

Konfigurationsbeispiel für UCS L2 Multicast mit Nexus Switches der Serien 5000 und 1000V

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkeinrichtung](#)

[Nexus 5000 IGMP Querier-Konfiguration](#)

[UCS IGMP Querier-Konfiguration](#)

[Überprüfen](#)

[Verifizierung für N1kV](#)

[Überprüfung auf dem UCS](#)

[Verifizierung auf dem Nexus 500](#)

[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt die Konfiguration und Fehlerbehebung von Layer-2-Multicast (L2) für virtuelle Systeme (VMs) bei der Einrichtung des Cisco Unified Computing System (UCS), der Cisco Nexus Switches der Serie 1000V (N1kV) und der Cisco Nexus Switches der Serie 5000 (N5k).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundlagen von Multicast
- Cisco UCS
- N1kV
- Nexus 500

Verwendete Komponenten

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

- Cisco Nexus Switches der Serie 5020, Version 5.0(3)N2(2a)
- Cisco UCS Version 2.1(1d)
- Cisco UCS B200 M3 Blade-Server mit Cisco Virtual Interface Card (VIC) 1240
- vSphere 5.1 (ESXi und vCenter)
- Cisco N1kV Version 4.2(1)SV2(1.1a)

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, vergewissern Sie sich, dass Sie die potenziellen Auswirkungen eines Befehls oder einer Paketerfassung kennen.

Hintergrundinformationen

Multicast wurde ursprünglich für die Layer-3-Funktionalität (L3) entwickelt, bei der mehrere Hosts aus einem Netzwerk eine Multicast-Adresse abonnieren. Der neue Trend besteht in der Verwendung von L2-Multicast-Funktionen, bei denen der Datenverkehr zwischen VMs, die an einer Multicast-Anwendung teilnehmen, über Hosts im selben VLAN fließt. Dieser Multicast-Datenverkehr bleibt innerhalb derselben L2-Domäne und benötigt keinen Router.

Wenn sich im VLAN kein Multicast-Router befindet, der die Abfragen generiert, müssen Sie einen IGMP-Snooping-Abfrager (Internet Group Management Protocol) konfigurieren, um Mitgliedschaftsabfragen zu senden. IGMP-Snooping ist auf UCS, N1kV und N5k standardmäßig aktiviert. Sie können IGMP Snooping Querier entweder auf dem UCS oder einem Nexus 500 aktivieren, abhängig vom Umfang des L2-Multicast. Wenn Multicast-Empfänger außerhalb des UCS vorhanden sind, konfigurieren Sie den Snooping Querier auf dem Nexus 5000.

Wenn ein IGMP-Snooping-Abfrager aktiviert ist, sendet er regelmäßige IGMP-Abfragen, die IGMP-Berichtsmeldungen von Hosts auslösen, die IP-Multicast-Datenverkehr empfangen möchten. IGMP-Snooping hört diese IGMP-Berichte an, um eine angemessene Weiterleitung zu ermöglichen.

Die IGMP-Snooping-Software prüft IGMP-Protokollmeldungen innerhalb eines VLAN, um die Schnittstellen zu Hosts oder anderen Geräten zu ermitteln, die an diesem Datenverkehr interessiert sind. Mithilfe der Schnittstelleninformationen kann IGMP-Snooping die Bandbreitennutzung in einer LAN-Umgebung mit mehreren Zugriffen reduzieren, um eine Überflutung des gesamten VLAN zu vermeiden. Die IGMP-Snooping-Funktion verfolgt die Ports, die an Multicast-fähige Router angeschlossen sind, um die Weiterleitung von IGMP-Mitgliedschaftsberichten zu erleichtern. Darüber hinaus reagiert die IGMP-Snooping-Software auf Benachrichtigungen zu Topologieänderungen.

Konfigurieren

In diesem Abschnitt können Sie L2-Multicast für VMs konfigurieren.

Netzwerkeinrichtung

In diesem Beispiel finden Sie einige wichtige Hinweise zur Netzwerkeinrichtung:

- Das UCS ist über einen Virtual Port Channel (vPC) mit einem Nexus 500 verbunden.
- Das Betriebssystem (OS), das auf beiden Hosts installiert ist, ist VMware ESXi 5.1. Jeder Host verfügt über VMs mit Microsoft Windows 2012 Guest-OSs.
- Die Quelle für Multicast ist **MCAST VM** (IP-Adresse 172.16.16.226) auf der Host-IP-Adresse 172.16.16.22 (UCS Blade 1/5), die Datenverkehr an die Multicast-IP-Adresse 239.14.14 sendet. ...
- Die Multicast-Empfänger sind **AD-1 VM** (IP-Adresse 172.16.16.224) auf der Host-IP-Adresse 172.16.16.220 (UCS Blade 1/6) und **TEST VM (IP-Adresse 172.16.16.228) auf Host-IP-Adresse 172.16.16.222 (UCS-Blade 1/5)**.
- Der IGMP Snooping Querier wird auf dem Nexus 500 mit der IP-Adresse 172.16.16.2 und auf dem UCS mit der IP-Adresse 172.16.16.233 konfiguriert.

Es ist nicht erforderlich, zwei Abfrageprozesse im gleichen VLAN zu konfigurieren (16). Wenn Multicast-Empfänger außerhalb des UCS vorhanden sind, konfigurieren Sie den Snooping Querier auf dem Nexus 5000. Wenn sich der Multicast-Datenverkehr in der UCS-Domäne befindet, erstellen Sie den Snooping Querier im Cisco Unified Computing System Manager (UCSM).

Hinweis: Der Nexus 5000 IGMP Querier wird gemäß **RFC 4605** gewählt, was den Querier-Wahlprozess erklärt.

Nexus 5000 IGMP Querier-Konfiguration

Nachfolgend finden Sie ein Beispiel für die Konfiguration eines IGMP Querier auf einem Nexus 5000:

```
vlan 16

 ip igmp snooping querier 172.16.16.2

!

int vlan 16

 ip address 172.16.16.2/24

 no shut
```

Die IP-Adresse des Abfragers muss nicht für eine virtuelle Switch-Schnittstelle verwendet werden, und es kann sich um eine andere IP-Adresse innerhalb desselben Subnetzes von VLAN 16 handeln.

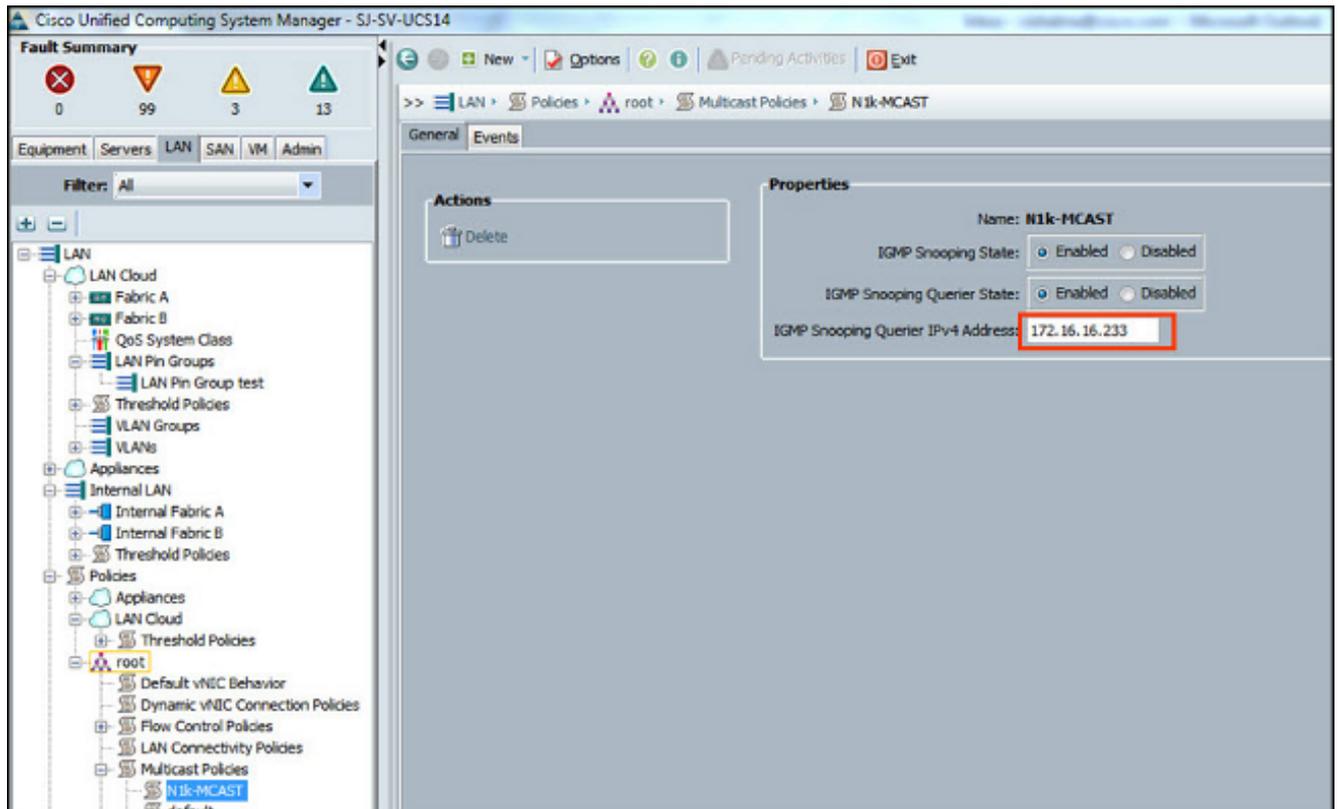
Hinweis: Informationen zur Konfiguration des **IGMP Querier** für Ihre spezifische Version

finden Sie im Abschnitt [Konfigurieren von IGMP-Snooping](#) im Konfigurationsleitfaden für die NX-OS-Software der Cisco Nexus 5000-Serie.

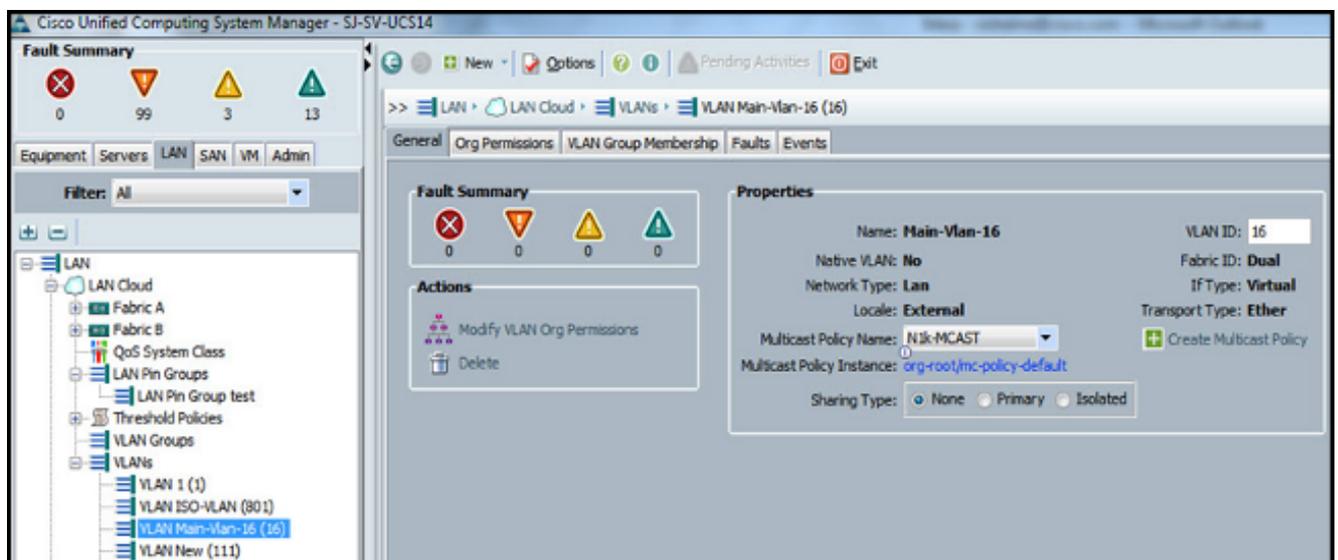
UCS IGMP Querier-Konfiguration

Gehen Sie wie folgt vor, um den IGMP Querier für UCS zu konfigurieren:

1. Erstellen Sie auf der Registerkarte **LAN** des UCSM eine neue Multicast-Richtlinie, wie hier gezeigt:



2. Wenden Sie die Multicast-Richtlinie **N1k-MCAST** auf VLAN 16 an:



3. Vergewissern Sie sich für das N1kV, dass IGMP-Snooping in VLAN 16 aktiviert ist (dies ist standardmäßig aktiviert). Für N1kV muss keine Konfiguration vorgenommen werden, um ein grundlegendes L2-Multicast zu unterstützen.

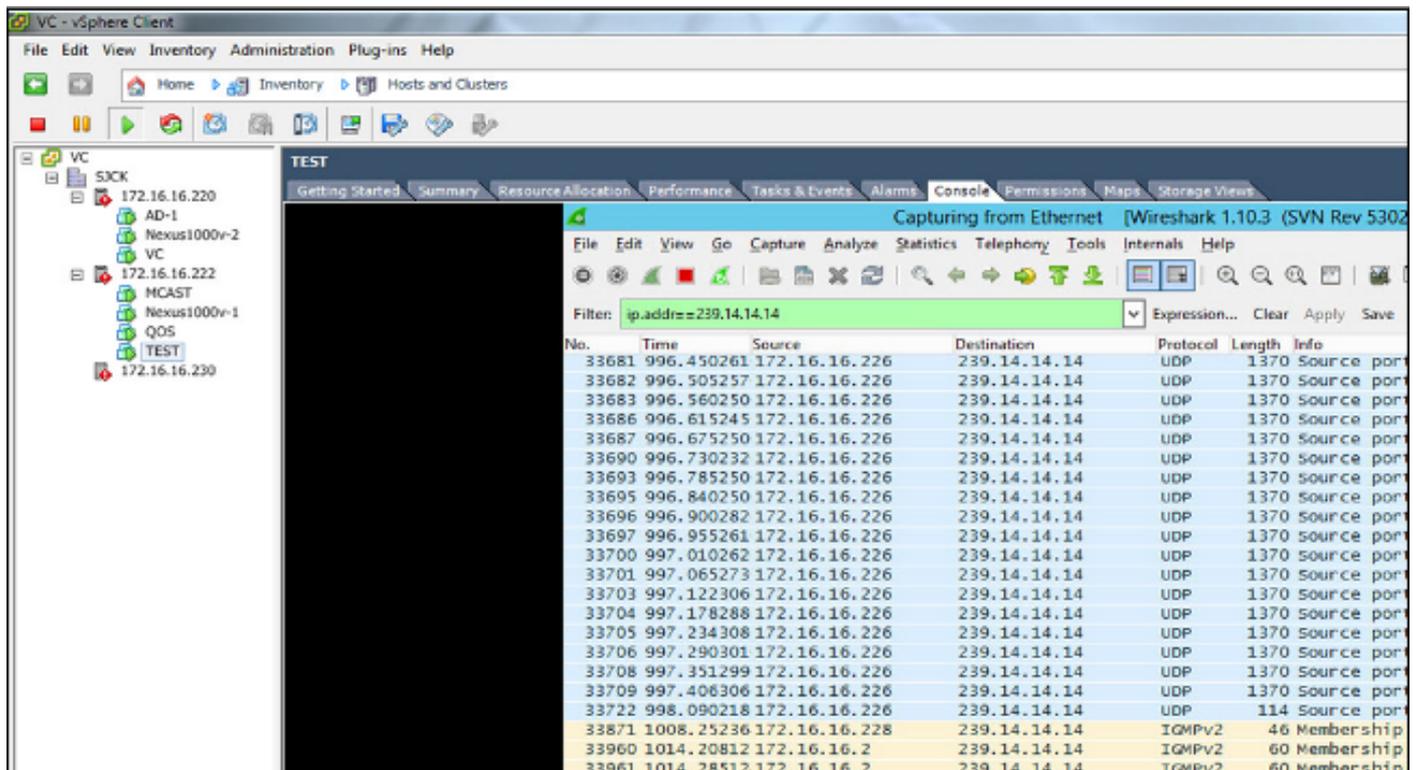
Hinweis: Zur Demonstration von Multicast wird ein VideoLAN Client (VLC) Media Player verwendet. Weitere Informationen zur Verwendung eines VLC-Players für Multicast-Streaming finden Sie im Artikel [How to use VLC Media Player to stream Multicast video \(Wie Sie den VLC Media Player zum Streamen von Multicast-Video verwenden\)](#).

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Verifizierung für N1kV

Stellen Sie sicher, dass die Multicast-Empfänger **TEST VM** und **AD-1 VM** dem Multicast-Stream **239.14.14.14** beigetreten sind, aus dem **MCAST VM** Datenverkehr stammt. Dieses Bild zeigt, dass der Multicast-Empfänger **TEST VM** den Stream empfängt:



Die N1kV-Snooping-Ausgabe zeigt die Gruppenadresse und die Veths des Multicast-Empfängers an, nicht das Veth der VM, das den Multicast-Datenverkehr (wie erwartet) verursacht:

```
Nexus1000v# sh ip igmp snooping groups

Type: S - Static, D - Dynamic, R - Router port

Vlan  Group Address      Ver  Type  Port list
16    */*                -    R     Eth3/2 Eth4/2
16    239.14.14.14      v2   D     Veth3 Veth6
```

Diese N1kV-Ausgabe zeigt die aktiven Ports für Multicast und den 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
```

Auf Hostebene können Sie überprüfen, ob der Multicast-Datenverkehr von den beteiligten VMs empfangen wird. Diese Ausgabe zeigt VM **AD-1**, das sich auf **Modul 3** des Virtual Supervisor Module (VSM) befindet:

```
Nexus1000v# module vem 3 execute vemcmd show bd
BD 7, vdc 1, vlan 16, swbd 16, 3 ports, ""

Portlist:
  18  vmn1c1
  49  vmk0
  50  AD-1 ethernet0

Multicast Group Table:
Group 239.14.14.14 Multicast LTL 4672
  18
  50
Group 0.0.0.0 Multicast LTL 4671
  18
```

Diese Ausgabe zeigt den VM-TEST, der sich auf **Modul 4** des VSM befindet:

```
Nexus1000v# module vem 4 execute vemcmd show bd
BD 7, vdc 1, vlan 16, swbd 16, 6 ports, ""

Portlist:
  18  vmn1c1
  49  vmk0
  50  TEST.eth0
  51  QOS.eth0
  52  MCAST.eth0 ← Source
  561

Multicast Group Table:
Group 239.14.14.14 Multicast LTL 4672
  50
  561
Group 0.0.0.0 Multicast LTL 4671
  561
```

Überprüfung auf dem UCS

Diese UCS-Ausgabe zeigt die aktiven Ports für Multicast und die Gruppenadresse:

```

SJ-SV-UCS14-B(nxos)# sh ip igmp snooping group
Type: S - Static, D - Dynamic, R - Router port

Vlan  Group Address          Ver  Type  Port list
1      */*                      -    R     Po1
11     */*                      -    R     Po1
15     */*                      -    R     Po1
16     */*                      -    R     Po1
16     239.14.14.14             v2   D     Veth1257 Veth1255
30     */*                      -    R     Po1
111    */*                      -    R     Po1
172    */*                      -    R     Po1
800    */*                      -    R     Po1

```

Diese UCS-Snooping-Ausgabe für VLAN 16 überprüft, ob der Abfrager auf dem UCSM und dem Nexus 500 konfiguriert ist, und zeigt, dass nur der Abfrager auf dem Nexus 500 aktiv ist (wie erwartet):

```

SJ-SV-UCS14-B(nxos)# sh ip igmp snooping vlan 16
IGMP Snooping information for vlan 16
IGMP snooping enabled
Optimised Multicast Flood (OMF) disabled
IGMP querier present, address: 172.16.16.2, version: 2, interface port-channel1
Switch-querier enabled, address 172.16.16.233, currently not 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: 1
Number of groups: 1
Active ports:
  Pol Veth1257          Veth1251          Veth1255
  Veth1279          Veth1281

```

Verifizierung auf dem Nexus 500

Überprüfen Sie auf dem Nexus 5000, ob die Multicast-Gruppenadresse **239.14.14.14** und der aktive Port-Channel mit den UCS Fabric Interconnects (FIs) verbunden sind:

```
n5k-Rack18-1# sh ip igmp snooping groups
Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port

Vlan  Group Address      Ver  Type  Port list
1      */*                -    R     Po40
15     */*                -    R     Po40 Po1110 Po1111
15     239.255.255.253   v2    D     Po10 Po11 Po12
                               Po13 Po40
16     */*                -    R     Po3 Po40
16     239.14.14.14     v2    D     Po15 Po16
17     */*                -    R     Po40
18     */*                -    R     Po40
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung in Ihrer Konfiguration verwenden können.

Im Folgenden finden Sie eine Liste mit grundlegenden Fragen zu Multicast in der L2-Domäne:

- Wenn IGMP-Snooping auf dem Switch nicht aktiviert ist, wird Multicast-Datenverkehr innerhalb der L2-Domäne übertragen.
- Wenn IGMP-Snooping aktiviert ist, muss ein Querier auf den Uplink-Switches im VLAN ausgeführt werden, die Multicast-Quellen und -Empfänger enthalten.
- Wenn im VLAN kein IGMP Querier vorhanden ist, leiten N1kV und UCS das Multicast nicht weiter. Dies ist die häufigste Fehlkonfiguration in Fällen des Cisco Technical Assistance Center (TAC).
- IGMP-Snooping ist auf dem N1kV und dem UCS standardmäßig aktiviert.
- Mit UCS Version 2.1 und höher kann IGMP-Snooping für jedes VLAN aktiviert oder deaktiviert werden. Der IGMP Querier kann auf UCS-Ebene konfiguriert werden.