在UCS上配置组播

目录

简介

本文档介绍在统一计算系统(UCS)内配置组播所需的过程。 组播(MCAST)是指能够通过网络同时向多个用户发送数据（一对多或多对多组通信）。 互联网组管理协议(IGMP)是组播的关键组件。 IGMP的主要用途是允许主机将其接收组播流量的愿望传达给本地网络上的IP组播路由器。作为回报，允许IP组播路由器“加入”指定的组播组，并开始将组播流量转发到网段到主机。

先决条件

要求

Cisco 建议您了解以下主题：

- UCS
- Nexus组播交换

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 交换矩阵互联 — 6100 / 6200
- UCSM（统一计算系统管理器）
- 上游交换机(EX;Nexus 5000)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在Unified Computing System Manager(UCS-M)版本2.1之前：

- UCS上的组播默认启用IGMP监听，且无法禁用。(思科技术支持中心(TAC)可以通过调试插件禁用)。
- UCS交换矩阵互联没有IGMP查询器功能；这要求您在上游L2网络中的设备上启用查询器功能。
- 要使此功能正常运行，您需要VLAN中的组播路由器或VLAN中的IGMP查询器。

Del Mar 2.1注释：

- 默认情况下，IGMP监听已启用，网络管理员应仔细检查禁用IGMP监听的任何要求以及可能遇到的有害性能。
- IGMP监听配置仅可用于每个VLAN并且可以配置，您无法全局启用或禁用IGMP监听。
- 终端主机模式(EHM)和交换机模式均支持禁用IGMP监听的功能。
- 不支持网络组上的组播策略（Del Mar中的另一项新功能）。

交换矩阵互联细节：

- 对于6100系列交换矩阵互联(FI)，所有VLAN只能使用默认组播策略；但是，用户可以修改此默认策略的IGMP监听/查询器状态。如果配置任何其他组播策略，则会引发错误“对于X交换矩阵互联中的VLAN，仅支持默认组播策略”。
- 仅6200个FI支持更改特定VLAN的组播策略（更改为默认组播策略以外的策略），6100不支持。6100个FI在其VLAN上不能有不同的组播策略的原因是Gatos ASIC的限制。此限制在具有Carmel ASIC的6200 FI上不存在。

UCS组播配置选项

终端主机模式下的配置

启用IGMP监听/启用IGMP查询器

- 它只将查询发送到刀片。它不向上游网络发送IGMP查询。

- FI不会向上游交换机发送IGMP查询，因为这与网络中终端主机模式的角色相冲突。这可能导致不需要的组播流量（控制和数据）发送到FI。这就是为什么决定让EHM FI负责将IGMP查询仅传输到其刀片的原因。
- 因此，需要以下其中一项已批准配置：

批准的配置：

在上游交换机上配置启用IGMP监听的IGMP查询器，或在上游交换机上禁用IGMP监听以泛洪组播流量。或者，将FI更改为交换机模式。

启用IGMP监听/禁用IGMP查询器

- 默认模式，与Del Mar之前的版本相同。
- 需要：VLAN上游交换机中的IGMP查询器启用IGMP监听或VLAN中的组播路由器。

禁用IGMP监听/禁用IGMP查询器

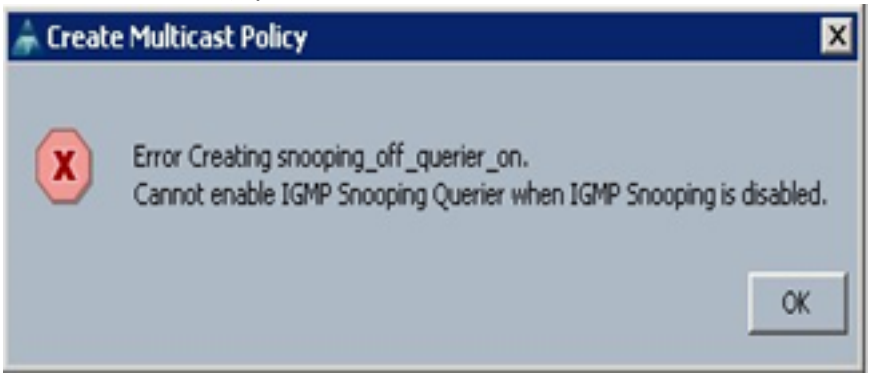
- FI泛洪VLAN中的组播流量。
- 需要批准的配置之一才能成功运行：

批准的配置：

上游交换机可以启用IGMP监听或在上游交换机上禁用它以泛洪组播流量。

禁用IGMP监听/启用IGMP查询器

- 此配置无效。
- UCSM已正确阻止此操作。



交换模式下的配置

启用IGMP监听/启用IGMP查询器

- FI将IGMP查询转发到上游网络。
- 上游交换机了解在FI上配置的IGMP查询器，然后构建MCAST流量并将其转发到FI。
- 需要：启用IGMP监听或禁用监听的上游交换机泛洪组播流量。

启用IGMP监听/禁用IGMP查询器

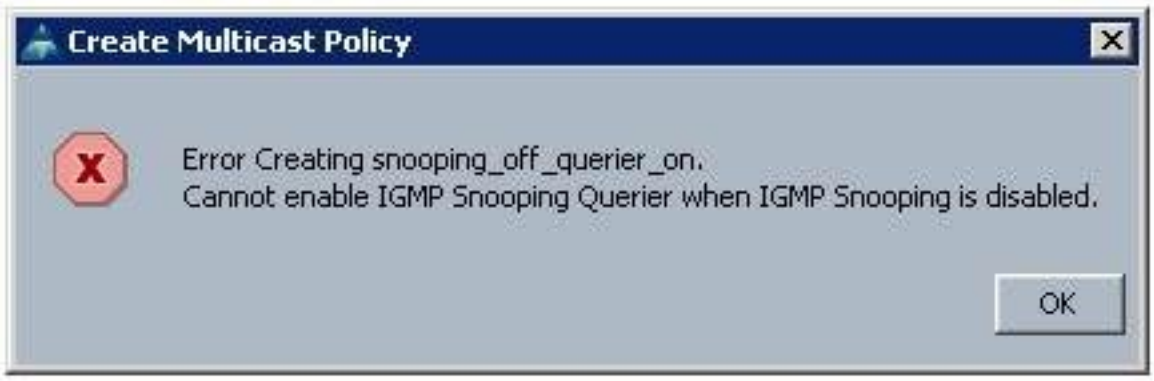
- 默认模式，与Del Mar版本相同。
- 需要：VLAN上游交换机中的IGMP查询器，启用IGMP监听或VLAN中的组播路由器。

禁用IGMP监听/禁用IGMP查询器

- FI泛洪VLAN中的组播流量。
- 需要：启用或禁用IGMP监听的上游交换机泛洪组播流量。

禁用IGMP监听/启用IGMP查询器

- 此配置无效。
- UCSM已正确阻止此操作。



UCS和上游配置

配置 — 创建

IGMP监听在VLAN上可用，在接口级别不可用。从UCSM中，可以在命名VLAN上配置组播策略。

1.在LAN> LAN > Policies> root**下添**加新的**组播策略节点**。

2.支持创建、修改和删除组播策略。

3.当创建VLAN时，可以选择现有组播策略。

4.支持将现有组播策略与已创建的VLAN相连。

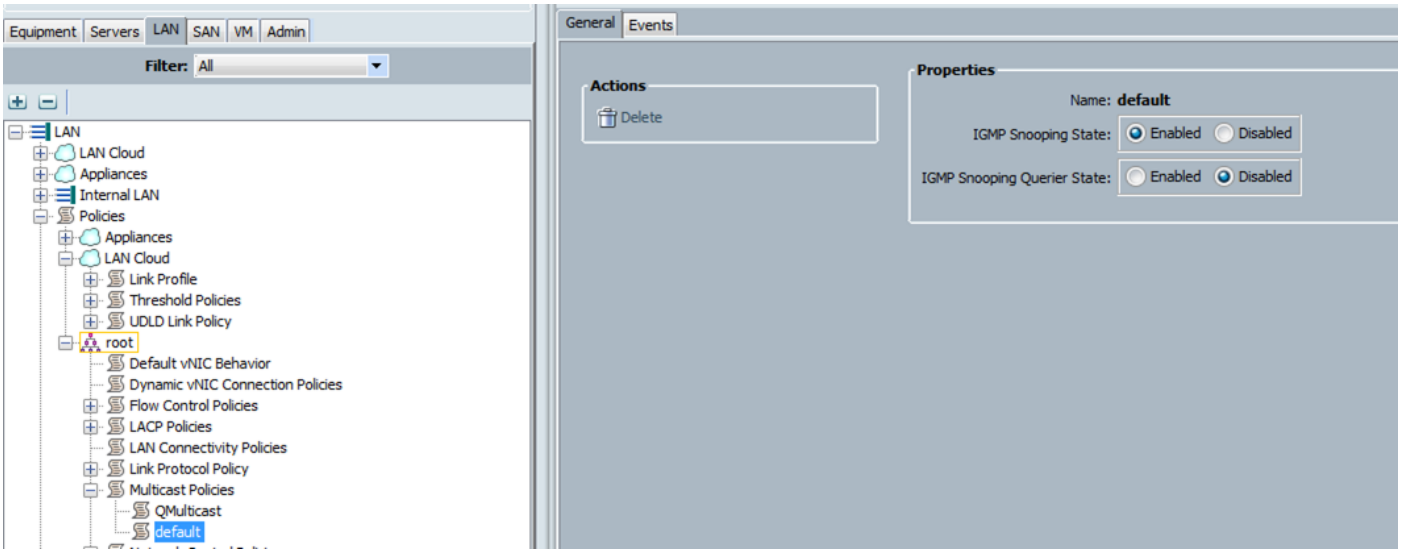
> **注意：**组播策略仅在根策略树下，不能在子组织下创建单个策略。

默认策略

默认组播策略与2.1 Del Mar版本之前的交换矩阵互联行为保持一致：

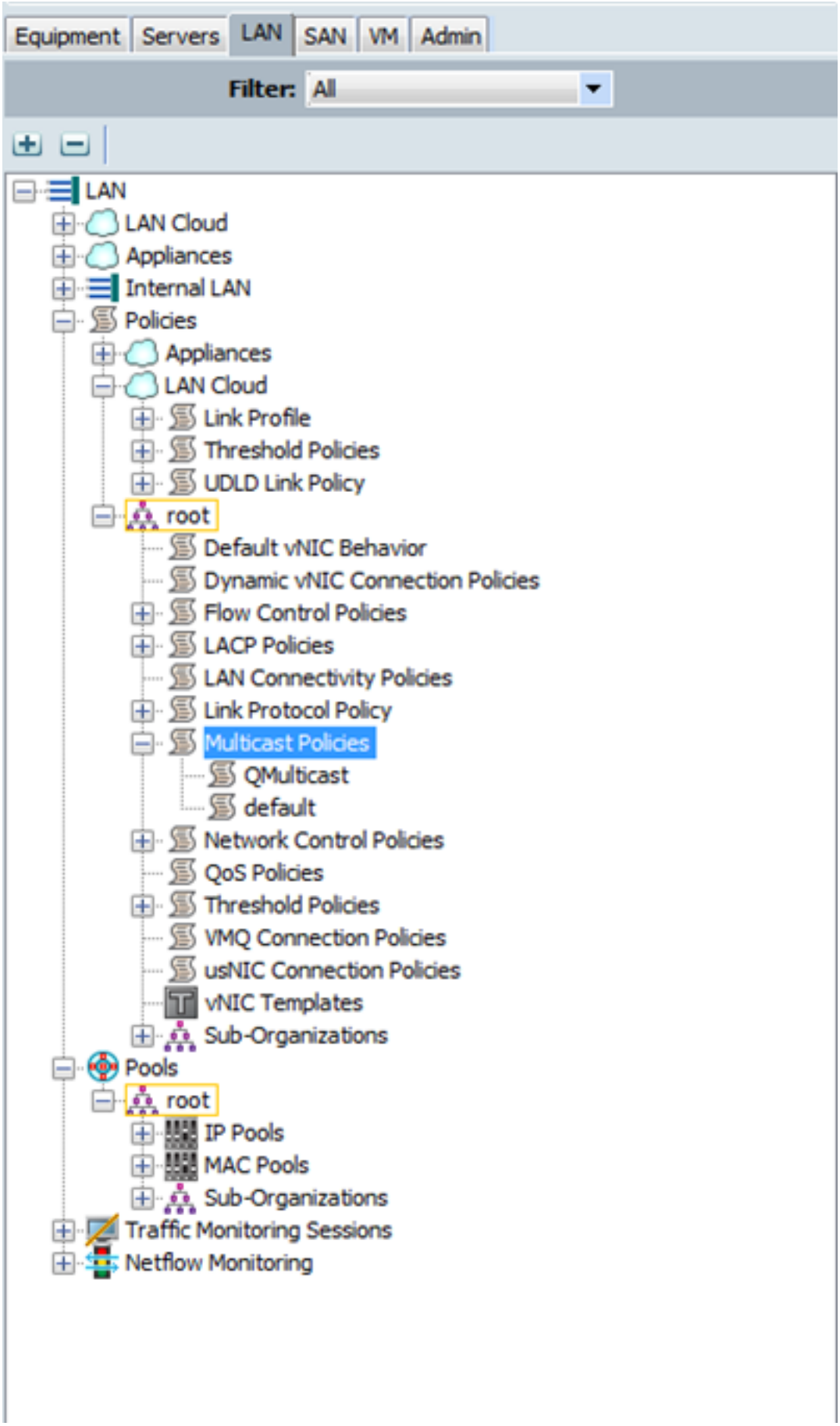
IGMP 侦听- 启用

IGMP查询器 — 禁用



配置 — 创建（续）

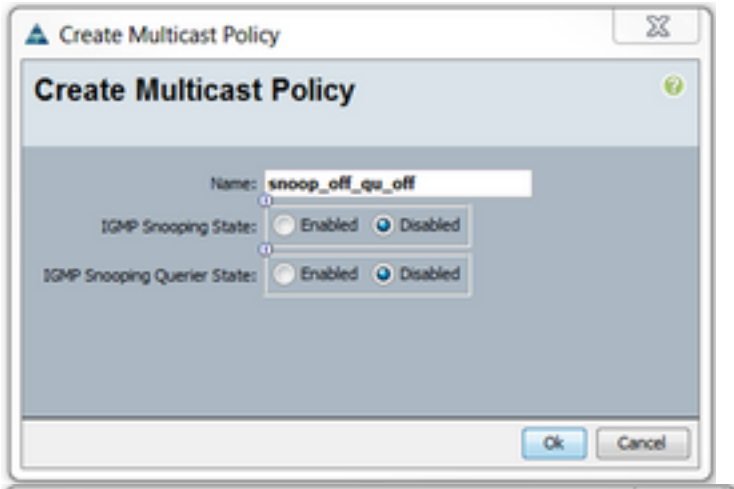
步骤1.在LAN > LAN > **Policies >** root下添**加新的组播策略节点。**

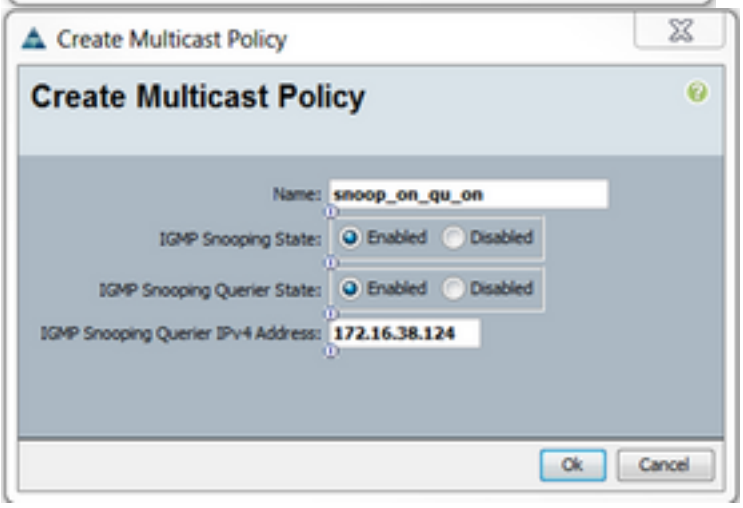


步骤2.右键单击Multicast Policies，然后单击Create Multicast Policy。

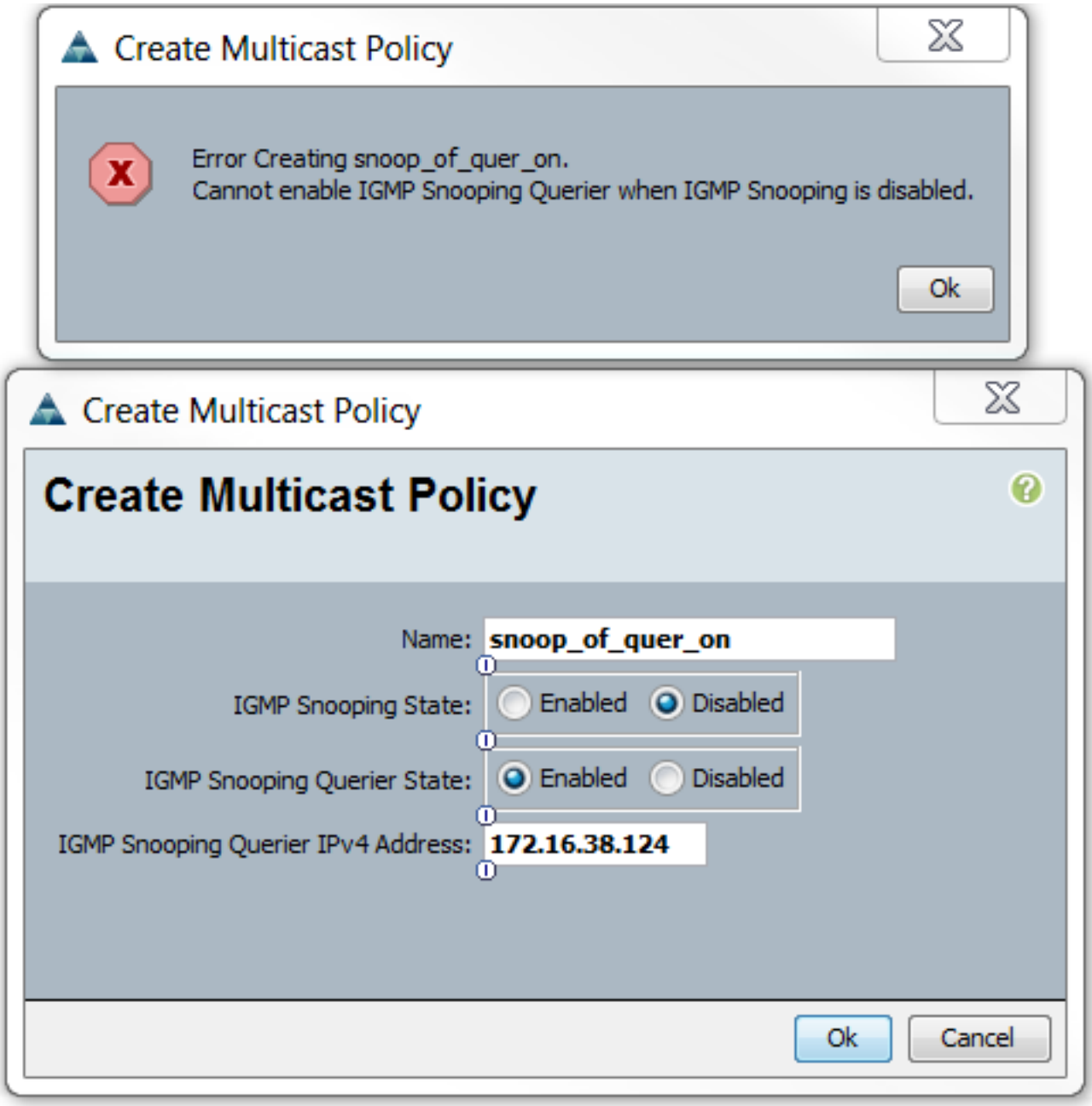
步骤3.然后，您将看到：

提供名称并配置IGMP监听和监听查询器状态。

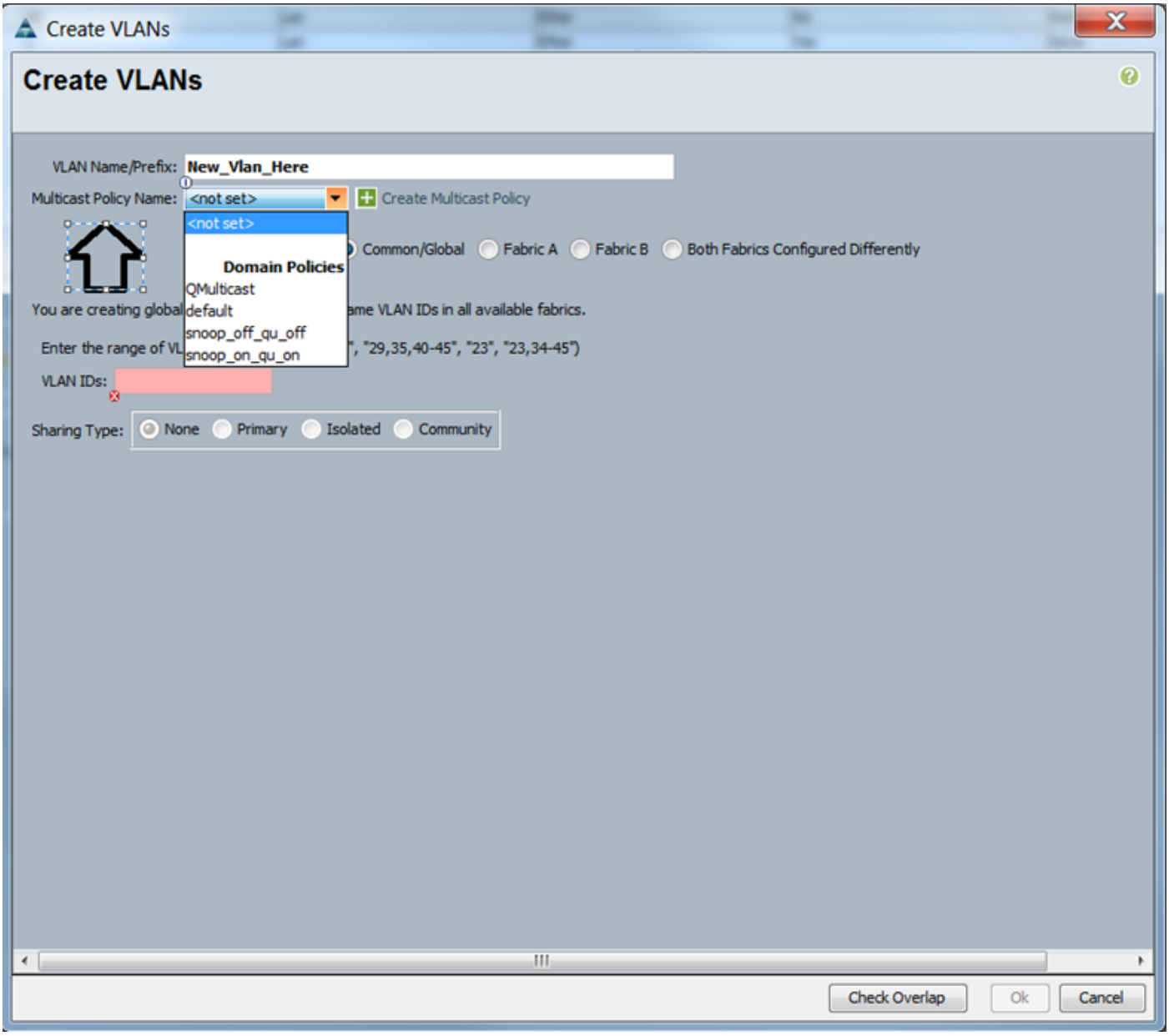




步骤4.如果在启用IGMP监听查询器时尝试禁用IGMP监听，这会引发错误，因为这不是有效配置。

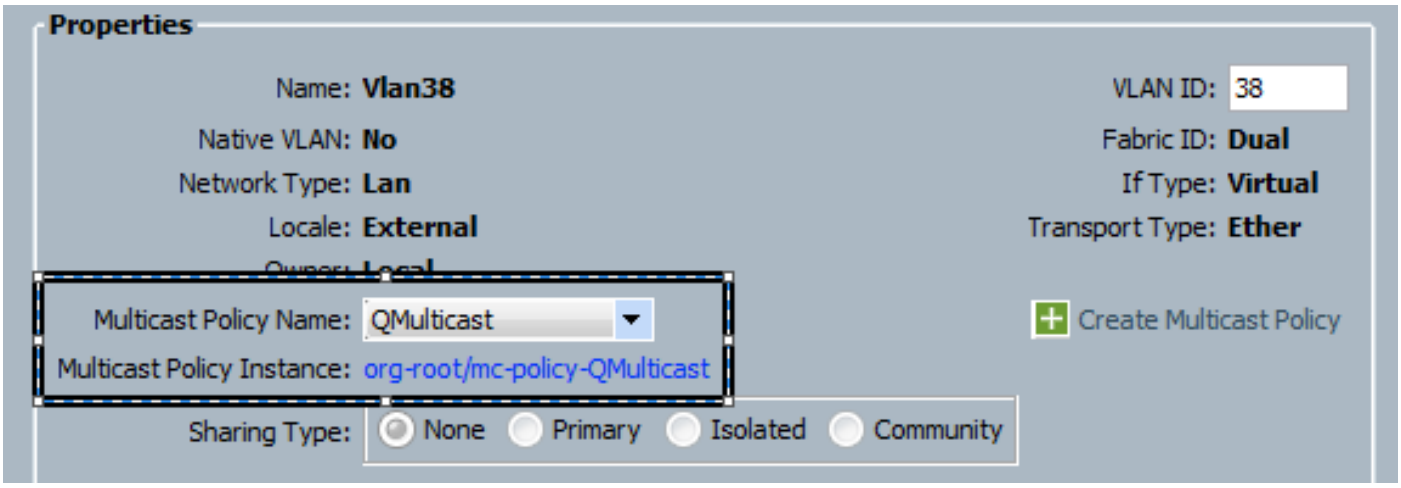


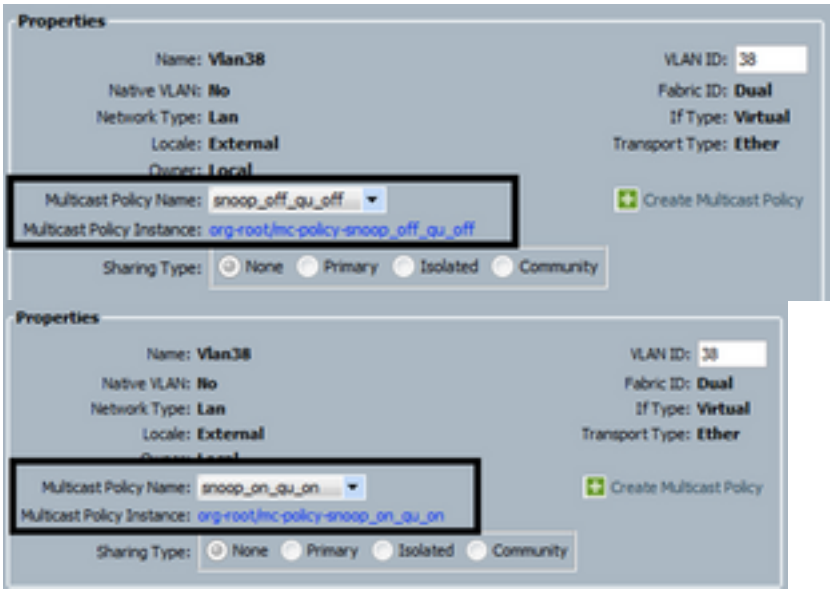
步骤5.在创建新VLAN期间，现在有e选项可指定组播策略名称。



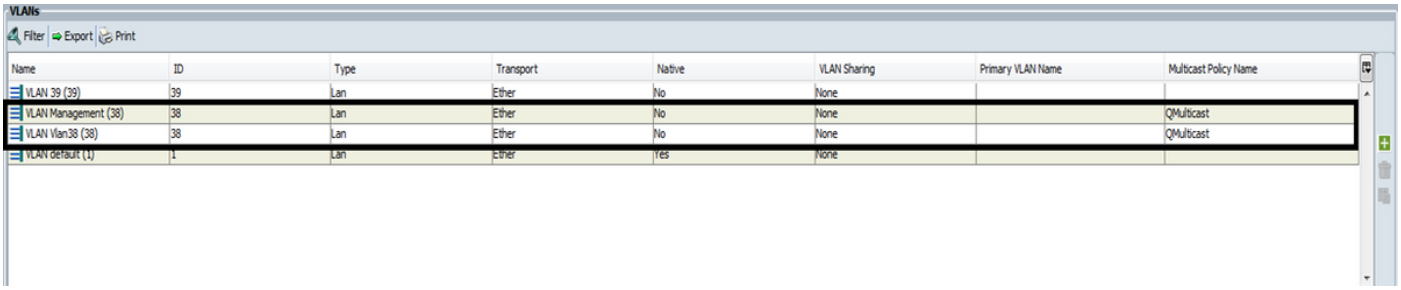
配置 — 分配

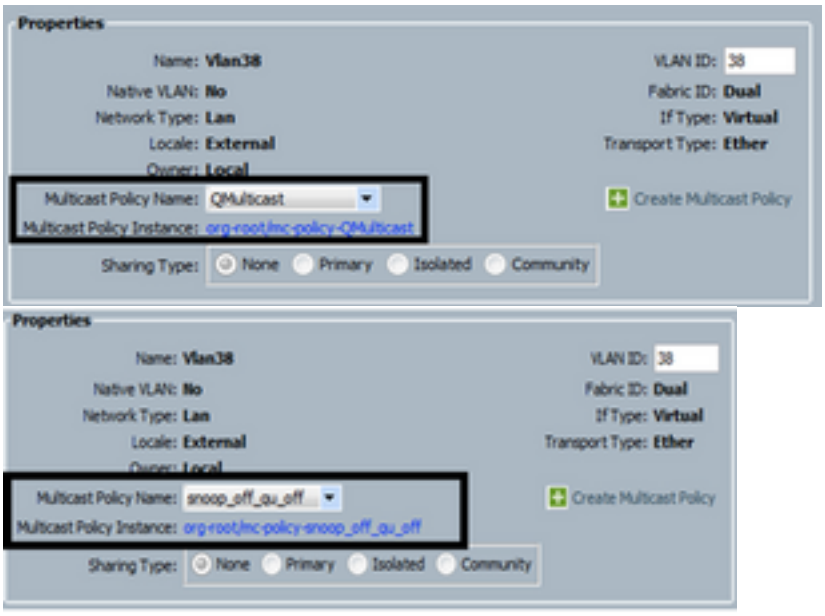
在VLAN上设置不同策略的示例。组播策略名称是您配置的组播策略实例实际被交换矩阵互联使用的位置。





如果创建多个VLAN对象，这些对象指向相同的VLAN ID，则当应用组播策略时，它将应用于具有相同VLAN ID的**所有**VLAN对象。应用的最新组播策略应用于所有。例如：QMulticast更改为Snoop_off_qu_off(Vlan 38)。





通过CLI创建UCS组播策略

- 添加新命令以在范围组织下创建组播策略。

MiniMe-B#范围组织

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

- 设置组播策略的属性。

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

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

- 查看现有组播策略的新命令。

MiniMe-B #范围组织

MiniMe-B /org # show mcast-policy

- 删除现有组播策略的新命令。

MiniMe-B #范围组织

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

- 创建VLAN时，用户允许向VLAN添加现有组播策略。

MiniMe-B#范围eth-uplink

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

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

上游交换机上的配置

- 在上游交换机上，您必须在特定VLAN上配置IGMP监听查询器，并且IGMP监听查询器必须与UCS组播策略中的IP匹配。

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

AGR012-5K-A(config-vlan)# vlan配置38

AGR012-5K-A(config-vlan-config)# ip igmp snooping querier 172.16.38.124（IP可能不同）

验证

- **Show ip igmp snooping vlan <vlan id>**（这可以在上游交换机或交换矩阵互联上完成。）

(VLAN 38的UCS监听命令输出验证查询器是否在UCSM和N5k上配置，并且显示只有N5k上的查询器当前处于活动状态（如预期）。 而未配置VLAN 39。

```
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>（这可以在上游交换机或交换矩阵互联上完成。）

```
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#
```

- 显示ip igmp监听组vlan <vlan id>（这可以在上游交换机或交换矩阵互联上完成。）
- 这显示组播和IGMP查询器的活动端口。

```
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
```

- 显示ip igmp snooping statistics vlan <vlan id>（这可以在上游交换机或交换矩阵互联上完成。）

```
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)
```

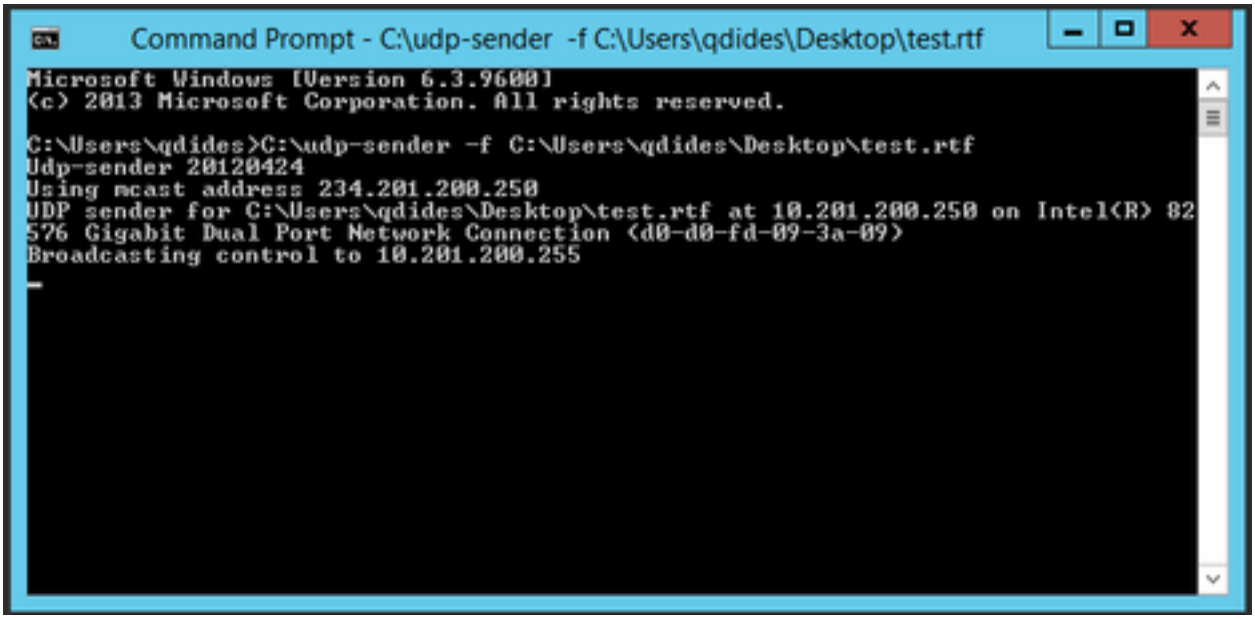
- AGR012-5K-A# ethanalyzer local interface inbound-low display-filter igmp 限制

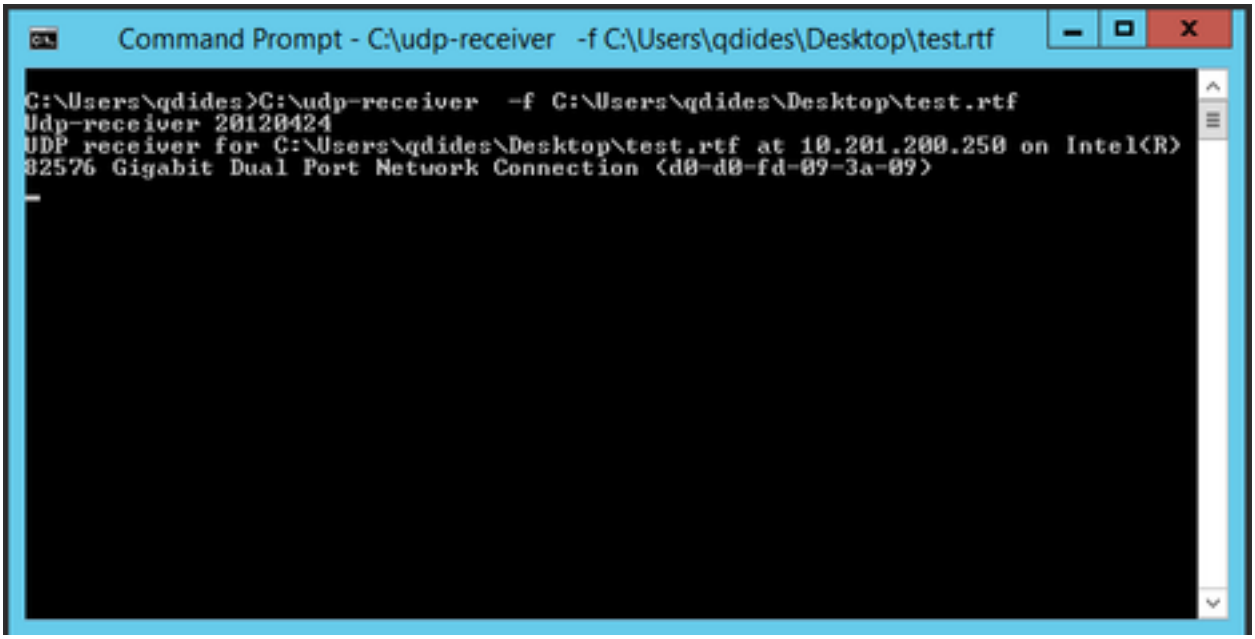
这不会捕获实际视频流数据，只捕获IGMP数据。此工具可捕获控制流量。(例如：它显示主机何时加入或离开组。)

```
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
```

故障排除

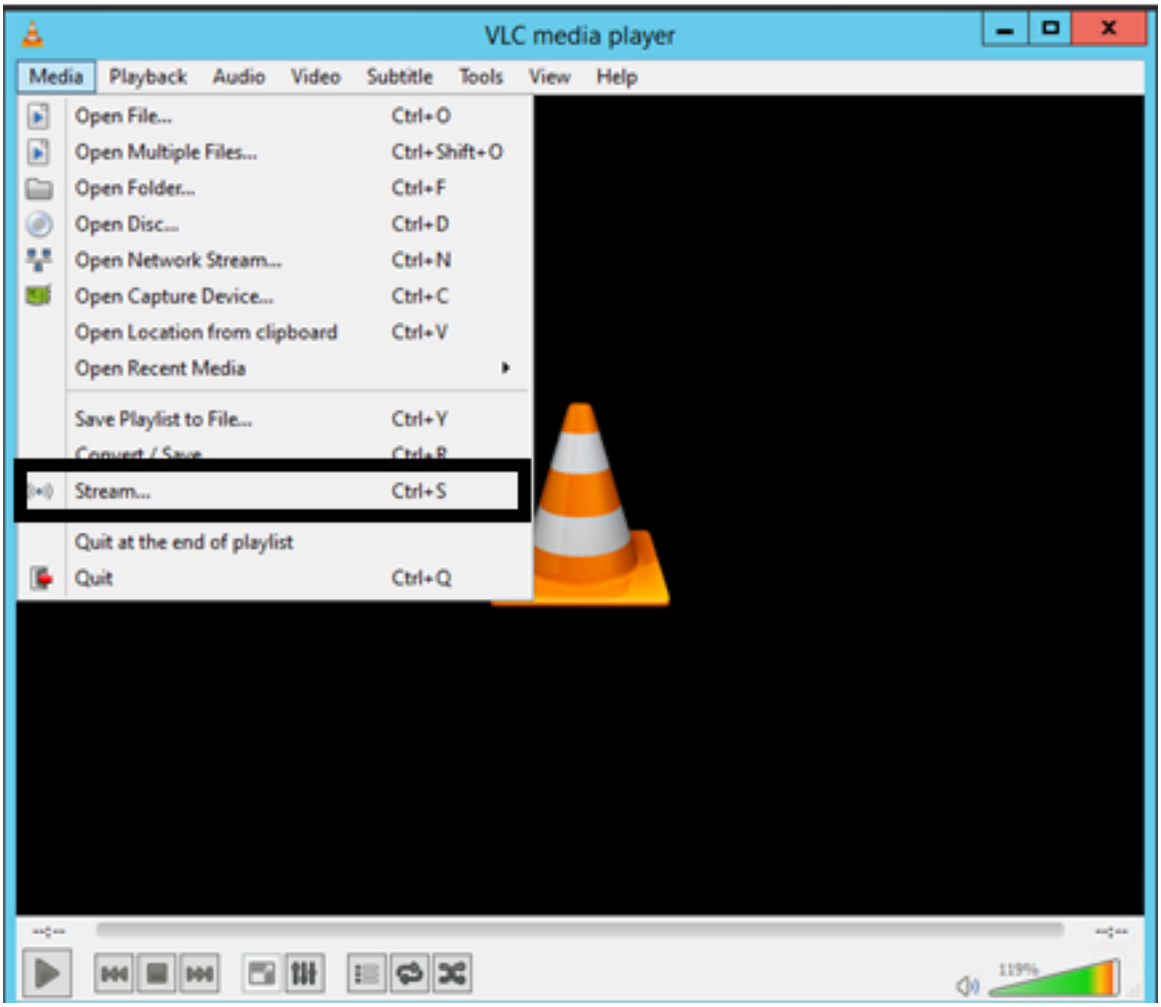
- UDPCAST(http://www.udpcast.linux.lu/cmd.html)
- 此应用程序下载于发送方和接收方两台不同的主机。借助它，您可以通过使用单个命令同时将一个文件从源传输到多个目标来生成组播流量。

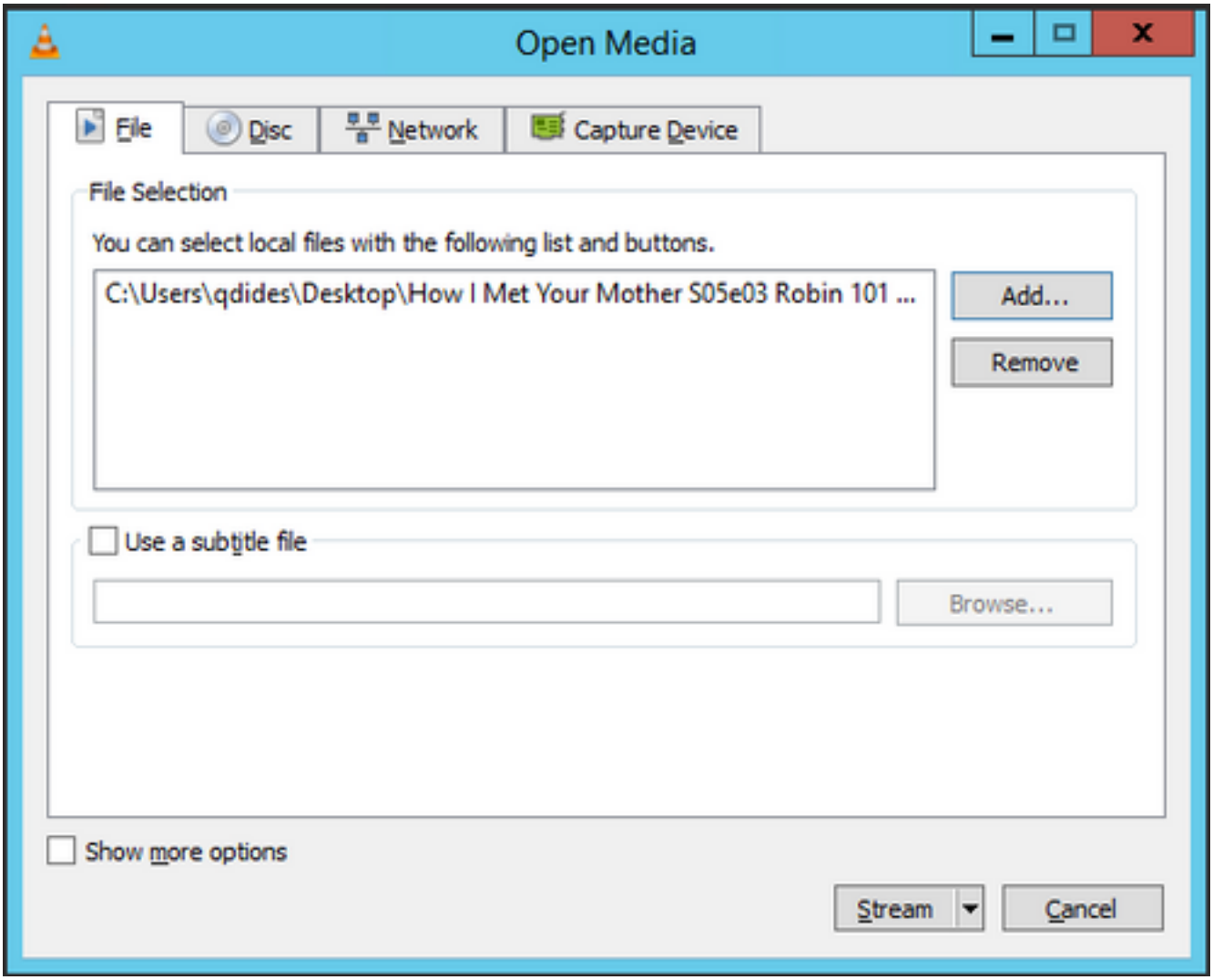


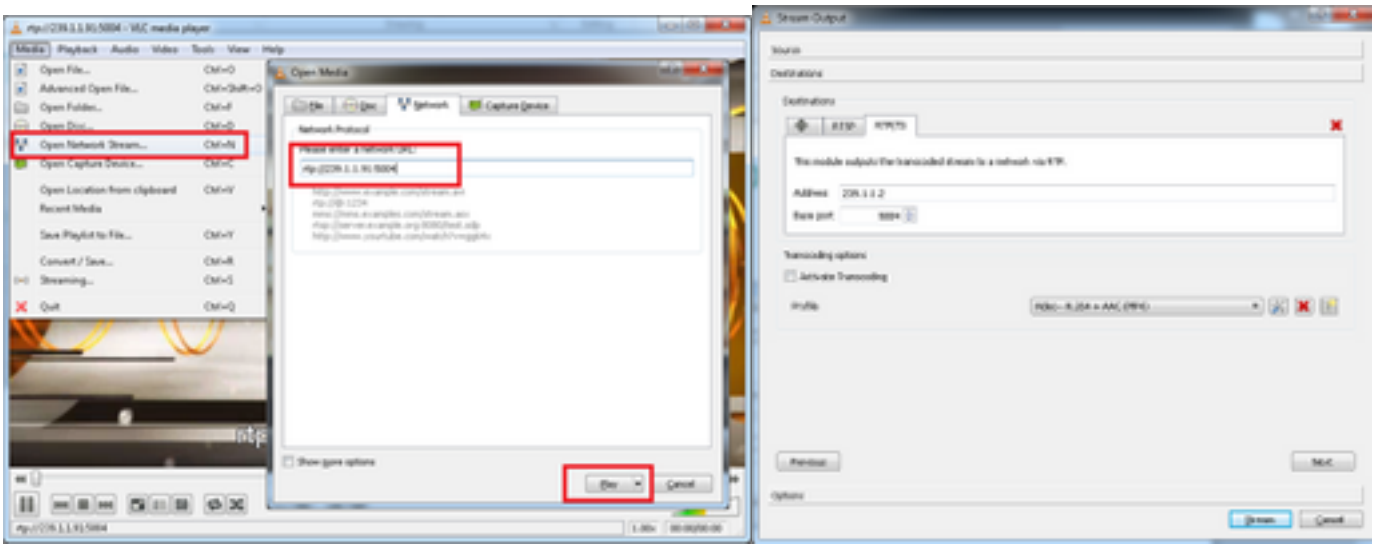


- VLC(http://www.videolan.org/vlc/index.html)

(以下是显示如何在VLC上流的图像。关于如何在线完成此过程，有很多信息。)


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





如何使用Iperf生成IGMP和组播流量？

- Iperf或Jperf是一个非常有用的工具，可以生成IGMP和组播流量，它可以在Linux和Windows操作系统上运行。
- 组播发件人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
```

- 组播接收器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
```

相关信息

- Cisco Nexus 5000系列NX-OS组播路由配置指南，版本5.0(3)N1(1)
- 技术支持和文档 - Cisco Systems