Configure Multicast on UCS

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
UCS Multicast Configuration Options
Configuration in End Host Mode
IGMP Snooping Enabled / IGMP Querier Enabled
IGMP Snooping Enabled / IGMP Querier Disabled
IGMP Snooping Disabled / IGMP Querier Disabled
IGMP Snooping Disabled / IGMP Querier Enabled
Configuration in Switching Mode
IGMP Snooping Enabled / IGMP Querier Enabled
IGMP Snooping Enabled / IGMP Querier Disabled
IGMP Snooping Disabled / IGMP Querier Disabled
IGMP Snooping Disabled / IGMP Querier Enabled
UCS and Upstream Configuration
Configuration - Create
Default Policy
Configuration – Create Continued
Configuration – Assign
Creating UCS Multicast Policy via CLI
Configuration on Upstream Switch
Verify
Troubleshoot
How to Generate IGMP and Multicast Traffic with Iperf?
Related Information

Introduction

This document describes the procedure required to configure multicast within Unified Computing Systems (UCS). Multicast (MCAST) is the ability to send data across a network to multiple users at the same time (one-to-many or many-many group communication). Internet Group Management Protocol (IGMP) is a crucial component of Multicast. The Primary purpose of IGMP is to permit hosts to communicate their desire to receive multicast traffic, to the IP Multicast router(s) on the local network. This in return, permits the IP Multicast router(s) to “Join” the specified multicast group and to begin to forward the multicast traffic onto the network segment towards the host.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- UCS
- Nexus Multicast Switching

Components Used

The information in this document is based on these software and hardware versions:

- Fabric Interconnect - 6100 / 6200
- UCSM (Unified Computing System Manager)
- Upstream Switch (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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Prior to Unified Computing System Manager (UCS-M) Version 2.1:

- Multicast on the UCS has IGMP snooping enabled by default and this cannot be disabled. (Cisco Technical Assistance Centers (TAC) could disable via the debug plugin).
- The UCS Fabric Interconnects have no IGMP querier functionality; this requires you to enable the querier functionality on a device in the upstream L2 network.
- For this to work, you need a Multicast Router in the VLAN or an IGMP querier in the VLAN.

Del Mar 2.1 Notes:

- By default, IGMP Snooping is enabled, Network Administrators should carefully examine any requirements to disable IGMP Snooping and the detrimental performance that might be experienced.
- IGMP Snooping configuration is only available and configurable on a per VLAN basis, you cannot enable or disable IGMP Snooping globally.
- The ability to disable IGMP Snooping is supported in both End Host Mode (EHM) and Switch Mode.
- No support for Multicast Policies on network groups (another new feature in Del Mar).

Fabric Interconnect Specifics:

- For a 6100 series Fabric Interconnect (FI), all VLANs can only use the default multicast policy; however, the user can modify the IGMP Snooping/Querier states of this default policy. If you configure any other multicast policy it will throw an error, "For Vlans in X Fabric Interconnect, only default Multicast Policy is supported."
- To change the multicast policy for a certain VLAN (to policy other than the default multicast policy) is only supported on 6200 FIs and NOT on 6100s. The reason that is the 6100 FIs

cannot have different multicast policies on its VLANs is due to a limitation in the Gatos ASIC. This limitation does not exist on the 6200 FIs with Carmel ASICs.

UCS Multicast Configuration Options

Configuration in End Host Mode

IGMP Snooping Enabled / IGMP Querier Enabled

- It only sends the queries to the blades. It does not send IGMP queries to the upstream network.
- The FIs don’t send the IGMP queries to the upstream switch as this contradicts the role of End Host mode in the network. This can lead to unwanted multicast traffic (both control and data) sent to the FIs. This is the reason why it was decided to have EHM FIs be responsible to transmit IGMP queries down to its blades only.
- As a result, require one of the approved configurations:

Approved Configurations:

Either configure IGMP querier on the upstream switch with IGMP snooping enabled or Disable IGMP snooping on the upstream switch to flood multicast traffic. Alternatively, change the FIs to switch mode.

IGMP Snooping Enabled / IGMP Querier Disabled

- The default mode, same as releases prior to Del Mar.
- Requires either: IGMP Querier in the upstream switch for the VLAN with IGMP snooping enabled or Multicast router in the VLAN.

IGMP Snooping Disabled / IGMP Querier Disabled

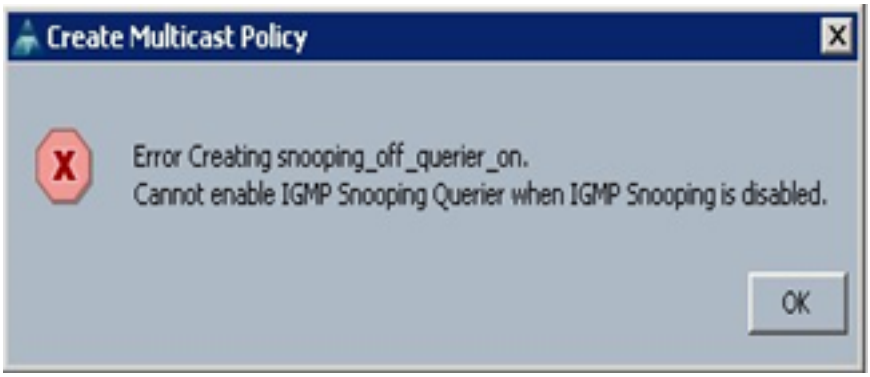
- FIs flood the multicast traffic in the VLAN.
- Requires one of the approved configurations to work successfully:

Approved Configurations:

The upstream switch can have IGMP snooping enabled or have it disabled on the upstream switch to flood multicast traffic.

IGMP Snooping Disabled / IGMP Querier Enabled

- This is not a valid configuration.
- This is correctly blocked by the UCSM.



Configuration in Switching Mode

IGMP Snooping Enabled / IGMP Querier Enabled

- FIs forward IGMP queries to the upstream network.
- Upstream switches learn about IGMP querier configured on FIs, then it builds and forwards the MCAST traffic towards FIs.
- Requires either: Upstream switch with IGMP snooping enabled or have snooping disabled to flood multicast traffic.

IGMP Snooping Enabled / IGMP Querier Disabled

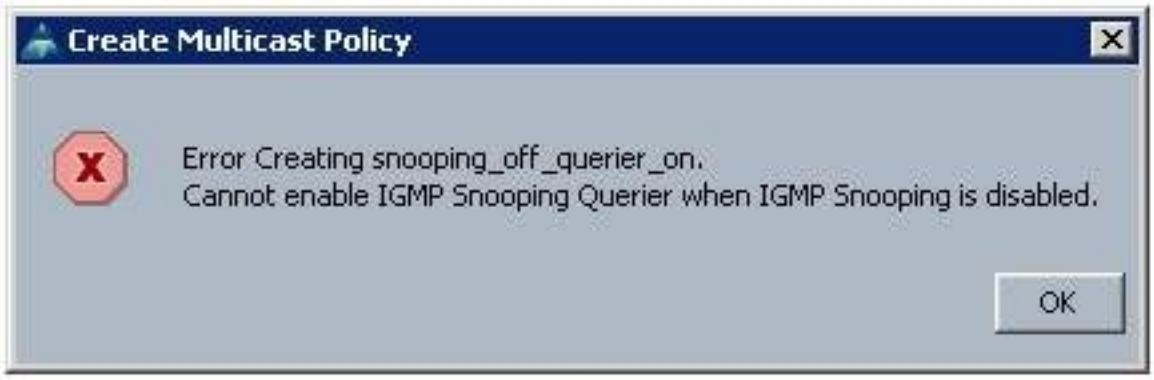
- The default mode, same as pre Del Mar release.
- Requires either: IGMP Querier in the upstream switch for the VLAN with IGMP snooping enabled or multicast router in the VLAN.

IGMP Snooping Disabled / IGMP Querier Disabled

- FIs flood multicast traffic in the VLAN.
- Requires either: Upstream switch with IGMP snooping enabled or to have it disabled to flood multicast traffic.

IGMP Snooping Disabled / IGMP Querier Enabled

- This is not a valid configuration.
- This is correctly blocked by the UCSM.



UCS and Upstream Configuration

Configuration - Create

IGMP snooping is available on a VLAN basis and not on the interface level. From UCSM, this can be configured with a Multicast Policy on a named VLAN.

1. Add a new **Multicast Policies** node under **LAN> LAN > Policies> root**.

2. There is support for the creation, modification, and deletion of Multicast Policies.

3. There is an option for selecting existing Multicast Policy when a VLAN is created.

4. And support for attaching an existing Multicast Policy with a VLAN that is already created.

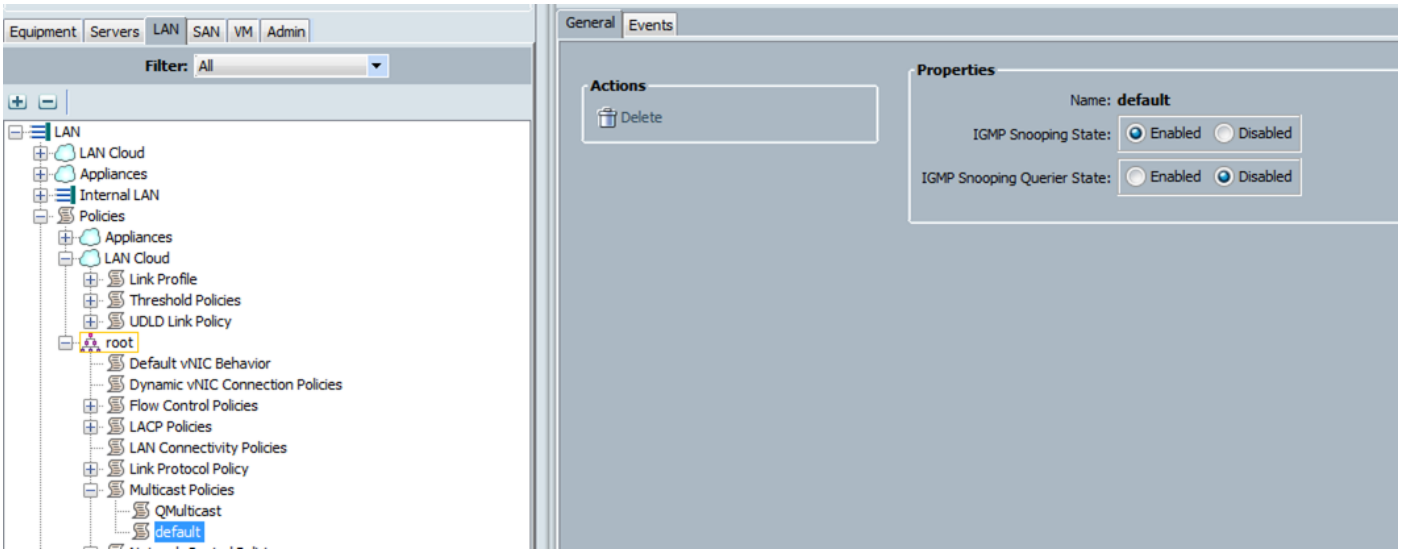
> **Note**: Multicast Policies are only under the root policies tree and you cannot create individual policies under a sub-organization.

Default Policy

Default Multicast Policy keeps in line with Fabric Interconnect behavior prior to 2.1 Del Mar release:

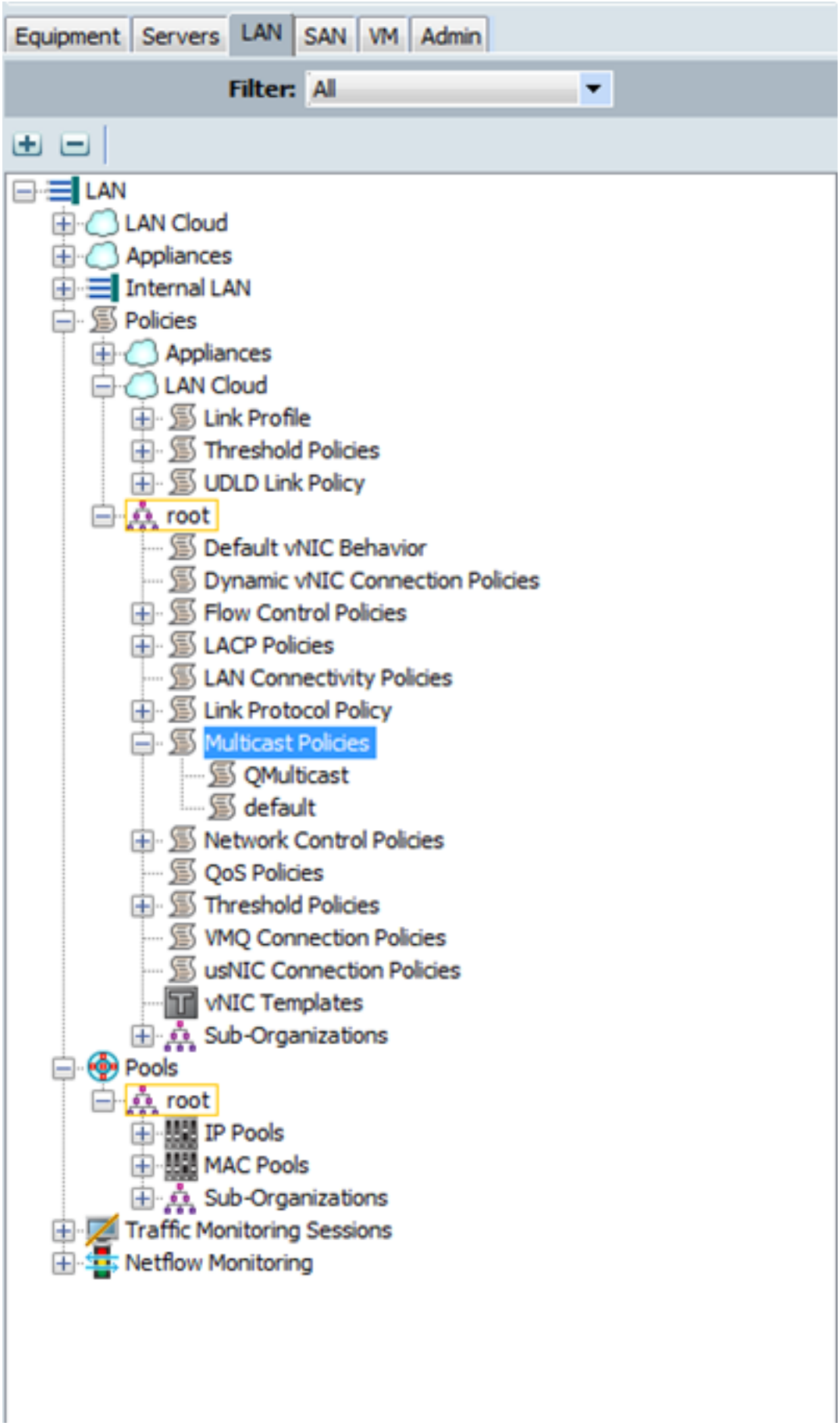
IGMP Snooping- Enabled

IGMP Querier- Disabled



Configuration – Create Continued

Step 1. Add a new **Multicast Policies** node under **LAN > LAN > Policies > root.**

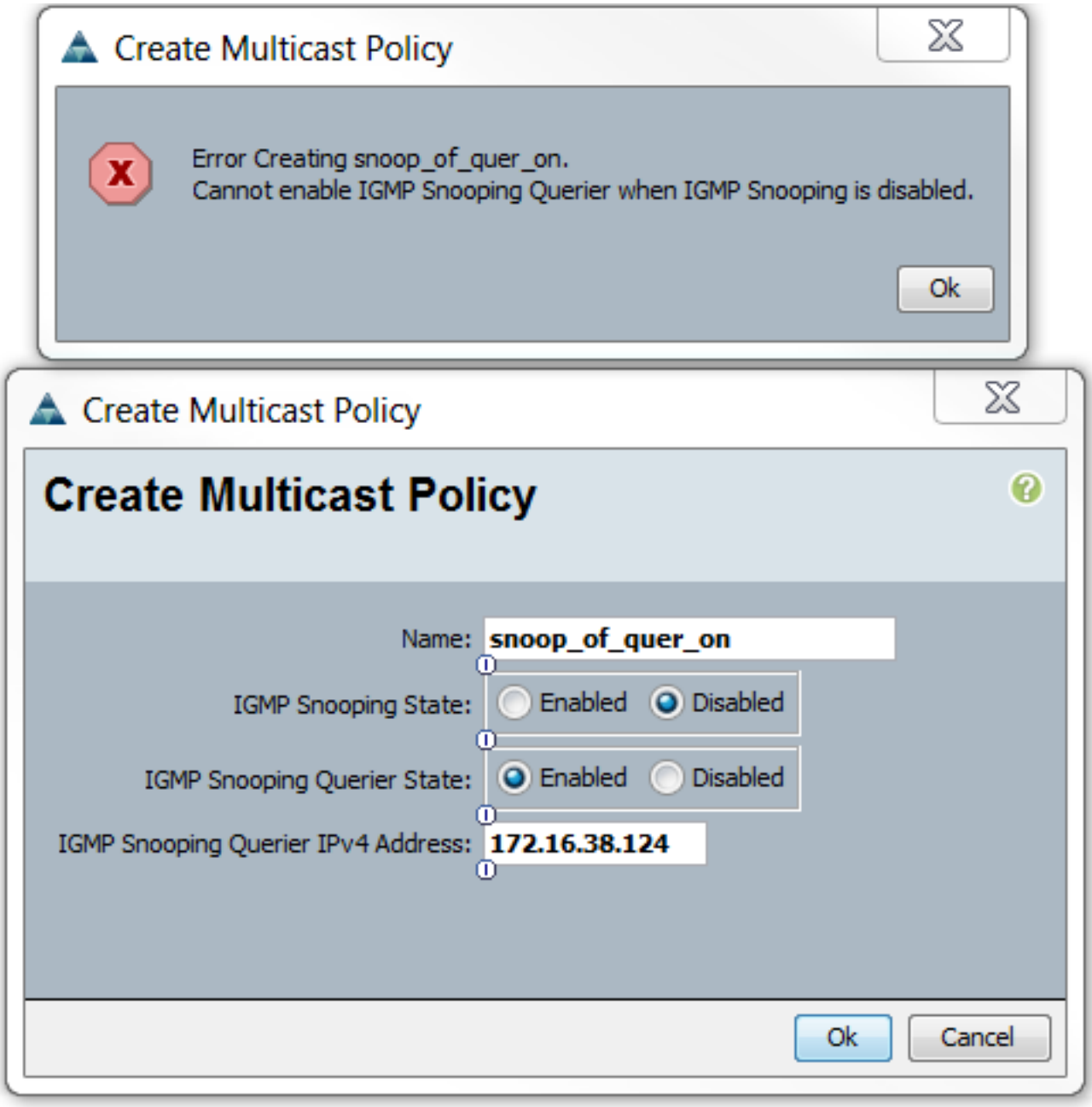


Step 2. Right Click on Multicast Policies, then **Create Multicast Policy**.

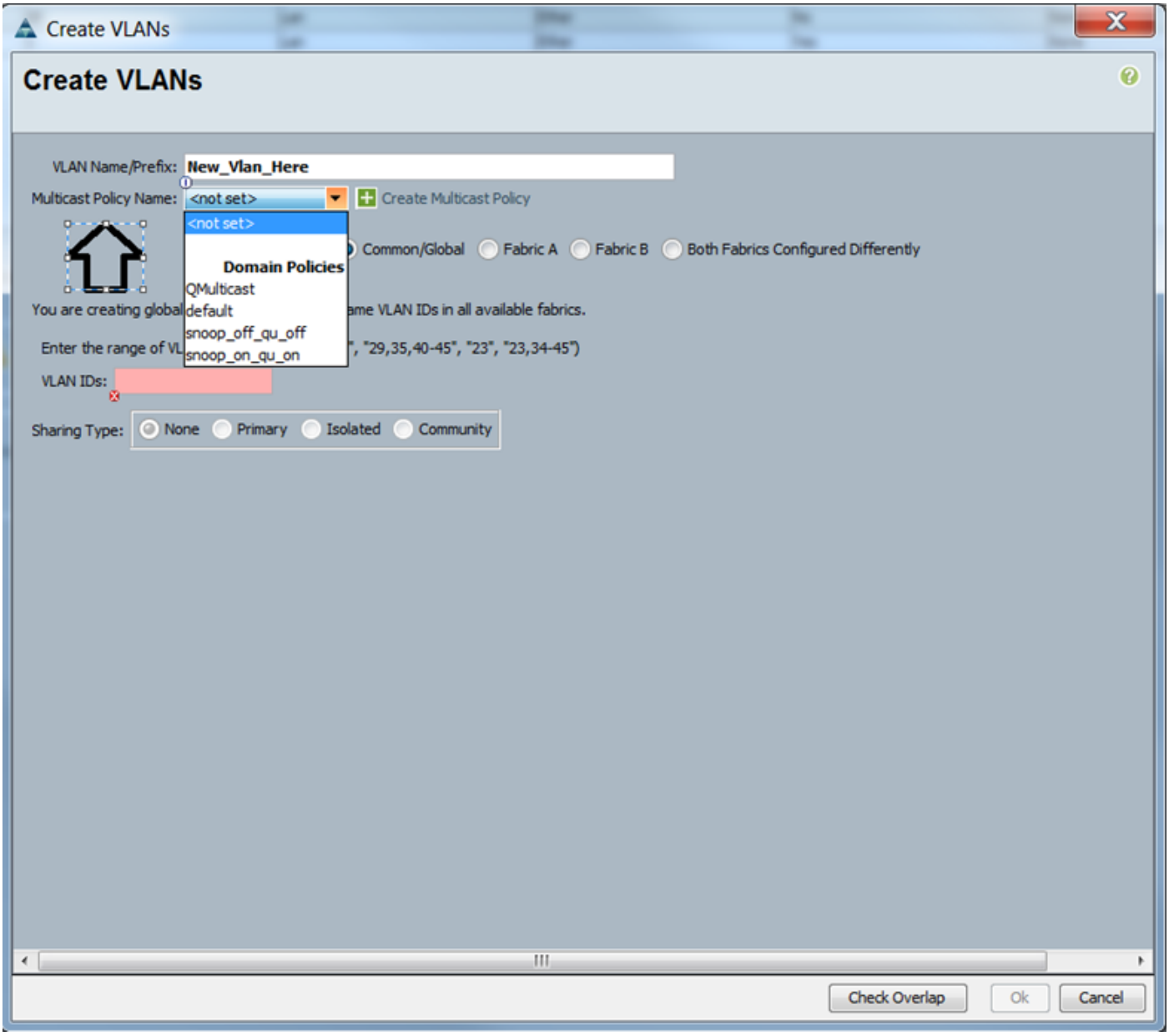
Step 3. You are then presented with this:

Provide a Name and configure the IGMP Snooping and Snooping Querier states.

Step 4. If you attempt to disable IGMP Snooping while the IGMP Snooping Querier is enabled, this throws an error, as this isn’t a valid configuration.

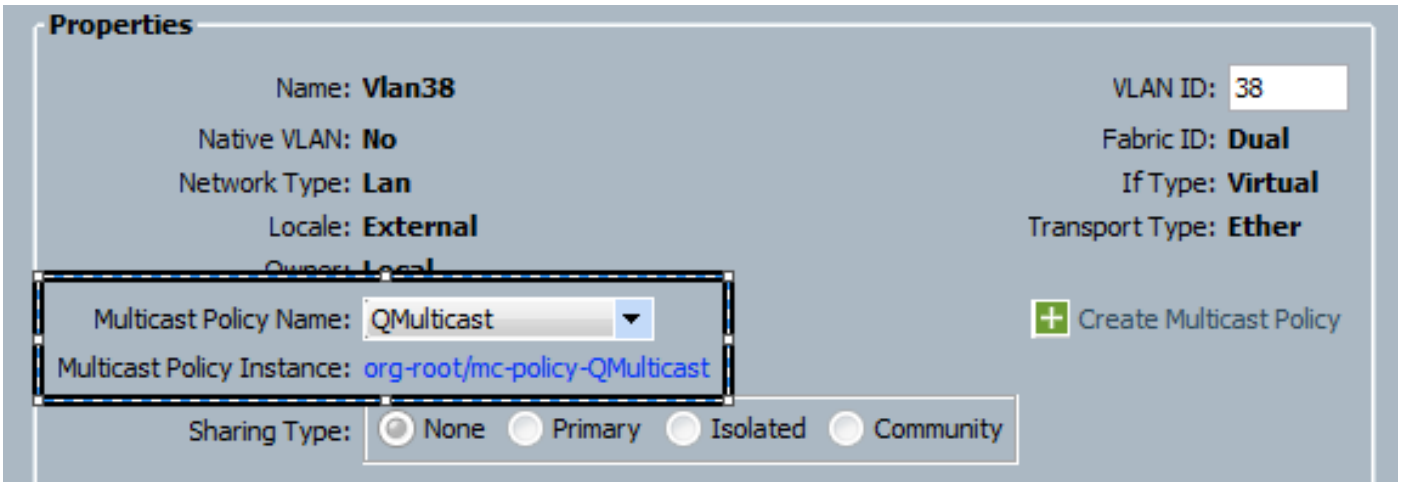


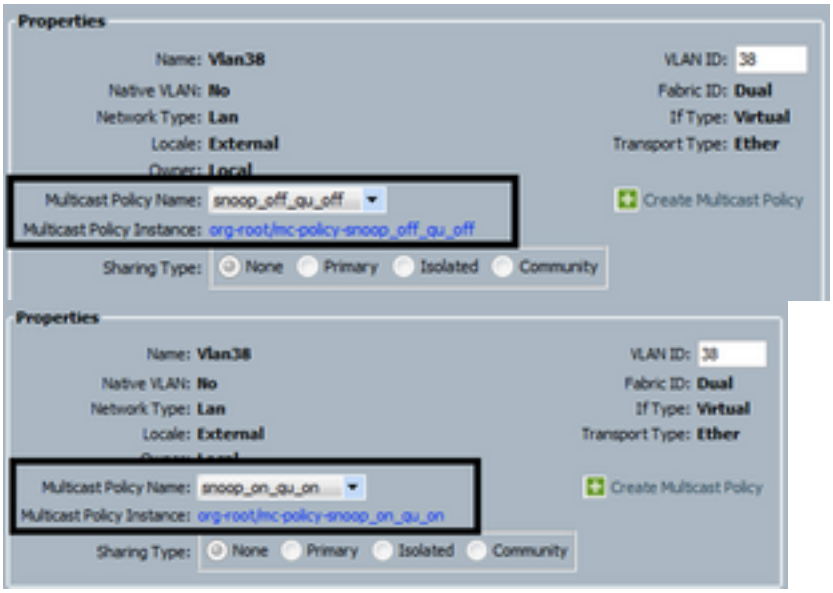
Step 5. During the creation of a new VLAN, now there is an e option to specify Multicast Policy Name.



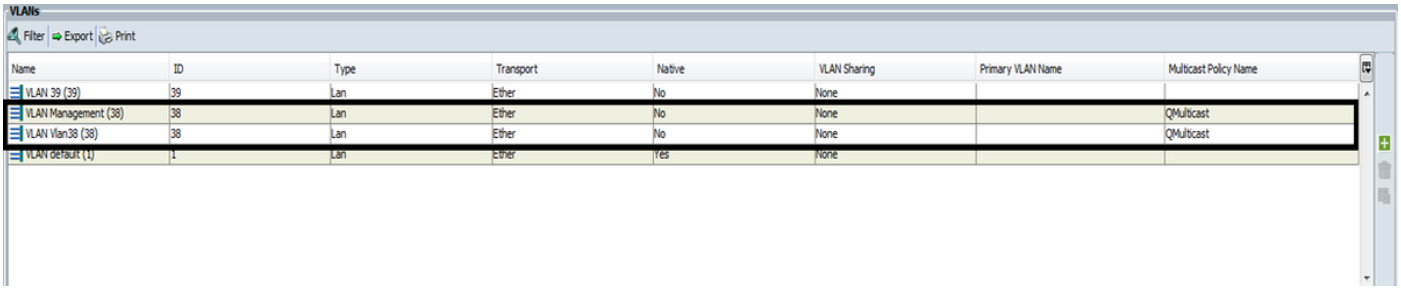
Configuration – Assign

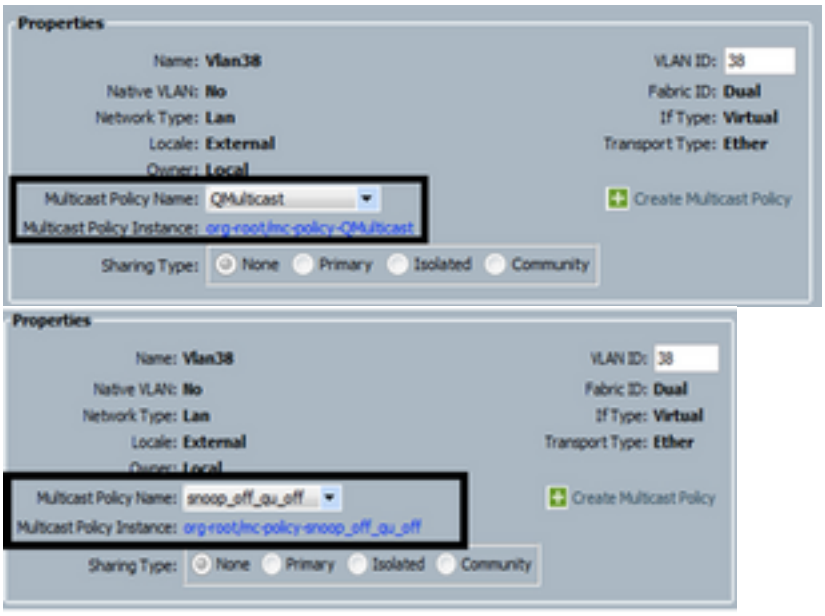
Examples with different policies set on the VLAN. Multicast Policy Name is what you configure where Multicast Policy Instance is actually being used by the Fabric Interconnects.





If you create multiple VLAN objects, which point to the same VLAN ID, then, when you apply a Multicast policy, it is applied to **all** VLAN objects with the same VLAN ID. The latest Multicast Policy applied is applied to all. Eg: QMulticast changed to Snoop_off_qu_off (Vlan 38).





Creating UCS Multicast Policy via CLI

- Add a new command to create a multicast policy under scope org.

MiniMe-B# scope org

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

- Set properties for multicast policy.

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

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

- New command to view existing multicast policies.

MiniMe-B # scope org

MiniMe-B /org # show mcast-policy

- New command to delete the existing multicast policy.

MiniMe-B # scope org

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

- When you create a VLAN, the user allowed to add an existing multicast policy to the VLAN.

MiniMe-B# scope eth-uplink

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

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

Configuration on Upstream Switch

- On the upstream switch, you must configure the IGMP snooping querier on a specific VLAN and the IGMP snooping querier must match the IP in the UCS multicast policy.

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

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

AGR012-5K-A(config-vlan-config)# ip igmp snooping querier **172.16.38.124**(IP is likely to be different)

Verify

- **Show ip igmp snooping vlan <vlan id>** (This can be done on either the Upstream switch or Fabric Interconnect.)

(UCS snooping command output for VLAN 38 verifies that the querier is configured on the UCSM and the N5k, and it shows that only the querier on the N5k is currently active (as expected). While VLAN 39 is not configured.

```
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>** (This can be done on either the Upstream switch or 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>** (This can be done on either the Upstream switch or Fabric Interconnect.)

- This shows the active ports for multicast and the IGMP querier.

```
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>** (This can be done on either the Upstream switch or 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)
```

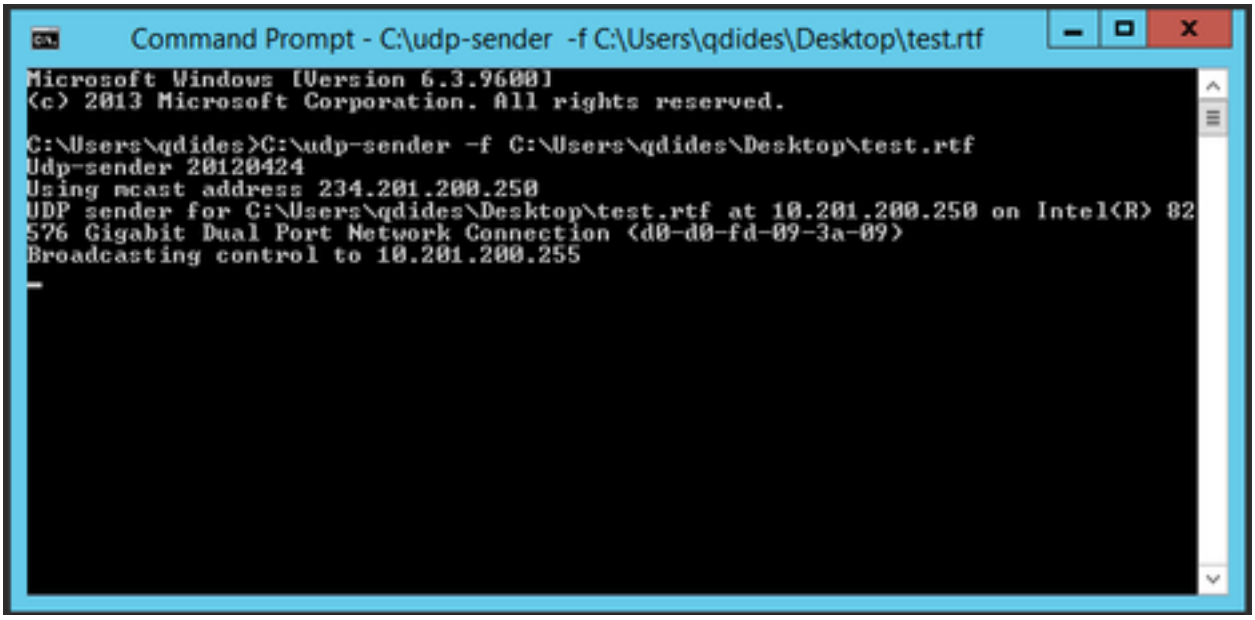
- **AGR012-5K-A# ethanalyzer local interface inbound-low display-filter igmp limit**

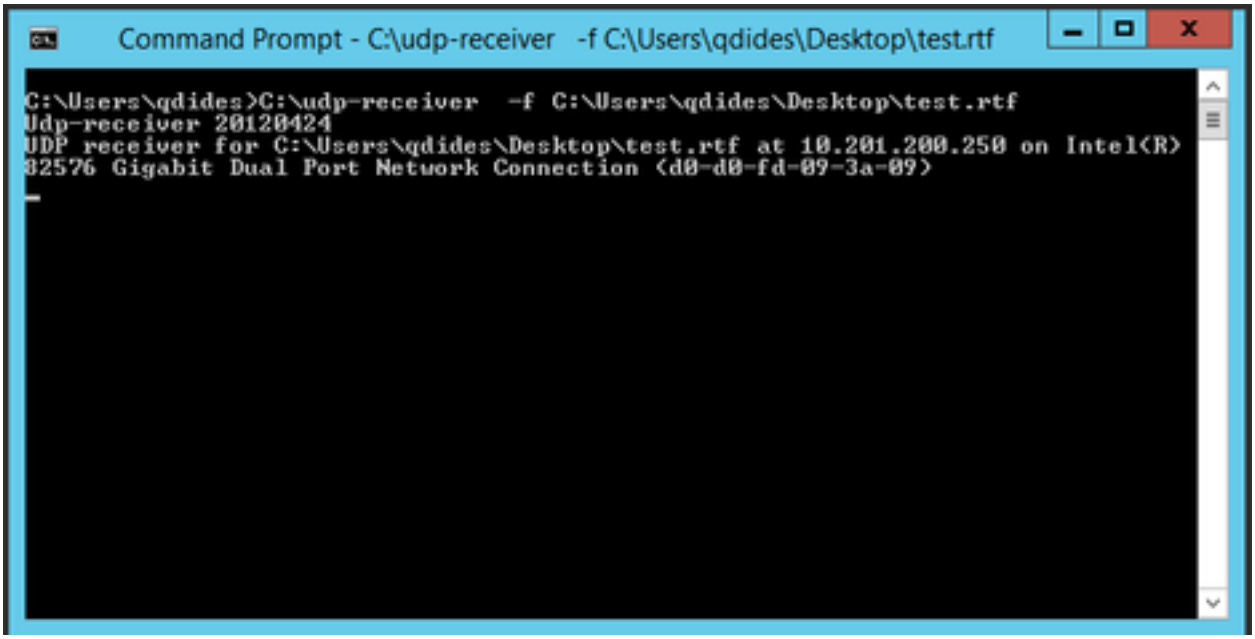
This does not capture actual video stream data, just IGMP data. This tool captures control traffic. (EX; it shows when a host joins or leaves the group.)

```
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

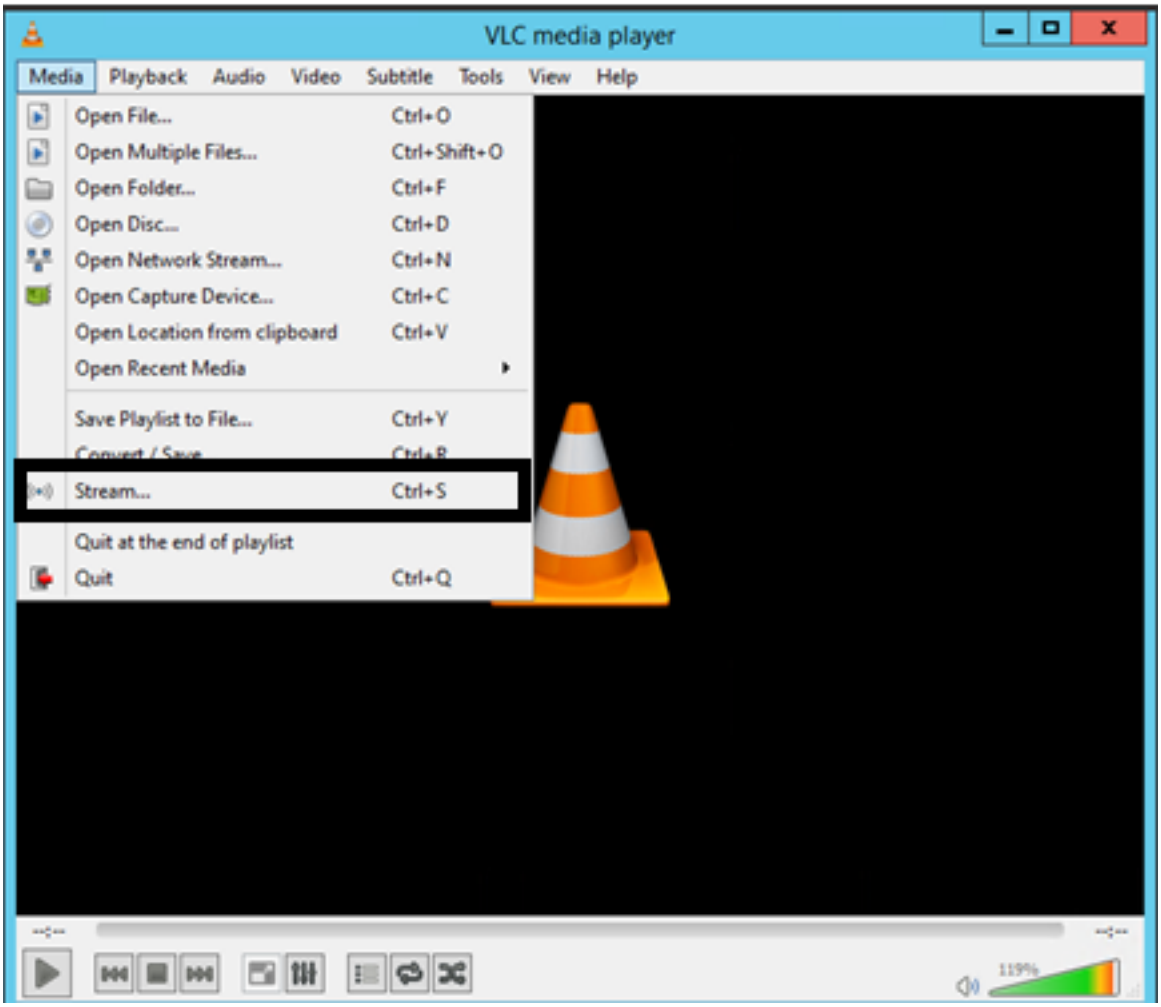
- **UDPCAST (http://www.udpcast.linux.lu/cmd.html)**
- This application is downloaded on two different hosts, sender and receiver. With it, you can generate multicast traffic with a transfer of one file from a source to multiple destinations at once with a single command.

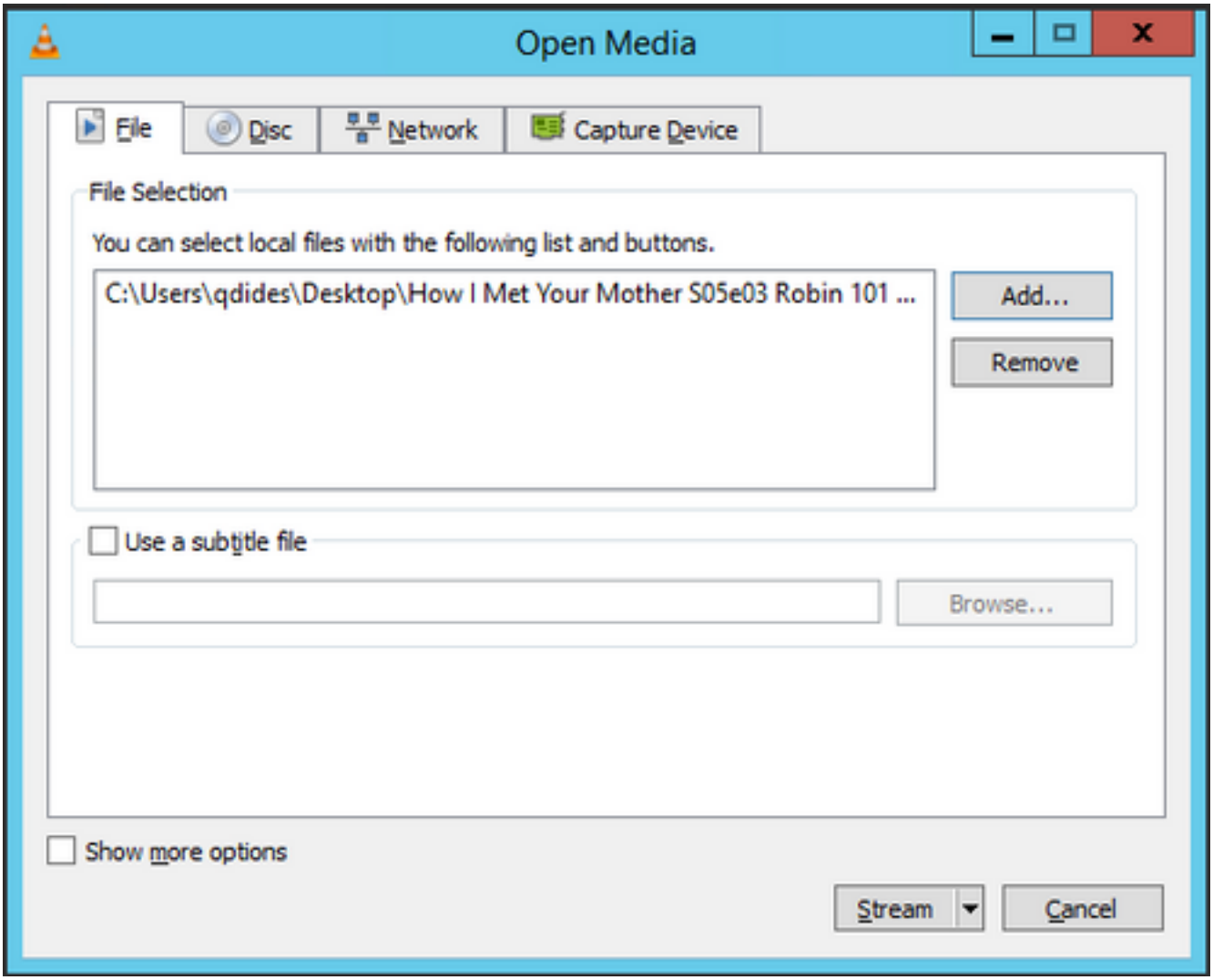


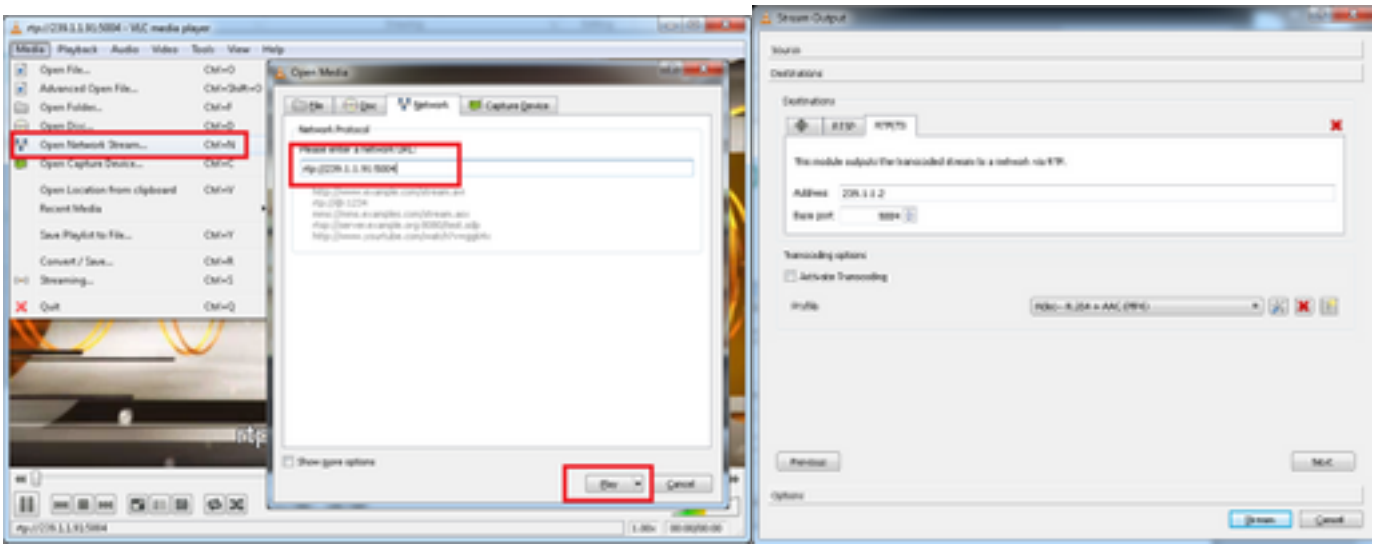


- **VLC (http://www.videolan.org/vlc/index.html)**

(Here are the images that show how to stream on VLC. There is quite a bit of information regarding how to do this process online.)


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





How to Generate IGMP and Multicast Traffic with Iperf?

- Iperf or Jperf is a very useful tool that can generate IGMP and multicast traffic, it can run on Linux and Windows OS.
- Multicast sender CLI.

```
# 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
```

- Multicast receiver CLI.

```
# 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
```

Related Information

- **Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide, Release 5.0(3)N1(1)**
- **Technical Support & Documentation - Cisco Systems**