

Configurar o multicast L2 na ACI

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Topologia de rede](#)

[Configurações](#)

[Passo 1: Configurar as políticas de acesso à estrutura para o servidor multicast e a conectividade do host cliente](#)

[Passo 2: Crie o EPG, BD e VRF para o receptor e origem multicast](#)

[Passo 3: Conecte um domínio físico ao EPG e configure a porta estática](#)

[Passo 4: Configurar o IGMP Querier](#)

[Verificar](#)

[Explicação do fluxo de pacote multicast L2](#)

[Requisito de consultas IGMP](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar e verificar o multicast da Camada 2 (L2) no mesmo Grupo de Endpoints (EPG) em uma única estrutura da ACI (Application Centric Infrastructure, Infraestrutura Centrada em Aplicações).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Suporte a multicast L2 na ACI - sempre compatível
- Rastreamento de Internet Group Management Protocol (IGMP) na ACI - ativado por padrão

Note: Para obter mais informações sobre espionagem de IGMP, consulte o documento [Cisco APIC e IGMP Snoop Layer 2 Multicast Configuration](#).

Componentes Utilizados

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

- N9K-C93180YC-FX
- Versão 4.2(7q)

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O multicast L2 refere-se a pacotes multicast IP encaminhados em um segmento de rede L2 (domínio de bridge (BD)/sub-rede), não a pacotes multicast L2 não IP que são pacotes multicast com um endereço MAC multicast de destino sem um cabeçalho IP. O multicast L2 também exclui o multicast local de link (224.0.0.0/24). O multicast de link local é sempre encaminhado a todas as portas no BD.

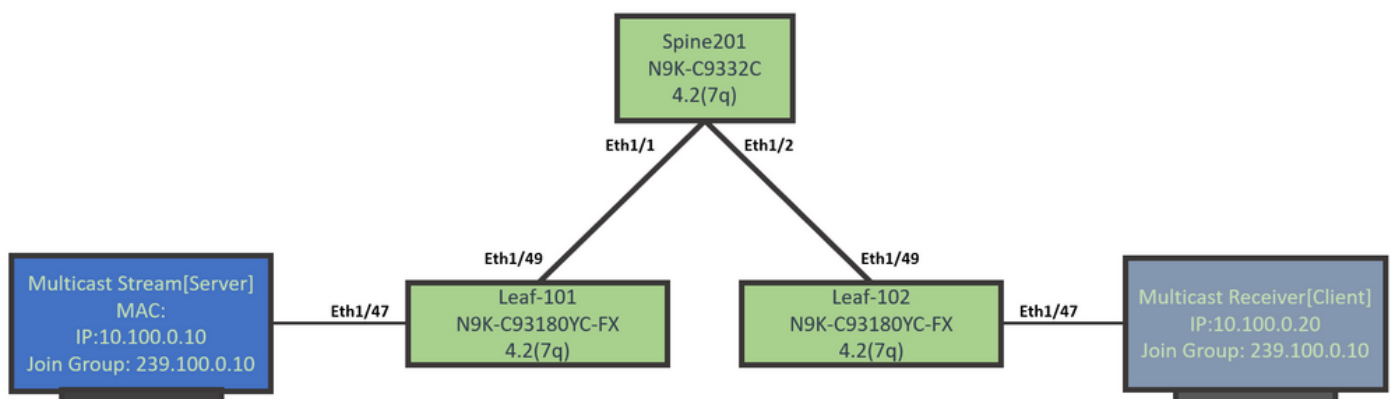
O multicast L2 na ACI é encaminhado somente dentro do BD. Se você tiver vários EPGs que usam o mesmo BD, a inundação de tráfego multicast em todos os EPGs, independentemente dos contratos em vigor entre os EPGs.

A Cisco ACI encaminha quadros multicast na árvore multicast de sobreposição criada entre switches leaf e spine. O tráfego de L2 usa árvores de FTAG (Forwarding Tag) para fornecer balanceamento de carga eficiente em vários links de custo redundantes. Para obter mais informações sobre os detalhes da árvore FTAG, consulte o documento [Fundamentos da ACI](#).

Observação: recomendamos que você não desative o IGMP snoop no BD. Se você desabilitar o IGMP Snoop, poderá ver um desempenho de multicast reduzido devido à inundação falsa excessiva no BD.

Configurar

Topologia de rede



Configurações

Este é um resumo das etapas de configuração. Não há muita configuração para multicast L2, exceto para habilitar um consultante IGMP.

- **Passo 1:** Configurar as políticas de acesso à estrutura para o servidor multicast e a

conectividade do host cliente

- **Passo 2:** Crie o EPG, BD e VRF para o receptor e origem multicast
- **Passo 3:** Conecte um domínio físico ao EPG e configure a porta estática
- **Passo 4:** Configurar o IGMP Querier

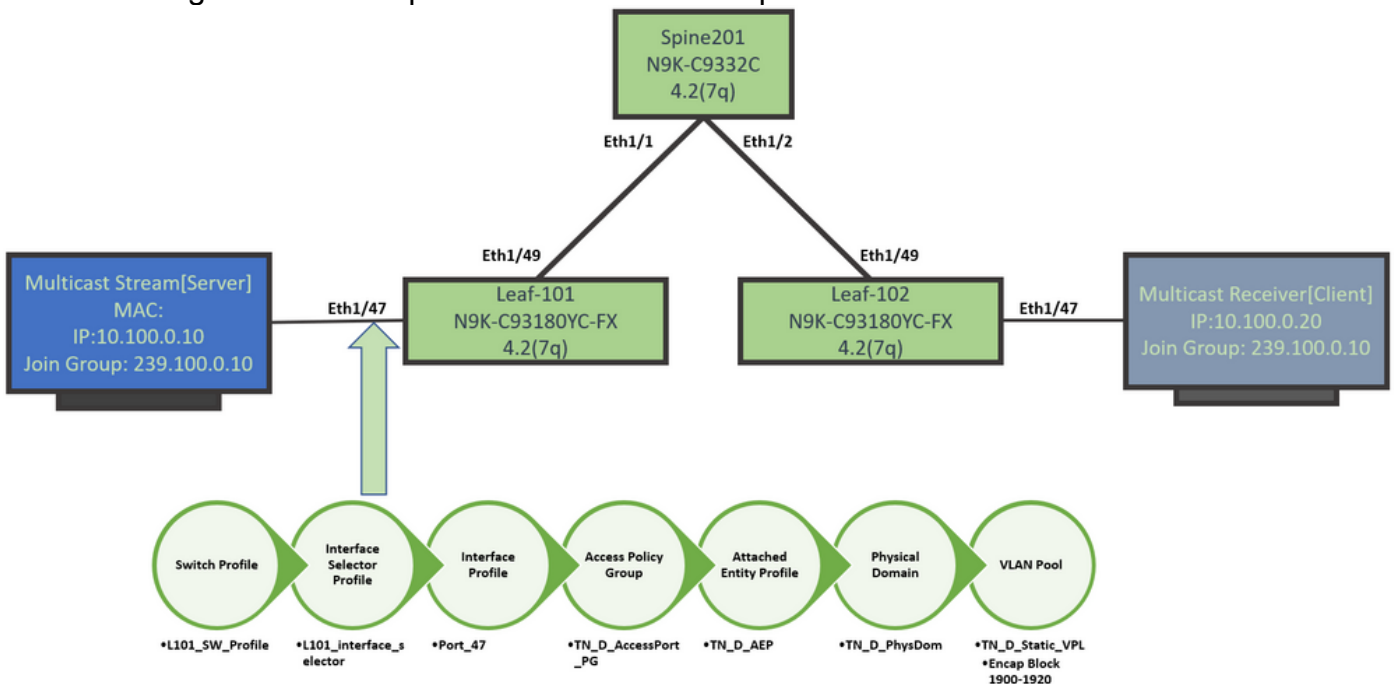
Esta seção descreve as etapas detalhadas de configuração.

Passo 1: Configurar as políticas de acesso à estrutura para o servidor multicast e a conectividade do host cliente

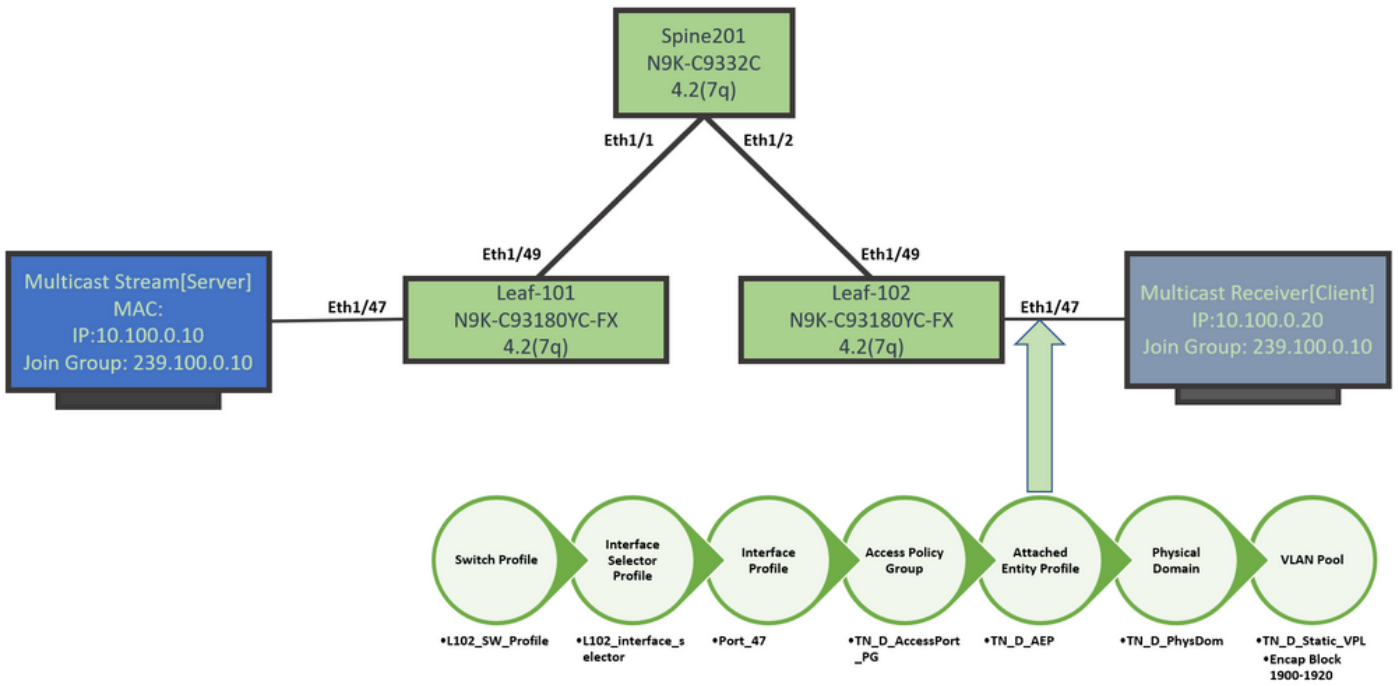
As imagens mostram a abordagem de alto nível da configuração. Detalhes adicionais sobre políticas de acesso estão disponíveis no documento [Implantação inicial da ACI](#).

Você pode pular esta etapa se as políticas de acesso já estiverem em vigor.

- Esta imagem mostra as políticas de estrutura de porta do servidor multicast.



- Esta imagem mostra as políticas de estrutura da porta do receptor de multicast (cliente).



Passo 2: Crie o EPG, BD e VRF para o receptor e origem multicast

- O EPG, BD e VRF são criados com parâmetros padrão.

Por padrão, um BD usa a política de snoop IGMP padrão predefinida no Espaço 'Comum'.

O consultante IGMP não é ativado por padrão na sub-rede BD, o que é o caso de uma implantação baseada em NXOS ou Cisco IOS® legado também.

- Para verificar a política de rastreamento IGMP padrão, escolha o 'Comum' localitário > **Políticas > Protocolo > IGMP Snoop > default** para ver se a política IGMP padrão não tem a caixa **Ativar consulta** marcada.

ALL TENANTS | Add Tenant | Tenant Search: name or descr | **common** | TN_D | mgmt | infra | Test1_Aks

common

- Quick Start
- common
 - Application Profiles
 - Networking
 - IP Address Pools
 - Contracts
 - Policies
 - Protocol
 - BFD
 - BGP
 - Custom QoS
 - DHCP
 - Data Plane Policing
 - EIGRP
 - End Point Retention
 - First Hop Security
 - HSRP
 - IGMP Interface
 - IGMP Snoop
 - default

IGMP Snoop Policy - default

Properties

Name: default
Description: optional

Admin State: Disabled Enabled

Control: Fast leave
 Enable querier

Last Member Query Interval (sec): 1

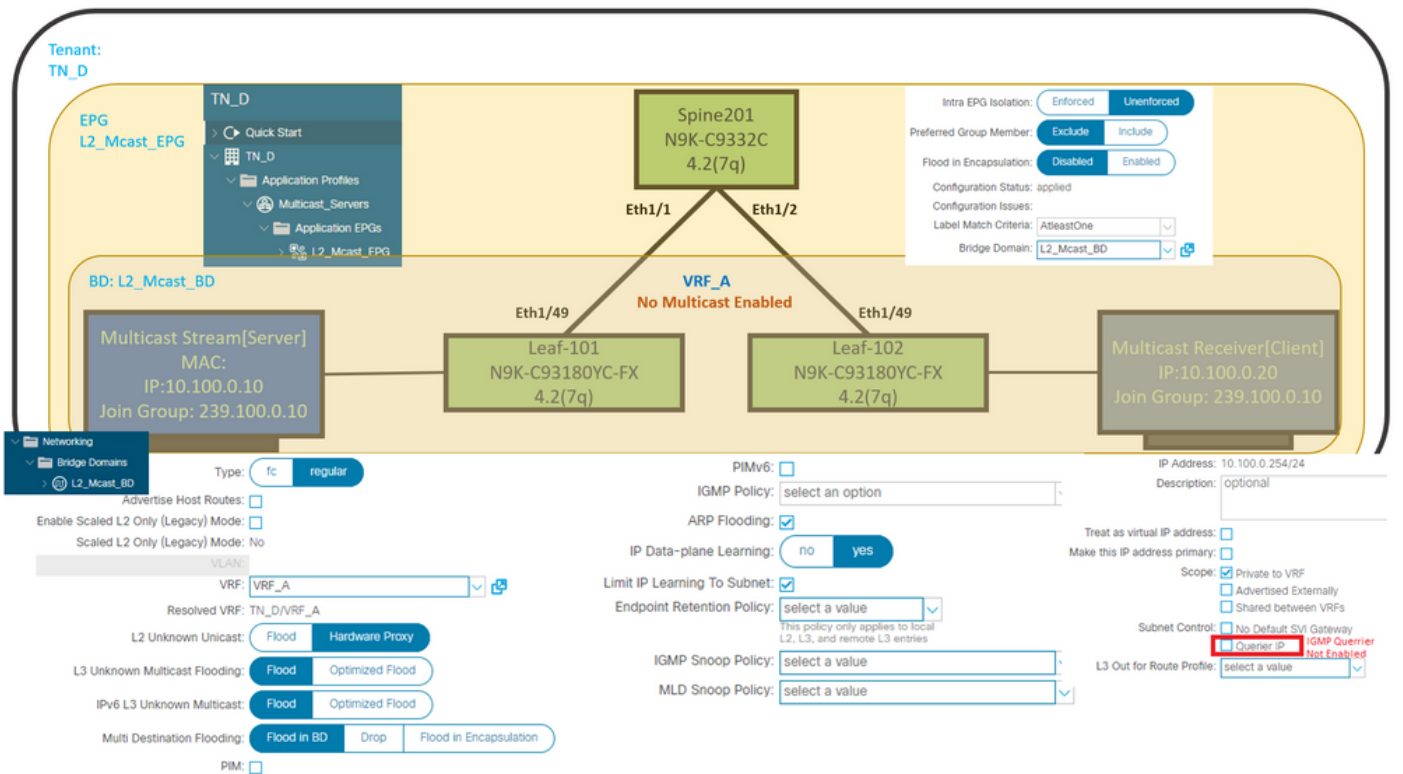
Query Interval (sec): 125

Query Response Interval (sec): 10

Start Query Count: 2

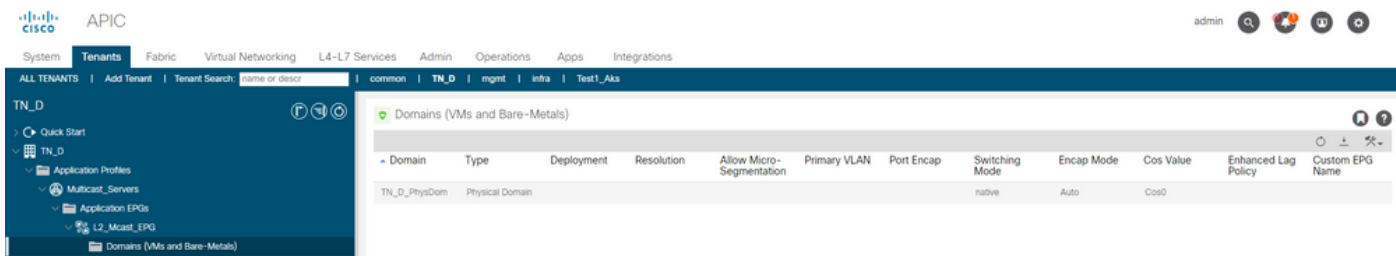
Start Query Interval (sec): 31

- Esta imagem mostra o resumo da configuração EPG, BD e VRF (exibição lógica).

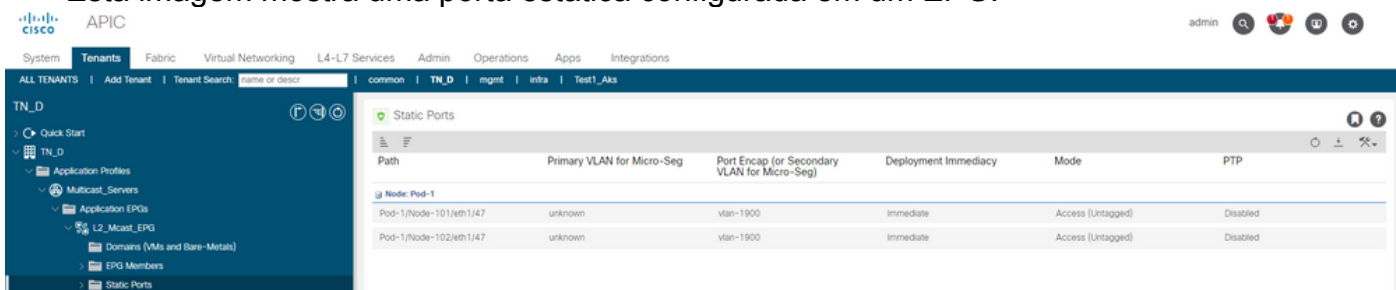


Passo 3: Conecte um domínio físico ao EPG e configure a porta estática

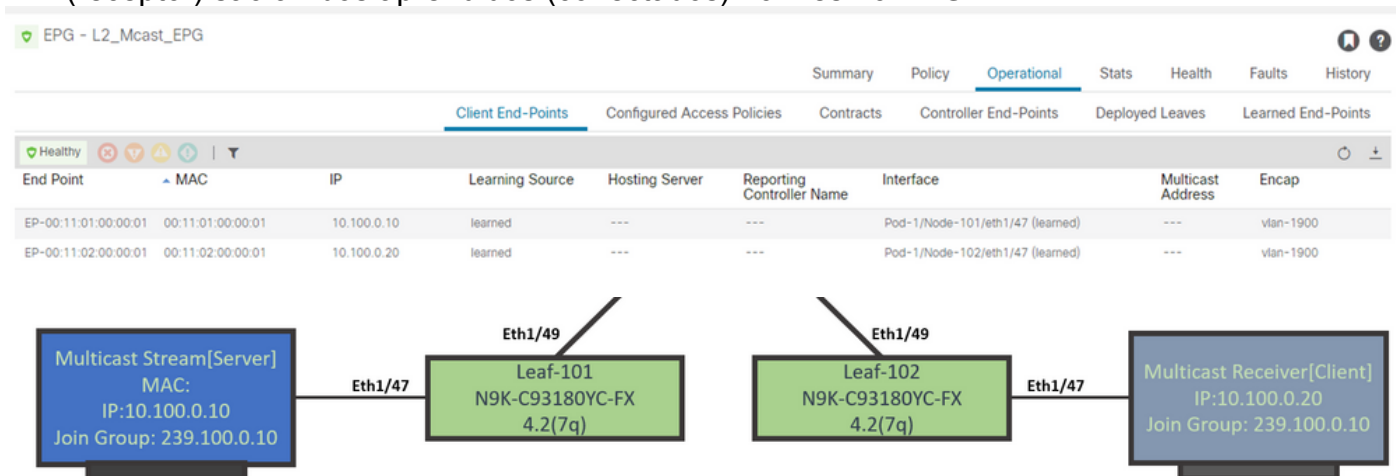
- Esta imagem mostra um domínio físico conectado a um EPG.



- Esta imagem mostra uma porta estática configurada em um EPG.



- Esta imagem mostra que os terminais do servidor multicast (origem) e do cliente multicast (receptor) são ambos aprendidos (conectados) no mesmo EPG.



Passo 4: Configurar o IGMP Querier

O solicitante IGMP deve estar habilitado em dois lugares, sob a respectiva política de IGMP snoop e sob a sub-rede BD.

Note: Como a política de rastreamento IGMP com **Enable querier enabled** requer um endereço IP de origem para enviar a consulta IGMP, é necessário configurar enable the IGMP **Querier IP** sob a sub-rede BD. Caso contrário, o switch leaf não enviará a consulta IGMP ao receptor multicast.

É sempre recomendável configurar uma nova política de espionagem IGMP com o verificador IGMP ativado em vez de usar uma política de rastreamento IGMP padrão. Observe que a política de rastreamento IGMP padrão não tem um consultante IGMP ativado por padrão e é anexado por padrão a cada BD. Uma alteração em qualquer configuração sob a política de rastreamento IGMP padrão afeta cada BD anexado à política de rastreamento IGMP padrão, portanto, não é recomendável alterar os parâmetros da política de rastreamento IGMP padrão na ACI.

- Para criar uma nova política de rastreamento IGMP, escolha o **espaço TN_D > Políticas > Protocolos** e clique com o botão direito do mouse em **IGMP Snoop** e clique em **Criar política de rastreamento IGMP**.

