Konfigurieren von Multicast auf dem UCS

Inhalt

Einführung

In diesem Dokument wird das erforderliche Verfahren zur Konfiguration von Multicast in Unified Computing Systems (UCS) beschrieben. Multicast (MCAST) ist die Fähigkeit, Daten über ein Netzwerk gleichzeitig an mehrere Benutzer zu senden (One-to-Many- oder Many-Gruppenkommunikation). Internet Group Management Protocol (IGMP) ist eine wichtige Komponente von Multicast. Der Hauptzweck von IGMP besteht darin, Hosts zu ermöglichen, ihren Wunsch nach Empfang von Multicast-Datenverkehr an die IP-Multicast-Router im lokalen Netzwerk zu kommunizieren. Dies wiederum ermöglicht es dem/den IP-Multicast-Router, der angegebenen Multicast-Gruppe beizutreten und den Multicast-Datenverkehr an das Netzwerksegment zum Host weiterzuleiten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- UCS
- Nexus Multicast-Switching

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Fabric Interconnect - 6100/6200
- UCSM (Unified Computing System Manager)
- Upstream-Switch (EX; Nexus 5000)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

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

- Bei Multicast im UCS ist IGMP-Snooping standardmäßig aktiviert. Diese Funktion kann nicht deaktiviert werden. (Cisco Technical Assistance Centers (TAC) können über das Debug-Plugin deaktiviert werden.)
- Die UCS Fabric Interconnects verfügen über keine IGMP Querier-Funktionalität. Dazu müssen Sie die Abfragefunktion auf einem Gerät im Upstream-L2-Netzwerk aktivieren.
- Hierfür ist ein Multicast-Router im VLAN oder ein IGMP Querier im VLAN erforderlich.

Hinweise zu Dell März 2.1:

- Standardmäßig ist IGMP-Snooping aktiviert. Netzwerkadministratoren sollten alle Anforderungen zur Deaktivierung von IGMP-Snooping und die möglicherweise auftretende nachteilige Leistung sorgfältig prüfen.
- Die IGMP-Snooping-Konfiguration ist nur auf VLAN-Basis verfügbar und konfigurierbar. IGMP-Snooping kann nicht global aktiviert oder deaktiviert werden.
- Die Möglichkeit, IGMP-Snooping zu deaktivieren, wird sowohl im End-Host-Modus (EHM) als auch im Switch-Modus unterstützt.
- Keine Unterstützung für Multicast-Richtlinien in Netzwerkgruppen (eine weitere neue Funktion in Del Mar).

Fabric Interconnect-Spezifikationen:

- Bei einem Fabric Interconnect der Serie 6100 (FI) können alle VLANs nur die standardmäßige Multicast-Richtlinie verwenden. Der Benutzer kann jedoch die IGMP-Snooping-/Querier-

Zustände dieser Standardrichtlinie ändern. Wenn Sie eine andere Multicast-Richtlinie konfigurieren, wird der Fehler "Für VLANs in X Fabric Interconnect wird nur die Standard-Multicast-Richtlinie unterstützt." ausgelöst.
- Die Änderung der Multicast-Richtlinie für ein bestimmtes VLAN (in eine andere Richtlinie als die standardmäßige Multicast-Richtlinie) wird nur für 6200 FIs und NICHT für 6100 unterstützt. Der Grund dafür, dass die 6100 FIs keine unterschiedlichen Multicast-Richtlinien für ihre VLANs haben können, liegt in einer Beschränkung im Gatos ASIC. Diese Einschränkung gilt nicht für die 6200 FIs mit Carmel ASICs.

UCS Multicast-Konfigurationsoptionen

Konfiguration im End-Host-Modus

IGMP-Snooping aktiviert/IGMP Querier aktiviert

- Es sendet nur die Abfragen an die Blades. IGMP-Abfragen werden nicht an das Upstream-Netzwerk gesendet.
- Die FIs senden die IGMP-Abfragen nicht an den Upstream-Switch, da dies der Rolle des End-Host-Modus im Netzwerk widerspricht. Dies kann zu unerwünschtem Multicast-Datenverkehr (sowohl Steuerungs- als auch Datenverkehr) führen, der an die FIs gesendet wird. Aus diesem Grund wurde entschieden, dass EHM FIs für die Übertragung von IGMP-Abfragen nur an ihre Blades zuständig sind.
- Daher benötigen Sie eine der genehmigten Konfigurationen:

Genehmigte Konfigurationen:

Konfigurieren Sie IGMP Querier auf dem Upstream-Switch entweder mit aktiviertem IGMP-Snooping oder deaktivieren Sie IGMP-Snooping auf dem Upstream-Switch, um Multicast-Verkehr zu überfluten. Alternativ können Sie die FIs in den Switch-Modus ändern.

IGMP-Snooping aktiviert/IGMP-Abfrager deaktiviert

- Der Standardmodus entspricht dem der Versionen vor Del Mar.
- Erfordert entweder: IGMP Querier im Upstream-Switch für das VLAN mit aktiviertem IGMP-Snooping oder Multicast-Router im VLAN.

IGMP-Snooping deaktiviert/IGMP-Abfrager deaktiviert

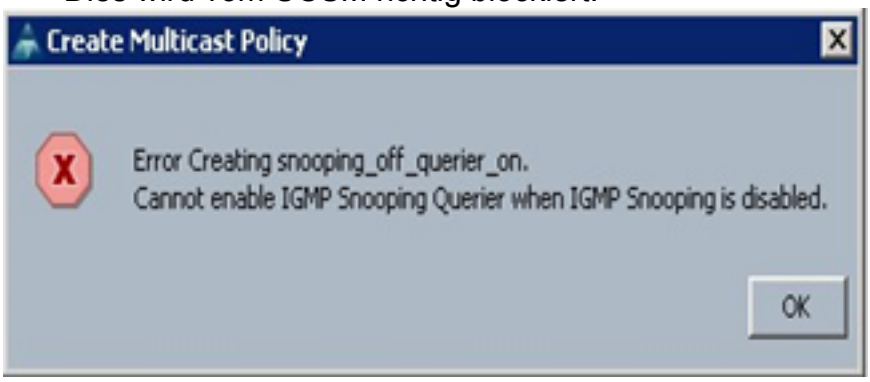
- FIs überfluten den Multicast-Verkehr im VLAN.
- Erfordert die erfolgreiche Ausführung einer der genehmigten Konfigurationen:

Genehmigte Konfigurationen:

Der Upstream-Switch kann IGMP-Snooping aktivieren oder auf dem Upstream-Switch deaktiviert lassen, um Multicast-Datenverkehr zu überfluten.

IGMP-Snooping deaktiviert/IGMP Querier aktiviert

- Dies ist keine gültige Konfiguration.
- Dies wird vom UCSM richtig blockiert.



Konfiguration im Switching-Modus

IGMP-Snooping aktiviert/IGMP Querier aktiviert

- FIs leiten IGMP-Abfragen an das Upstream-Netzwerk weiter.
- Upstream-Switches informieren über IGMP Querier, die auf FIs konfiguriert sind. Anschließend erstellt und leitet er den MCAST-Datenverkehr an FIs weiter.
- Erfordert entweder: Upstream-Switch mit IGMP-Snooping aktiviert oder Snooping deaktiviert, um Multicast-Datenverkehr zu überfluten.

IGMP-Snooping aktiviert/IGMP-Abfrager deaktiviert

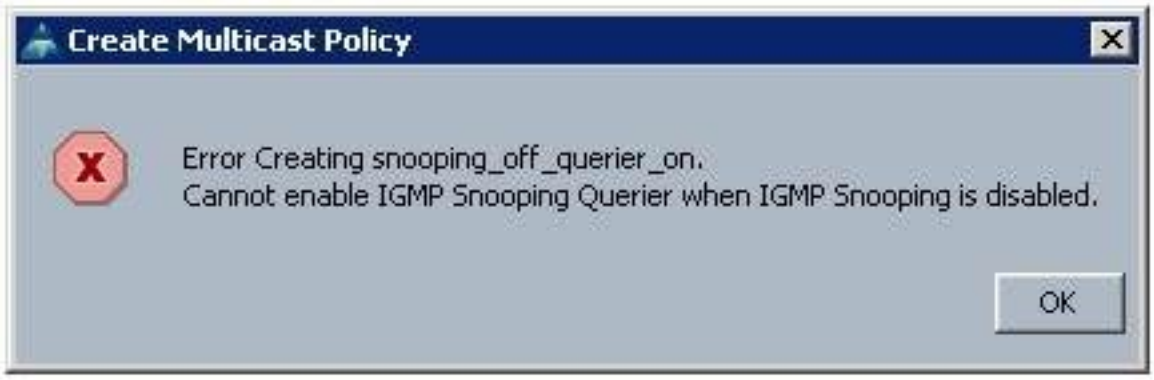
- Der Standardmodus, der mit der Version vor Del Mar identisch ist.
- Erfordert entweder: IGMP Querier im Upstream-Switch für das VLAN mit aktiviertem IGMP-Snooping oder Multicast-Router im VLAN.

IGMP-Snooping deaktiviert/IGMP-Abfrager deaktiviert

- FIs überfluten Multicast-Datenverkehr im VLAN.
- Erfordert entweder: Upstream-Switch mit IGMP-Snooping aktiviert oder deaktiviert, um Multicast-Datenverkehr zu überfluten.

IGMP-Snooping deaktiviert/IGMP Querier aktiviert

- Dies ist keine gültige Konfiguration.
- Dies wird vom UCSM richtig blockiert.



UCS- und Upstream-Konfiguration

Konfiguration - Erstellen

IGMP-Snooping ist auf VLAN-Basis und nicht auf Schnittstellenebene verfügbar. Aus UCSM kann dies mit einer Multicast-Richtlinie in einem benannten VLAN konfiguriert werden.

1. Fügen Sie einen neuen **Multicast Policies-**Knoten unter **LAN> LAN > Policies> root hinzu**.

2. Die Erstellung, Änderung und Löschung von Multicast-Richtlinien wird unterstützt.

3. Beim Erstellen eines VLAN können Sie die vorhandene Multicast-Richtlinie auswählen.

4. Unterstützung für das Anfügen einer vorhandenen Multicast-Richtlinie an ein bereits erstelltes VLAN.

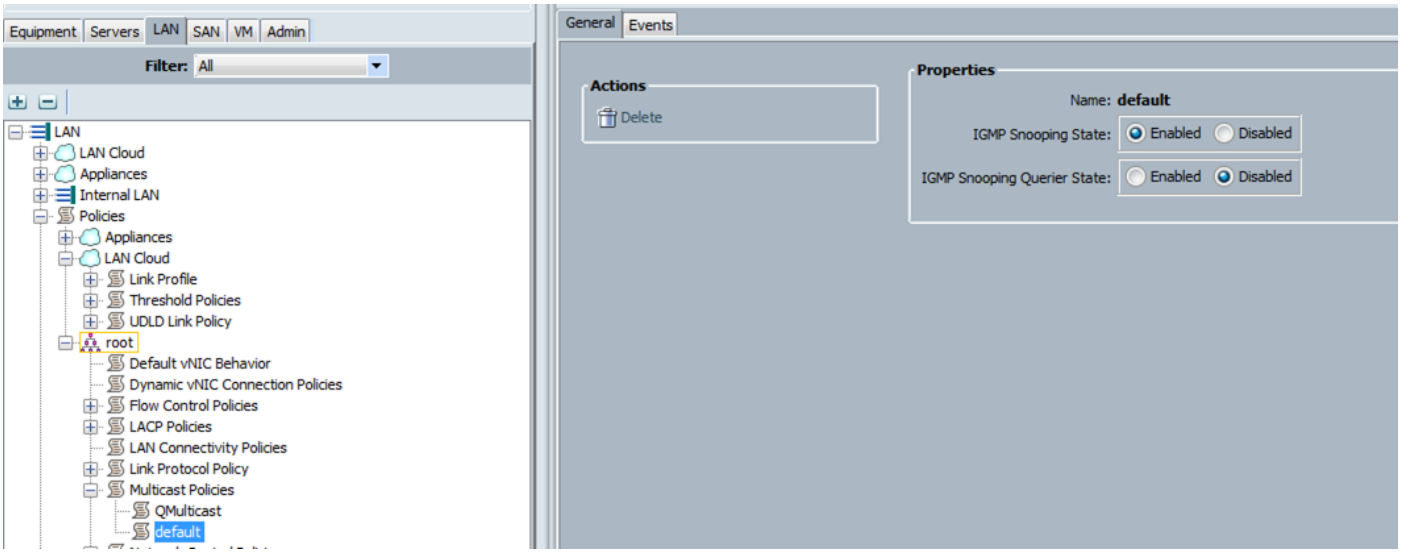
> **Hinweis**: Multicast-Richtlinien befinden sich nur in der Root-Richtlinienstruktur, und Sie können unter einer Unterorganisation keine individuellen Richtlinien erstellen.

Standardrichtlinie

Die Standard-Multicast-Richtlinie hält mit dem Fabric Interconnect-Verhalten vor der Version 2.1 von Dell März im Einklang:

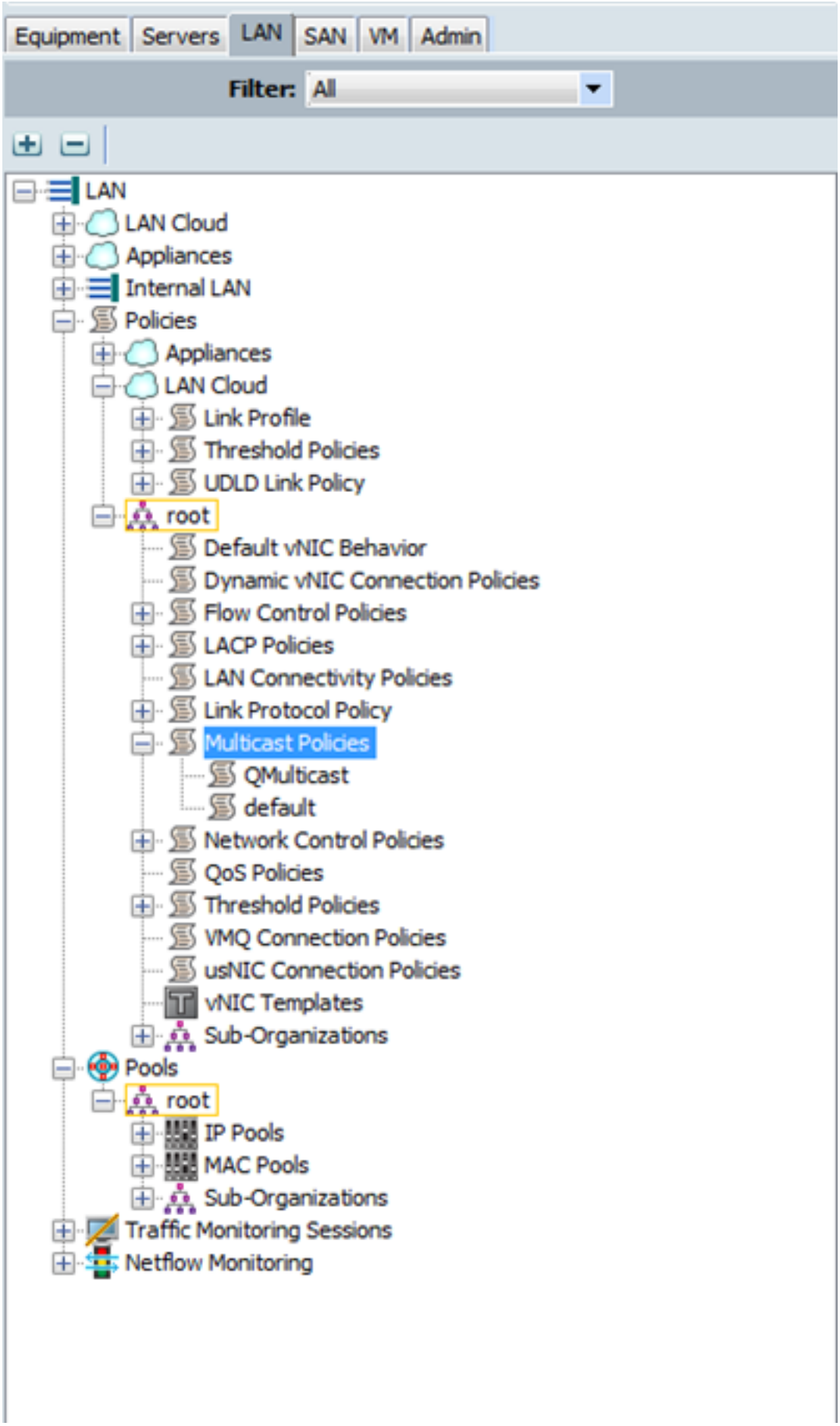
IGMP-Snooping Aktiviert

IGMP-Abfrager - Deaktiviert



Konfiguration - Fortsetzung erstellen

Schritt 1: Fügen Sie einen neuen **Multicast Policies**-Knoten unter **LAN>LAN >**Policies > root hinzu.

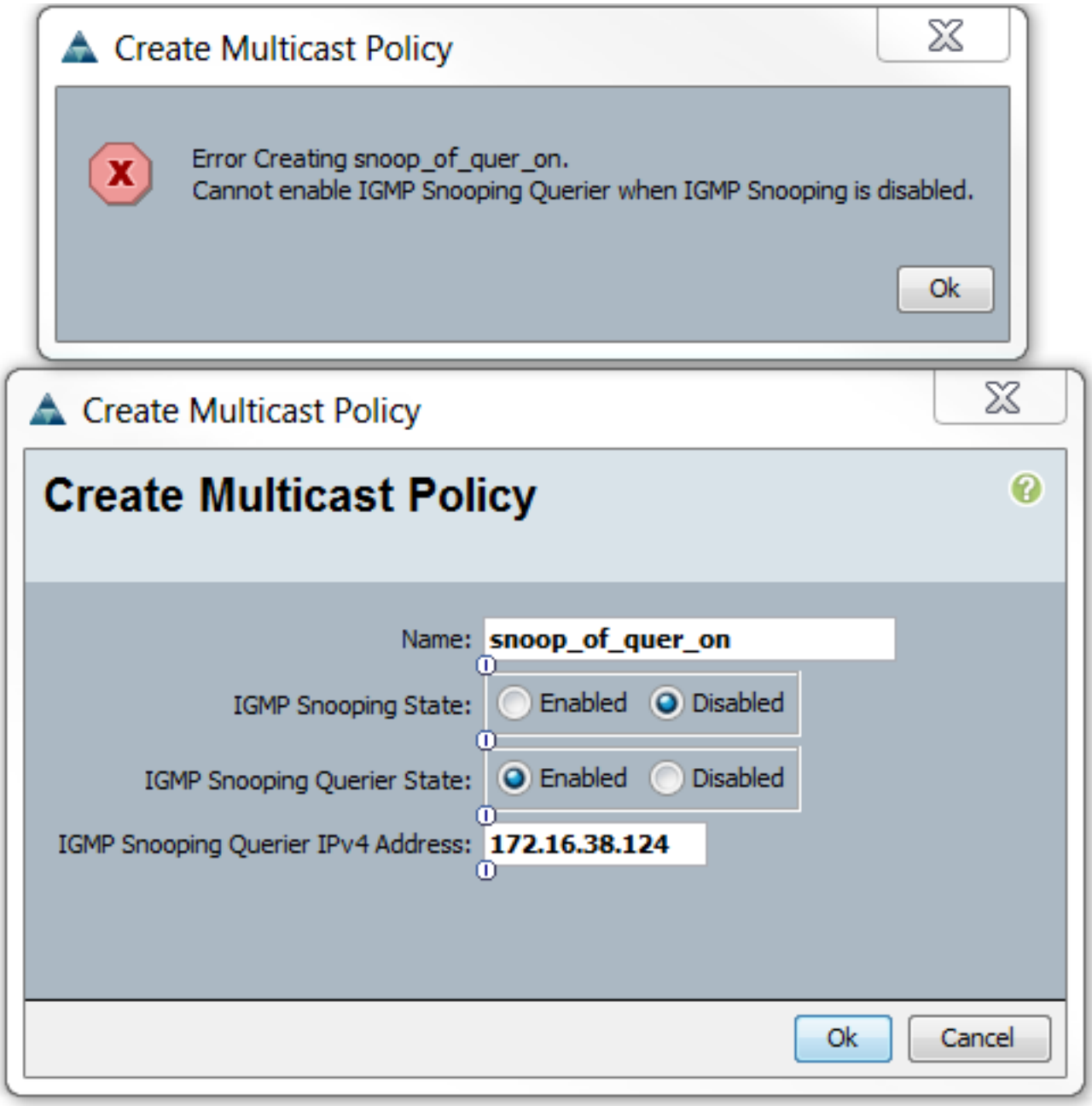


Schritt 2: Klicken Sie mit der rechten Maustaste auf Multicast-Richtlinien, und **erstellen Sie dann Multicast Policy**.

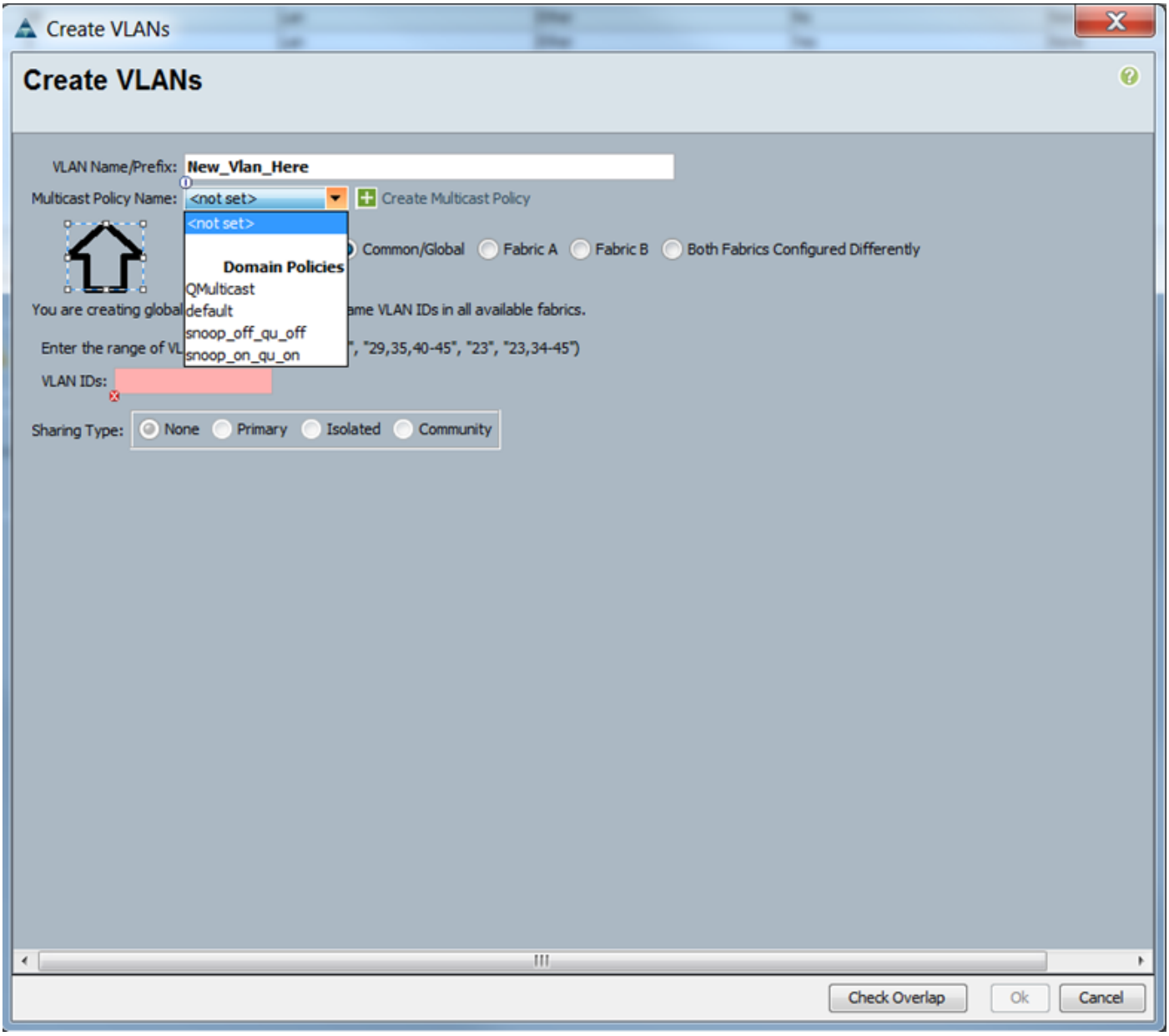
Schritt 3: Daraufhin wird Ihnen Folgendes angezeigt:

Geben Sie einen Namen ein, und konfigurieren Sie die IGMP-Snooping- und Snooping-Querier-Zustände.

Schritt 4: Wenn Sie versuchen, IGMP-Snooping zu deaktivieren, während der IGMP Snooping Querier aktiviert ist, wird ein Fehler ausgelöst, da es sich um keine gültige Konfiguration handelt.

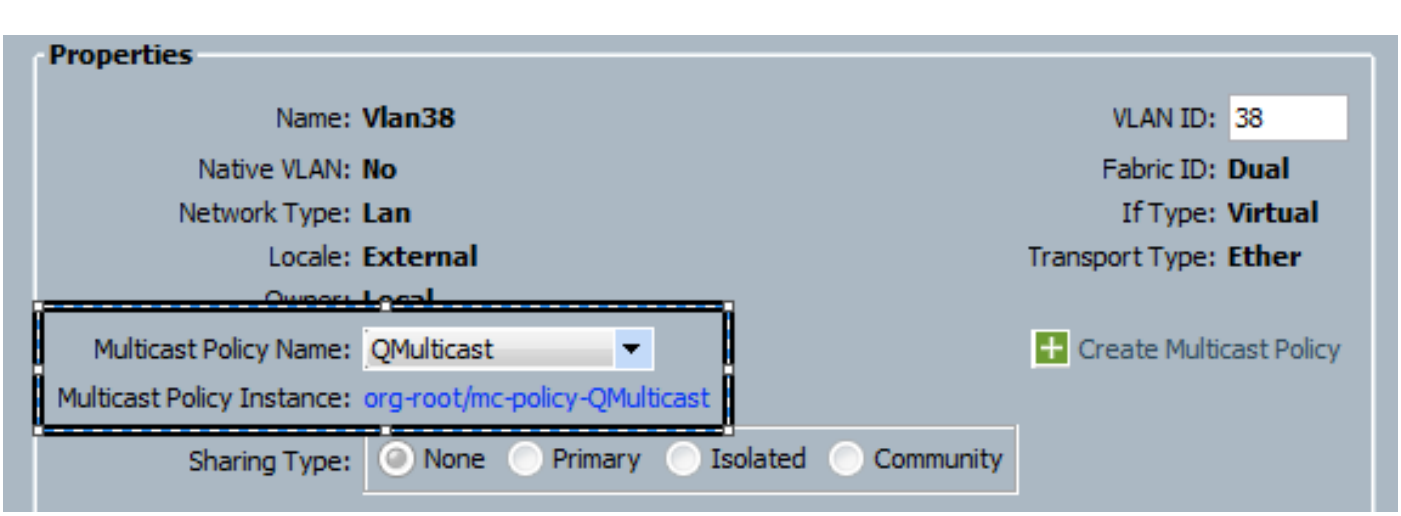


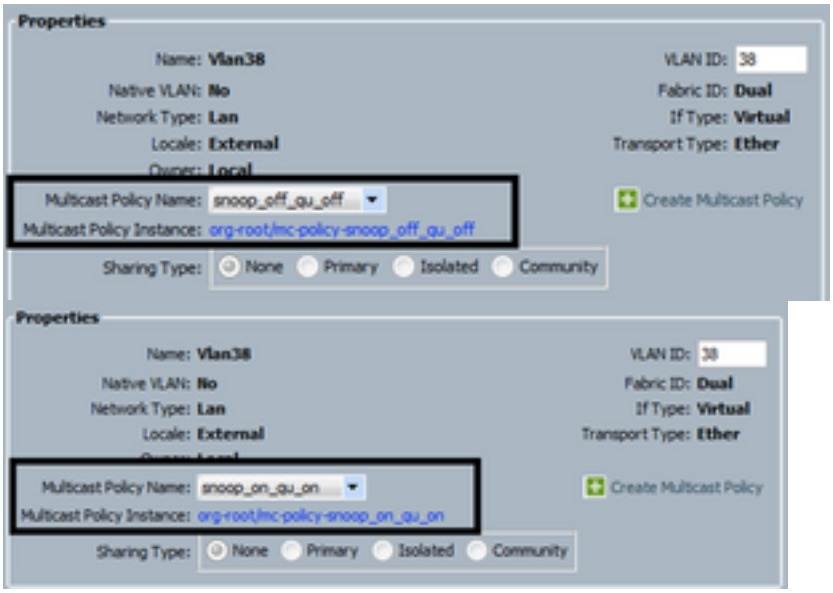
Schritt 5: Bei der Erstellung eines neuen VLANs gibt es jetzt die Option e, den Namen der Multicast-Richtlinie anzugeben.



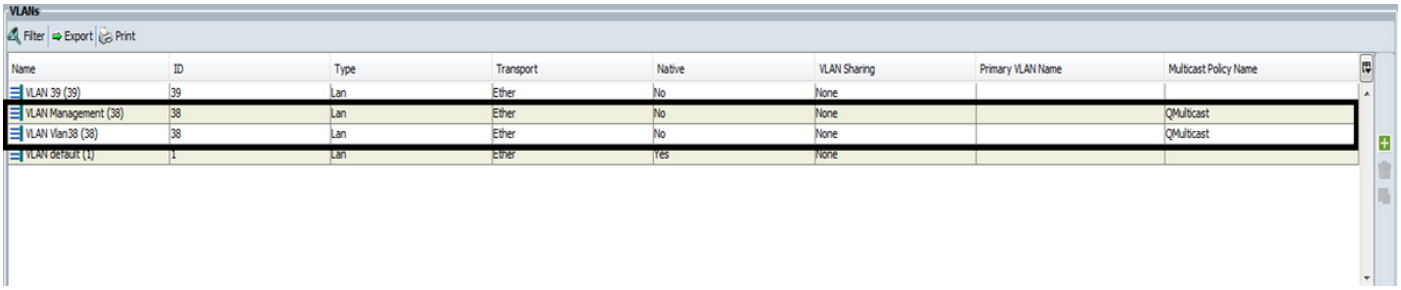
Konfiguration - Zuweisen

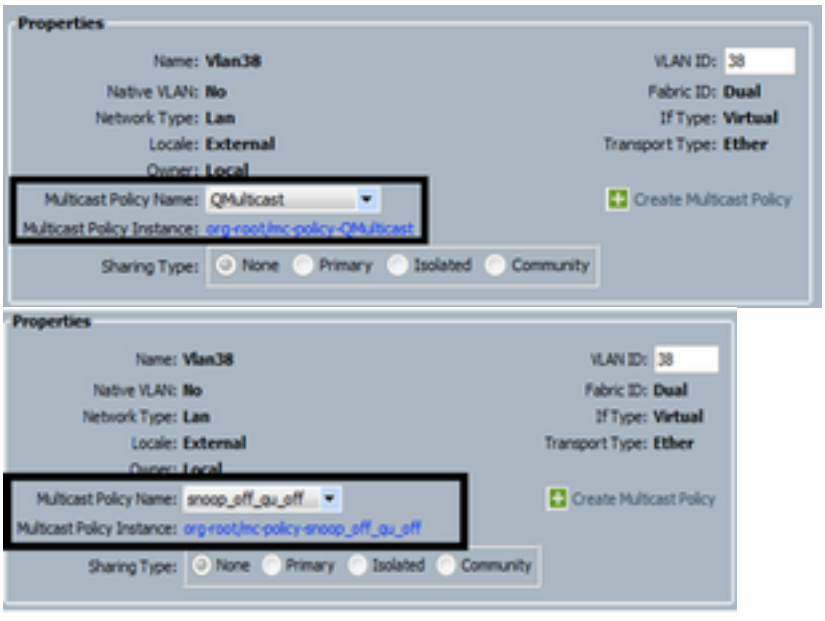
Beispiele mit unterschiedlichen Richtlinien, die im VLAN festgelegt wurden. Der Name der Multicast-Richtlinie ist das, was Sie konfigurieren, wenn die Multicast-Richtlinieninstanz von den Fabric Interconnects verwendet wird.





Wenn Sie mehrere VLAN-Objekte erstellen, die auf dieselbe VLAN-ID verweisen, wird sie bei Anwendung einer Multicast-Richtlinie auf **alle** VLAN-Objekte mit derselben VLAN-ID angewendet. Die neueste angewendete Multicast Policy wird auf alle angewendet. Beispiel: QMulticast wurde in Snoop_off_qu_off (VLAN 38) geändert.





Erstellen von UCS-Multicast-Richtlinien über CLI

- Fügen Sie einen neuen Befehl hinzu, um unter dem Bereichsorg eine Multicast-Richtlinie zu erstellen.

MiniMe-B#-Bereichsorg

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

- Legen Sie Eigenschaften für Multicast-Richtlinien fest.

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

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

- Neuer Befehl zum Anzeigen vorhandener Multicast-Richtlinien.

MiniMe-B # Scope Org

MiniMe-B /org # show mcast-policy

- Neuer Befehl zum Löschen der vorhandenen Multicast-Richtlinie.

MiniMe-B # Scope Org

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

- Wenn Sie ein VLAN erstellen, darf der Benutzer dem VLAN eine vorhandene Multicast-Richtlinie hinzufügen.

MiniMe-B# scope eth-Uplink

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

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

Konfiguration auf Upstream-Switch

- Auf dem Upstream-Switch müssen Sie den IGMP-Snooping-Abfrager in einem bestimmten VLAN konfigurieren, und der IGMP-Snooping-Abfrager muss mit der IP in der UCS-Multicast-Richtlinie übereinstimmen.

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

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

AGR012-5K-A(config-vlan-config)# ip igmp snooping querier 172.16.38.124 (die IP-Adresse ist wahrscheinlich unterschiedlich)

Überprüfen

- **Zeigen Sie ip igmp snooping vlan <VLAN-ID>** (Dies kann entweder über den Upstream-Switch oder Fabric Interconnect erfolgen.)

(Die Ausgabe des UCS-Snooping-Befehls für VLAN 38 überprüft, ob der Abfrager auf dem UCSM und dem Nexus 500 konfiguriert ist. Es zeigt, dass nur der Abfrager auf dem Nexus 500 aktiv ist (wie erwartet). VLAN 39 ist jedoch nicht konfiguriert.

```
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)#
```

- **Zeigen Sie ip igmp snooping querier vlan <vlan id>** (Dies kann entweder über den Upstream-Switch oder Fabric Interconnect erfolgen.)

```
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> (Dies kann entweder auf dem Upstream-Switch oder Fabric Interconnect erfolgen.)

- Es werden die aktiven Ports für Multicast und den IGMP Querier angezeigt.

```
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
```

- **Zeigt ipigmp snooping statistics vlan <vlan id>** (Dies kann entweder auf dem Upstream-Switch oder Fabric Interconnect erfolgen.)

```
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)
```

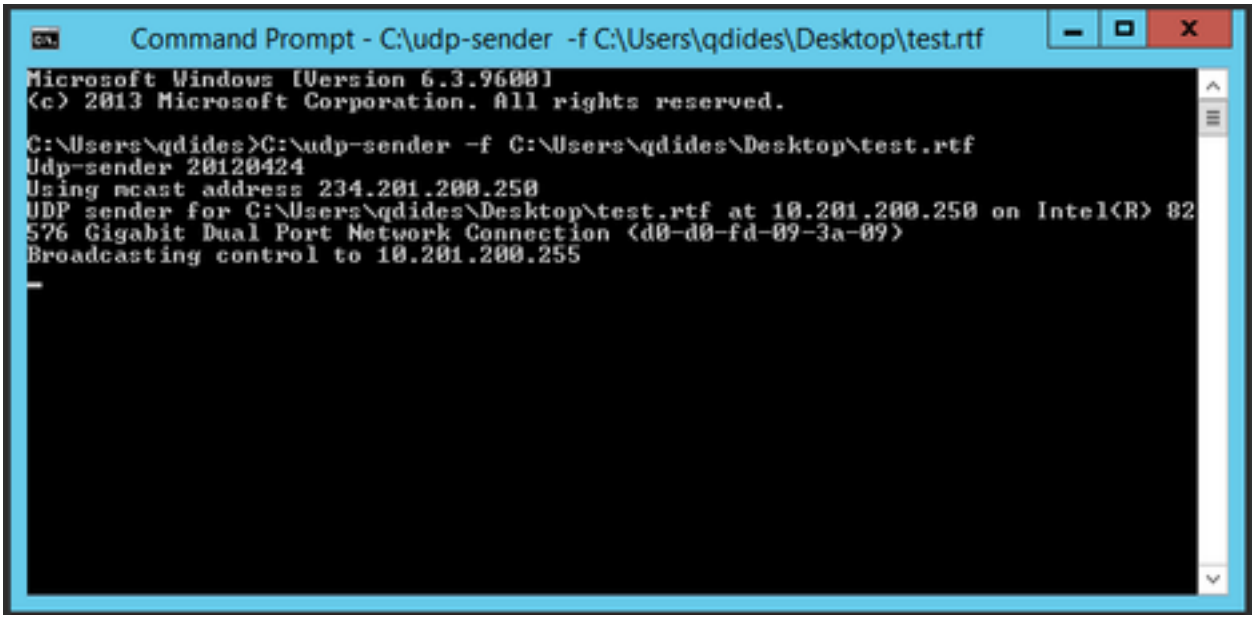
- AGR012-5K-A# Ethanalyzer Local Interface Inbound-Low Display Filter Zacken Grenze

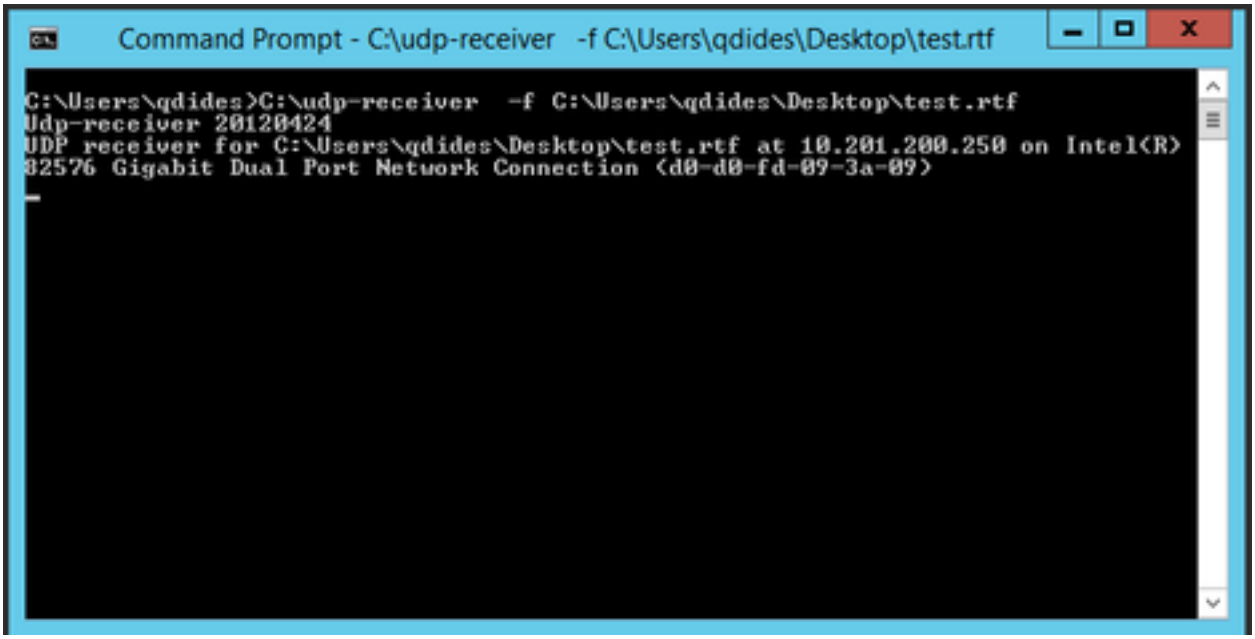
Dabei werden keine tatsächlichen Video-Stream-Daten erfasst, sondern nur IGMP-Daten. Dieses Tool erfasst Kontrolldatenverkehr. (EX; wird angezeigt, wenn ein Host der Gruppe beitritt oder sie verlässt.)

```
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
```

Fehlerbehebung

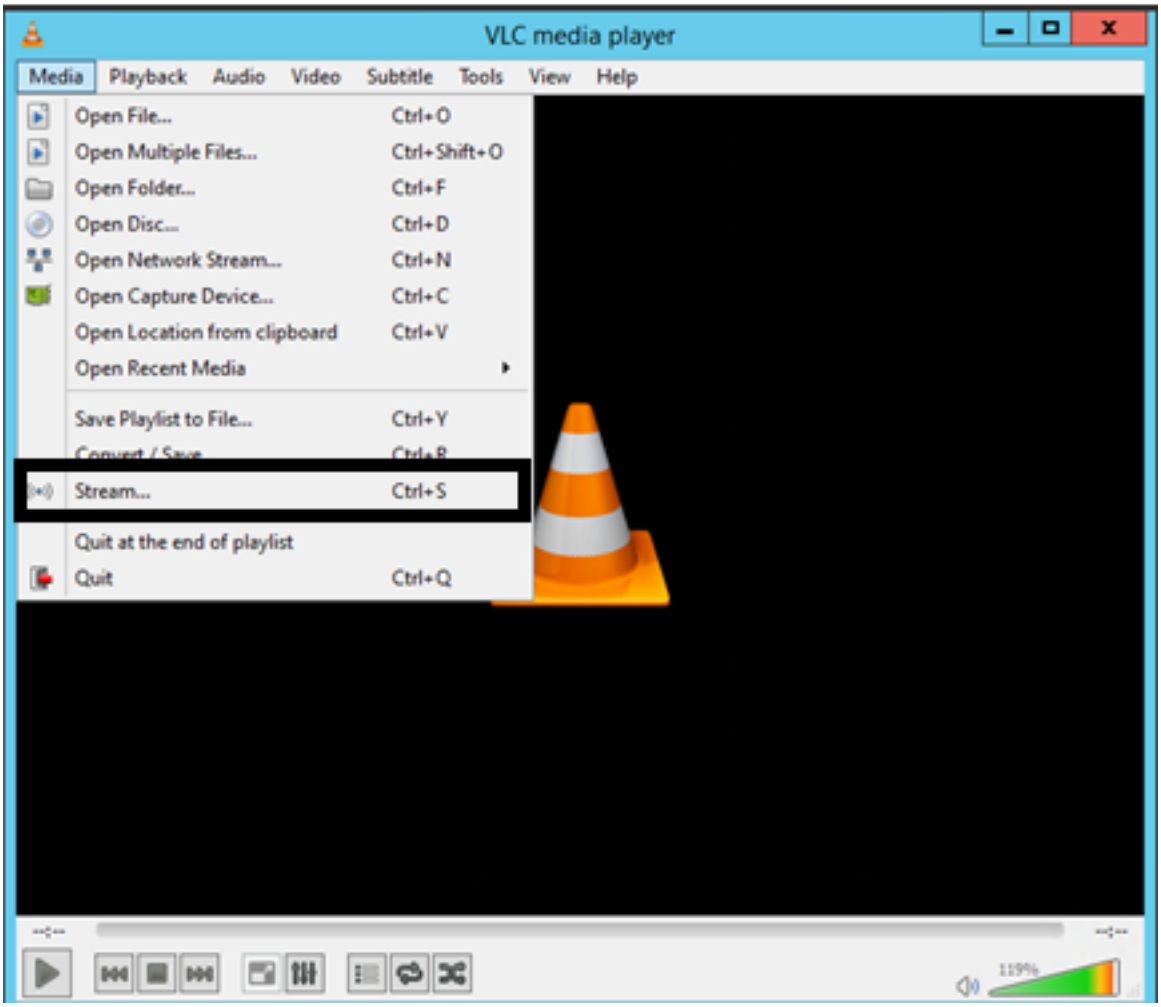
- UDPCAST (http://www.udpcast.linux.lu/cmd.html)
- Diese Anwendung wird auf zwei verschiedenen Hosts heruntergeladen: Sender und Empfänger. Mit diesem Befehl können Sie Multicast-Datenverkehr mit der Übertragung einer Datei von einer Quelle an mehrere Ziele gleichzeitig mit einem einzigen Befehl generieren.

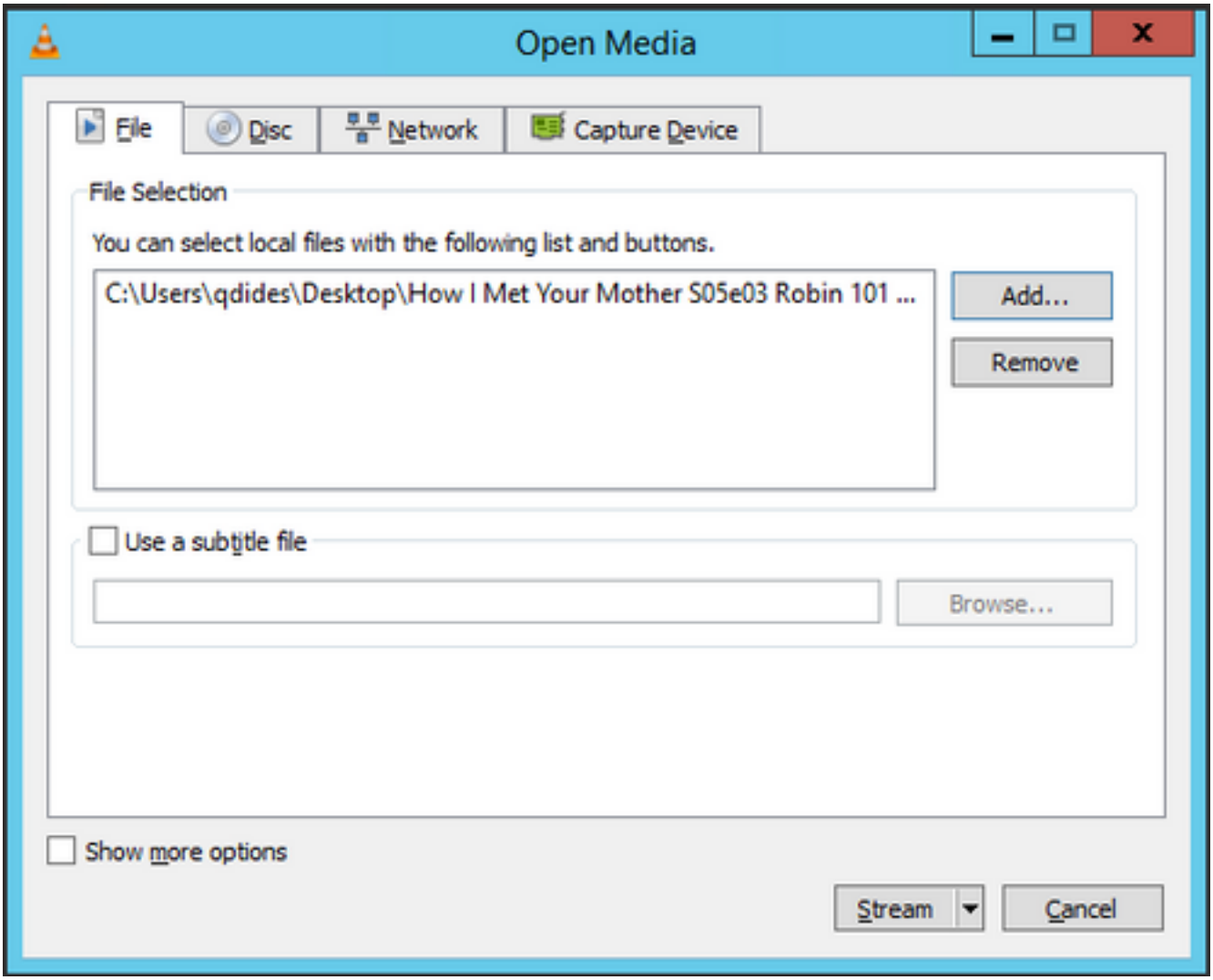


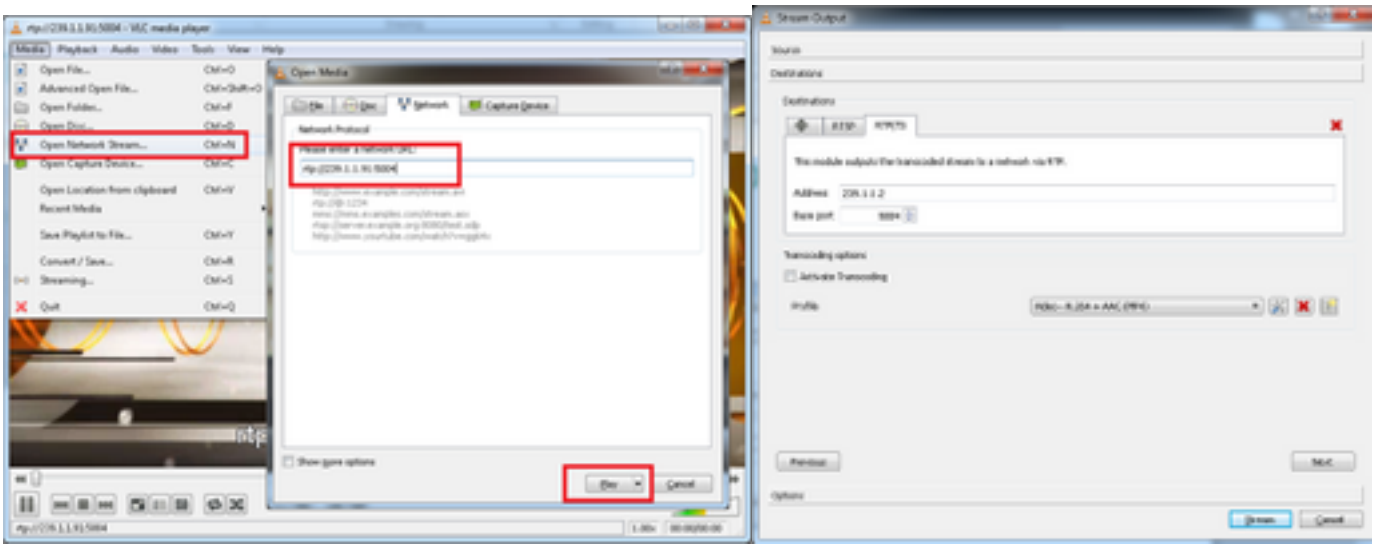


- VLC (http://www.videolan.org/vlc/index.html)

(Die folgenden Bilder zeigen, wie Sie auf VLC streamen. Es gibt eine ganze Menge Informationen, wie man diesen Prozess online macht.)


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





Wie wird IGMP- und Multicast-Datenverkehr mit Iperf generiert?

- Iperf oder Jperf ist ein sehr nützliches Tool, das IGMP- und Multicast-Datenverkehr generieren kann und unter Linux und Windows OS ausgeführt werden kann.
- CLI des Multicast-Absenders.

```
# 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 des Multicast-Empfängers

```
# 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
```

Zugehörige Informationen

- Cisco Nexus 5000 NX-OS Multicast Routing - Konfigurationsleitfaden, Version 5.0(3)N1(1)
- Technischer Support und Dokumentation - Cisco Systems