Configurer la multidiffusion sur UCS

Contenu

Introduction

Ce document décrit la procédure requise pour configurer la multidiffusion dans Unified Computing Systems (UCS). La multidiffusion (MCAST) permet d'envoyer simultanément des données sur un réseau à plusieurs utilisateurs (communication de groupe un à plusieurs ou plusieurs). Le protocole IGMP (Internet Group Management Protocol) est un composant essentiel de la multidiffusion. Le but principal d'IGMP est de permettre aux hôtes de communiquer leur désir de recevoir le trafic de multidiffusion, au(x) routeur(s) de multidiffusion IP sur le réseau local. En retour, cela permet au ou aux routeurs de multidiffusion IP de “ se joindre ” le groupe de multidiffusion spécifié et de commencer à transférer le trafic de multidiffusion sur le segment de réseau vers l'hôte.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCS
- Commutation multicast Nexus

Components Used

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

- Interconnexion de fabric - 6100 / 6200
- UCSM (Unified Computing System Manager)
- Commutateur en amont (EX); Nexus 5000)

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.

Informations générales

Avant la version 2.1 de Unified Computing System Manager (UCS-M) :

- La surveillance IGMP est activée par défaut sur la multidiffusion sur UCS et ne peut pas être désactivée. (Les centres d'assistance technique Cisco (TAC) peuvent désactiver via le plug-in de débogage).
- Les interconnexions de fabric UCS n'ont pas de fonctionnalité d'interrogation IGMP ; pour cela, vous devez activer la fonctionnalité querier sur un périphérique du réseau L2 en amont.
- Pour que cela fonctionne, vous avez besoin d'un routeur de multidiffusion dans le VLAN ou d'un interrogateur IGMP dans le VLAN.

Del Mar 2.1 Notes :

- Par défaut, IGMP Snooping est activé, les administrateurs réseau doivent examiner attentivement toutes les conditions requises pour désactiver IGMP Snooping et les performances négatives qui pourraient être rencontrées.
- La configuration IGMP Snooping n'est disponible et configurable que pour chaque VLAN, vous ne pouvez pas activer ou désactiver la surveillance IGMP globalement.
- La possibilité de désactiver la surveillance IGMP est prise en charge en mode hôte final (EHM) et en mode commutateur.
- Aucune prise en charge des politiques de multidiffusion sur les groupes réseau (autre nouvelle fonctionnalité de Del Mar).

Spécifications d'interconnexion de fabric :

- Pour une interconnexion de fabric de la gamme 6100, tous les VLAN peuvent uniquement utiliser la politique de multidiffusion par défaut ; cependant, l'utilisateur peut modifier les états

IGMP Snooping/Querier de cette stratégie par défaut. Si vous configurez une autre stratégie de multidiffusion, une erreur s'affiche : « Pour les réseaux locaux virtuels dans l'interconnexion de fabric X, seule la stratégie de multidiffusion par défaut est prise en charge. »
- Pour modifier la stratégie de multidiffusion pour un VLAN donné (en politique autre que la stratégie de multidiffusion par défaut) est uniquement prise en charge sur 6200 FI et NOT sur 6100. La raison pour laquelle les FI 6100 ne peuvent pas avoir de politiques de multidiffusion différentes sur ses VLAN est due à une limitation dans l'ASIC Gatos. Cette limitation n'existe pas pour les 6200 FI avec ASIC Carmel.

Options de configuration de multidiffusion UCS

Configuration en mode hôte final

Surveillance IGMP activée / Requête IGMP activée

- Il envoie uniquement les requêtes aux lames. Il n'envoie pas de requêtes IGMP au réseau en amont.
- Les FI n'envoient pas les requêtes IGMP au commutateur en amont, car cela contredit le rôle du mode hôte final dans le réseau. Cela peut conduire à un trafic de multidiffusion indésirable (contrôle et données) envoyé aux FI. C'est la raison pour laquelle il a été décidé de confier aux FI EHM la responsabilité de transmettre les requêtes IGMP à ses lames uniquement.
- Par conséquent, exigez une des configurations approuvées :

Configurations approuvées :

Configurez le demandeur IGMP sur le commutateur en amont avec la surveillance IGMP activée ou Désactivez la surveillance IGMP sur le commutateur en amont pour inonder le trafic de multidiffusion. Vous pouvez également modifier les FI en mode de commutation.

Surveillance IGMP activée / Requête IGMP désactivée

- Le mode par défaut, identique aux versions antérieures à Del Mar.
- Nécessite : IGMP Querier dans le commutateur en amont pour le VLAN avec la surveillance IGMP activée ou le routeur de multidiffusion dans le VLAN.

Surveillance IGMP désactivée / Requête IGMP désactivée

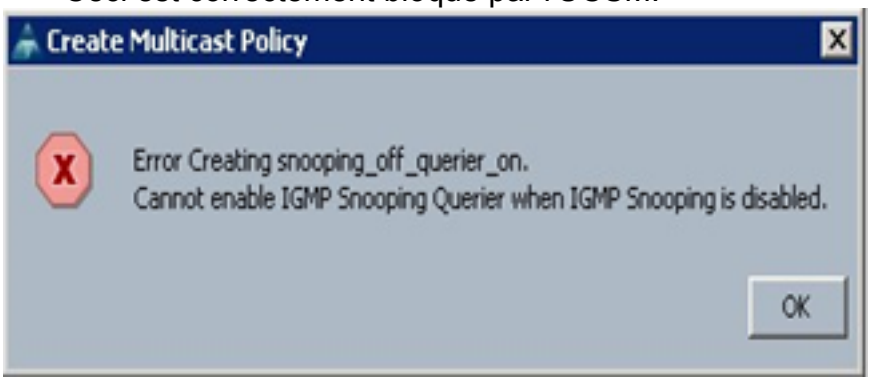
- Les FI inondent le trafic de multidiffusion dans le VLAN.
- Nécessite une des configurations approuvées pour fonctionner correctement :

Configurations approuvées :

Le commutateur en amont peut avoir la surveillance IGMP activée ou l'avoir désactivée sur le commutateur en amont pour inonder le trafic de multidiffusion.

Surveillance IGMP désactivée / Requête IGMP activée

- Cette configuration n'est pas valide.
- Ceci est correctement bloqué par l'UCSM.



Configuration en mode de commutation

Surveillance IGMP activée / Requête IGMP activée

- Les FI transmettent les requêtes IGMP au réseau en amont.
- Les commutateurs en amont découvrent le demandeur IGMP configuré sur les FI, puis ils créent et transmettent le trafic MCAST vers les FI.
- Nécessite : Commutateur en amont avec surveillance IGMP activée ou avec surveillance désactivée pour inonder le trafic multicast.

Surveillance IGMP activée / Requête IGMP désactivée

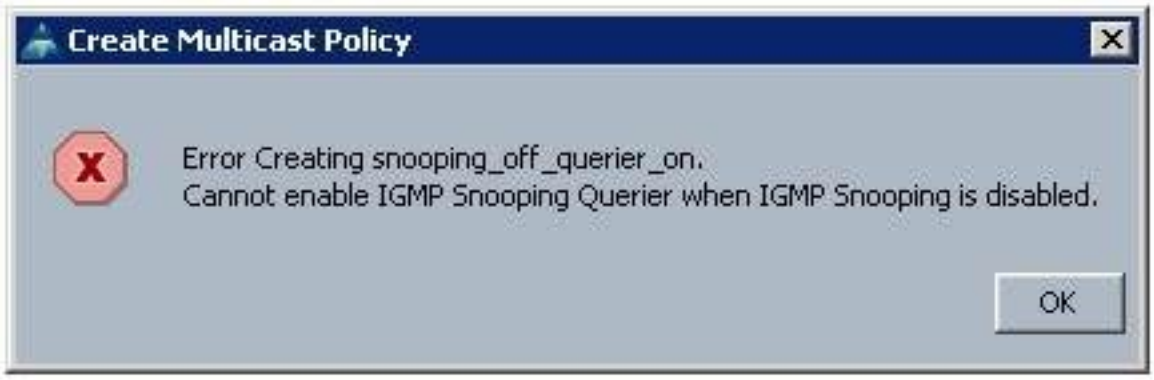
- Le mode par défaut, identique à la version précédente de Del Mar.
- Nécessite : IGMP Querier dans le commutateur en amont pour le VLAN avec la surveillance IGMP activée ou le routeur de multidiffusion dans le VLAN.

Surveillance IGMP désactivée / Requête IGMP désactivée

- Les FI diffusent le trafic de multidiffusion dans le VLAN.
- Nécessite : Commutateur en amont avec surveillance IGMP activée ou pour le désactiver pour inonder le trafic de multidiffusion.

Surveillance IGMP désactivée / Requête IGMP activée

- Cette configuration n'est pas valide.
- Ceci est correctement bloqué par l'UCSM.



Configuration UCS et en amont

Configuration - Créer

La surveillance IGMP est disponible sur une base VLAN et non au niveau de l'interface. À partir d'UCSM, ceci peut être configuré avec une stratégie de multidiffusion sur un VLAN nommé.

1. Ajoutez un nouveau noeud **Politiques de multidiffusion** sous **LAN> LAN > Policies> root**.

2. La création, la modification et la suppression des politiques de multidiffusion sont prises en charge.

3. Il existe une option permettant de sélectionner la stratégie de multidiffusion existante lors de la création d'un VLAN.

4. Et la prise en charge de l'association d'une stratégie de multidiffusion existante avec un VLAN déjà créé.

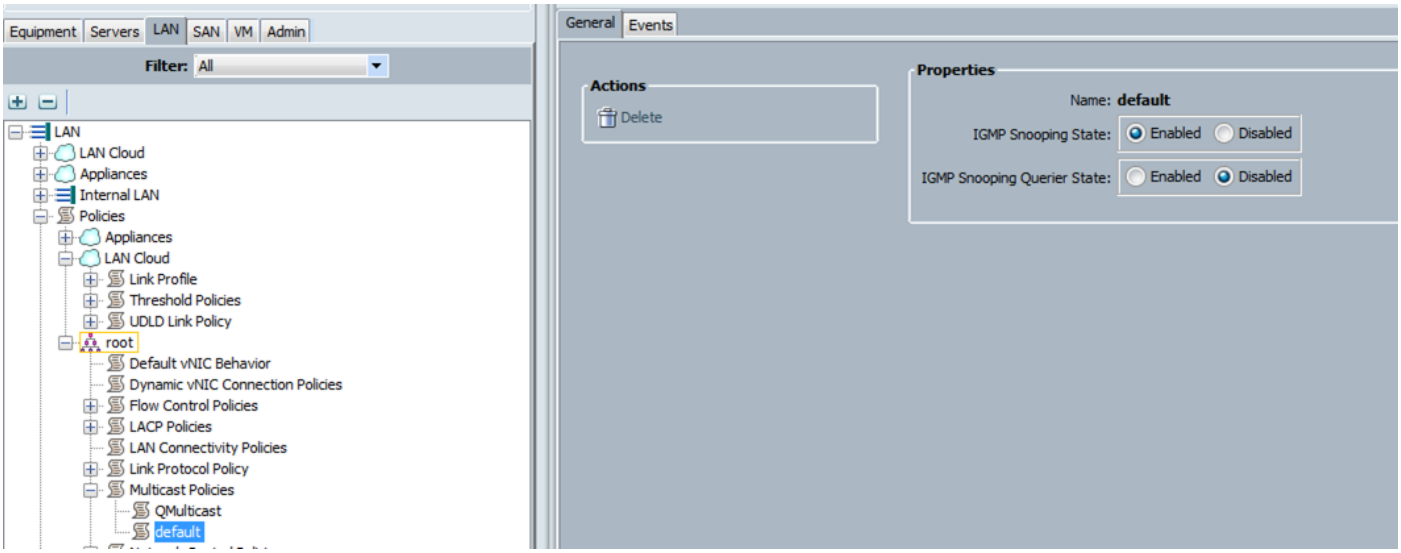
> **Note**: Les stratégies de multidiffusion sont uniquement sous l'arborescence des stratégies racine et vous ne pouvez pas créer de stratégies individuelles sous une sous-organisation.

Stratégie par défaut

La stratégie de multidiffusion par défaut reste conforme au comportement d'interconnexion de fabric avant la version 2.1 Del Mar :

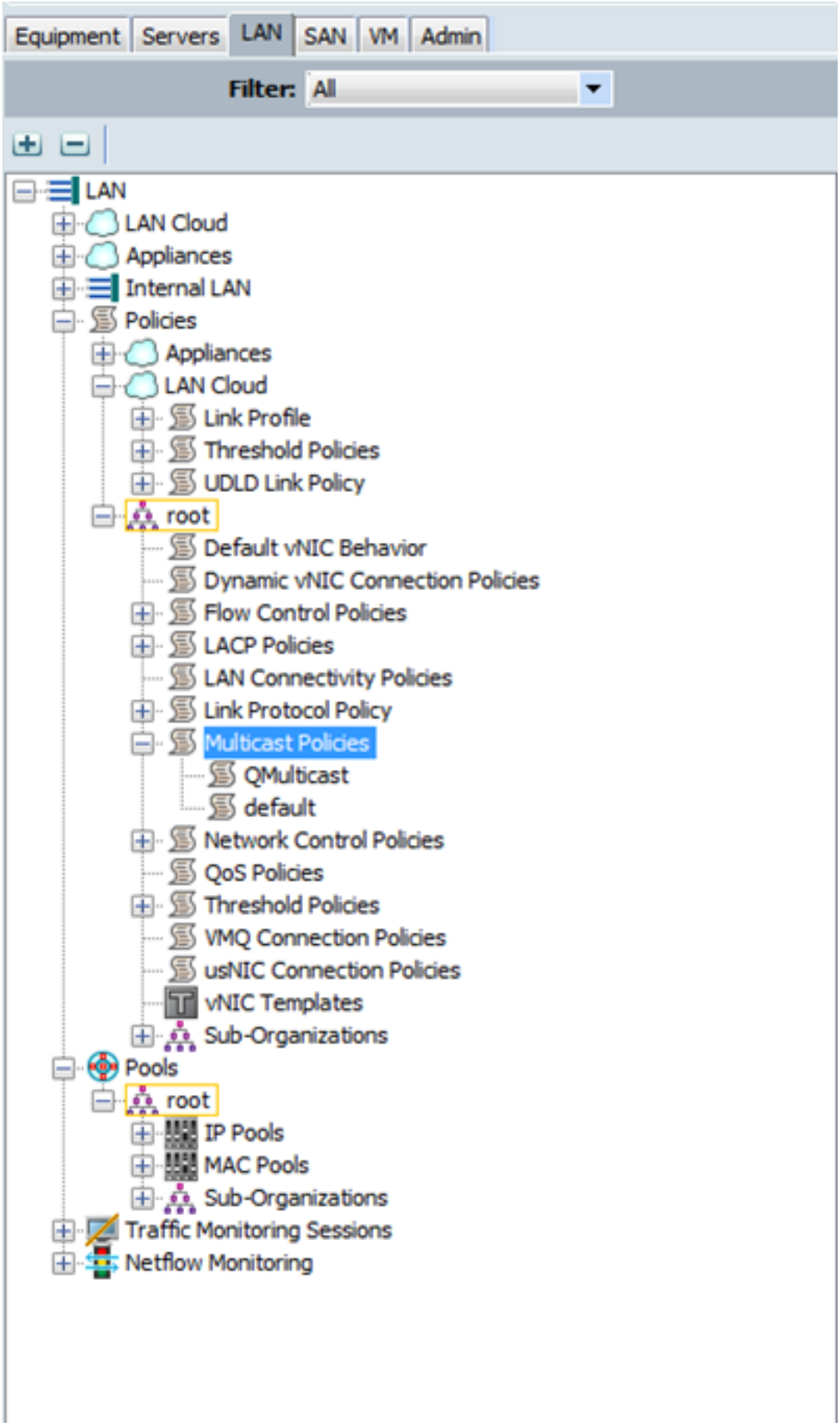
Surveillance IGMP - Activée

Requête IGMP - Désactivée



Configuration - Créer suite

Étape 1. Ajoutez un nouveau noeud **Politiques de multidiffusion** sous **LAN > LAN > Policies > root.**

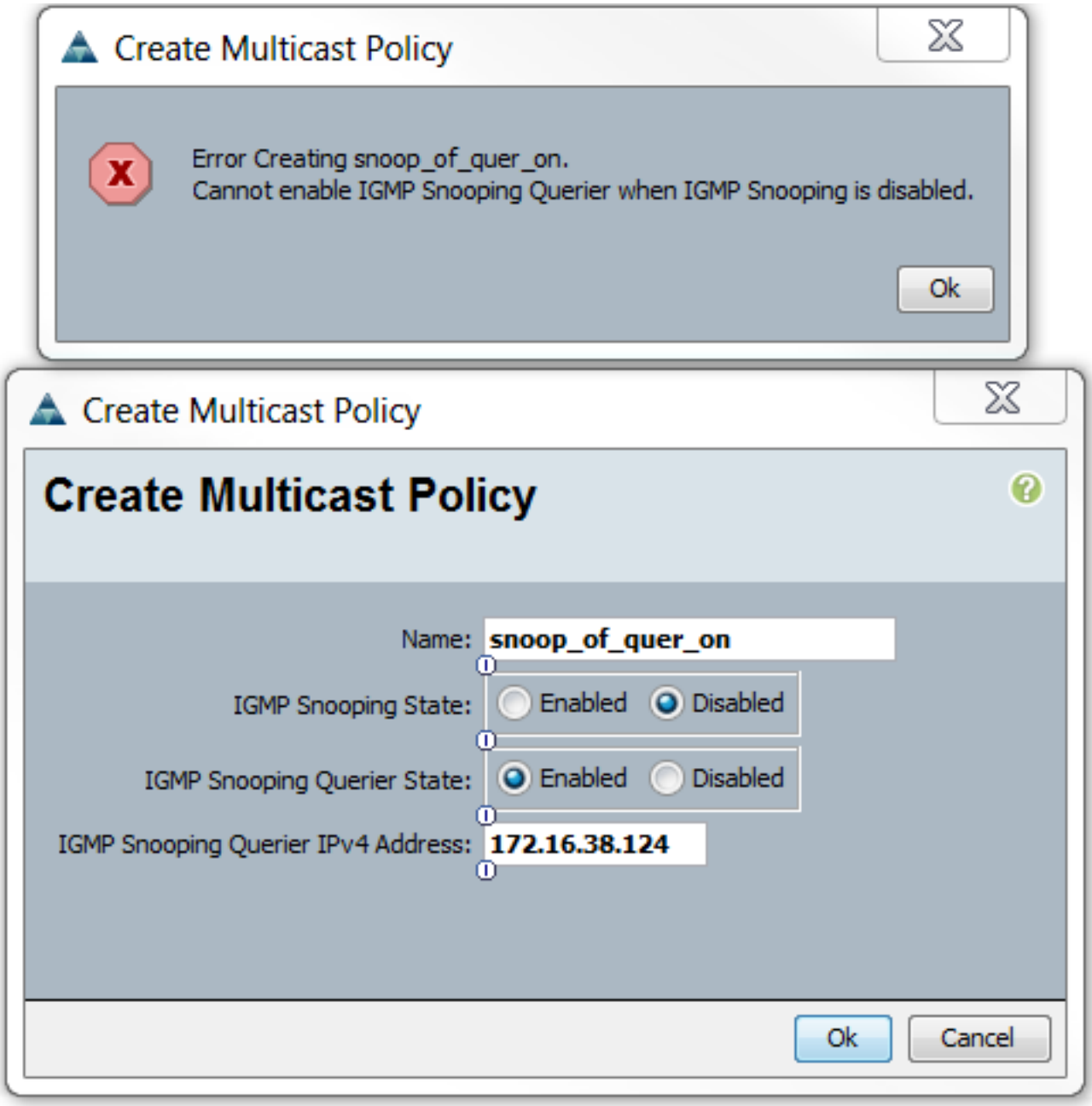


Étape 2. Cliquez avec le bouton droit de la souris sur Stratégies de multidiffusion, puis **créez une stratégie de multidiffusion**.

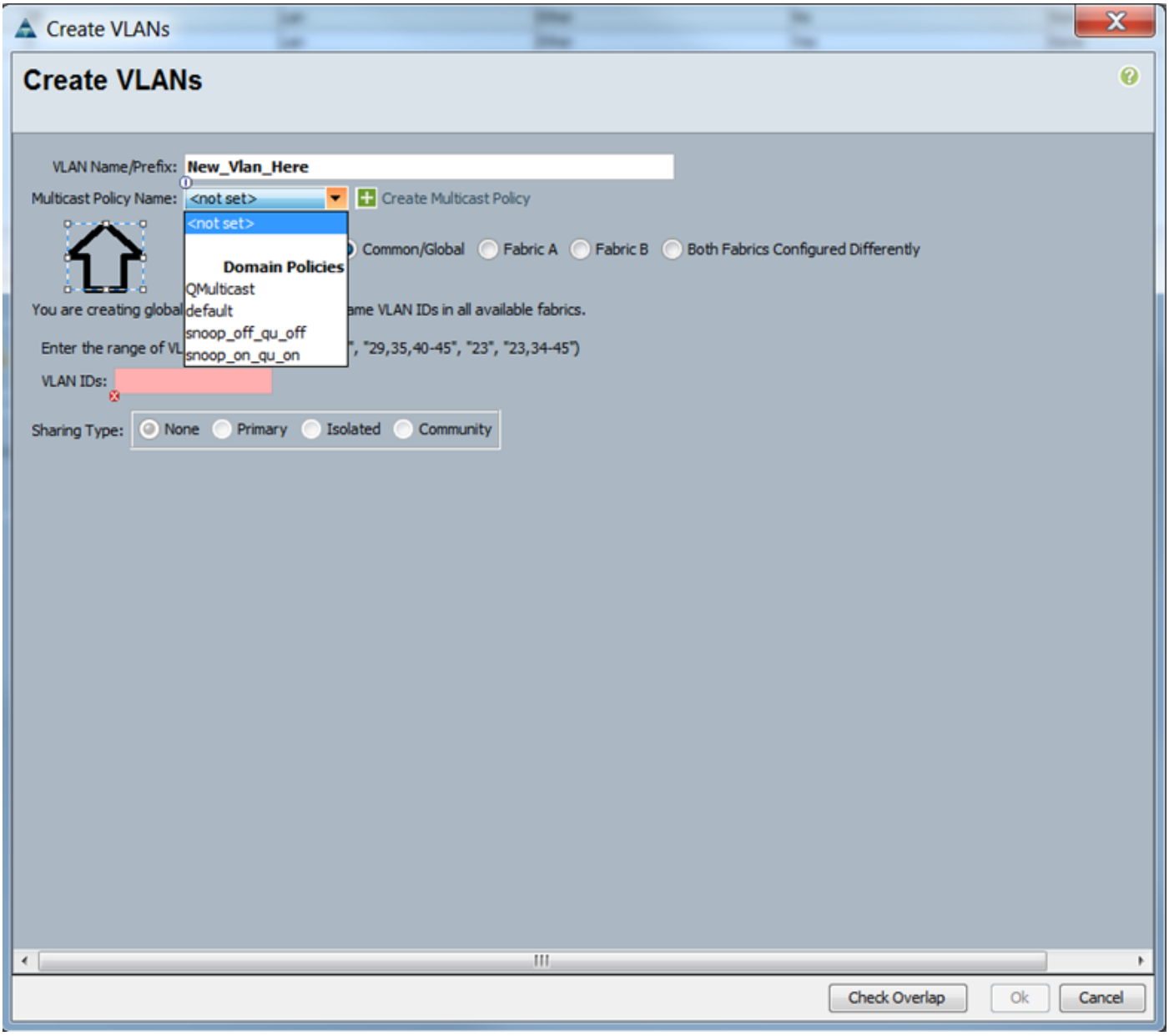
Étape 3. On vous présente ensuite ceci :

Fournissez un nom et configurez les états de la file d'attente IGMP Snooping et Snooping.

Étape 4. Si vous tentez de désactiver la surveillance IGMP pendant que la file d'attente IGMP Snooping est activée, cela génère une erreur, car il ne s'agit pas d'une configuration valide.

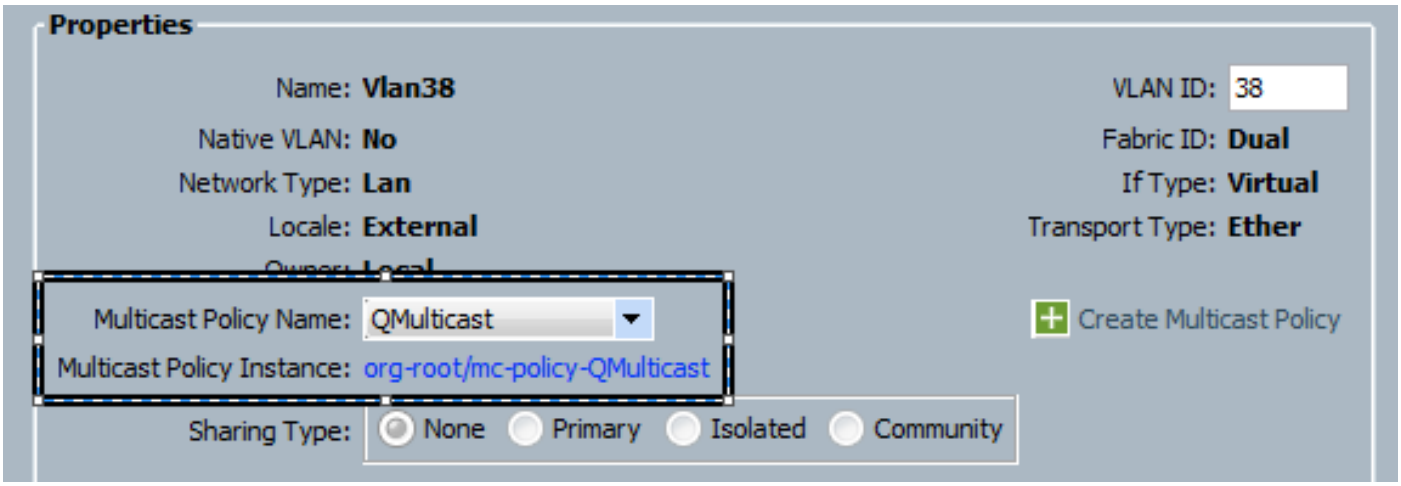


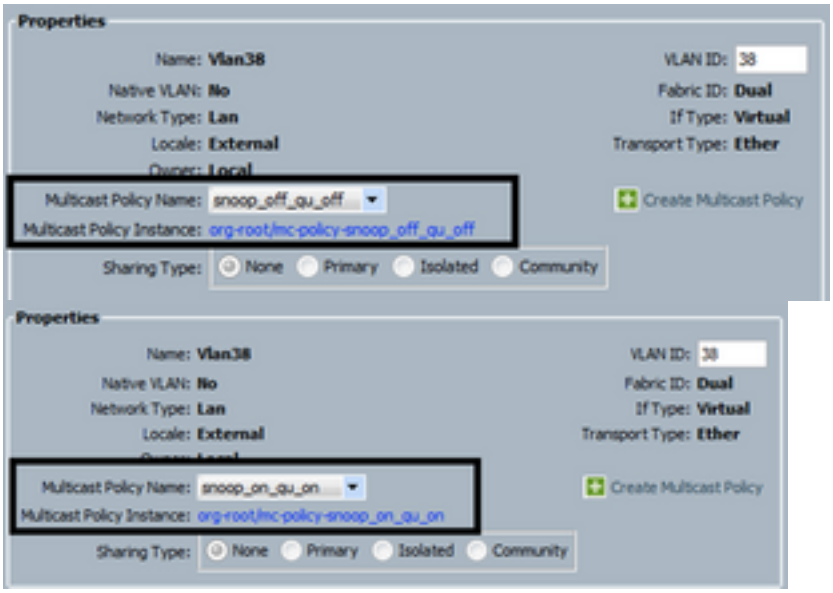
Étape 5. Lors de la création d'un nouveau VLAN, il existe maintenant une option e pour spécifier le nom de la stratégie de multidiffusion.



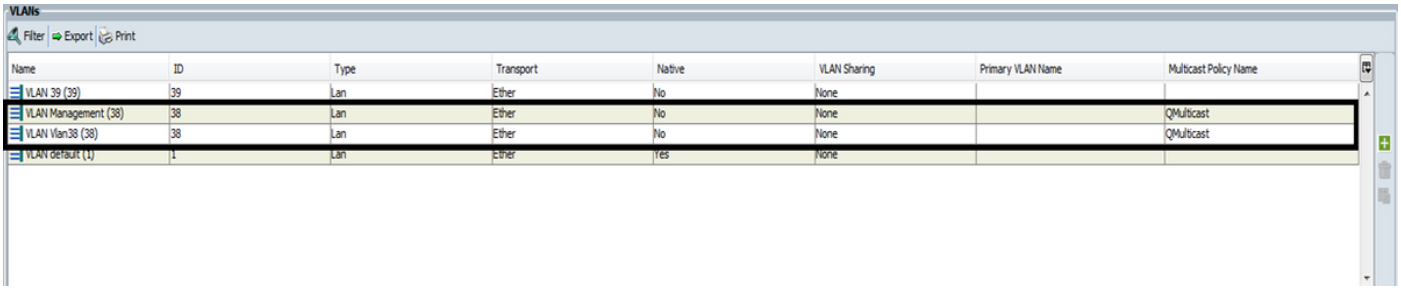
Configuration - Affecter

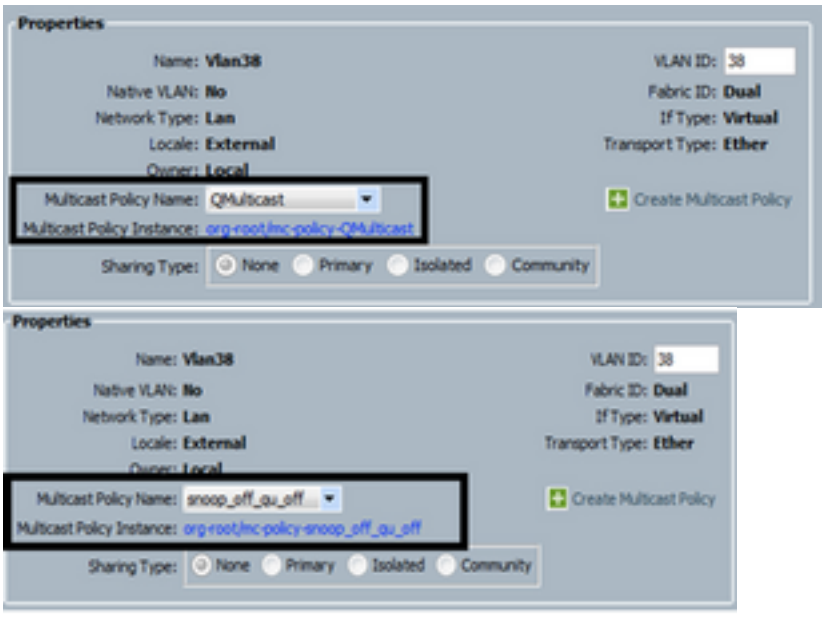
Exemples de stratégies différentes définies sur le VLAN. Le nom de la stratégie de multidiffusion est ce que vous configurez où l'instance de la stratégie de multidiffusion est réellement utilisée par les interconnexions de fabric.





Si vous créez plusieurs objets VLAN, qui pointent vers le même ID VLAN, alors, lorsque vous appliquez une stratégie de multidiffusion, elle est appliquée à **tous les** objets VLAN ayant le même ID VLAN. La dernière stratégie de multidiffusion appliquée est appliquée à tous. Par exemple : QMulticast est passé à Snoop_off_qu_off (Vlan 38).





Création d'une stratégie de multidiffusion UCS via CLI

- Ajoutez une nouvelle commande pour créer une stratégie de multidiffusion dans l'organisation de portée.

org de portée MiniMe-B#

MiniMe-B /org # create mcast-policy <nom>

- Définir les propriétés de la stratégie de multidiffusion.

MiniMe-B /org/mcast-policy #set querier <enable/disable>

MiniMe-B /org/mcast-policy #set snooping <enable/disable>

- Nouvelle commande permettant d'afficher les stratégies de multidiffusion existantes.

MiniMe-B # org de portée

MiniMe-B /org # show mcast-policy

- Nouvelle commande pour supprimer la stratégie de multidiffusion existante.

MiniMe-B # org de portée

MiniMe-B /org # delete mcast-policy <nom>

- Lorsque vous créez un VLAN, l'utilisateur est autorisé à ajouter une stratégie de multidiffusion existante au VLAN.

MiniMe-B# scope eth-uplink

MiniMe-B /eth-uplink # scope vlan <vlan>

MiniMe-B /eth-uplink/vlan # set mcastpolicy <nom>

Configuration du commutateur en amont

- Sur le commutateur en amont, vous devez configurer le demandeur IGMP Snooping sur un VLAN spécifique et le demandeur IGMP Snooping doit correspondre à l'IP dans la stratégie de multidiffusion UCS.

AGR012-5K-A(config)# vlan 38

AGR012-5K-A(config-vlan)# configuration vlan 38

AGR012-5K-A(config-vlan-config)# ip igmp snooping querier 172.16.38.124(IP est susceptible d'être différent)

Vérification

- **Show ip igmp snooping vlan <vlan id>** (ceci peut être fait sur le commutateur en amont ou sur Fabric Interconnect.)

(La sortie de la commande de surveillance UCS pour VLAN 38 vérifie que le demandeur est configuré sur l'UCSM et le N5k, et montre que seul le demandeur sur le N5k est actuellement actif (comme prévu). Tandis que le VLAN 39 n'est pas configuré.

```
MiniMe-B(nxos)# show ip igmp snooping vlan 38
IGMP Snooping information for vlan 38
  IGMP snooping enabled
  Optimised Multicast Flood (OMF) disabled
  IGMP querier present, address: 172.16.38.124, version: 3
  Querier interval: 125 secs
  Querier last member query interval: 0 secs
  Querier robustness: 2
  Switch-querier enabled, address 172.16.38.124, currently running
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Link Local Groups suppression enabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 2
  Number of groups: 0
  VLAN vPC function disabled
  Group gpin if: 0x1a001000 - Eth1/2
  Vlan flood if: 0x1a001000 - Eth1/2
  Active ports:
    Eth1/2      Veth698 Veth699 Veth734
    Veth735
MiniMe-B(nxos)# show ip igmp snooping vlan 39
IGMP Snooping information for vlan 39
  IGMP snooping enabled
  Optimised Multicast Flood (OMF) disabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Link Local Groups suppression enabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
  VLAN vPC function disabled
  Group gpin if: 0x1a001000 - Eth1/2
  Vlan flood if: 0x1a001000 - Eth1/2
  Active ports:
    Eth1/2      Veth716 Veth725
MiniMe-B(nxos)#
```

- **Show ip igmp snooping querier vlan <vlan id>** (Ceci peut être fait sur le commutateur en amont ou sur Fabric Interconnect.)

```
AGR012-5K-A# show ip igmp snooping querier vlan 38
Vlan   IP Address       Version   Expires     Port
38     172.16.38.124    v3        00:00:23     Switch querier
AGR012-5K-A#
```

- **Show ip igmp snooping groups vlan <vlan id>** (Ceci peut être fait sur le commutateur en amont ou sur Fabric Interconnect.)

- Affiche les ports actifs pour la multidiffusion et le demandeur IGMP.

```
Nexus1000v# sh ip igmp snooping groups vlan 16
IGMP Snooping information for vlan 16
  IGMP snooping enabled
  IGMP querier present, address: 172.16.16.2, version: 2, interface Ethernet4/2
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression disabled
  IGMPv3 Report suppression disabled
  Link Local Groups suppression enabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 2
  Number of groups: 1
  Active ports:
    Veth1       Eth3/2  Veth2   Eth4/2
    Veth3       Veth4   Veth5   Veth6
```

- **Show ip igmp snooping statistics vlan <vlan id>** (Ceci peut être fait sur le commutateur en amont ou Fabric Interconnect.)

```
AGR012-5K-A# show ip igmp snooping statistics vlan 38
Global IGMP snooping statistics: (only non-zero values displayed)
  Packets received: 787250
  Packet errors: 22364
  Packets flooded: 33877
  vPC PIM DR queries sent: 1
  vPC PIM DR updates sent: 2
  vPC CFS send fail: 1
  vPC CFS message response sent: 1304
  vPC CFS message response rcvd: 27
  vPC CFS unreliable message sent: 107653
  vPC CFS unreliable message rcvd: 1258659
  vPC CFS reliable message sent: 4
  vPC CFS reliable message rcvd: 1304
  STP TCN messages rcvd: 740
  IM api failed: 2
  Native mct reports drop: 4
VLAN 168 IGMP snooping statistics, last reset: never (only non-zero values displayed)
  Packets received: 112070
  IGMPv2 reports received: 37297
  IGMPv3 reports received: 52407
  IGMPv3 queries received: 11422
  IGMPv2 leaves received: 7
  Invalid reports received: 61385
  IGMPv2 reports suppressed: 1598
  IGMPv2 leaves suppressed: 1
  Queries originated: 1
  IGMPv3 proxy-reports originated: 2
  Packets sent to routers: 88116
  STP TCN received: 4
  VIM IGMP leave sent on failover: 0
  vPC Peer Link CFS packet statistics:
      IGMP packets (sent/recv/fail): 25859/75274/0
```

- **AGR012-5K-A#show mac address-table multicast**

```
Legend:

- primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC age - seconds since last
seen,+ - primary entry using vPC Peer-Link

VLAN     MAC Address     Type     age     Secure NTFY   Ports

---------+----------------+--------+---------+------+----+------------------

38       0100.5e10.2604   igmp     0         F    F Eth1/2 Router

38       0100.5e7f.fffd   igmp     0         F    F Eth1/2 Router
```

```
0100.5e7f.2604 = 224.127.38.4 (Multicast Group Address)

0100.5e7f.fffd = 224.127.255.253 (Multicast Group Address)
```

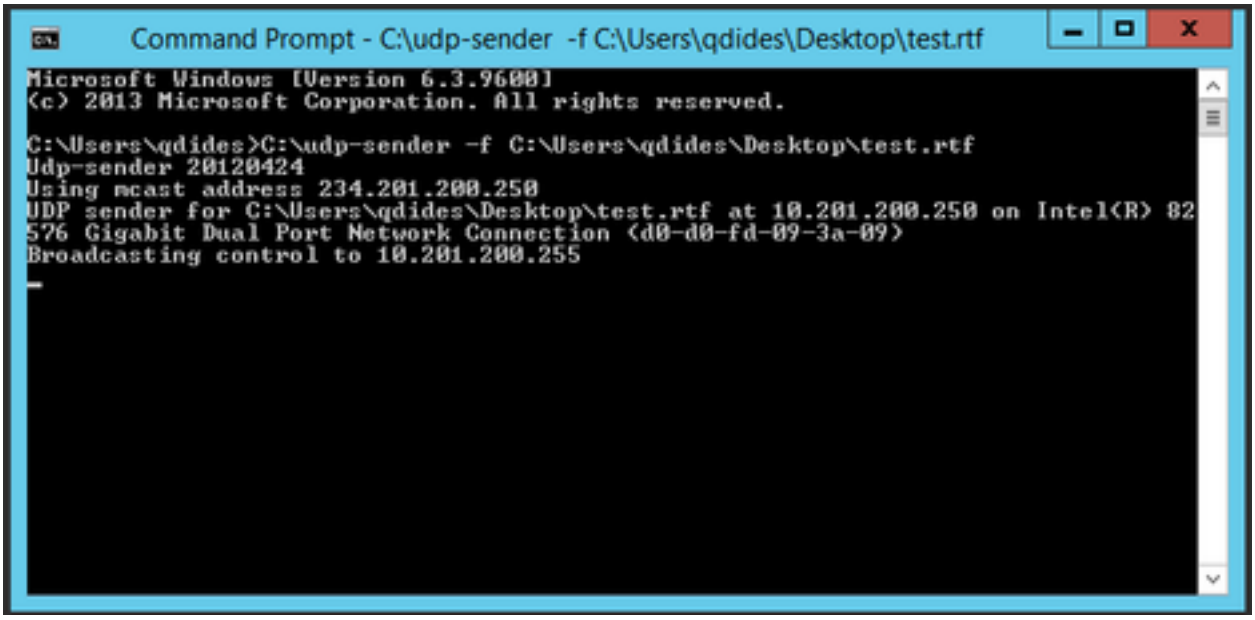
- **AGR012-5K-A# ethanalyzer local interface inbound-low display-filter igmp limite**

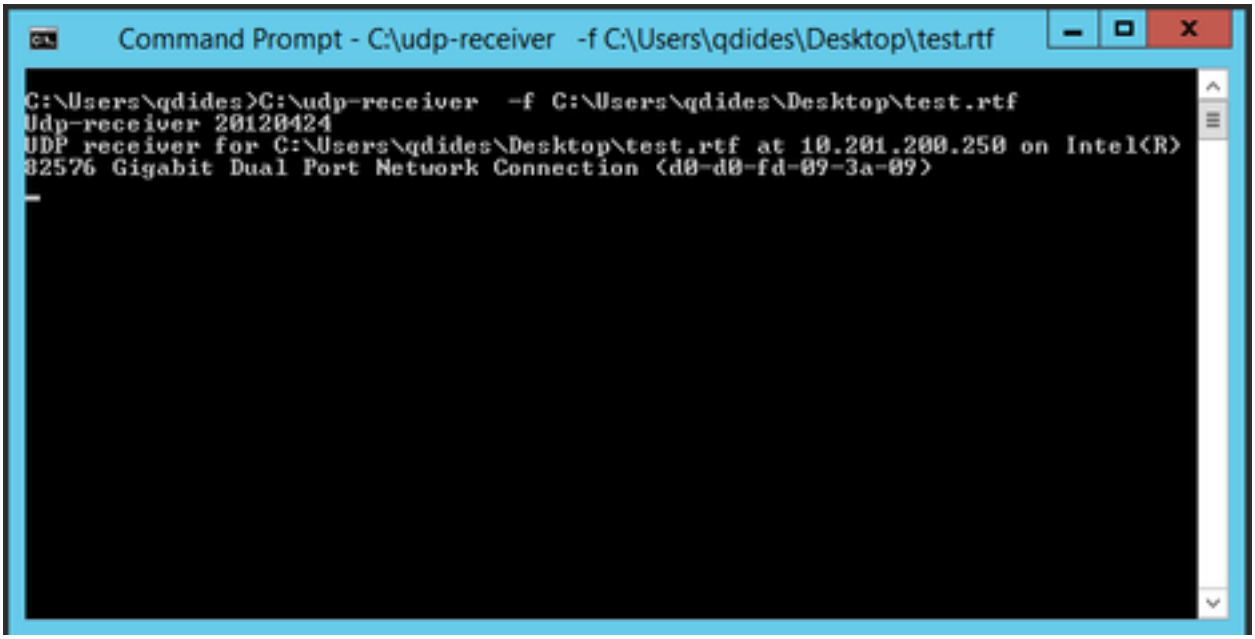
Cela ne capture pas les données de flux vidéo réelles, juste les données IGMP. Cet outil capture le trafic de contrôle. (EX) elle indique quand un hôte rejoint ou quitte le groupe.)

```
Capturing on inband

2009-12-02 02:11:34.435559 172.16.38.5 -> 224.0.0.22   IGMP V3 Membership Report / Join group
224.0.0.252 for any sources

2009-12-02 02:11:55.416507 172.16.38.6 -> 224.0.0.22   IGMP V3 Membership Report / Leave group
236.16.38.4

2009-12-02 02:11:55.802408 172.16.38.6 -> 224.0.0.22   IGMP V3 Membership Report / Leave group
236.16.38.4

2009-12-02 02:11:59.378576 172.16.38.6 -> 224.0.0.22   IGMP V3 Membership Report / Join group
236.16.38.4 for any sources
```

Dépannage

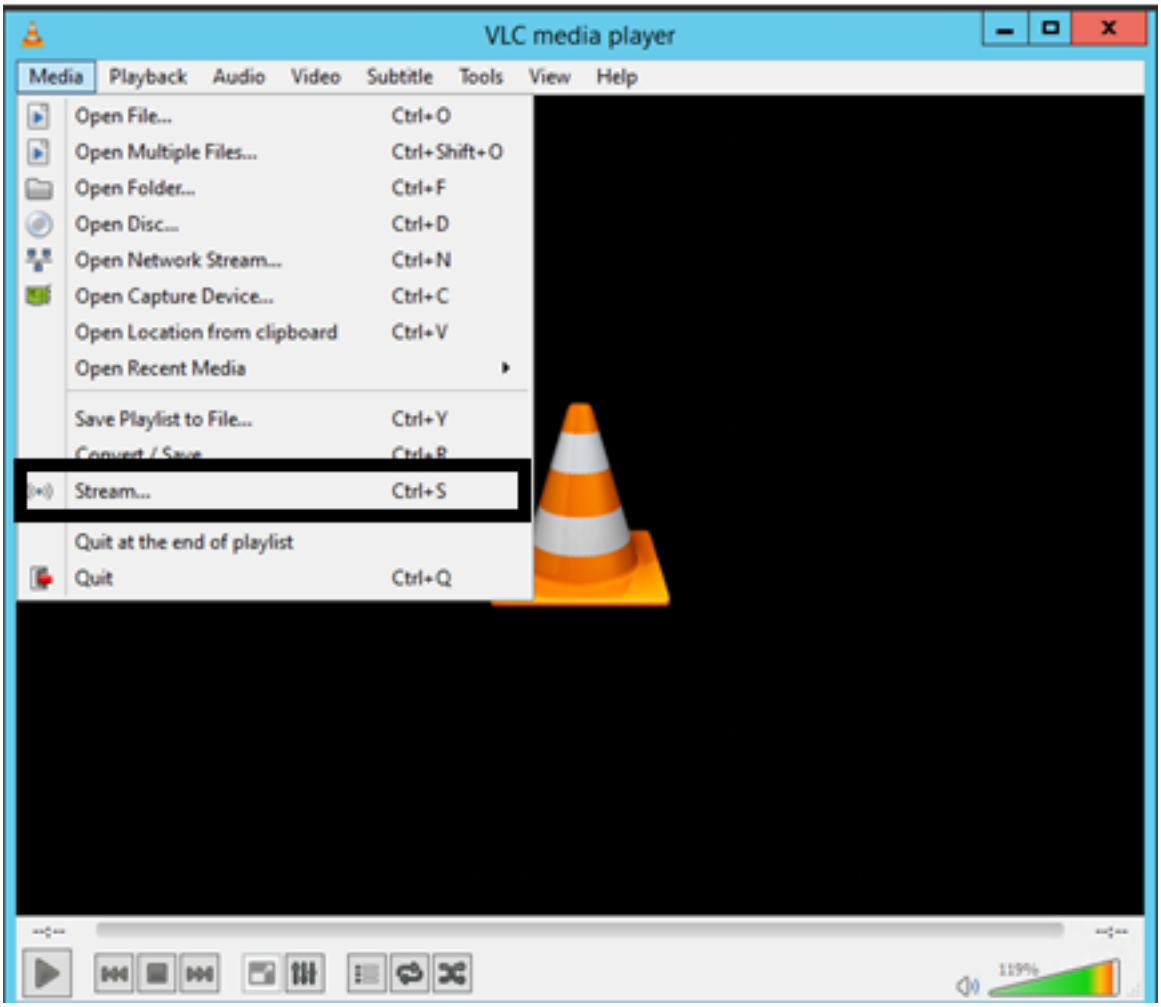
- **MISE À JOUR (http://www.udpcast.linux.lu/cmd.html)**
- Cette application est téléchargée sur deux hôtes différents, l'expéditeur et le destinataire. Avec elle, vous pouvez générer du trafic de multidiffusion avec un transfert d'un fichier d'une source vers plusieurs destinations simultanément à l'aide d'une seule commande.

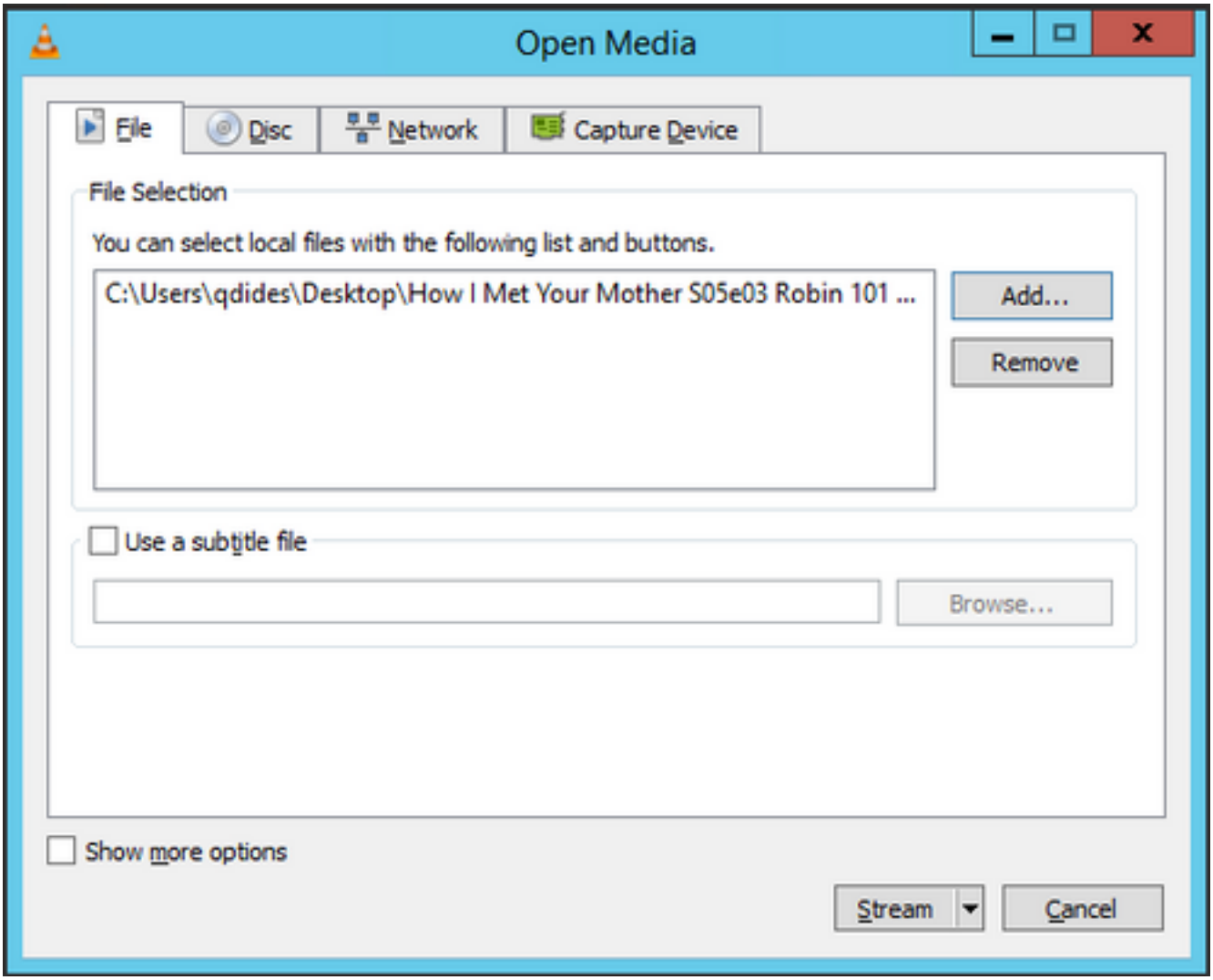


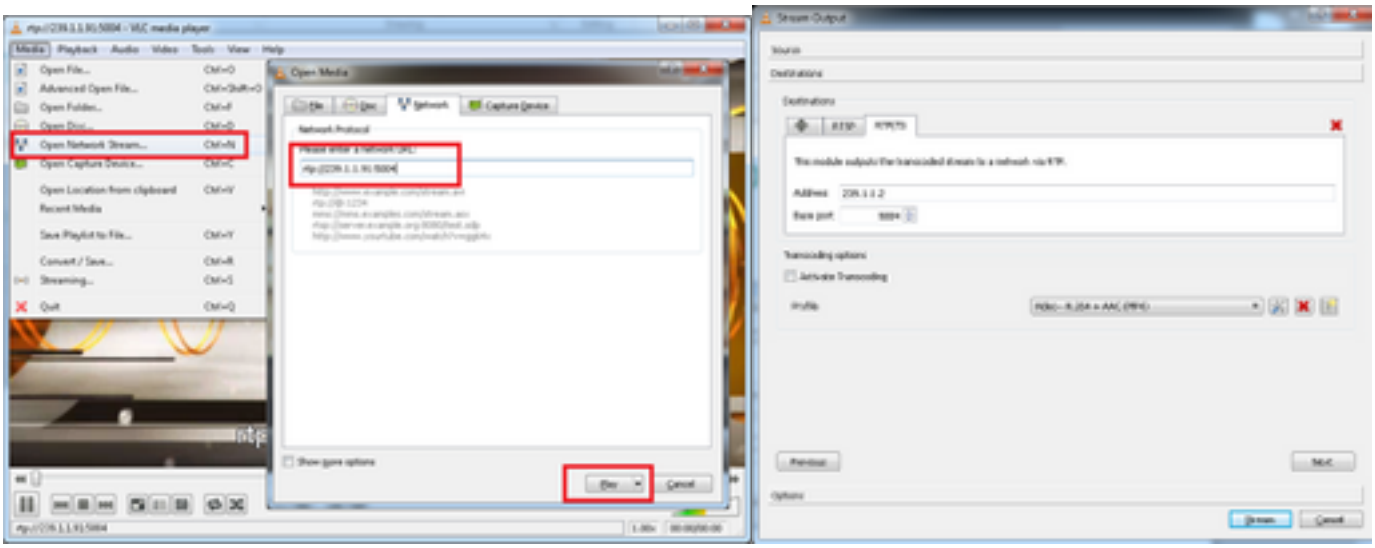


- VLC (http://www.videolan.org/vlc/index.html)

(Voici les images qui montrent comment diffuser sur VLC. Il y a pas mal d'informations sur la façon de procéder en ligne.)


VLC media player
Media
Playback
Audio
Video
Subtitle
Tools
View
Help
Open File... Ctrl+O
Open Multiple Files... Ctrl+Shift+O
Open Folder... Ctrl+F
Open Disc... Ctrl+D
Open Network Stream... Ctrl+N
Open Capture Device... Ctrl+C
Open Location from clipboard Ctrl+V
Open Recent Media
Save Playlist to File... Ctrl+Y
Stream... Ctrl+S
Quit at the end of playlist
Quit Ctrl+Q





Comment générer du trafic IGMP et multicast avec Iperf ?

- Iperf ou Jperf est un outil très utile qui peut générer du trafic IGMP et multicast, il peut fonctionner sur Linux et Windows OS.
- CLI de l'expéditeur multidiffusion.

```
# iperf -c 239.1.1.1 -i 1 -u -t 600 -b 10M
```

```
iperf sender options:

-c  239.1.1.1 : send traffic to multicast IP address 239.1.1.1

-i 1 : update interval is 1 second

-u : UDP traffic, multicast is based on UDP

-t 600 : send traffic for 600 seconds

-b 10M: UDP traffic bandwidth is10Mbps
```

- CLI du récepteur de multidiffusion.

```
# iperf -s -B 239.1.1.1 -i 1 -u



iperf receiver options:

-s : server mode

-B 239.1.1.1 : listening to IP address 239.1.1.1, as it is a multicast IP address, so this is a
multicast receiver.

-i 1 : update interval is 1 second

-u : UDP traffic, multicast is based on UDP
```

Informations connexes

- Guide de configuration du routage multidiffusion NX-OS de la gamme Cisco Nexus 5000, version 5.0(3)N1(1)
- Support et documentation techniques - Cisco Systems