

Exemplo de configuração de multicast UCS L2 com switches Nexus 5000 e 1000V Series

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Instalação de rede](#)

[Configuração do questionário de IGMP N5k](#)

[Configuração do verificador do UCS IGMP](#)

[Verificar](#)

[Verificação do N1kV](#)

[Verificação do UCS](#)

[Verificação do N5k](#)

[Troubleshoot](#)

Introduction

Este documento descreve como configurar e solucionar problemas de multicast de Camada 2 (L2) para Máquinas Virtuais (VMs) na configuração dos switches Cisco Unified Computing System (UCS), Cisco Nexus 1000V Series (N1kV) e Cisco Nexus 5000 Series (N5k).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conceitos básicos do multicast
- Cisco UCS
- N1kV
- N5k

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Switch Cisco Nexus 5020 Series versão 5.0(3)N2(2a)
- Cisco UCS versão 2.1(1d)
- Servidor blade Cisco UCS B200 M3 com Cisco Virtual Interface Card (VIC) 1240
- vSphere 5.1 (ESXi e vCenter)
- Cisco N1kV Versão 4.2(1)SV2(1.1a)

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. Se a sua rede estiver ativa, certifique-se de que você entende o impacto potencial de qualquer comando ou configuração de captura de pacotes.

Informações de Apoio

O multicast foi inicialmente projetado para usar a funcionalidade de Camada 3 (L3), na qual vários hosts de uma rede assinam um endereço multicast. A nova tendência é usar a funcionalidade multicast L2, onde o tráfego flui entre VMs que participam de um aplicativo multicast entre hosts na mesma VLAN. Esse tráfego multicast permanece no mesmo domínio L2 e não precisa de um roteador.

Quando não há um roteador multicast na VLAN que origine as consultas, você deve configurar um pesquisador de rastreamento do Internet Group Management Protocol (IGMP) para enviar consultas de associação. O rastreamento IGMP é ativado por padrão no UCS, N1kV e N5k. Você pode habilitar o pesquisador de rastreamento IGMP no UCS ou no N5k, dependendo do escopo do multicast L2. Se houver receptores multicast fora do UCS, configure o verificador de rastreamento no N5k.

Quando um pesquisador de rastreamento IGMP é ativado, ele envia consultas IGMP periódicas que disparam mensagens de relatório IGMP de hosts que desejam receber tráfego multicast IP. O rastreamento IGMP escuta esses relatórios IGMP para estabelecer o encaminhamento apropriado.

O software de rastreamento IGMP examina mensagens de protocolo IGMP em uma VLAN para descobrir as interfaces conectadas a hosts ou outros dispositivos interessados em receber esse tráfego. Com as informações da interface, o rastreamento IGMP pode reduzir o consumo de largura de banda em um ambiente de LAN multiacesso para evitar uma inundação de toda a VLAN. O recurso de espionagem de IGMP rastreia as portas conectadas a roteadores com capacidade de transmissão múltipla para ajudar a gerenciar o encaminhamento de relatórios de associação de IGMP. Além disso, o software de rastreamento IGMP responde às notificações de alteração de topologia.

Configurar

Use esta seção para configurar multicast L2 para VMs.

Instalação de rede

Aqui estão algumas notas importantes sobre a configuração de rede neste exemplo:

- O UCS é conectado a um N5k através de um Virtual Port Channel (vPC).
- O sistema operacional (SO) instalado em ambos os hosts é o VMware ESXi 5.1. Cada host tem VMs com SOs convidados do Microsoft Windows 2012.
- A origem do multicast é **MCAST VM** (endereço IP 172.16.16.226) no endereço IP do host 172.16.16.222 (UCS Blade 1/5), que envia tráfego para o endereço IP multicast 239.14.14.14.
- Os receptores multicast são **VM AD-1** (endereço IP 172.16.16.224) no endereço IP do host 172.16.16.220 (UCS Blade 1/6) e **TEST VM** (endereço IP 172.16.16.228) no endereço IP do host 172.16.16.222 (UCS Blade 1/5).
- O verificador de rastreamento IGMP é configurado no N5k com um endereço IP 172.16.16.2 e também no UCS com um endereço IP 172.16.16.233.

Não há necessidade de configurar dois consultantes na mesma VLAN (16). Se houver receptores multicast fora do UCS, configure o verificador de rastreamento no N5k. Se o tráfego multicast estiver no domínio UCS, crie o pesquisador de rastreamento no Cisco Unified Computing System Manager (UCSM).

Note: O solicitante de IGMP N5k é eleito de acordo com o **RFC 4605**, que explica o processo de eleição do solicitante.

Configuração do questionário de IGMP N5k

Aqui está um exemplo de configuração de um consultante IGMP em um N5k:

```
vlan 16

ip igmp snooping querier 172.16.16.2

!

int vlan 16

ip address 172.16.16.2/24

no shut
```

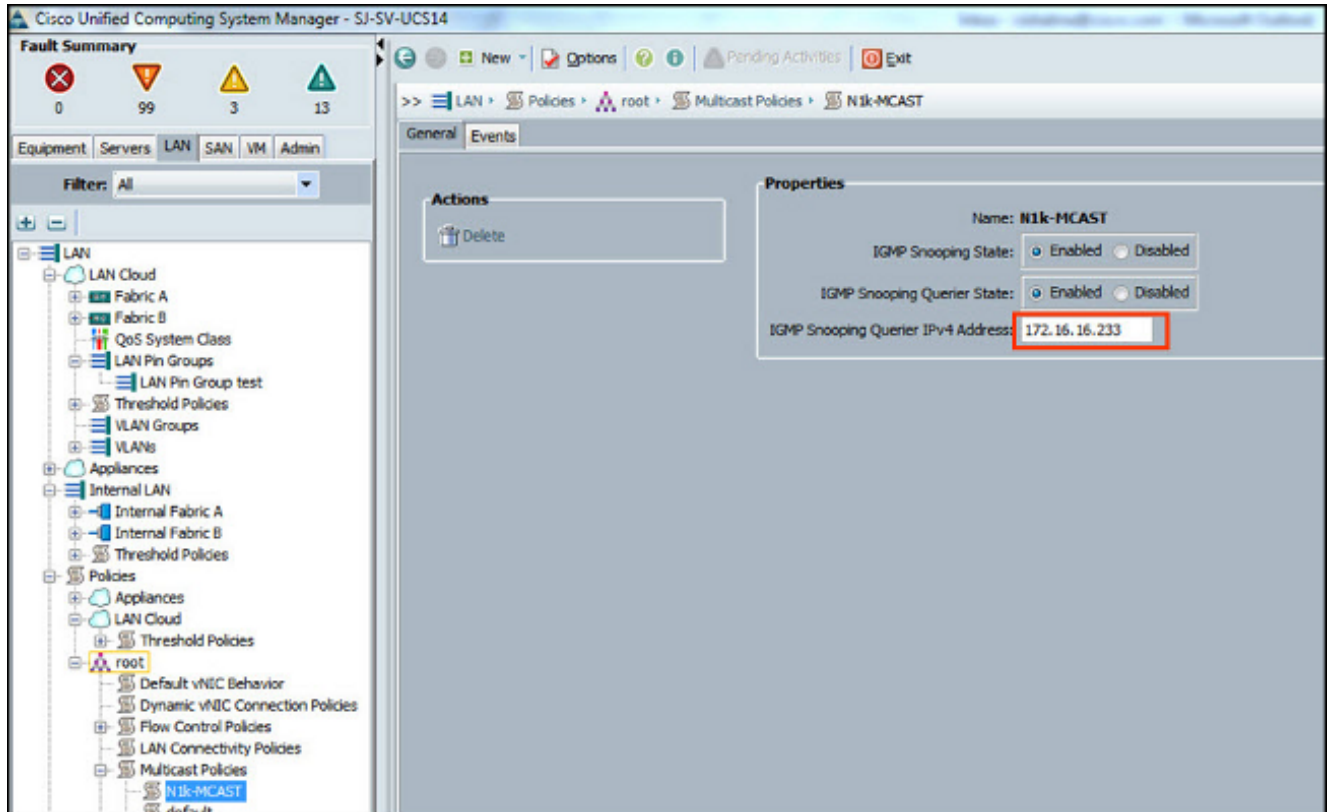
O endereço IP do solicitante não precisa ser para uma interface virtual comutada e pode ser um endereço IP diferente dentro da mesma sub-rede da VLAN 16.

Note: Consulte a seção [Configurando o IGMP Snooping](#) do **Cisco Nexus 5000 Series NX-OS Software Configuration Guide** para obter informações sobre como configurar o consultante IGMP para sua versão específica.

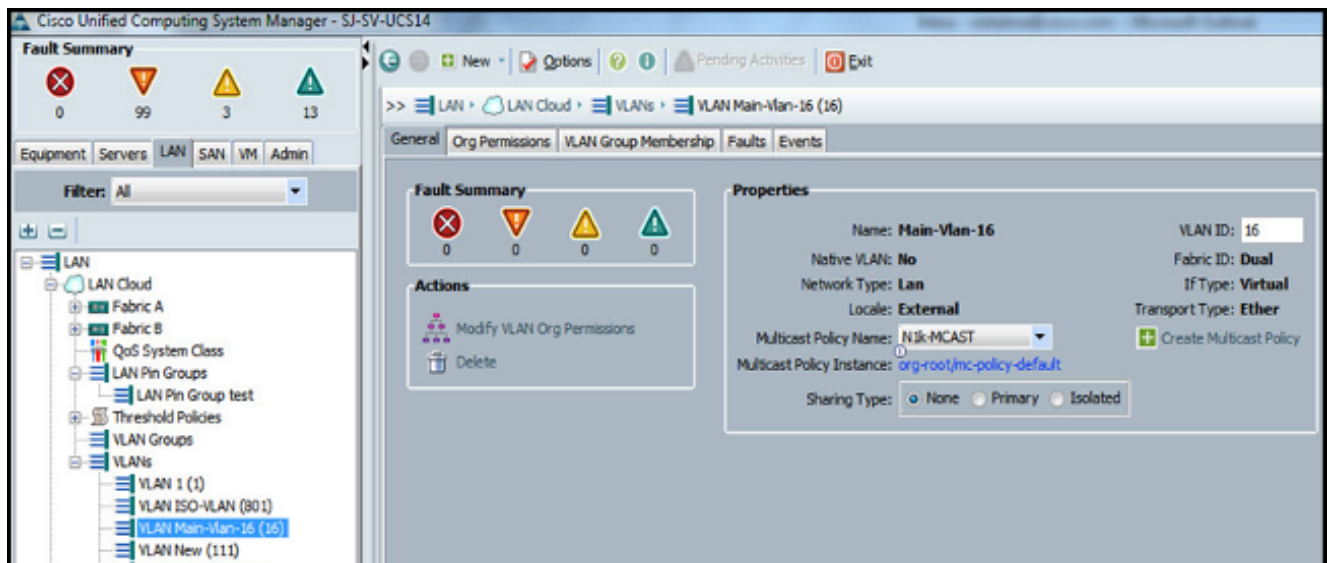
Configuração do verificador do UCS IGMP

Conclua estes passos para configurar o verificador IGMP para UCS:

1. Crie uma nova política de multicast na guia **LAN** do UCSM, como mostrado aqui:



2. Aplique a política multicast **N1k-MCAST** à VLAN 16:



3. Para o N1kV, confirme se a espionagem de IGMP está ativada na VLAN 16 (habilitada por padrão). Nenhuma configuração deve ser feita em um N1kV para suportar multicast L2 básico.

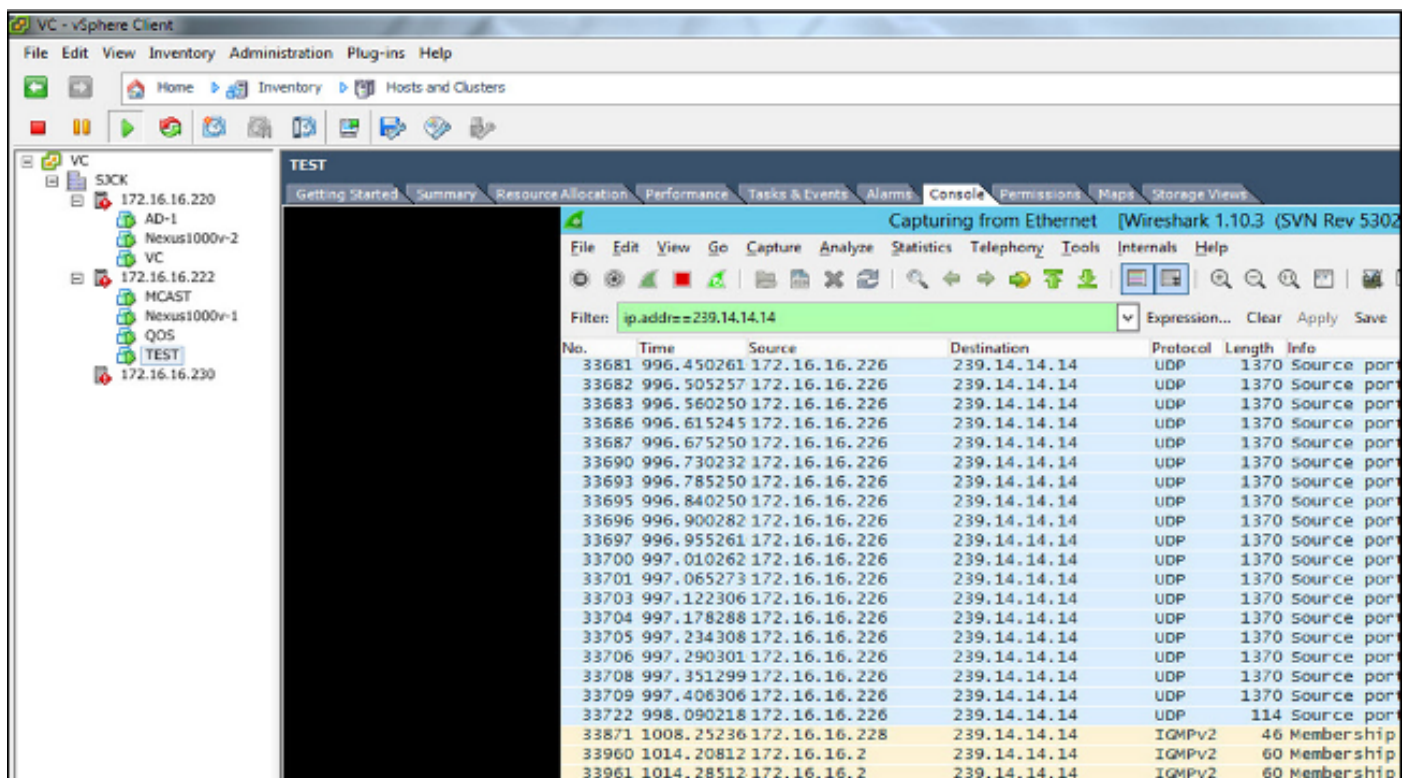
Note: Um player de mídia VideoLAN Client (VLC) é usado para demonstrar multicast. Para obter mais detalhes sobre como usar um VLC player para transmissão múltipla, consulte o [artigo Como usar o VLC Media Player para transmitir vídeo multicast](#).

Verificar

Use esta seção para verificar se sua configuração funciona corretamente.

Verificação do N1kV

Verifique se os receptores multicast **TEST VM** e **AD-1 VM** juntaram-se ao fluxo multicast **239.14.14.14**, a partir do qual **MCAST VM** gera tráfego. Esta imagem mostra que o receptor multicast **TEST VM** recebe o fluxo:



No.	Time	Source	Destination	Protocol	Length	Info
33681	996.450261	172.16.16.226	239.14.14.14	UDP	1370	Source port
33682	996.505257	172.16.16.226	239.14.14.14	UDP	1370	Source port
33683	996.560250	172.16.16.226	239.14.14.14	UDP	1370	Source port
33686	996.615245	172.16.16.226	239.14.14.14	UDP	1370	Source port
33687	996.675250	172.16.16.226	239.14.14.14	UDP	1370	Source port
33690	996.730232	172.16.16.226	239.14.14.14	UDP	1370	Source port
33693	996.785250	172.16.16.226	239.14.14.14	UDP	1370	Source port
33695	996.840250	172.16.16.226	239.14.14.14	UDP	1370	Source port
33696	996.900282	172.16.16.226	239.14.14.14	UDP	1370	Source port
33697	996.955261	172.16.16.226	239.14.14.14	UDP	1370	Source port
33700	997.010262	172.16.16.226	239.14.14.14	UDP	1370	Source port
33701	997.065273	172.16.16.226	239.14.14.14	UDP	1370	Source port
33703	997.122306	172.16.16.226	239.14.14.14	UDP	1370	Source port
33704	997.178288	172.16.16.226	239.14.14.14	UDP	1370	Source port
33705	997.234308	172.16.16.226	239.14.14.14	UDP	1370	Source port
33706	997.290301	172.16.16.226	239.14.14.14	UDP	1370	Source port
33708	997.351299	172.16.16.226	239.14.14.14	UDP	1370	Source port
33709	997.406306	172.16.16.226	239.14.14.14	UDP	1370	Source port
33722	998.090218	172.16.16.226	239.14.14.14	UDP	114	Source port
33871	1008.252386	172.16.16.228	239.14.14.14	IGMPv2	46	Membership
33960	1014.20812	172.16.16.2	239.14.14.14	IGMPv2	60	Membership
33961	1014.28512	172.16.16.2	239.14.14.14	IGMPv2	60	Membership

A saída de rastreamento N1kV mostra o endereço de grupo e os Veths do receptor multicast, não a Veth da VM que origina o tráfego multicast (como esperado):

```
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
```

Esta saída de N1kV mostra as portas ativas para multicast e o consultante de 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
```

No nível do host, você pode verificar se o tráfego multicast é recebido pelas VMs que participam. Esta saída mostra a VM **AD-1**, que está no **Módulo 3** do Virtual Supervisor Module (VSM):

```
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
```

Esta saída mostra o VM TEST, que está no **Módulo 4** do VSM:

```
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
```

Verificação do UCS

Esta saída do UCS mostra as portas ativas para multicast e o endereço de grupo:


```
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

Esta saída de rastreamento UCS para VLAN 16 verifica se o solicitante está configurado no UCSM e no N5k e mostra que apenas o verificador no N5k está ativo no momento (como esperado):

```
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:
  Po1 Veth1257      Veth1251      Veth1255
  Veth1279      Veth1281
```

Verificação do N5k

No N5k, confirme se o endereço do grupo multicast **239.14.14.14** e o canal de porta ativo estão conectados às Interconexões de estrutura (FIs) do UCS:

```
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
```

Troubleshoot

Esta seção fornece informações que você pode usar para solucionar problemas de sua configuração.

Aqui está uma lista de advertências básicas sobre multicast no domínio L2:

- Se o rastreamento IGMP não estiver habilitado no switch, o tráfego multicast será transmitido no domínio L2.
- Se a espionagem de IGMP estiver habilitada, um solicitante deve ser executado nos switches de uplink na VLAN que contêm fontes e receptores multicast.
- Se não houver um consultante IGMP na VLAN, o N1kV e o UCS não encaminham o multicast. Essa é a configuração incorreta mais comum observada nos casos do Cisco Technical Assistance Center (TAC).
- Por padrão, o rastreamento IGMP é ativado no N1kV e no UCS.
- Com o UCS versões 2.1 e posteriores, o rastreamento IGMP pode ser ativado ou desativado por VLAN, e o verificador IGMP pode ser configurado no nível do UCS.