

Configura multicast su UCS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Opzioni di configurazione del multicast UCS](#)

[Configurazione in modalità host finale](#)

[Snooping IGMP abilitato / Query IGMP abilitato](#)

[Snooping IGMP abilitato / Query IGMP disabilitato](#)

[Snooping IGMP disabilitato / Query IGMP disabilitato](#)

[Snooping IGMP disabilitato / Query IGMP abilitato](#)

[Configurazione in modalità di commutazione](#)

[Snooping IGMP abilitato / Query IGMP abilitato](#)

[Snooping IGMP abilitato / Query IGMP disabilitato](#)

[Snooping IGMP disabilitato / Query IGMP disabilitato](#)

[Snooping IGMP disabilitato / Query IGMP abilitato](#)

[UCS e configurazione upstream](#)

[Configurazione - Creazione](#)

[Criterio predefinito](#)

[Configurazione - Creazione continua](#)

[Configurazione - Assegna](#)

[Creazione dei criteri multicast UCS tramite CLI](#)

[Configurazione sullo switch upstream](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Come generare il traffico IGMP e multicast con Iperf?](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive la procedura richiesta per configurare il multicast all'interno di Unified Computing Systems (UCS). Il multicast (MCAST) è la capacità di inviare dati attraverso una rete a più utenti contemporaneamente (comunicazione di gruppo uno-a-molti o molti-molti). Il protocollo IGMP (Internet Group Management Protocol) è un componente cruciale del multicast. Lo scopo principale di IGMP è quello di consentire agli host di comunicare il proprio desiderio di ricevere il traffico multicast ai router multicast IP sulla rete locale. In cambio, consente ai router multicast IP di "unirsi" al gruppo multicast specificato e di iniziare a inoltrare il traffico multicast sul segmento di rete verso l'host.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- UCS
- Nexus Multicast Switching

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Fabric Interconnect - 6100 / 6200
- UCSM (Unified Computing System Manager)
- Interruttore a monte (EX; Nexus 5000)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Prima di Unified Computing System Manager (UCS-M) versione 2.1:

- Per impostazione predefinita, lo snooping IGMP è abilitato per il multicast nell'UCS e non può essere disabilitato. (Il Cisco Technical Assistance Center (TAC) potrebbero essere disabilitati tramite il plug-in di debug).
- Le interconnessioni fabric UCS non dispongono di funzionalità di query IGMP; è quindi necessario attivare la funzionalità di query in un dispositivo nella rete L2 upstream.
- Affinché l'operazione funzioni, è necessario avere un router multicast nella VLAN o un query IGMP nella VLAN.

Del Mar 2.1 Note:

- Per impostazione predefinita, lo snooping IGMP è abilitato, gli amministratori di rete devono esaminare attentamente eventuali requisiti per disabilitare lo snooping IGMP e le prestazioni dannose che potrebbero verificarsi.
- La configurazione dello snooping IGMP è disponibile e configurabile solo per VLAN; non è possibile abilitare o disabilitare lo snooping IGMP a livello globale.
- La capacità di disabilitare lo snooping IGMP è supportata sia in modalità host finale (EHM) che in modalità switch.
- Nessun supporto per Criteri multicast su gruppi di rete (un'altra nuova funzionalità di Del Mar).

Specifiche di Fabric Interconnect:

- Per un'interconnessione fabric serie 6100 (FI), tutte le VLAN possono usare solo la policy multicast predefinita; tuttavia, l'utente può modificare gli stati IGMP Snooping/Querier di

questo criterio predefinito. Se si configurano altri criteri multicast, viene generato un errore, "Per le Vlan in X Fabric Interconnect, è supportato solo il criterio multicast predefinito."

- La modifica del criterio multicast per una determinata VLAN (a un criterio diverso da quello predefinito) è supportata solo sugli switch 6200 e NON sugli switch 6100. Poiché i 6100 FI non possono avere criteri multicast diversi sulle proprie VLAN, è possibile che sia presente una limitazione nell'ASIC di Gatos. Questa limitazione non esiste per i 6200 FI con ASIC Carmel.

Opzioni di configurazione del multicast UCS

Configurazione in modalità host finale

Snooping IGMP abilitato / Query IGMP abilitato

- Invia solo le interrogazioni ai blade. Non invia query IGMP alla rete upstream.
- I FI non inviano le query IGMP allo switch a monte in quanto ciò contraddice il ruolo della modalità host finale nella rete. Ciò può causare traffico multicast indesiderato (sia di controllo che di dati) inviato agli FI. Questo è il motivo per cui si è deciso di affidare agli EHM FI la responsabilità di trasmettere le query IGMP solo ai propri blade.
- Di conseguenza, è necessario utilizzare una delle configurazioni approvate:

Configurazioni approvate:

Configurare il querier IGMP sullo switch a monte con lo snooping IGMP abilitato o disabilitare lo snooping IGMP sullo switch a monte per inondare il traffico multicast. In alternativa, modificare gli FI in modalità switch.

Snooping IGMP abilitato / Query IGMP disabilitato

- La modalità predefinita è la stessa delle versioni precedenti a Del Mar.
- Richiede: IGMP Querier nello switch a monte per la VLAN con snooping IGMP abilitato o router multicast nella VLAN.

Snooping IGMP disabilitato / Query IGMP disabilitato

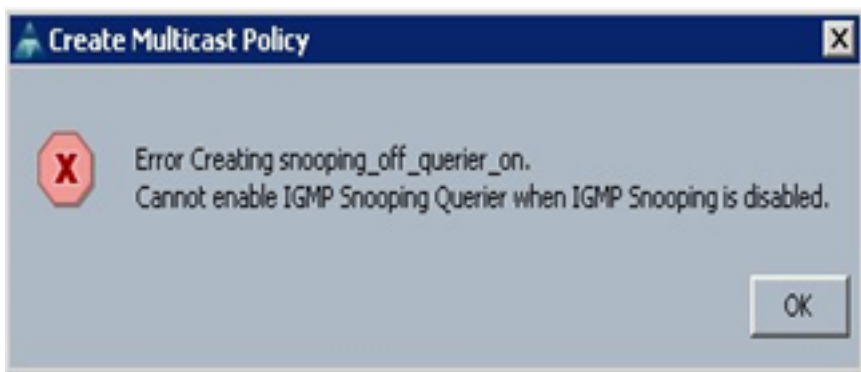
- Gli IF inondano il traffico multicast nella VLAN.
- Per il corretto funzionamento è necessaria una delle configurazioni approvate:

Configurazioni approvate:

Sullo switch a monte, lo snooping IGMP può essere abilitato o disabilitato per inondare il traffico multicast.

Snooping IGMP disabilitato / Query IGMP abilitato

- Configurazione non valida.
- Questo è bloccato correttamente dal modulo UCSM.



Configurazione in modalità di commutazione

Snooping IGMP abilitato / Query IGMP abilitato

- I FI inoltrano le query IGMP alla rete upstream.
- Gli switch a monte apprendono le informazioni sul querier IGMP configurato sugli FI, quindi genera e inoltra il traffico MCAST verso gli FI.
- Richiede: Switch a monte con snooping IGMP abilitato o con snooping disabilitato per inondare il traffico multicast.

Snooping IGMP abilitato / Query IGMP disabilitato

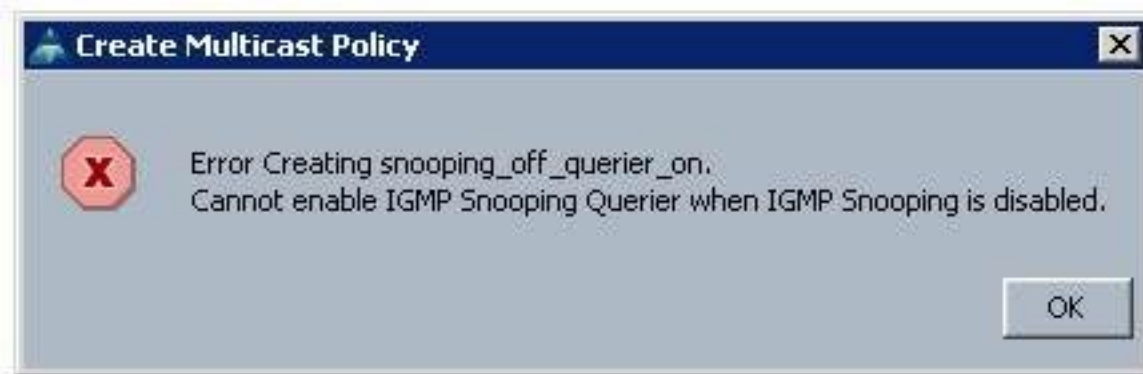
- La modalità predefinita è identica a quella delle versioni precedenti a Del Mar.
- Richiede: IGMP Querier nello switch a monte per la VLAN con snooping IGMP abilitato o router multicast nella VLAN.

Snooping IGMP disabilitato / Query IGMP disabilitato

- Gli IF inondano il traffico multicast nella VLAN.
- Richiede: Switch a monte con snooping IGMP abilitato o disabilitato per inondare il traffico multicast.

Snooping IGMP disabilitato / Query IGMP abilitato

- Configurazione non valida.
- Questo è bloccato correttamente dal modulo UCSM.



UCS e configurazione upstream

Configurazione - Creazione

Lo snooping IGMP è disponibile su base VLAN e non a livello di interfaccia. Da UCSM, questa può essere configurata con un criterio multicast su una VLAN denominata.

1. Aggiungere un nuovo nodo **Criteri multicast** in **LAN> LAN > Criteri> radice**.
2. È disponibile il supporto per la creazione, la modifica e l'eliminazione di criteri multicast.
3. Quando si crea una VLAN, è possibile selezionare un criterio multicast esistente.
4. E il supporto per collegare un criterio multicast esistente con una VLAN già creata.

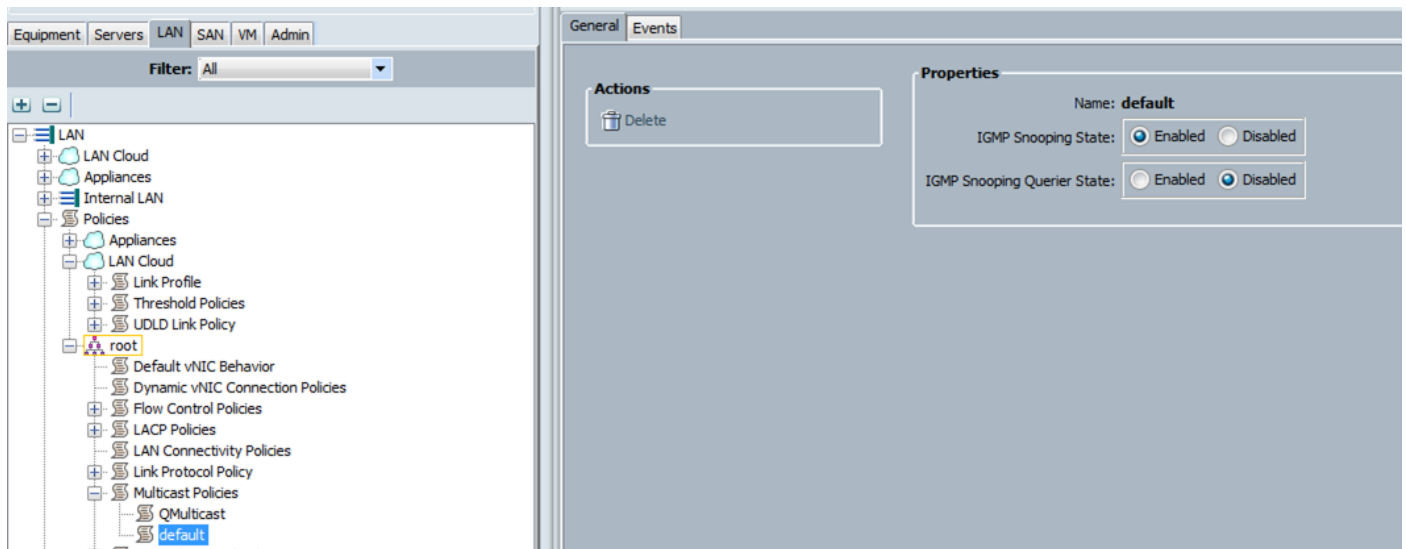
Nota: I criteri multicast si trovano solo nella struttura di criteri radice e non è possibile creare singoli criteri in una sottoorganizzazione.

Criterio predefinito

Il criterio multicast predefinito rimane in linea con il comportamento di interconnessione dell'infrastruttura prima della versione 2.1 di Mar:

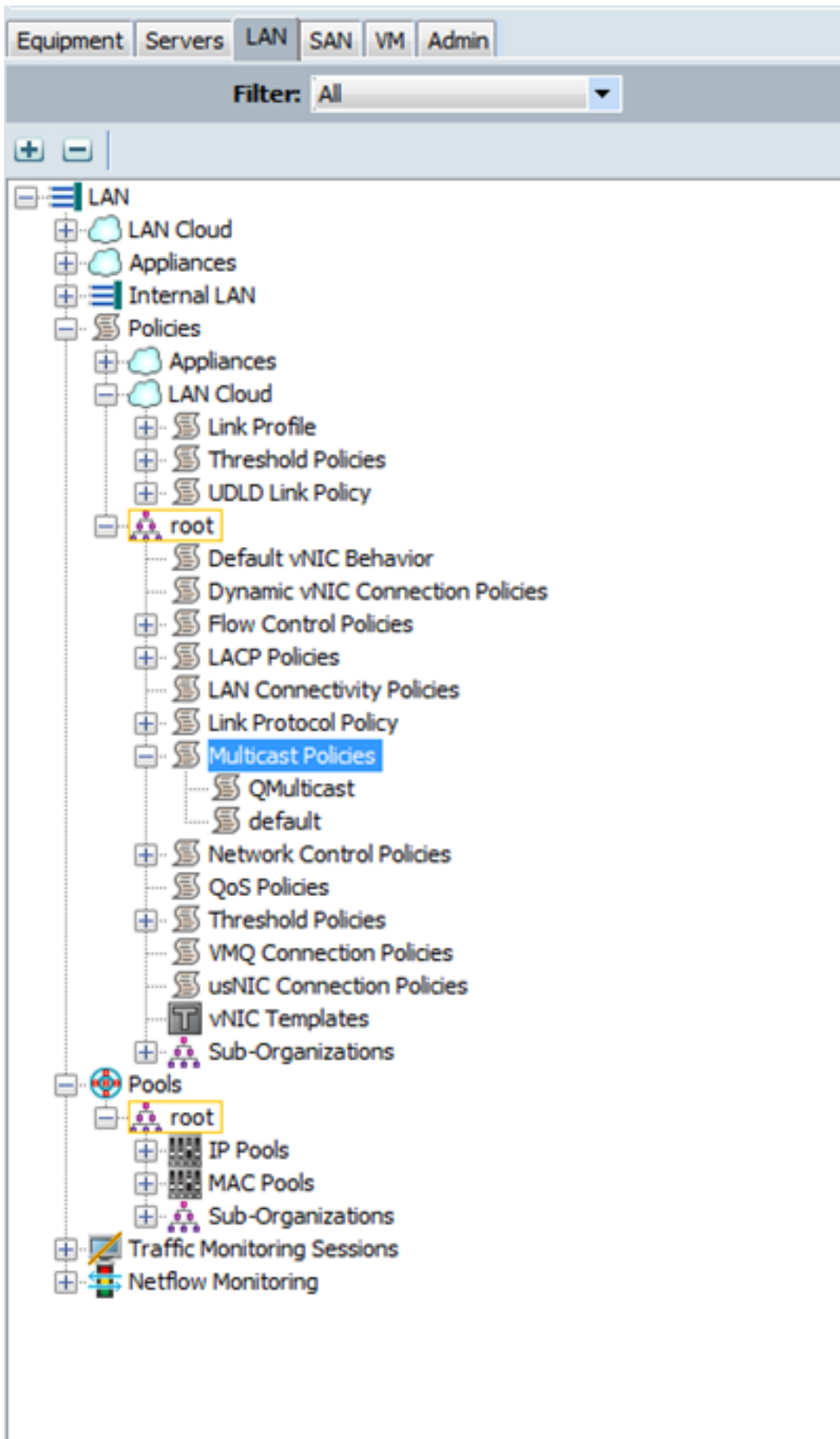
Snooping IGMP Attivato

IGMP Querier- Disabilitato



Configurazione - Creazione continua

Passaggio 1. Aggiungere un nuovo nodo **Criteri multicast** in **LAN > LAN > Criteri > radice**.



Passaggio 2. Fare clic con il pulsante destro del mouse su Criteri multicast, quindi scegliere **Crea criterio multicast**.

Passaggio 3. Viene quindi visualizzato quanto segue:

Fornire un nome e configurare gli stati di IGMP Snooping e Snooping Querier.



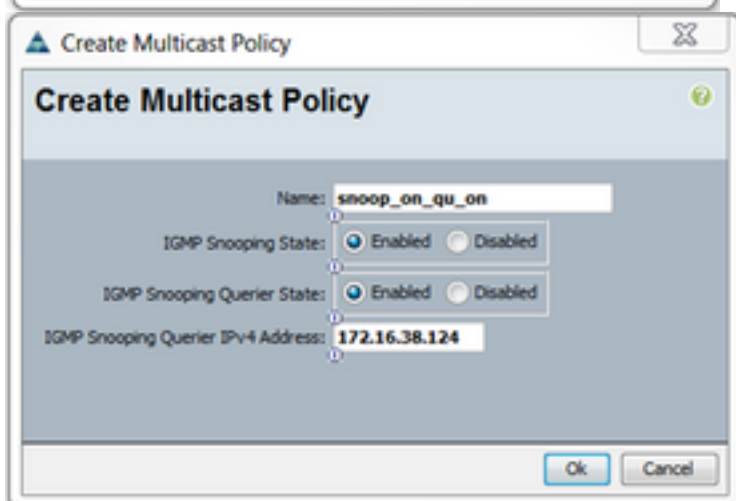
Create Multicast Policy

Name:

IGMP Snooping State: Enabled Disabled

IGMP Snooping Querier State: Enabled Disabled

Ok Cancel



Create Multicast Policy

Name:

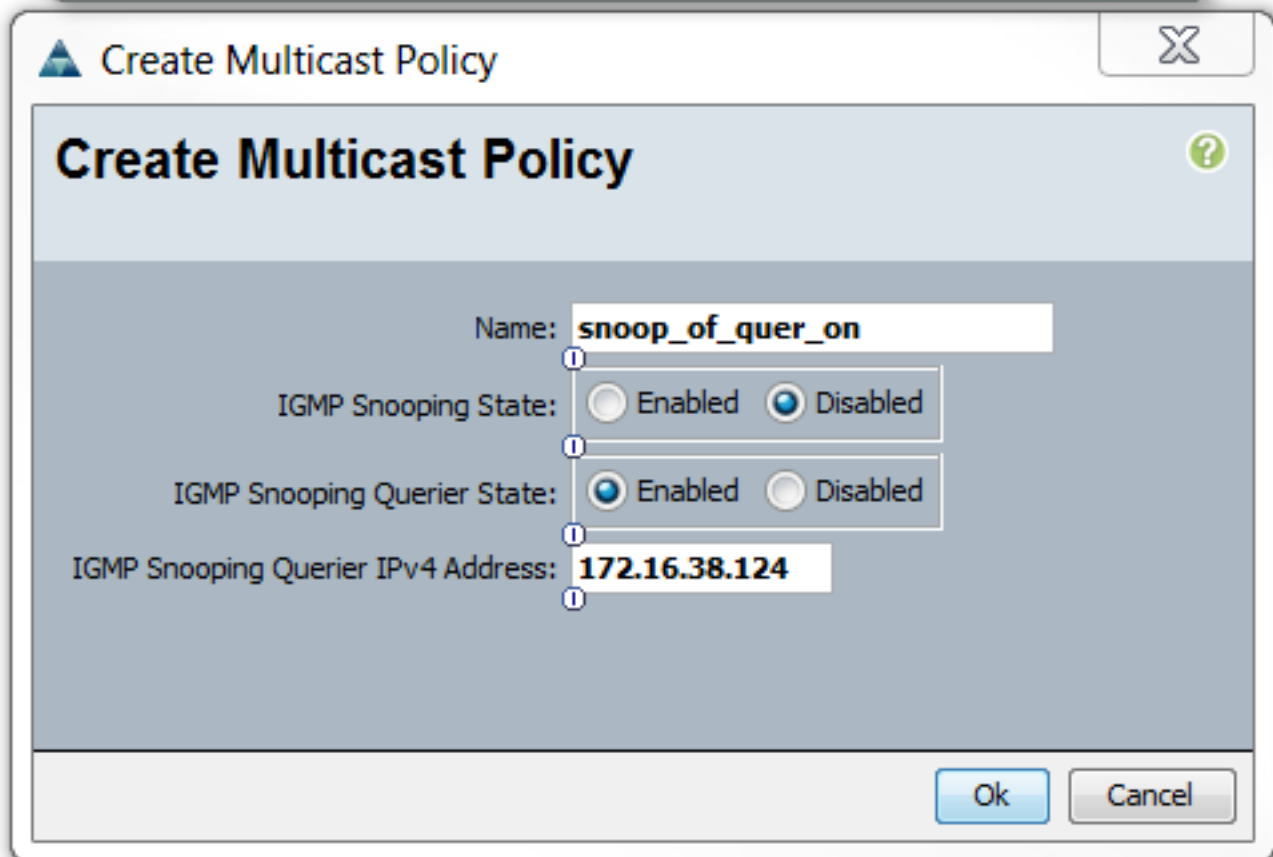
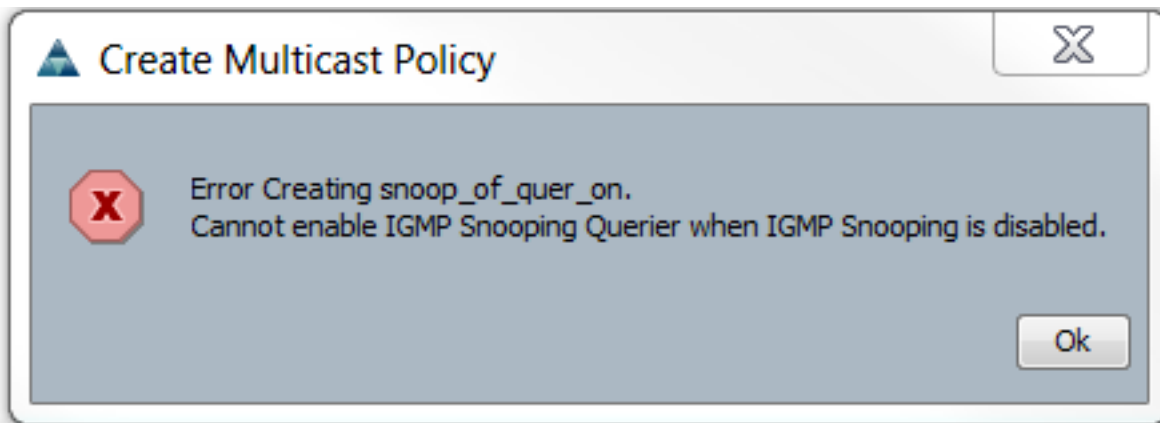
IGMP Snooping State: Enabled Disabled

IGMP Snooping Querier State: Enabled Disabled

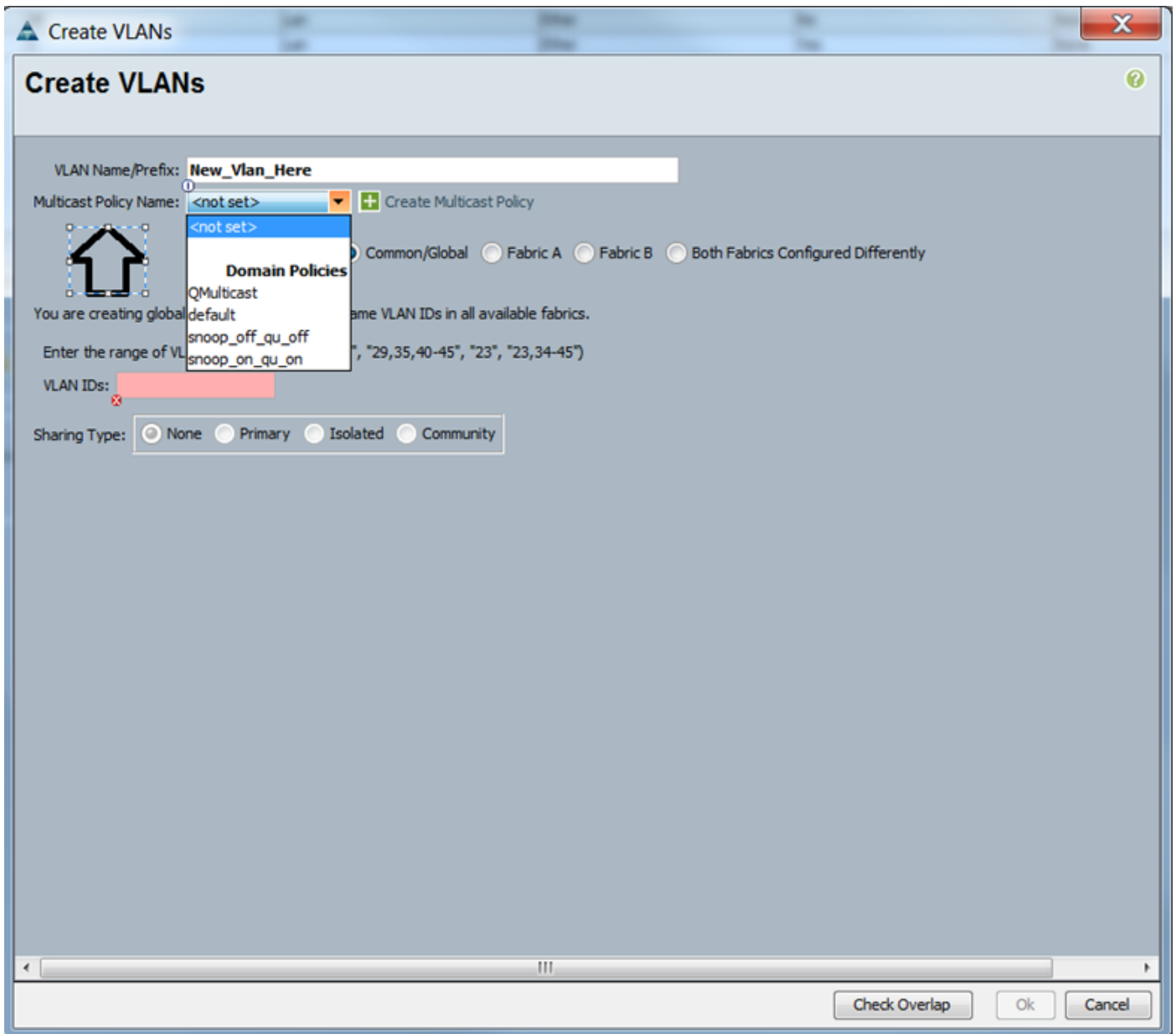
IGMP Snooping Querier IPv4 Address:

Ok Cancel

Passaggio 4. Se si tenta di disabilitare lo snooping IGMP quando il programma è abilitato, viene generato un errore, in quanto la configurazione non è valida.

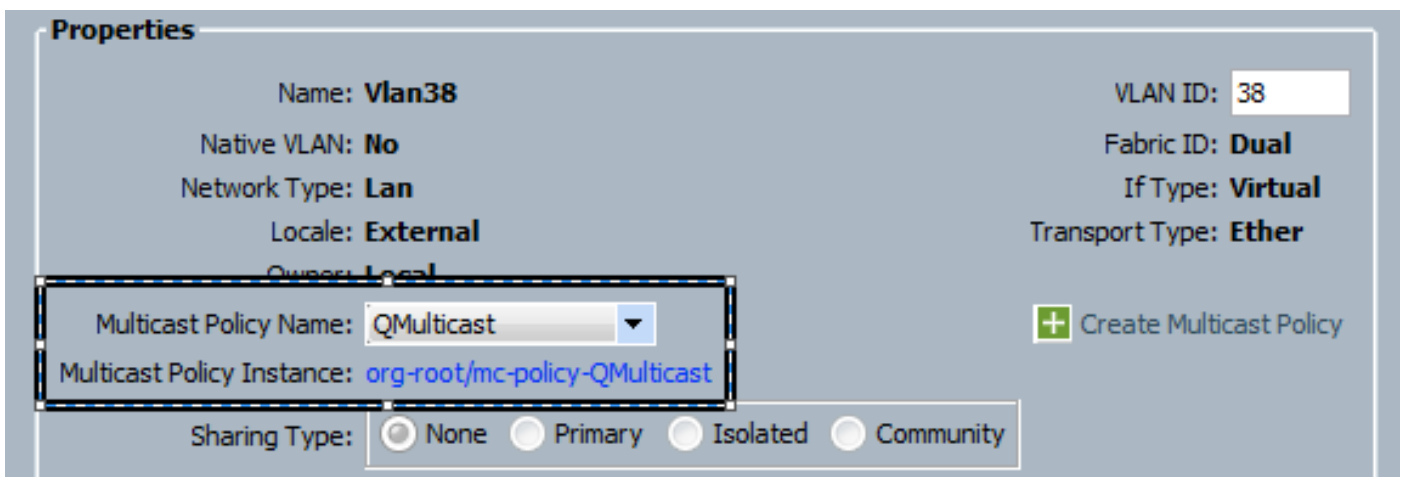


Passaggio 5. Durante la creazione di una nuova VLAN, è disponibile un'opzione e per specificare il nome del criterio multicast.



Configurazione - Assegna

Esempi di regole diverse impostate sulla VLAN. Il nome del criterio multicast è il nome configurato dove l'istanza del criterio multicast è effettivamente utilizzata dalle interconnessioni dell'infrastruttura.





Se si creano più oggetti VLAN che puntano allo stesso ID VLAN, quando si applica una policy multicast, questa viene applicata a **tutti** gli oggetti VLAN con lo stesso ID VLAN. L'ultimo criterio multicast applicato viene applicato a tutti. Esempio: QMulticast modificato in 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		



Creazione dei criteri multicast UCS tramite CLI

- Aggiungere un nuovo comando per creare un criterio multicast nell'ambito org.

MiniMe-B# ambito org

MiniMe-B /org # creazione mcast-policy <nome>

- Impostare le proprietà per i criteri multicast.

```
MiniMe-B /org/mcast-policy #set querier <abilita/disabilita>
```

```
MiniMe-B /org/mcast-policy #set snooping <abilita/disabilita>
```

- Nuovo comando per visualizzare i criteri multicast esistenti.

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

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

- Nuovo comando per eliminare il criterio multicast esistente.

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

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

- Quando si crea una VLAN, l'utente può aggiungere alla VLAN un criterio multicast esistente.

```
MiniMe-B# scope eth-uplink
```

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

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

Configurazione sullo switch upstream

- Sullo switch a monte, è necessario configurare il querier dello snooping IGMP su una VLAN specifica e il querier dello snooping IGMP deve corrispondere all'IP nel criterio multicast UCS.

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

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

```
AGR012-5K-A(config-vlan-config)# ip igmp snooping querier 172.16.38.124 (IP è probabilmente diverso)
```

Verifica

- **Show ip igmp snooping vlan <id vlan>** (questa operazione può essere eseguita sullo switch Upstream o sull'interconnessione dell'infrastruttura).

(L'output del comando snooping UCS per la VLAN 38 verifica che il querier sia configurato sull'UCSM e sull'N5k e mostra che solo il querier sull'N5k è attualmente attivo (come previsto). Mentre la VLAN 39 non è configurata.

```

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 <id vlan> (questa operazione può essere eseguita sullo switch Upstream o sull'interconnessione dell'infrastruttura).

```

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> (questa operazione può essere eseguita sullo switch Upstream o sull'interconnessione dell'infrastruttura).
- Mostra le porte attive per multicast e il querier 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>** (questa operazione può essere eseguita sullo switch Upstream o sull'interconnessione fabric).

```

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 limite

In questo modo non vengono acquisiti dati video effettivi, ma solo dati IGMP. Questo strumento acquisisce il traffico di controllo. (ES. indica quando un host si unisce o esce dal gruppo.)

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
```

Risoluzione dei problemi

- UDPCAST(<http://www.udpcast.linux.lu/cmd.html>)
- Questa applicazione viene scaricata su due host diversi, mittente e destinatario. che consente di generare traffico multicast con il trasferimento di un file da un'origine a più destinazioni contemporaneamente con un unico comando.

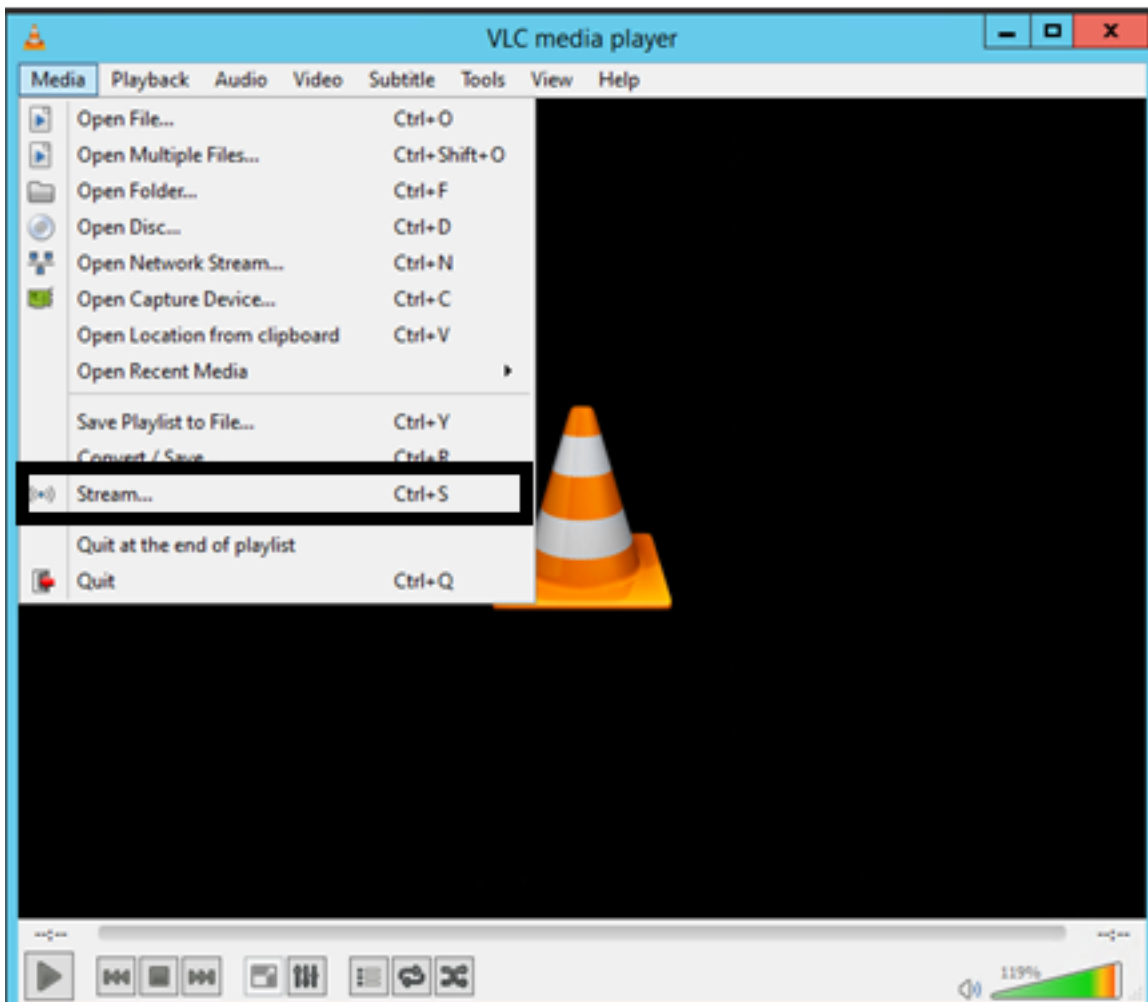
```
Command Prompt - C:\udp-sender -f C:\Users\qdides\Desktop\test.rtf
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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
```

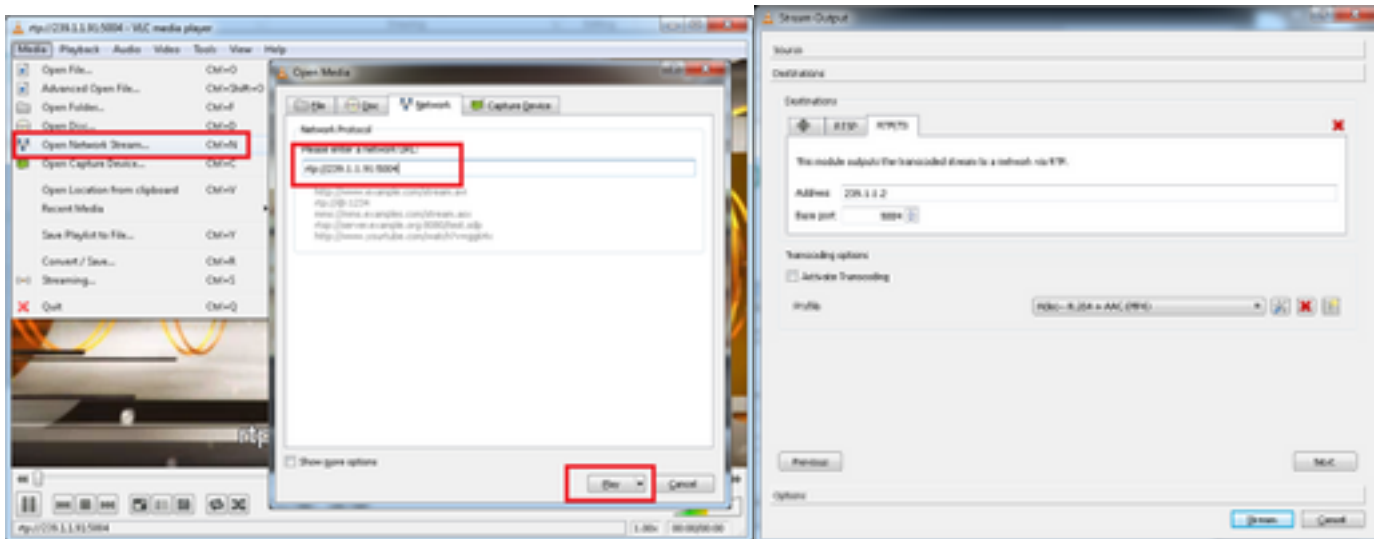
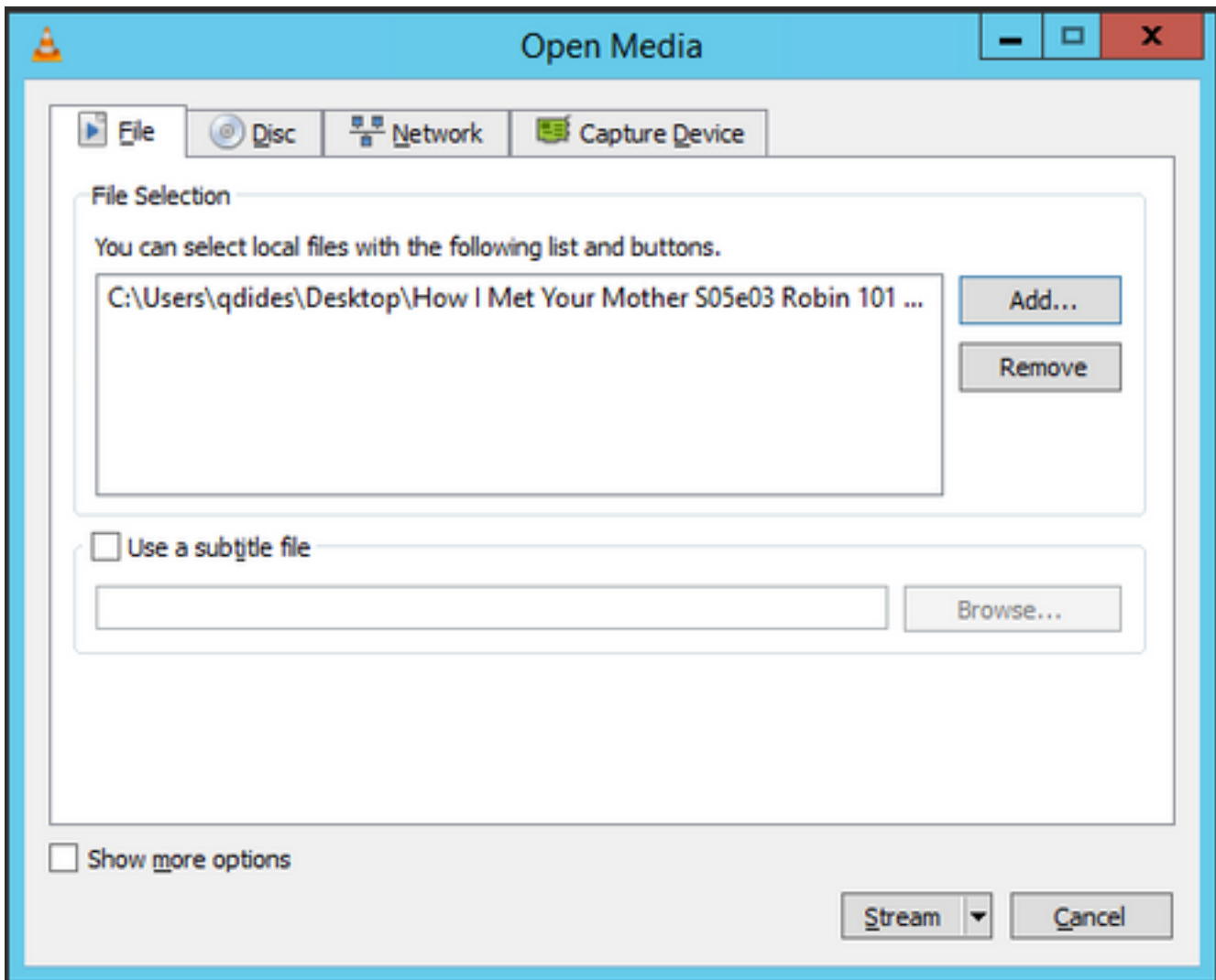
```
Command Prompt - C:\udp-receiver -f C:\Users\qdides\Desktop\test.rtf
C:\Users\qdides>C:\udp-receiver -f C:\Users\qdides\Desktop\test.rtf
Udp-receiver 20120424
UDP receiver for C:\Users\qdides\Desktop\test.rtf at 10.201.200.250 on Intel(R) 82576 Gigabit Dual Port Network Connection (d8-d8-fd-09-3a-09)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

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

(Ecco le immagini che mostrano come eseguire lo streaming sul VLC. Sono disponibili diverse informazioni su come eseguire questa procedura online.)



- 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
- Convert / Save
- Stream... Ctrl+S
- Quit at the end of playlist
- Quit Ctrl+Q



Come generare il traffico IGMP e multicast con Iperf?

- Iperf o Jperf è uno strumento molto utile che può generare traffico IGMP e multicast, può essere eseguito su Linux e Windows OS.
- CLI mittente multicast.

```
# 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 ricevitore multicast.

```
# 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

Informazioni correlate

- [Guida alla configurazione di Cisco Nexus serie 5000 NX-OS Multicast Routing, versione 5.0\(3\)N1\(1\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)