flags: 0x4 FIB-index: 0x20DE ADJ-index: 0x74002 NF-addr: 0xFFFFFFFF
ML3 entry type: 0x0 [(S,G) shortcut]
Flags: 0xA1000000 Vpn: 0 Rpf: 1020 Rw_index: 0x7FFA
Adj_mtu: 1514 Met2: 0x8427 Met3: 0x8405
V6-data: NULL
```

```
---Secondary entry [1]---
```

```
HAL L3-data : [0x1831F8F8]
Flags: 0x4 FIB-index: 0x20DF ADJ-index: 0x74003 NF-addr: 0xFFFFFFFF
ML3 entry type: 0x0 [(S,G) shortcut]
Flags: 0x90000000 Vpn: 0 Rpf: 1017 Rw_index: 0x7FFA
Adj_mtu: 1514 Met2: 0x0 Met3: 0x8405
V6-data: NULL
```

---TE entries---

Found 1 entries. 1 are mfd entries

Concentrez-vous sur le décalage de départ I : valeurs

Starting Offset: 0x8427

V E L0 C:1017 I:0x02028

Starting Offset: 0x8405

V E C: 102 I:0x02013

Utilisez ces valeurs pour voir quelles interfaces sont programmées sur le matériel.

R1#**remote command switch test mcast ltl-info index 02028**

index 0x02028 contain ports 1/T1,T2, 2/T1

R1#**remote command switch test mcast ltl-info index 02013**

index 0x02013 contain ports 1/21-33,44, 2/21,23

Le premier index indique que le paquet doit être transféré à la carte de ligne 1 vers les moteurs de réplication 1 et 2 et vers le moteur de réplication de la carte de ligne 2 1.

Le deuxième index indique le paquet qui transfère sur les ports 1/21-33 et 44, ce qui signifie que le moteur de réplication 1 de la carte de ligne 1 couvre les ports de 1/1 à 1/23, tandis que le moteur de réplication 2 couvre jusqu'à 48, ainsi que le port 2/21 et le port 2/23 qui utilisent le moteur de réplication 1 de la carte de ligne 2, les deux.