

# Configuración de multidifusión en UCS

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Opciones de configuración de multidifusión UCS](#)

[Configuración en Modo Host Final](#)

[Detección IGMP activada / Consulta IGMP habilitada](#)

[Detección IGMP activada / Consulta IGMP desactivada](#)

[Detección de IGMP desactivada / Consulta de IGMP desactivada](#)

[Detección de IGMP desactivada / Consulta de IGMP habilitada](#)

[Configuración en modo de switching](#)

[Detección IGMP activada / Consulta IGMP habilitada](#)

[Detección IGMP activada / Consulta IGMP desactivada](#)

[Detección de IGMP desactivada / Consulta de IGMP desactivada](#)

[Detección de IGMP desactivada / Consulta de IGMP habilitada](#)

[Configuración de UCS y de flujo ascendente](#)

[Configuración - Crear](#)

[Política predeterminada](#)

[Configuración - Crear continuación](#)

[Configuración - Asignar](#)

[Creación de una política de multidifusión UCS mediante CLI](#)

[Configuración en el switch ascendente](#)

[Verificación](#)

[Troubleshoot](#)

[¿Cómo se Genera el Tráfico de IGMP y Multicast con Iperf?](#)

[Información Relacionada](#)

## Introducción

Este documento describe el procedimiento necesario para configurar la multidifusión en Unified Computing Systems (UCS). La multidifusión (MCAST) es la capacidad de enviar datos a través de una red a varios usuarios al mismo tiempo (comunicación de grupo de uno a varios o de varios). El protocolo de administración de grupos de Internet (IGMP) es un componente crucial de la multidifusión. El propósito principal de IGMP es permitir que los hosts comuniquen su deseo de recibir tráfico multicast, a los routers IP Multicast en la red local. Esto, a cambio, permite que los routers IP Multicast "se unan" al grupo multicast especificado y comiencen a reenviar el tráfico multicast al segmento de red hacia el host.

## Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCS
- Switching de multidifusión Nexus

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Fabric Interconnect: 6100/6200
- UCSM (Unified Computing System Manager)
- Switch ascendente (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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Anterior a la versión 2.1 de Unified Computing System Manager (UCS-M):

- La multidifusión en UCS tiene la función IGMP snooping activada de forma predeterminada y no se puede desactivar. (Cisco Technical Assistance Centers (TAC) podría desactivarse mediante el complemento de depuración).
- Los Fabric Interconnects UCS no tienen funcionalidad de consultas IGMP; esto requiere que habilite la funcionalidad del consultor en un dispositivo en la red L2 ascendente.
- Para que esto funcione, necesita un router de multidifusión en la VLAN o un consultor IGMP en la VLAN.

Del Mar 2.1 Notas:

- De forma predeterminada, IGMP Snooping está habilitado, los administradores de red deben examinar cuidadosamente cualquier requisito para inhabilitar la indagación IGMP y el rendimiento perjudicial que podría experimentarse.
- La configuración de IGMP Snooping sólo está disponible y se puede configurar por VLAN, no puede habilitar o inhabilitar la función IGMP Snooping globalmente.
- La capacidad de inhabilitar la detección IGMP se admite tanto en el modo de host final (EHM) como en el modo de switch.
- No es compatible con políticas de multidifusión en grupos de red (otra nueva función en Del Mar).

Especificaciones de Fabric Interconnect:

- Para una Fabric Interconnect (FI) de la serie 6100, todas las VLAN sólo pueden utilizar la política de multidifusión predeterminada; sin embargo, el usuario puede modificar los estados

Snooping/Queridor de IGMP de esta política predeterminada. Si configura cualquier otra política de multidifusión, producirá un error, "Para las VLAN en X Fabric Interconnect, sólo se admite la política de multidifusión predeterminada".

- Para cambiar la política de multidifusión para una VLAN determinada (a una política que no sea la política de multidifusión predeterminada) sólo se admite en FI 6200 y NO en los 6100. La razón por la que las FI 6100 no pueden tener diferentes políticas de multidifusión en sus VLAN se debe a una limitación en el ASIC Gatos. Esta limitación no existe en las FI 6200 con ASIC Carmel.

#### Opciones de configuración de multidifusión UCS

##### Configuración en Modo Host Final

#### **Detección IGMP activada / Consulta IGMP habilitada**

- Sólo envía las consultas a los blades. No envía consultas IGMP a la red ascendente.
- Las FI no envían las consultas IGMP al switch ascendente ya que esto contradice el rol del modo de host final en la red. Esto puede dar lugar a que se envíe tráfico de multidifusión no deseado (tanto control como datos) a las FI. Esta es la razón por la que se decidió que las FI EHM fueran responsables de transmitir las consultas IGMP a sus blades solamente.
- Como resultado, se requiere una de las configuraciones aprobadas:

Configuraciones aprobadas:

Configure el buscador IGMP en el switch ascendente con la indagación IGMP habilitada o Deshabilite la indagación IGMP en el switch ascendente para inundar el tráfico multicast. Alternativamente, cambie los FIs al modo switch.

#### **Detección IGMP activada / Consulta IGMP desactivada**

- El modo predeterminado, igual que las versiones anteriores a Del Mar.
- Requiere: El solicitante IGMP en el switch ascendente para la VLAN con la indagación IGMP habilitada o el router de multidifusión en la VLAN.

#### **Detección de IGMP desactivada / Consulta de IGMP desactivada**

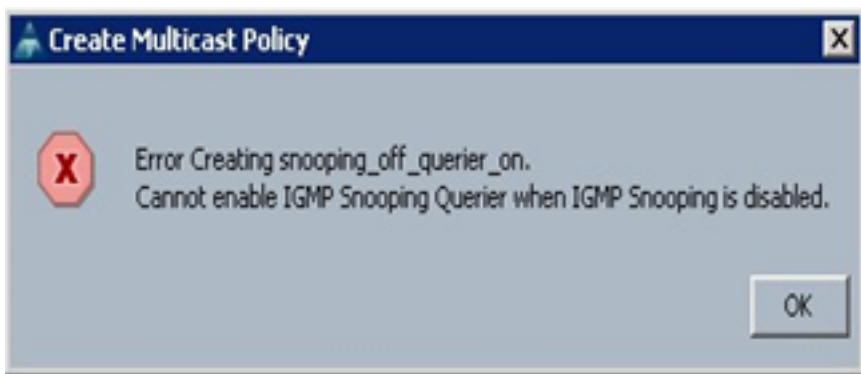
- Las FI inundan el tráfico multicast en la VLAN.
- Requiere que una de las configuraciones aprobadas funcione correctamente:

Configuraciones aprobadas:

El switch ascendente puede tener habilitada la indagación IGMP o tener inhabilitada en el switch ascendente para inundar el tráfico multicast.

#### **Detección de IGMP desactivada / Consulta de IGMP habilitada**

- Esta configuración no es válida.
- El UCSM ha bloqueado esta operación correctamente.



Configuración en modo de switching

### **Detección IGMP activada / Consulta IGMP habilitada**

- Las FI reenvían las consultas IGMP a la red ascendente.
- Los switches ascendentes aprenden sobre el solicitante IGMP configurado en FI, luego construyen y reenvían el tráfico MCAST a FI.
- Requiere: Switch ascendente con indagación IGMP habilitada o con indagación inhabilitada para inundar el tráfico multicast.

### **Detección IGMP activada / Consulta IGMP desactivada**

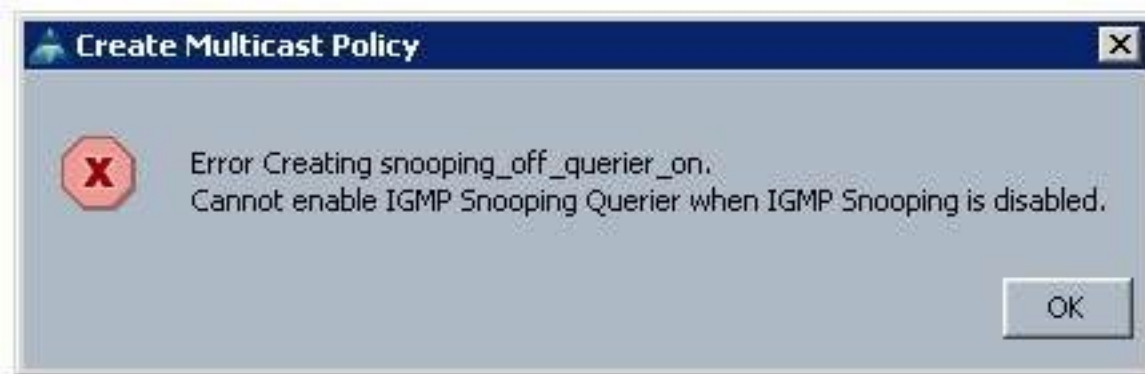
- El modo predeterminado, igual que antes de la versión Del Mar.
- Requiere: El solicitante IGMP en el switch ascendente para la VLAN con la indagación IGMP habilitada o el router multicast en la VLAN.

### **Detección de IGMP desactivada / Consulta de IGMP desactivada**

- Las FI inundan el tráfico multicast en la VLAN.
- Requiere: Switch ascendente con indagación IGMP habilitado o para que esté inhabilitado para inundar el tráfico multicast.

### **Detección de IGMP desactivada / Consulta de IGMP habilitada**

- Esta configuración no es válida.
- El UCSM ha bloqueado esta operación correctamente.



## Configuración de UCS y de flujo ascendente

### Configuración - Crear

El snooping de IGMP está disponible en VLAN y no en el nivel de interfaz. Desde UCSM, esto se puede configurar con una política de multidifusión en una VLAN con nombre.

1. Agregue un nuevo nodo de **Políticas Multicast bajo LAN > LAN > Políticas > root**.
2. Hay soporte para la creación, modificación y eliminación de políticas de multidifusión.
3. Existe una opción para seleccionar la política de multidifusión existente cuando se crea una VLAN.
4. Y soporte para adjuntar una política de multidifusión existente con una VLAN que ya se ha creado.

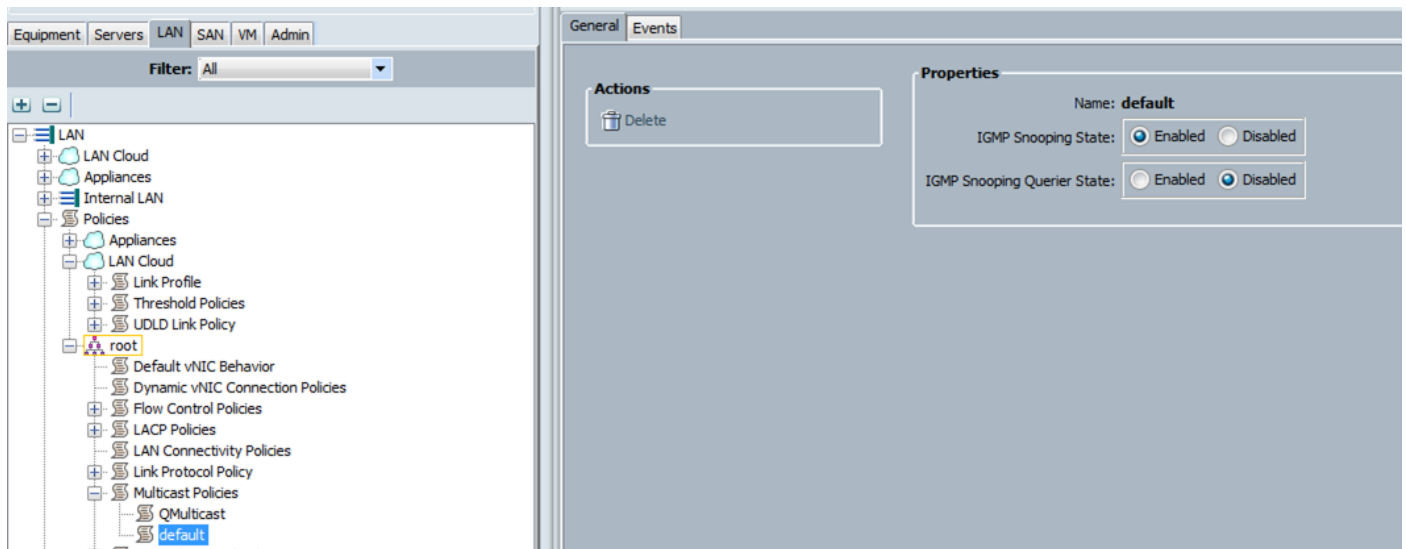
**Nota:** Las políticas de multidifusión sólo se encuentran en el árbol de políticas raíz y no puede crear políticas individuales en una suborganización.

### Política predeterminada

La política de multidifusión predeterminada se mantiene en línea con el comportamiento de Fabric Interconnect antes de la versión 2.1 Del Mar:

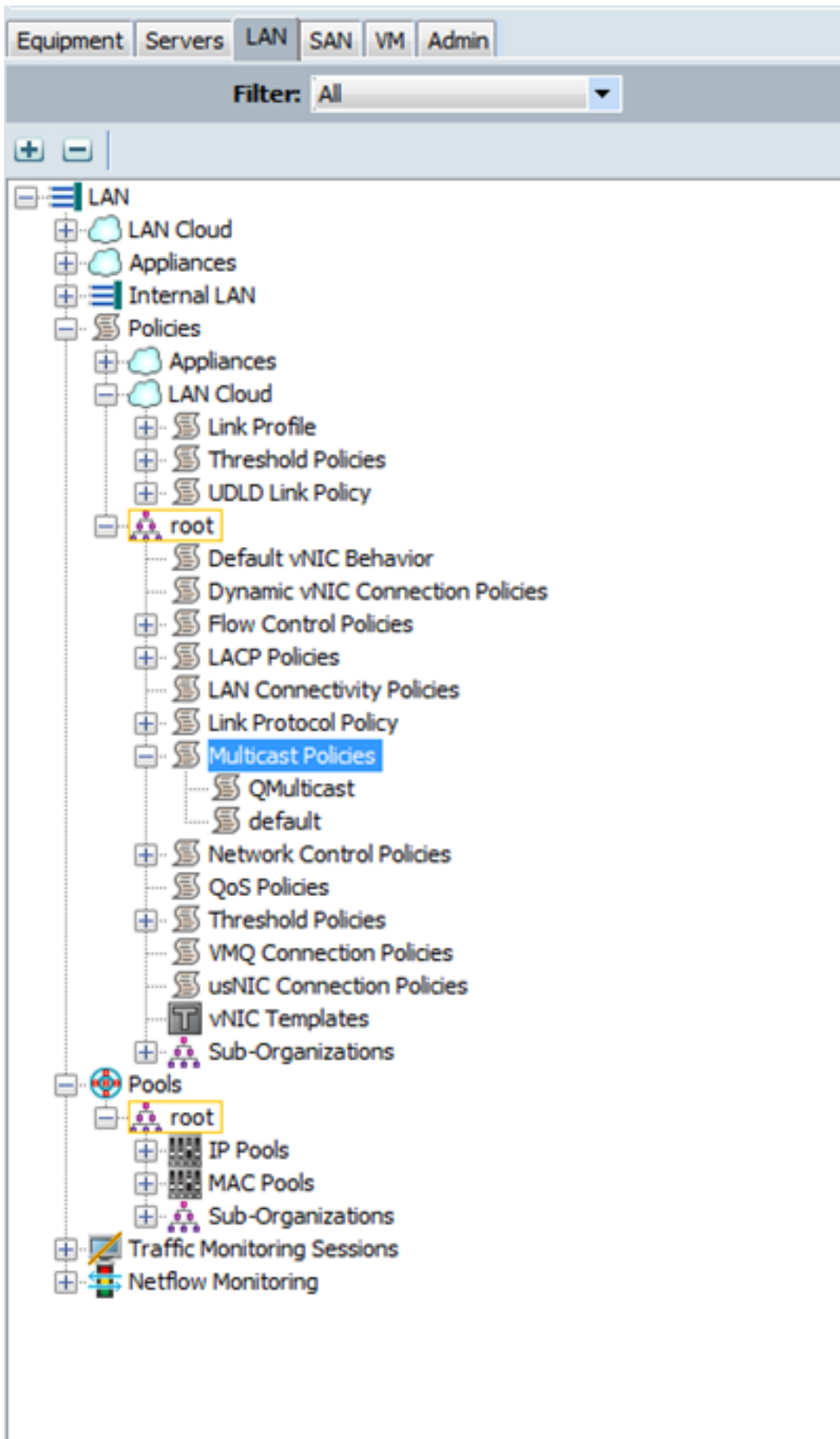
IGMP Snooping- Habilitado

Consultor IGMP: desactivado



## Configuración - Crear continuación

Paso 1. Agregue un nuevo nodo **Políticas Multicast** bajo LAN > LAN > Políticas > root.



Paso 2. Haga clic con el botón derecho en Políticas de multidifusión y, a continuación, **Crear política de multidifusión**.

Paso 3. A continuación, se le presenta lo siguiente:

Proporcione un nombre y configure los estados IGMP Snooping y Snooping Querier.



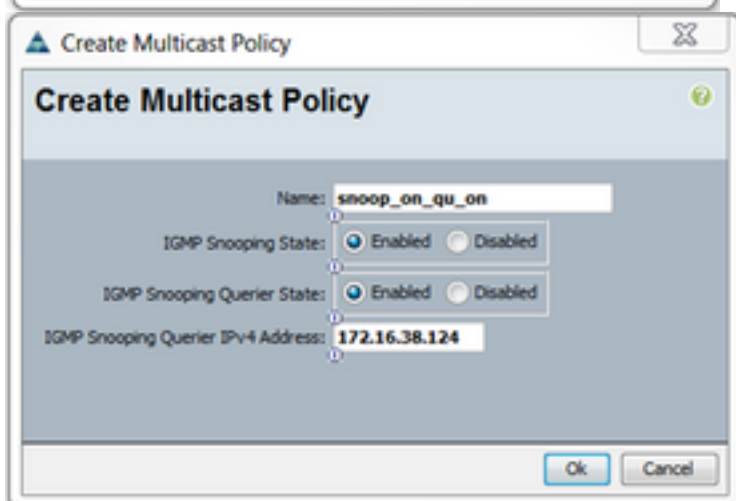
**Create Multicast Policy**

Name:

IGMP Snooping State:  Enabled  Disabled

IGMP Snooping Querier State:  Enabled  Disabled

Ok Cancel



**Create Multicast Policy**

Name:

IGMP Snooping State:  Enabled  Disabled

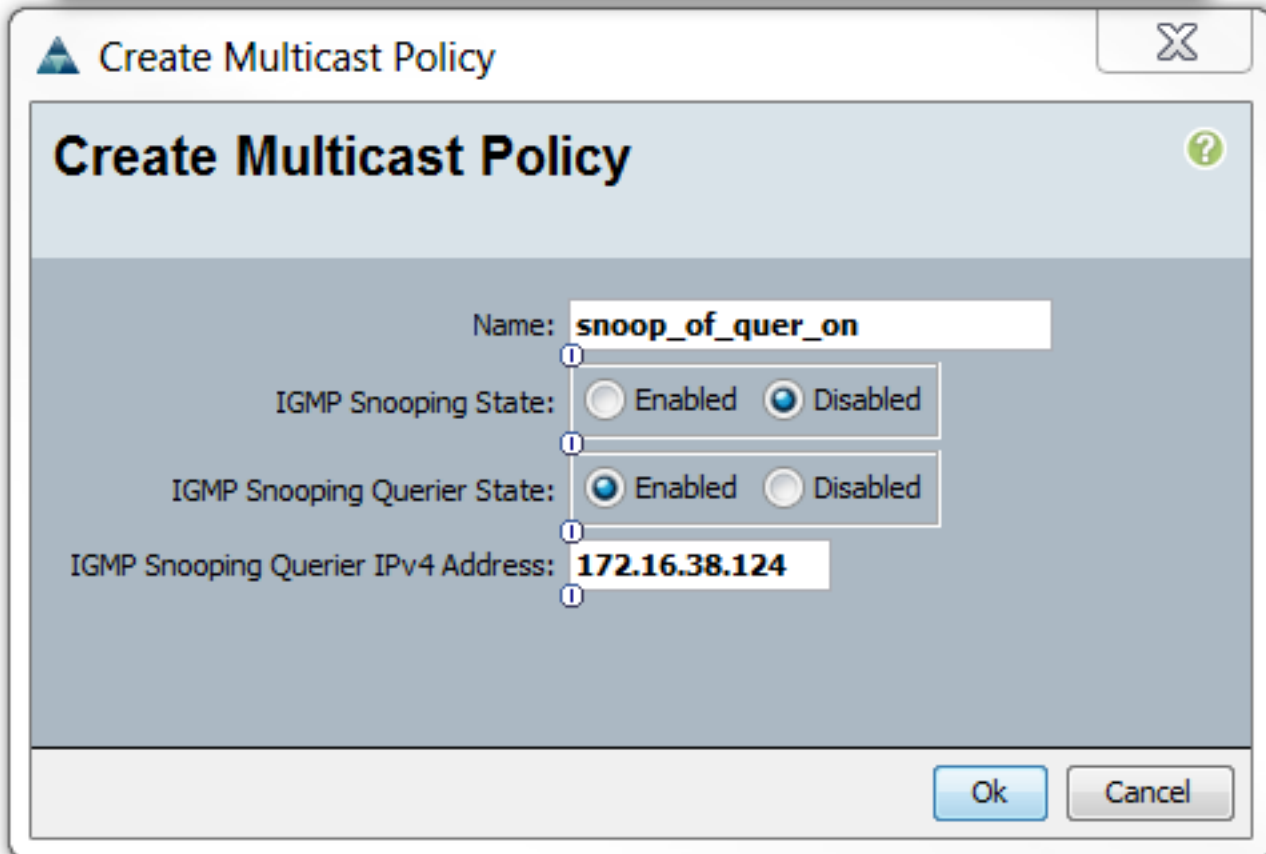
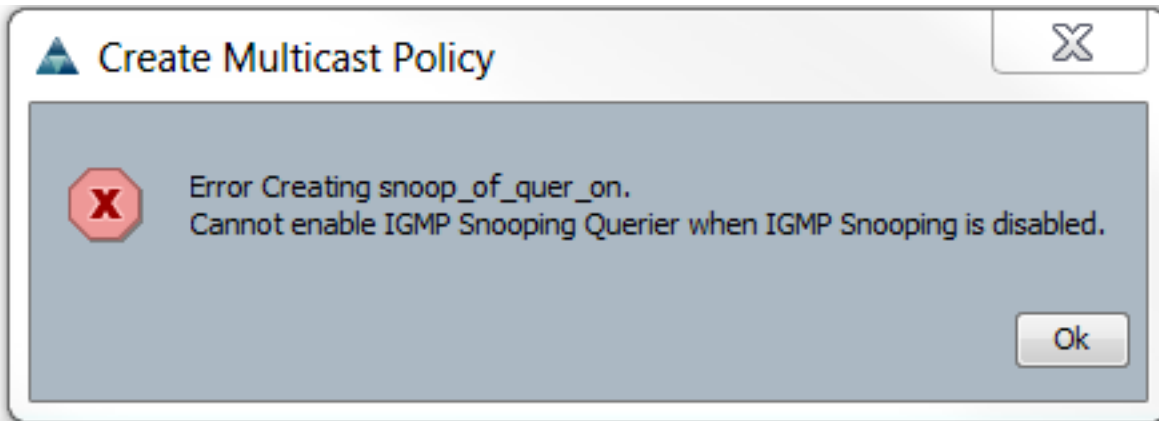
IGMP Snooping Querier State:  Enabled  Disabled

IGMP Snooping Querier IPv4 Address:

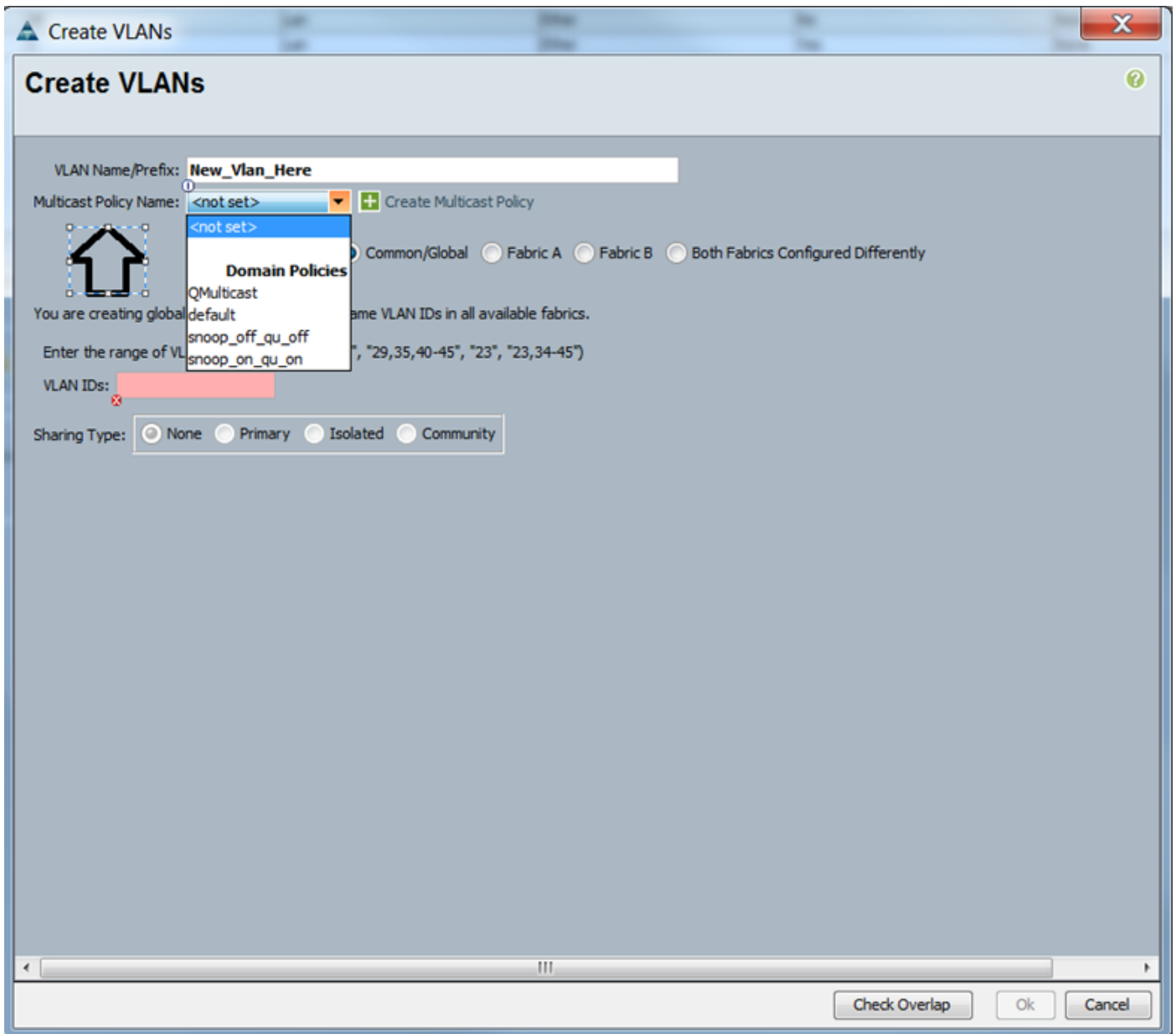
Ok Cancel

Paso 4. Si intenta inhabilitar la indagación IGMP mientras el solicitante de indagación IGMP está habilitado, esto produce un error, ya que no es una configuración válida.



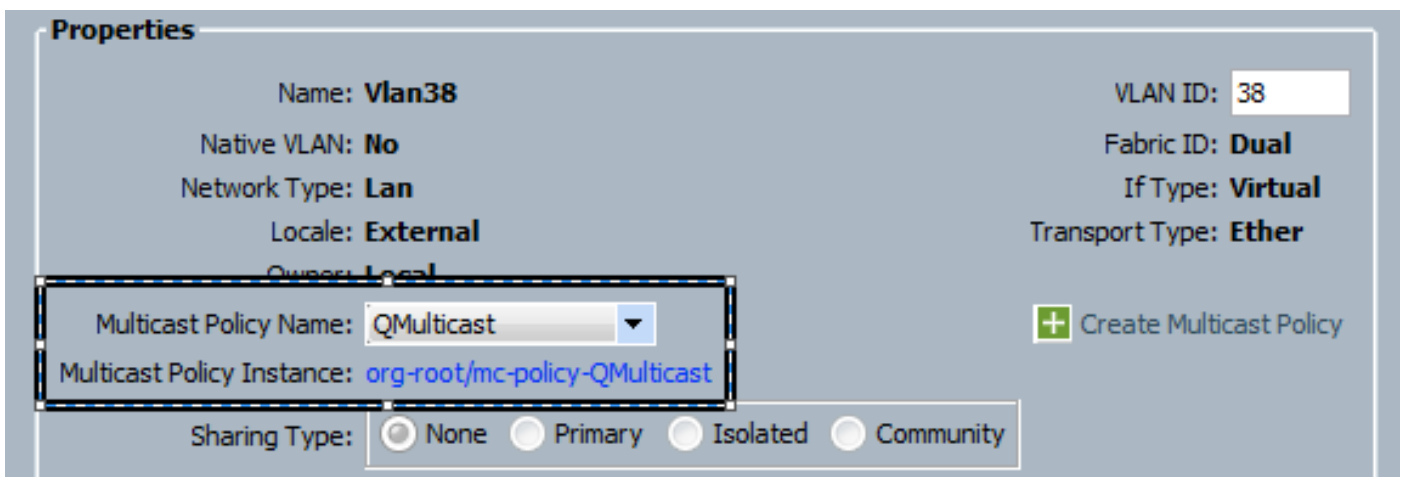


Paso 5. Durante la creación de una nueva VLAN, ahora hay una opción e para especificar el nombre de la política de multidifusión.



## Configuración - Asignar

Ejemplos con diferentes políticas configuradas en la VLAN. El nombre de la política de multidifusión es lo que se configura en el caso de que las Fabric Interconnects estén utilizando realmente la instancia de la política de multidifusión.





Si crea varios objetos VLAN, que apuntan al mismo ID de VLAN, entonces, cuando aplica una política Multicast, se aplica a **todos** los objetos VLAN con el mismo ID de VLAN. La última política de multidifusión aplicada se aplica a todos. Por ejemplo: QMulticast cambiado a Snoop\_off\_qu\_off (Vlan 38).

Name	ID	Type	Transport	Native	VLAN Sharing	Primary VLAN Name	Multicast Policy Name
VLAN 39 (39)	39	Lan	Ether	No	None		
VLAN Management (38)	38	Lan	Ether	No	None		QMulticast
VLAN Vlan38 (38)	38	Lan	Ether	No	None		QMulticast
VLAN default (1)	1	Lan	Ether	Yes	None		



## Creación de una política de multidifusión UCS mediante CLI

- Agregue un nuevo comando para crear una política multicast bajo scope org. alcance de MiniMe-B# org

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

- Establezca las propiedades para la política multicast.

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

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

- Nuevo comando para ver las políticas multicast existentes.

```
MiniMe-B # scope org
```

```
MiniMe-B /org # show mcast-policy
```

- Nuevo comando para eliminar la política multicast existente.

```
MiniMe-B # scope org
```

```
MiniMe-B /org # delete mcast-policy <name>
```

- Cuando crea una VLAN, el usuario puede agregar una política de multidifusión existente a la VLAN.

```
Enlace eth-uplink de alcance MiniMe-B#
```

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

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

## Configuración en el switch ascendente

- En el switch ascendente, debe configurar el solicitante de indagación IGMP en una VLAN específica y el solicitante de indagación IGMP debe coincidir con la IP en la política de multidifusión de UCS.

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

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

```
AGR012-5K-A(config-vlan-config)# ip igmp snooping querier 172.16.38.124 (es probable que la IP sea diferente)
```

## Verificación

- `Show ip igmp snooping vlan <vlan id>` (Esto se puede hacer en el switch ascendente o en Fabric Interconnect).

(El resultado del comando de indagación de UCS para la VLAN 38 verifica que el solicitante esté configurado en el UCSM y el N5k, y muestra que sólo el consultor en el N5k está actualmente activo (como se esperaba). Mientras que la VLAN 39 no está configurada.

```

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> (Esto se puede hacer en el switch ascendente o en 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> (Esto se puede hacer en el switch ascendente o Fabric Interconnect.)
- Muestra los puertos activos para multicast y el solicitante 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> (Esto se puede hacer en el switch ascendente o en 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/rcv/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 límite**

Esto no captura los datos reales del flujo de vídeo, solo los datos IGMP. Esta herramienta captura el tráfico de control. (EX; se muestra cuando un host se une o abandona el grupo.)

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

```

## Troubleshoot

- **UDPCAST (<http://www.udpcast.linux.lu/cmd.html>)**
- Esta aplicación se descarga en dos hosts diferentes, el remitente y el receptor. Con él, puede generar tráfico multicast con una transferencia de un archivo de un origen a varios destinos a la vez con un único comando.

```
Command Prompt - C:\udp-sender -f C:\Users\qdides\Desktop\test.rtf
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

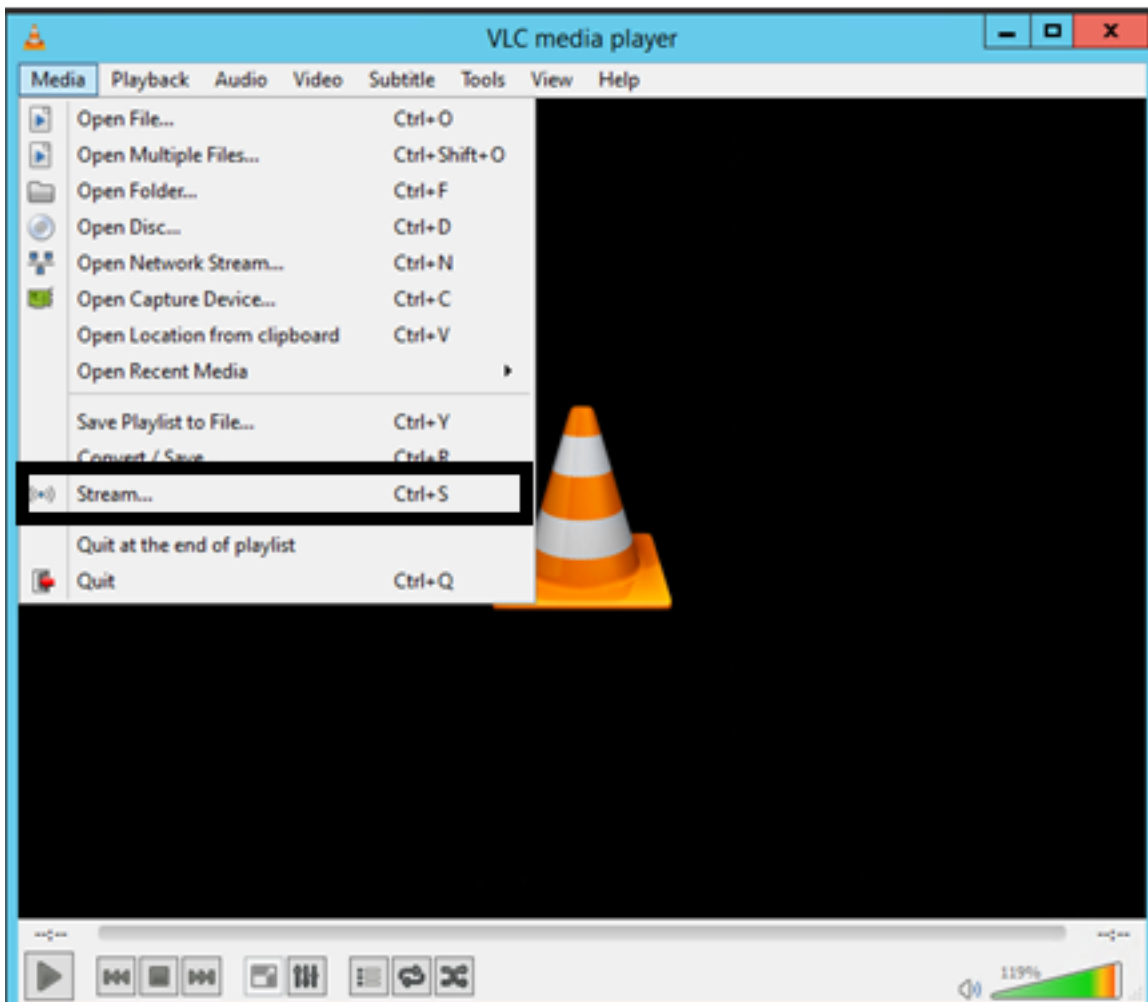
C:\Users\qdides>C:\udp-sender -f C:\Users\qdides\Desktop\test.rtf
Udp-sender 20120424
Using mcast address 234.201.200.250
UDP sender for C:\Users\qdides\Desktop\test.rtf at 10.201.200.250 on Intel(R) 82576 Gigabit Dual Port Network Connection (d8-d8-fd-09-3a-09)
Broadcasting control to 10.201.200.255
```

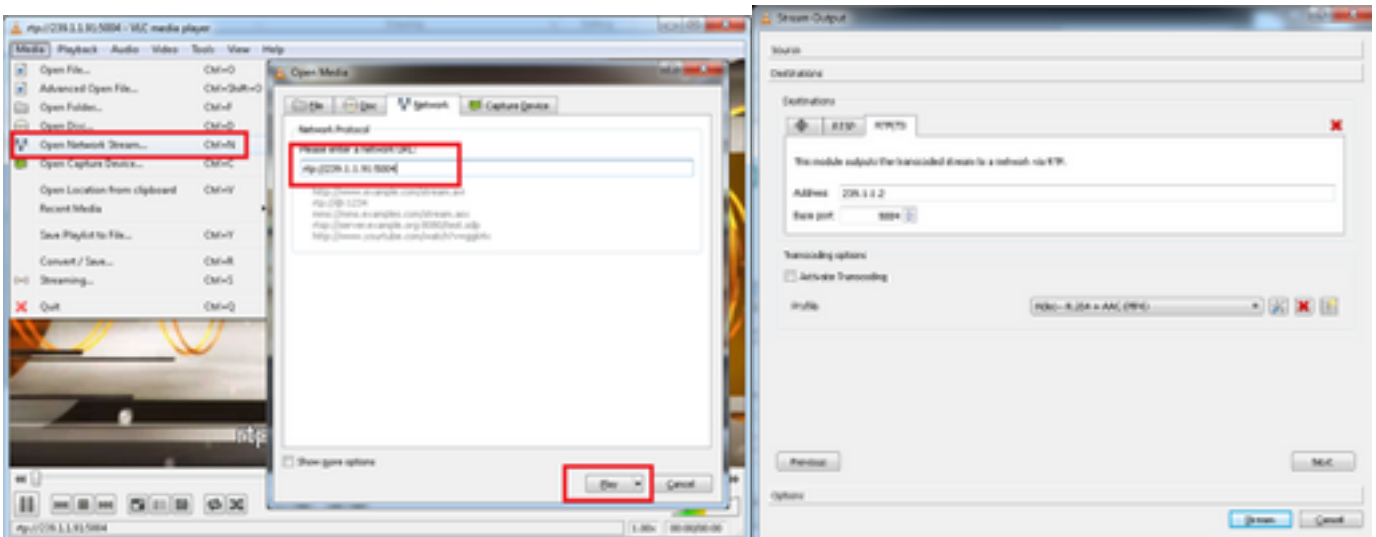
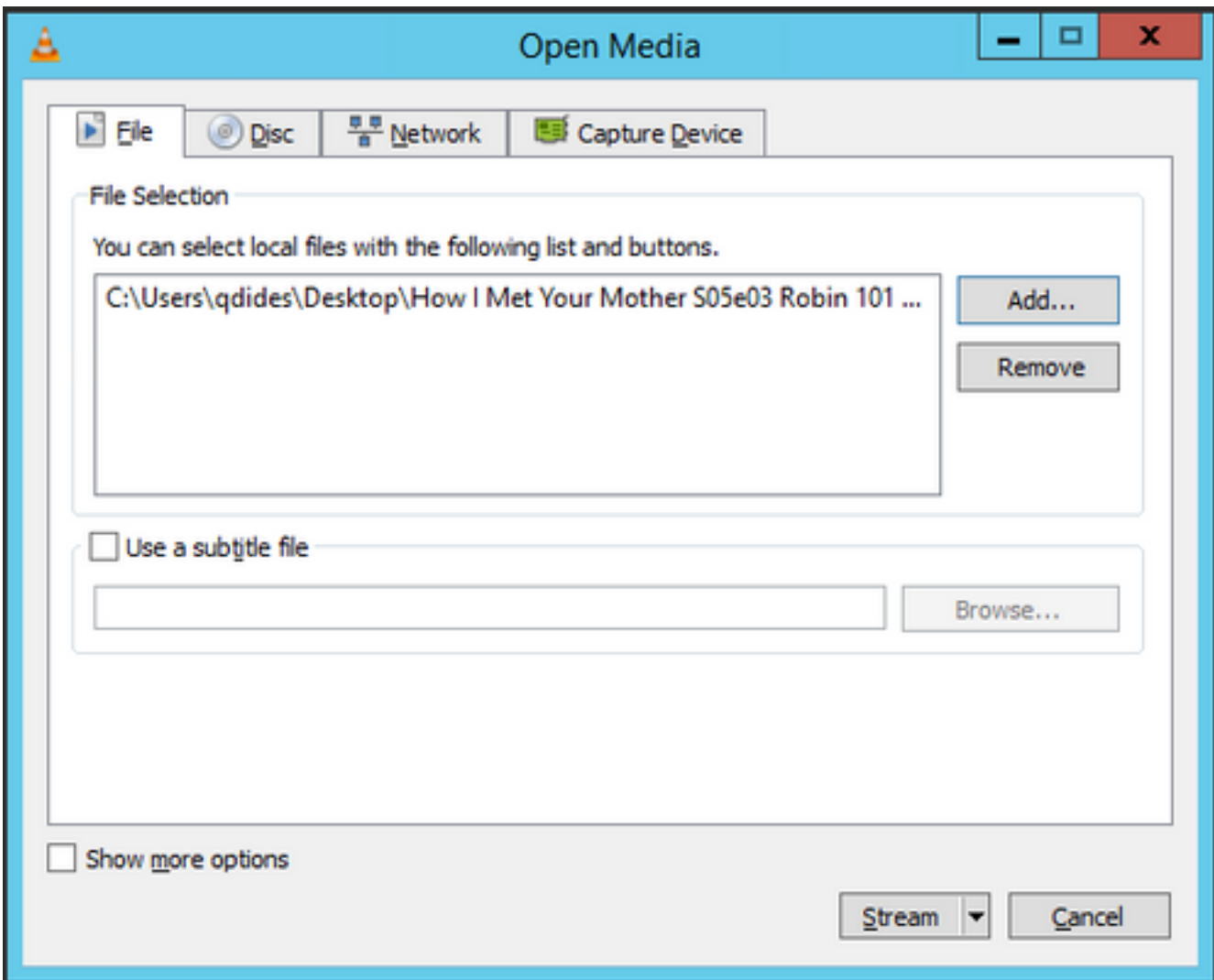
```
Command Prompt - C:\udp-receiver -f C:\Users\qdides\Desktop\test.rtf
C:\Users\qdides>C:\udp-receiver -f C:\Users\qdides\Desktop\test.rtf
Udp-receiver 20120424
UDP receiver for C:\Users\qdides\Desktop\test.rtf at 10.201.200.250 on Intel(R) 82576 Gigabit Dual Port Network Connection (d8-d8-fd-09-3a-09)
```

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

(Aquí están las imágenes que muestran cómo transmitir en VLC. Hay bastante información sobre cómo realizar este proceso en línea).







## ¿Cómo se Genera el Tráfico de IGMP y Multicast con Iperf?

- Iperf o Jperf es una herramienta muy útil que puede generar tráfico IGMP y multidifusión, puede ejecutarse en Linux y Windows OS.
- CLI de remitente multidifusión.

```
# 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 is 10Mbps

- CLI del receptor de multidifusión.

```
# 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

## Información Relacionada

- [Guía de Configuración de Cisco Nexus 5000 Series NX-OS Multicast Routing, Versión 5.0\(3\)N1\(1\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)