

# De L2-multicast in ACI configureren

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerktopologie](#)

[Configuraties](#)

[Stap 1: Het fabric-toegangsbeleid voor de multicast server en clienthostconnectiviteit configureren](#)

[Stap 2: Maak de EPG, BD en VRF voor de multicast ontvanger en bron](#)

[Stap 3: Hang een fysiek domein aan de EPG en stel de statische poort in](#)

[Stap 4: IGMP-wachtrij configureren](#)

[Verifiëren](#)

[Uitleg van de L2-multicast pakketstroom](#)

[IGMP Hogere vereisten](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe u Layer 2 (L2) multicast in hetzelfde Endpoint Group (EPG) kunt configureren en controleren op één Application Centric Infrastructure (ACI)-fabric.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- L2 multicast ondersteuning in ACI - altijd ondersteund
- Internet Group Management Protocol (IGMP)-snooping in ACI - standaard ingeschakeld

**Opmerking:** Zie [Cisco APIC- en IGMP Layer 2 Multicast Configuration](#)-document voor meer informatie over IGMP-[snooping](#).

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- N9K-C93180YC-FX
- release 4.2(7q)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Achtergrondinformatie

L2 multicast verwijst naar IP multicast-pakketten die op een L2 netwerk-segment (bridge-domein (BD)/plus) worden doorgestuurd, niet L2 niet-IP multicast-pakketten die multicast-pakketten zijn met een doelmulticast MAC-adres zonder een IP-header. L2 multicast sluit ook link naar lokale multicast uit (224.0.0.0/24). De lokale multicast van de verbinding wordt altijd naar alle havens in de BD verzonden.

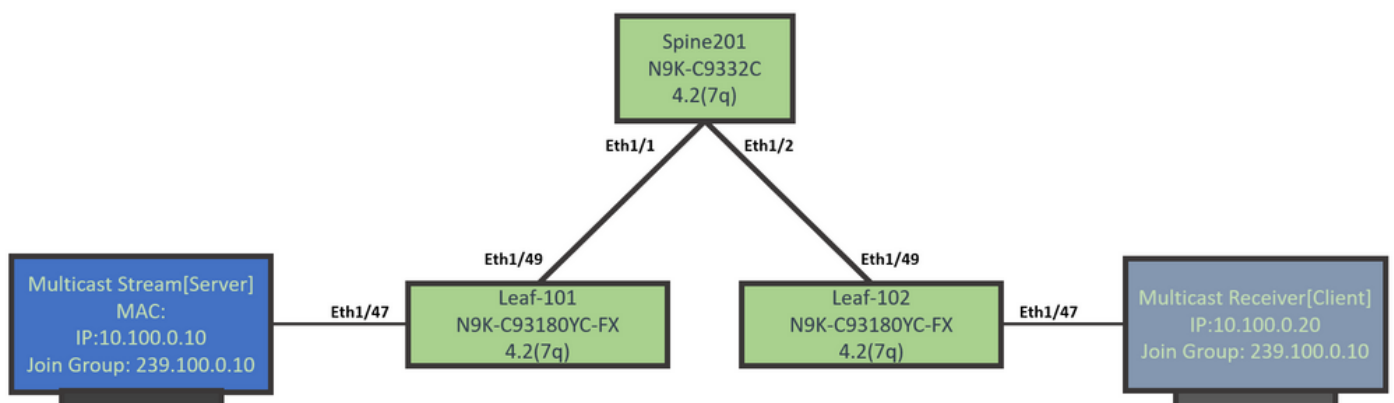
L2 multicast in ACI wordt alleen binnen de BD verzonden. Als u meerdere EPG's heeft die dezelfde BD gebruiken, zou multicast verkeer in alle EPG's kunnen overstromen, ongeacht contracten tussen EPG's.

Cisco ACI voorwaarts multicast frames op de lay-multicast boom die tussen switches van blad en wervelkolom is gebouwd. L2 traffic use Forwarding Tag (FTAG)-bomen om een efficiënte taakverdeling te bieden over meerdere, redundante, zelfde kostenkoppelingen. Zie het [ACI fundamentals](#)-document voor meer informatie over de details van de FTAG-boom.

**Opmerking:** we raden u aan om IGMP-snoop op de BD niet uit te schakelen. Als u IGMP-snoop uitschakelt, worden de multicast-prestaties mogelijk verminderd door een buitensporige valse overstroming binnen de BD.

## Configureren

### Netwerktopologie



## Configuraties

Dit is een samenvatting van de configuratiestappen. Er is niet veel configuratie voor L2 multicast behalve om een IGMP-zoeker in te schakelen.

- **Stap 1:** Het fabric-toegangsbeleid voor de multicast server en clienthostconnectiviteit configureren

- **Stap 2:** Maak de EPG, BD en VRF voor de multicast ontvanger en bron
- **Stap 3:** Hang een fysiek domein aan de EPG en stel de statische poort in
- **Stap 4:** IGMP-wachtrij configureren

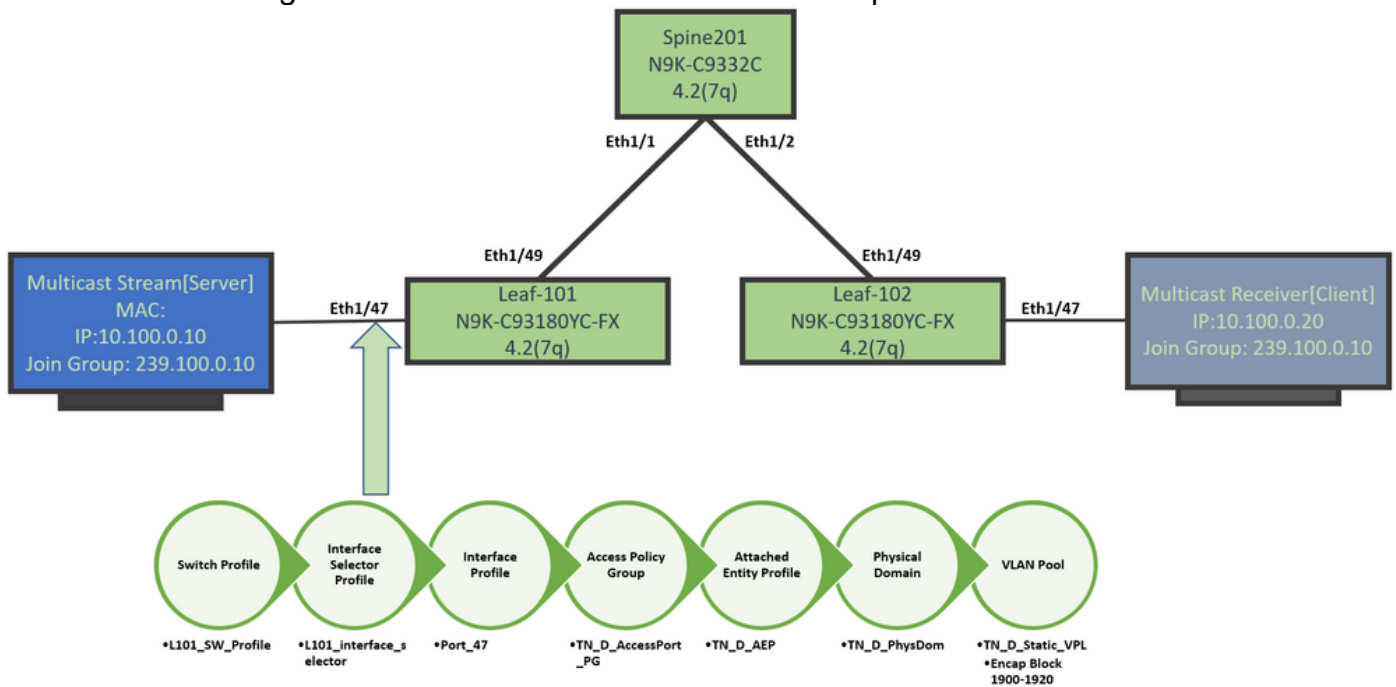
In dit gedeelte worden de gedetailleerde configuratiestappen beschreven.

### Stap 1: Het fabric-toegangsbeleid voor de multicast server en clienthostconnectiviteit configureren

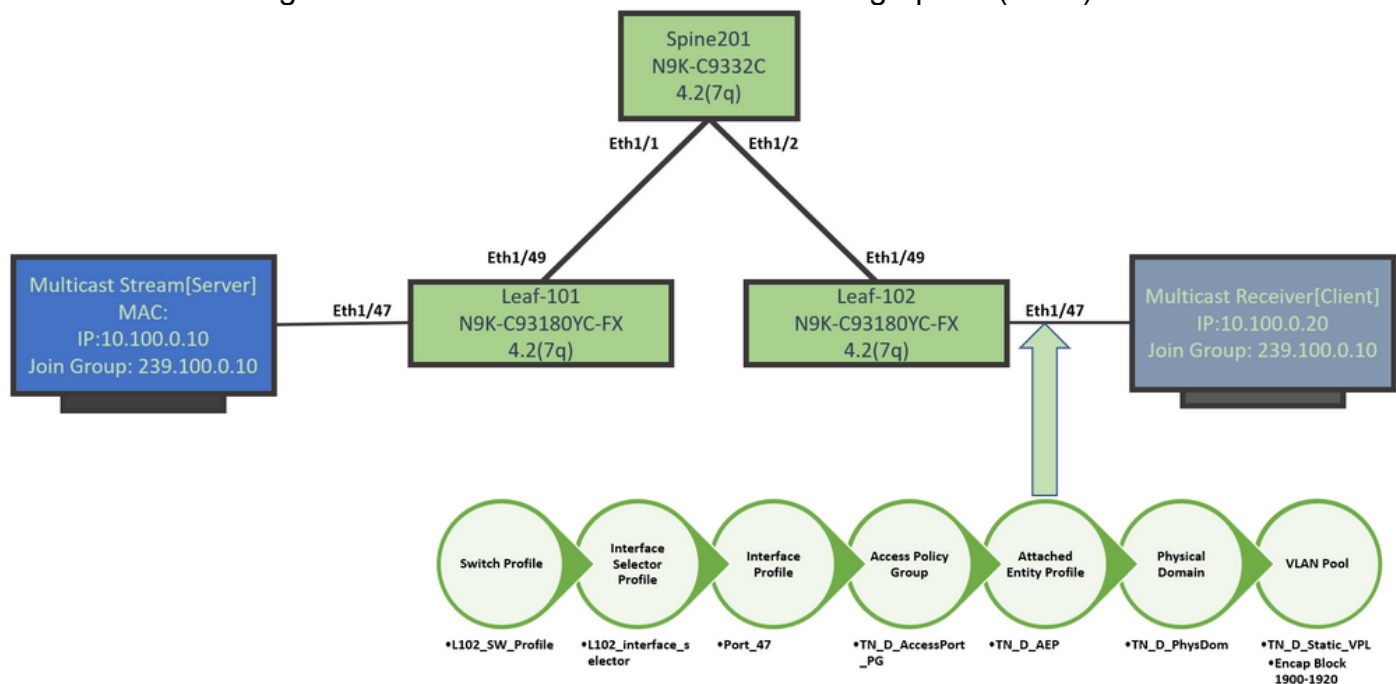
De beelden tonen de benadering op hoog niveau van de configuratie. Aanvullende informatie over het toegangsbeleid is beschikbaar in het [ACI Initiële](#) implementatiedocument.

U kunt deze stap overslaan als het toegangsbeleid al is ingesteld.

- Deze afbeelding toont het beleid van de multicast server port stof.



- Deze afbeelding toont het beleid van de multicast ontvangerpoort (client) van de fabric.



## Stap 2: Maak de EPG, BD en VRF voor de multicast ontvanger en bron

- De EPG, BD en VRF worden gemaakt met standaardparameters.

The screenshot displays three configuration windows in the Cisco NXOS GUI:

- EPG - L2\_Mcast\_EPG:** Shows properties for the EPG, including Name (L2\_Mcast\_EPG), Description (optional), and Bridge Domain (L2\_Mcast\_BD).
- Bridge Domain - L2\_Mcast\_BD:** Shows properties for the Bridge Domain, including Name (L2\_Mcast\_BD), Description (optional), and Type (regular).
- VRF - VRF\_A:** Shows properties for the VRF, including Name (VRF\_A), Description (optional), and various routing options like L2 Unknown Unicast and L3 Unknown Multicast.

Red arrows indicate the relationships between the configurations: one arrow points from the Bridge Domain dropdown in the EPG window to the Bridge Domain window, and another points from the VRF dropdown in the EPG window to the VRF\_A window. A third arrow points from the VRF\_A window to the Multicast configuration window.

Standaard gebruikt een BD het standaard IGMP-sneeuwbeleid dat is vastgelegd in de 'Common' Tenant.

De IGMP-kwader is niet standaard ingeschakeld onder het BD-subsysteem, wat ook het geval is voor een bestaande NXOS- of Cisco IOS®-gebaseerde implementatie.

- Om het standaard IGMP-snoepbeleid te controleren kies de optie 'Common' > Opties > Protocol > IGMP-standaard > IGMP om te zien dat het standaard IGMP-beleid niet het vakje Enable querier heeft ingeschakeld.

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

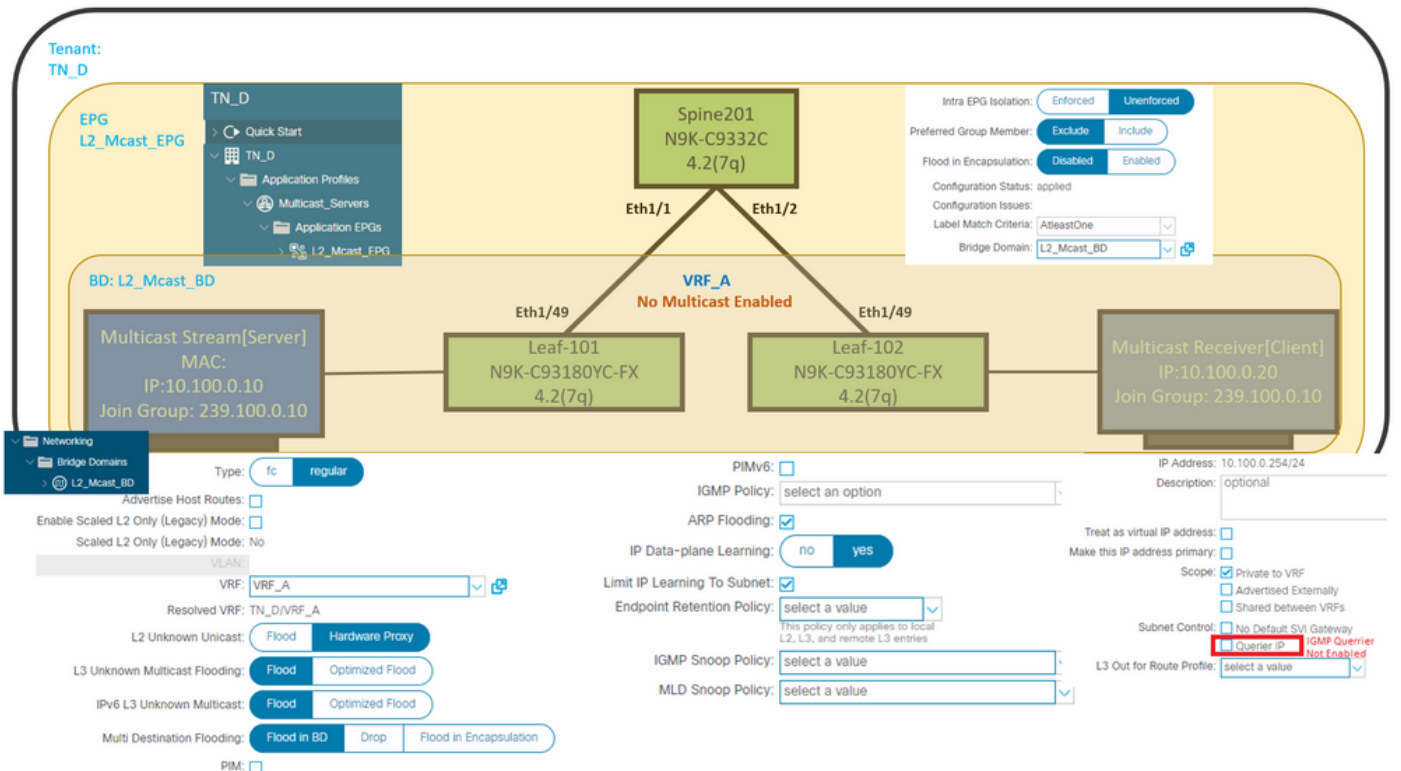
Query Interval (sec): 125

Query Response Interval (sec): 10

Start Query Count: 2

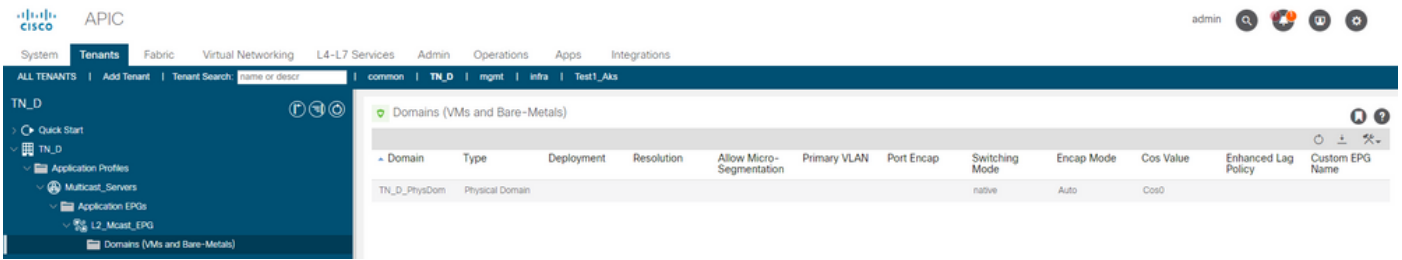
Start Query Interval (sec): 31

- Deze afbeelding toont de samenvatting van de configuratie van het EPG, het BD en het VRF (logische weergave).

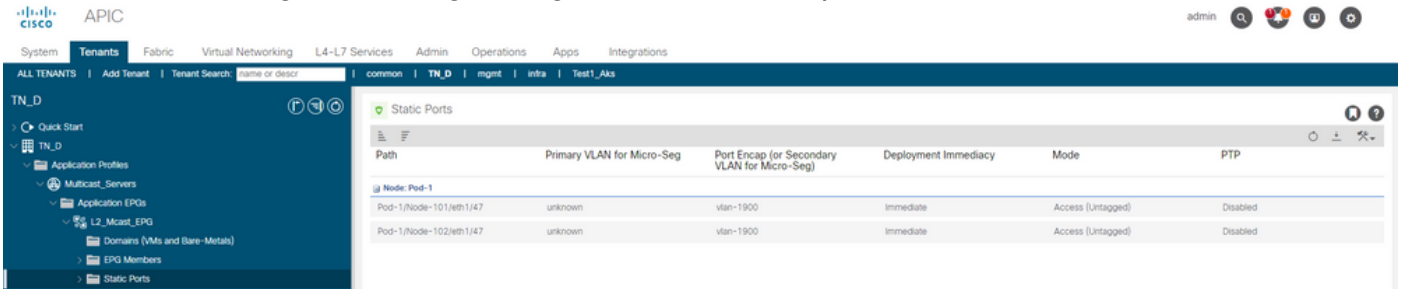


Stap 3: Hang een fysiek domein aan de EPG en stel de statische poort in

- Deze afbeelding toont een fysiek domein dat aan een EPG is gekoppeld.



- Deze afbeelding toont een geconfigureerde statische poort onder een EPG.



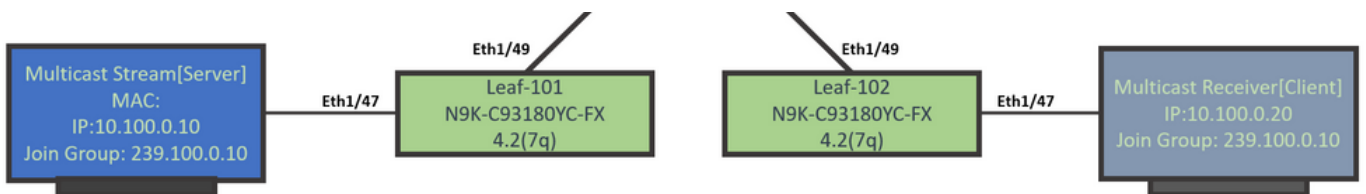
- Dit beeld toont aan dat het multicast server (bron) eindpunt en het multicast client (ontvanger) eindpunten beiden geleerd (verbonden) worden onder dezelfde EPG.

EPG - L2\_Mcast\_EPG

Summary Policy **Operational** Stats Health Faults History

Client End-Points Configured Access Policies Contracts Controller End-Points Deployed Leaves Learned End-Points

End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap
EP-00:11:01:00:00:01	00:11:01:00:00:01	10.100.0.10	learned	---	---	Pod-1/Node-101/eth1/47 (learned)	---	vlan-1900
EP-00:11:02:00:00:01	00:11:02:00:00:01	10.100.0.20	learned	---	---	Pod-1/Node-102/eth1/47 (learned)	---	vlan-1900



#### Stap 4: IGMP-wachtrij configureren

Het IGMP kwader moet twee plaatsen, onder het respectieve IGMP snoopbeleid en onder het BD Subnet worden toegelaten.

**Opmerking:** Aangezien het IGMP snooping beleid met **Querier** toelaat een bron IP adres vereist om de IGMP query te verzenden is het vereist om IGMP **Querier IP** onder BD sub te configureren toe te **schakelen**. Anders zal de bladeswitch switch de IGMP-query niet naar de multicast ontvanger sturen.

Het wordt altijd aanbevolen om een nieuw IGMP-sneeuwbeleid te configureren met een IGMP-versterkerfunctie die eerder is ingeschakeld dan met een standaard IGMP-sneopingbeleid. Merk op dat het standaard IGMP-snooping beleid geen IGMP-querier heeft ingeschakeld en dat dit standaard bij elke BD is aangesloten. Een verandering in om het even welke configuratie onder het standaard IGMP-sneeuwbeleid beïnvloedt elke BD die verbonden is met het standaard IGMP-sneopiniebeleid, dus wordt het niet aanbevolen om de standaard IGMP-parameters voor snooping in ACI te wijzigen.

- Om een nieuw IGMP-sneopingbeleid te maken, kiest u de **TN\_D huurder > Beleid > Protocols**, dan klikt u met de rechtermuisknop op **IGMP-snoop** en vervolgens klikt u met de rechtermuisknop op **IGMP-snoopbeleid maken**.

