Configure the L2 Multicast in ACI

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
Network Topology
Configurations
Step 1: Configure the Fabric Access Policies for the Multicast Server and Client Host Connectivity
Step 2: Create the EPG, BD, and VRF for the Multicast Receiver and Source
Step 3: Attach a Physical Domain to the EPG and Configure the Static Port
Step 4: Configure IGMP Querier
Verify
Explanation of the L2 Multicast Packet Flow
IGMP Querier Requirement
Troubleshoot
Related Information

Introduction

This document describes how to configure and verify Layer 2 (L2) multicast in the same Endpoint Group (EPG) on a single Application Centric Infrastructure (ACI) fabric.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- L2 multicast support in ACI - always supported
- Internet Group Management Protocol (IGMP) snooping in ACI - enabled by default

  Note: For more information on IGMP snooping, see the Cisco APIC and IGMP Snoop Layer 2 Multicast Configuration document.

Components Used

The information in this document is based on these software and hardware versions:

- N9K-C93180YC-FX
- Release 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

L2 multicast refers to IP multicast packets forwarded on a L2 network segment (bridge domain(BD)/subnet), not L2 non-IP multicast packets which are multicast packets with a destination multicast MAC address without an IP header. L2 multicast also excludes link local multicast (224.0.0.0/24). Link local multicast is always forwarded to all ports in the BD.

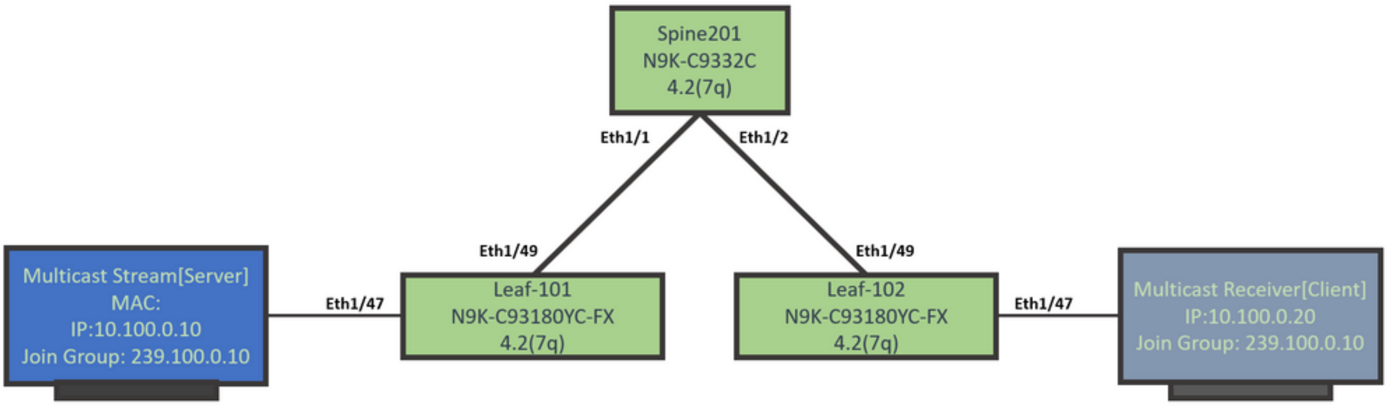
L2 multicast in ACI is only forwarded within the BD. If you have multiple EPGs that use the same BD, multicast traffic flood in all EPGs regardless of contracts in place between EPGs.

Cisco ACI forwards multicast frames on the overlay multicast tree that is built between leaf and spine switches. L2 traffic uses Forwarding Tag (FTAG) trees to provide efficient load balancing across multiple, redundant, same cost links. For more information on the details of FTAG tree, see the ACI Fundamentals document.

> **Note**: We recommend that you do not disable IGMP snoop on the BD. If you disable IGMP snoop, you might see reduced multicast performance because of excessive false flood within the BD.

Configure

Network Topology



Configurations

This is a summary of the configuration steps. There is not much configuration for L2 multicast except to enable an IGMP querier.

- **Step 1:** Configure the Fabric Access Policies for the Multicast Server and Client Host Connectivity
- **Step 2:** Create the EPG, BD, and VRF for the Multicast Receiver and Source
- **Step 3:** Attach a Physical Domain to the EPG and Configure the Static Port
- **Step 4:** Configure the IGMP Querier

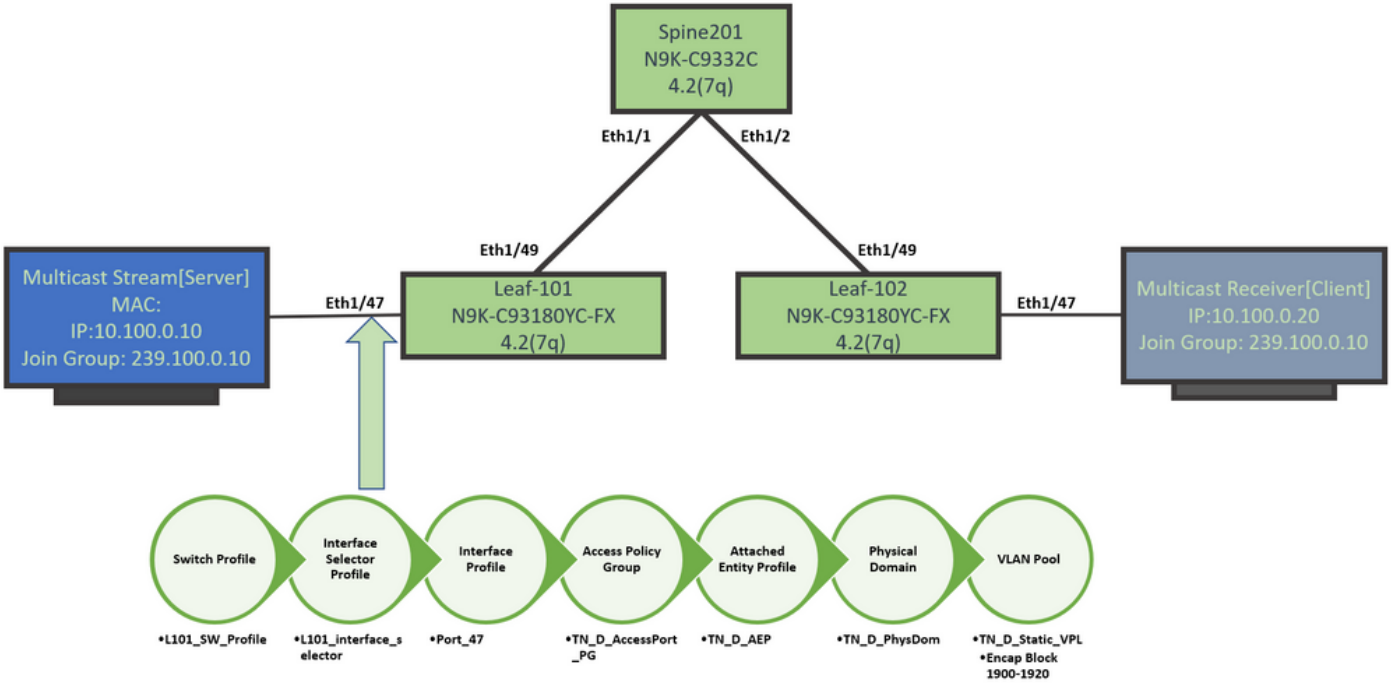
This section describes the detailed configuration steps.

Step 1: Configure the Fabric Access Policies for the Multicast Server and Client Host Connectivity

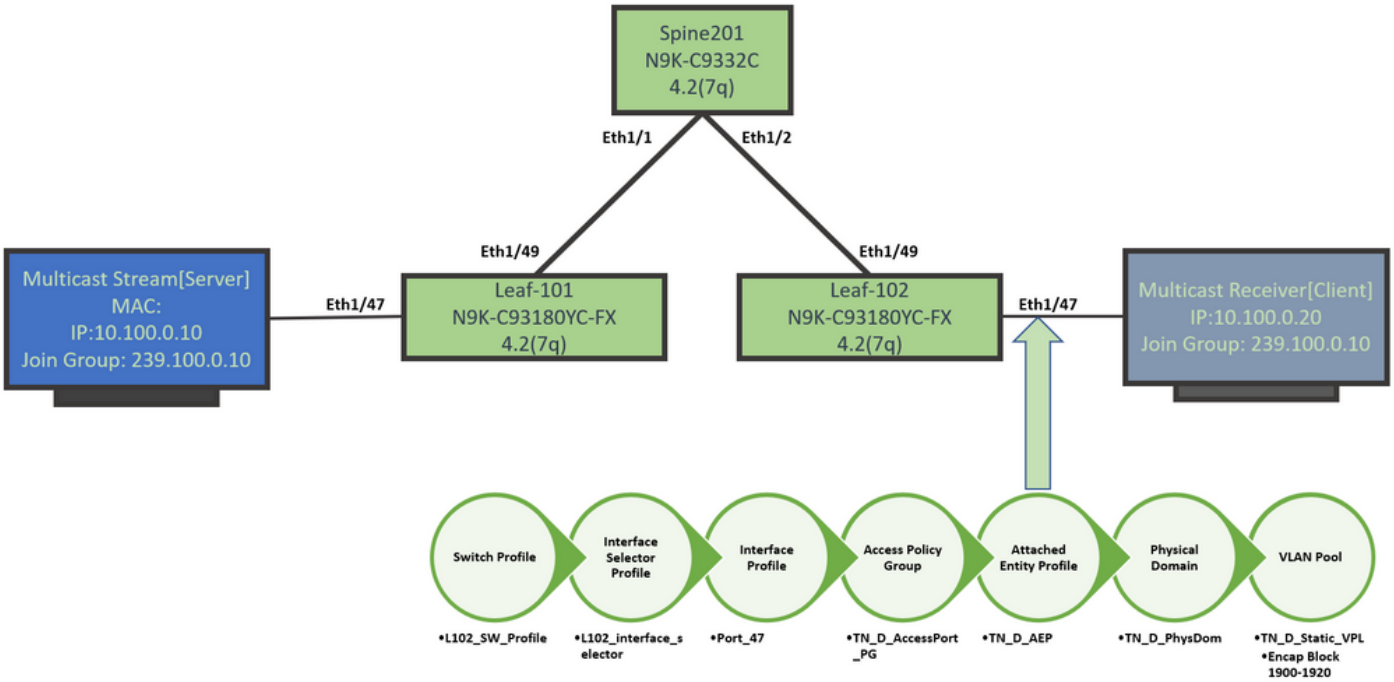
The images show the high-level approach to the configuration. Additional details about access policies is available in the ACI Initial Deployment document.

You can skip this step if the access policies are already in place.

- This image shows the multicast server port fabric polices.

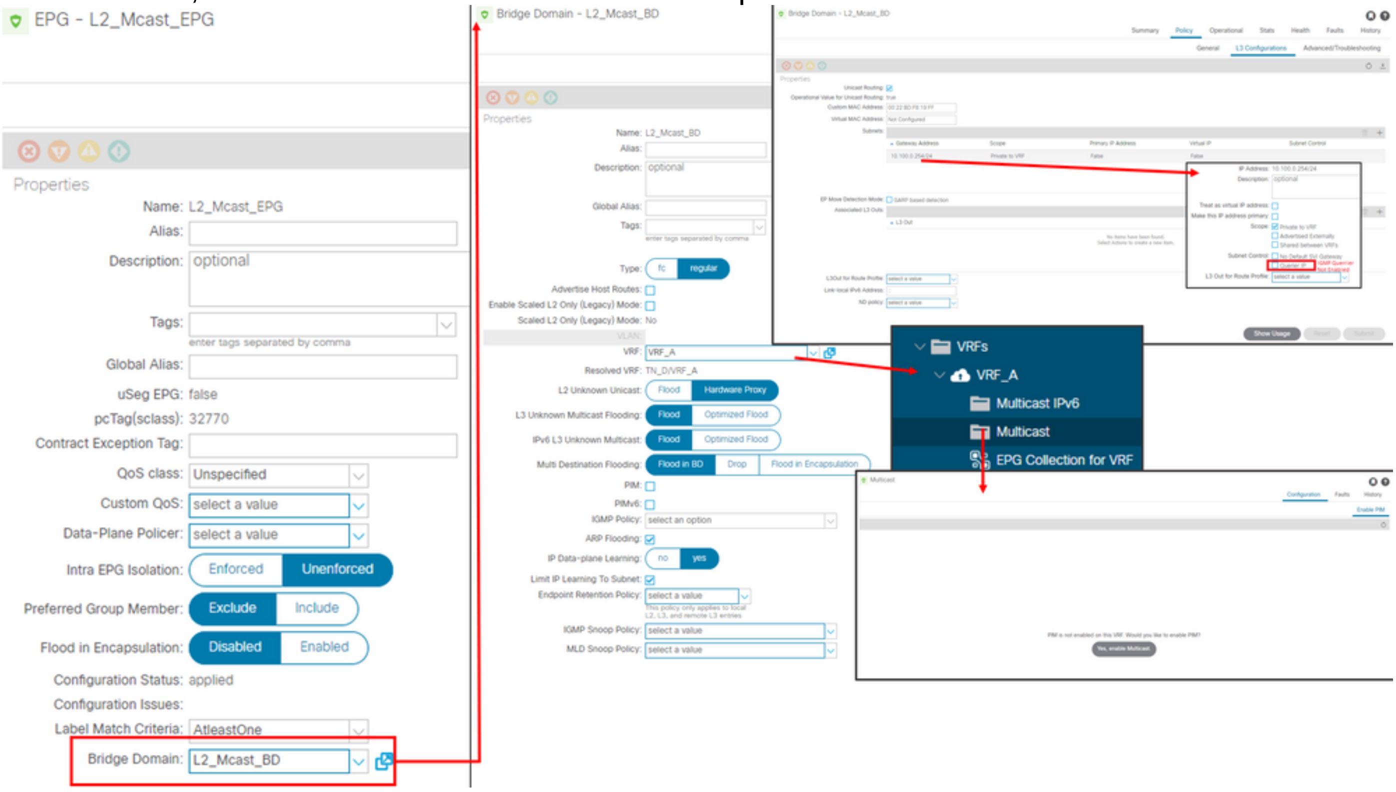


- This image shows the multicast receiver port (client) fabric polices.



Step 2: Create the EPG, BD, and VRF for the Multicast Receiver and Source

- The EPG, BD and VRF are created with default parameters.



EPG - L2_Mcast_EPG

Properties

Name: L2_Mcast_EPG
Alias:
Description: optional
Tags: enter tags separated by comma
Global Alias:
uSeg EPG: false
pcTag(sclass): 32770
Contract Exception Tag:
QoS class: Unspecified
Custom QoS: select a value
Data-Plane Policer: select a value
Intra EPG Isolation: Enforced [✓ Unenforced]
Preferred Group Member: [✓ Exclude] Include
Flood in Encapsulation: [✓ Disabled] Enabled
Configuration Status: applied
Configuration Issues:
Label Match Criteria: AtleastOne
Bridge Domain: L2_Mcast_BD

Bridge Domain - L2_Mcast_BD

Properties

Name: L2_Mcast_BD
Alias:
Description: optional
Global Alias:
Tags: enter tags separated by comma
Type: fc [✓ regular]
Advertise Host Routes: □
Enable Scaled L2 Only (Legacy) Mode: □
Scaled L2 Only (Legacy) Mode: No
VLAN:
VRF: VRF_A
Resolved VRF: TN_D/VRF_A
L2 Unknown Unicast: Flood [✓ Hardware Proxy]
L3 Unknown Multicast Flooding: [✓ Flood] Optimized Flood
IPv6 L3 Unknown Multicast: [✓ Flood] Optimized Flood
Multi Destination Flooding: [✓ Flood in BD] Drop Flood in Encapsulation
PIM: □
PIMv6: □
IGMP Policy: select an option
ARP Flooding: ☑
IP Data-plane Learning: no [✓ yes]
Limit IP Learning To Subnet: ☑
Endpoint Retention Policy: select a value
This policy only applies to local L2, L3, and remote L3 entries
IGMP Snoop Policy: select a value
MLD Snoop Policy: select a value

Bridge Domain - L2_Mcast_BD

Summary Policy Operational Stats Health Faults History
General L3 Configurations Advanced/Troubleshooting

Properties

Unicast Routing: ☑
Operational Value for Unicast Routing: true
Custom MAC Address: 00:22:BD:F8:19:FF
Virtual MAC Address: Not Configured
Subnets:

Gateway Address	Scope	Primary IP Address	Virtual IP	Subnet Control
10.100.0.254/24	Private to VRF	False	False	

EP Move Detection Mode: □ GARP based detection
Associated L3 Outs:
L3 Out
No items have been found. Select Actions to create a new item.
L3Out for Route Profile: select a value
Link-local IPv6 Address: ::
ND policy: select a value

IP Address: 10.100.0.254/24
Description: optional
Treat as virtual IP address: □
Make this IP address primary: □
Scope: ☑ Private to VRF
□ Advertised Externally
□ Shared between VRFs
Subnet Control: □ No Default SVI Gateway
□ Querier IP
IGMP Querier Not Enabled
L3 Out for Route Profile: select a value

Show Usage Reset Submit

VRFs
VRF_A
Multicast IPv6
Multicast
EPG Collection for VRF

Multicast

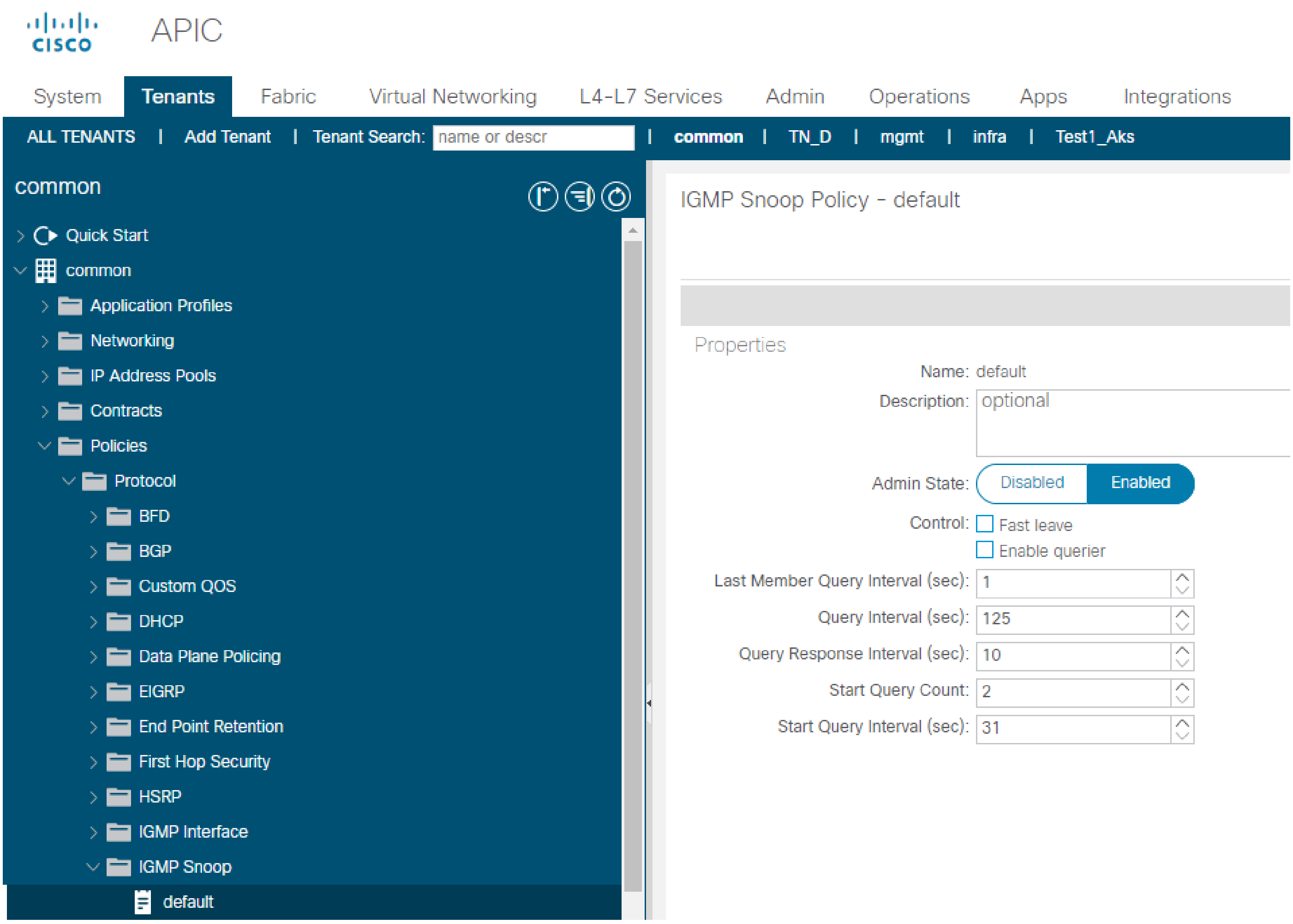
Configuration Faults History
Enable PIM

PIM is not enabled on this VRF. Would you like to enable PIM?
Yes, enable Multicast

By default, a BD uses the default **IGMP snoop policy that is predefined in the 'Common' Tenant**.

The IGMP querier is not enabled by default under the BD subnet, which is the case for a legacy NXOS or Cisco IOS® based deployment as well.

- In order to check the default IGMP snoop policy, choose the **'Common' tenant > Polices > Protocol > IGMP Snoop > default** to see that the default IGMP policy does not have the **Enable querier** box checked.



IGMP Snoop Policy - default

Properties

Name: default

Description: optional

Admin State: Disabled [✓ Enabled]

Control: □ Fast leave

□ Enable querier

Last Member Query Interval (sec): 1

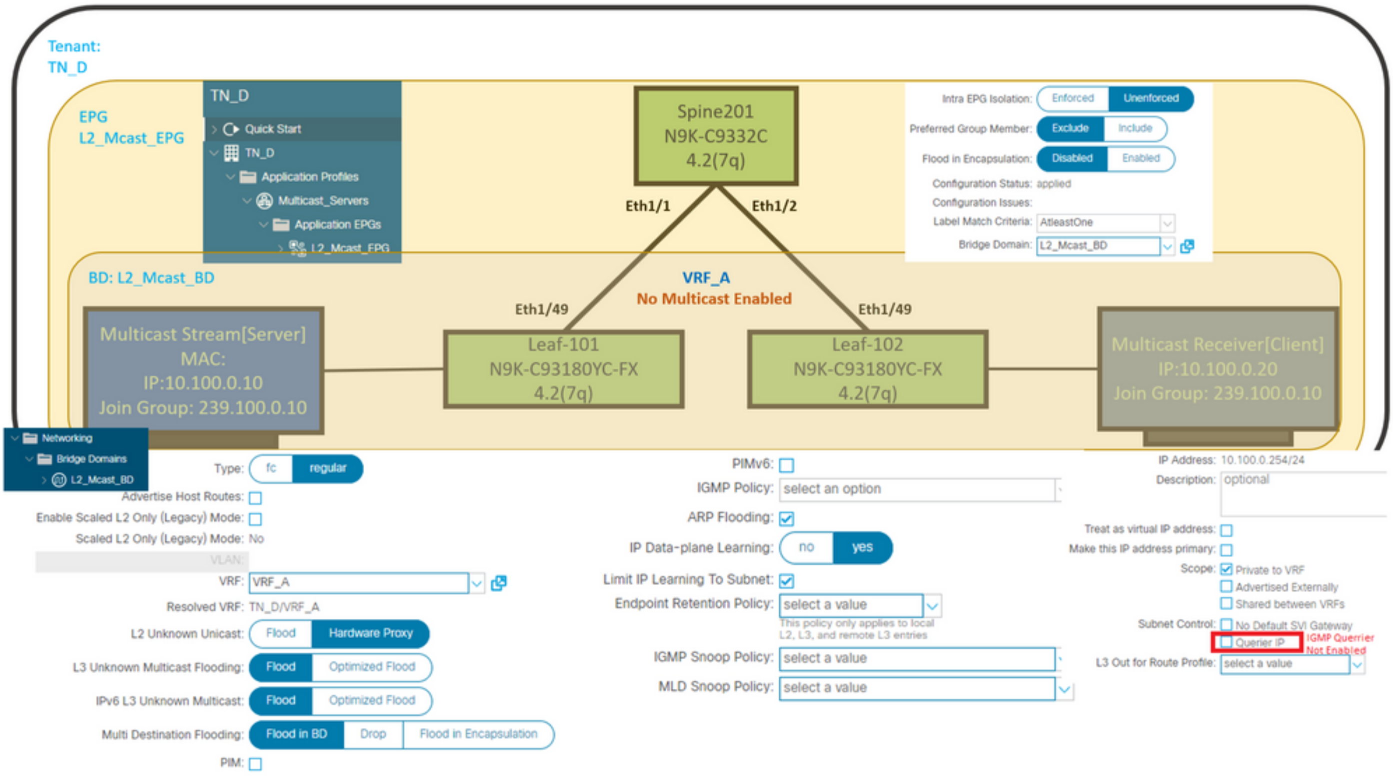
Query Interval (sec): 125

Query Response Interval (sec): 10

Start Query Count: 2

Start Query Interval (sec): 31

- This image shows the summary of the EPG, BD, and VRF configuration (logical view).



Intra EPG Isolation: Enforced [✓ Unenforced]

Preferred Group Member: [✓ Exclude] Include

Flood in Encapsulation: [✓ Disabled] Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: L2_Mcast_BD

Type: fc [✓ regular]

Advertise Host Routes: □

Enable Scaled L2 Only (Legacy) Mode: □

Scaled L2 Only (Legacy) Mode: No

VLAN:

VRF: VRF_A

Resolved VRF: TN_D/VRF_A

L2 Unknown Unicast: Flood [✓ Hardware Proxy]

L3 Unknown Multicast Flooding: [✓ Flood] Optimized Flood

IPv6 L3 Unknown Multicast: [✓ Flood] Optimized Flood

Multi Destination Flooding: [✓ Flood in BD] Drop Flood in Encapsulation

PIM: □

PIMv6: □

IGMP Policy: select an option

ARP Flooding: ☑

IP Data-plane Learning: no [✓ yes]

Limit IP Learning To Subnet: ☑

Endpoint Retention Policy: select a value

This policy only applies to local L2, L3, and remote L3 entries

IGMP Snoop Policy: select a value

MLD Snoop Policy: select a value

IP Address: 10.100.0.254/24

Description: optional

Treat as virtual IP address: □

Make this IP address primary: □

Scope: ☑ Private to VRF

□ Advertised Externally

□ Shared between VRFs

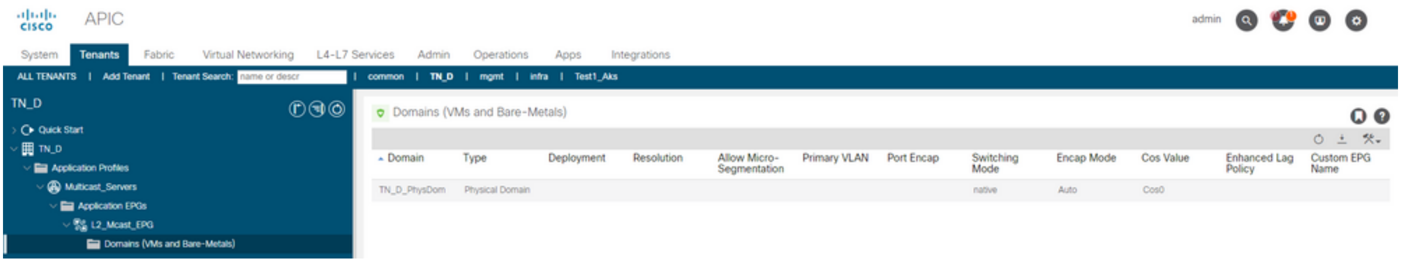
Subnet Control: □ No Default SVI Gateway

□ Querier IP

L3 Out for Route Profile: select a value

Step 3: Attach a Physical Domain to the EPG and Configure the Static Port

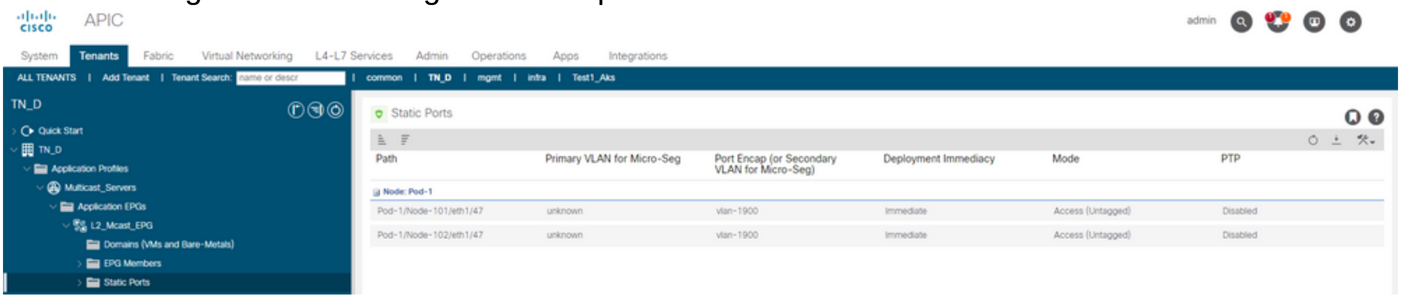
- This image shows a physical domain attached to an EPG.



Domains (VMs and Bare-Metals)

Domain	Type	Deployment	Resolution	Allow Micro-Segmentation	Primary VLAN	Port Encap	Switching Mode	Encap Mode	Cos Value	Enhanced Lag Policy	Custom EPG Name
TN_D_PhysDom	Physical Domain						native	Auto	Cos0		

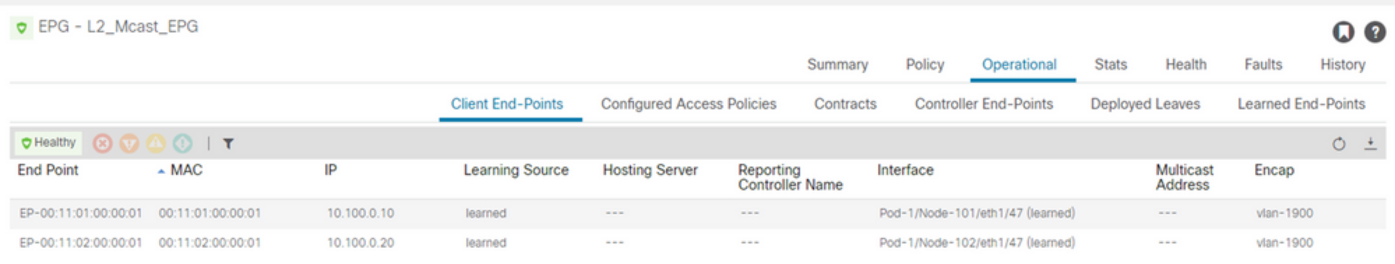
- This image shows a configured static port under an EPG.



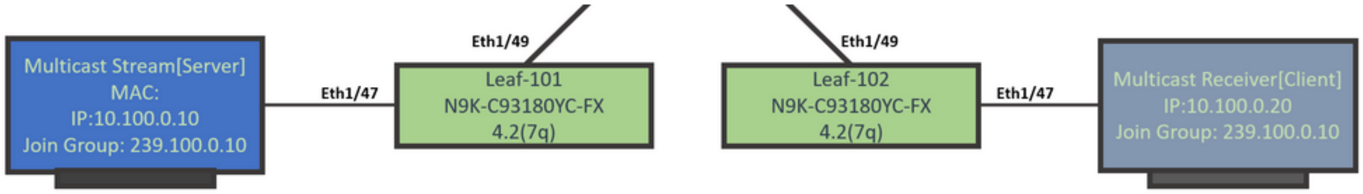
Static Ports

Path	Primary VLAN for Micro-Seg	Port Encap (or Secondary VLAN for Micro-Seg)	Deployment Immediacy	Mode	PTP
Node: Pod-1					
Pod-1/Node-101/eth1/47	unknown	vlan-1900	Immediate	Access (Untagged)	Disabled
Pod-1/Node-102/eth1/47	unknown	vlan-1900	Immediate	Access (Untagged)	Disabled

- This image shows that the multicast server (source) endpoint and multicast client (receiver) end points are both learned (connected) under same EPG.



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



Step 4: Configure IGMP Querier

The IGMP querier must be enabled two places, under the respective IGMP snoop policy and under the BD subnet.

Note: Since the IGMP snooping policy with **Enable querier** enabled requires a source IP address to send the IGMP query, it is required to configure enable the IGMP **Querier IP** under the BD subnet. Otherwise, the leaf switch will not send the IGMP query to the multicast receiver.

It is always recommended to configure a new IGMP snooping policy with IGMP querier enabled instead of using a default IGMP snooping policy. Note that the default IGMP snooping policy does not have an IGMP querier enabled by default and it is default attached with every BD. A change to any configuration under the default IGMP snooping policy affects each BD attached with the default IGMP snoop policy, so it is not recommended to change the the default IGMP snooping policy parameters in ACI.

- In order to create a new IGMP snooping policy, choose the **TN_D tenant > Policies > Protocols**, then right-click on **IGMP Snoop** and click **Create IGMP Snoop Policy**.