# Konfigurieren des L2-Multicast in der ACI

## Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Netzwerktopologie Konfigurationen Schritt 1: Konfigurieren der Fabric-Zugriffsrichtlinien für die Verbindung von Multicast-Server und **Client-Host** Schritt 2: Erstellen Sie EPG, BD und VRF für den Multicast Receiver und die Quelle. Schritt 3: Anfügen einer physischen Domäne an die EPG und Konfigurieren des statischen Ports Schritt 4: Konfigurieren von IGMP Querier Überprüfung Erläuterung des L2-Multicast-Paketflusses **IGMP** Querier-Anforderung Fehlerbehebung Zugehörige Informationen

## Einleitung

In diesem Dokument wird beschrieben, wie Layer-2-Multicast (L2) in derselben Endpunktgruppe (EPG) in einer einzigen ACI-Fabric (Application Centric Infrastructure) konfiguriert und verifiziert wird.

## Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- L2-Multicast-Unterstützung in der ACI immer unterstützt
- Internet Group Management Protocol (IGMP)-Snooping in der ACI standardmäßig aktiviert

**Anmerkung:** Weitere Informationen zu IGMP-Snooping finden Sie im Dokument <u>zur</u> <u>Multicast-Konfiguration für Layer 2 des Cisco APIC und IGMP-Snoop</u>.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

L2-Multicast bezieht sich auf IP-Multicast-Pakete, die auf einem L2-Netzwerksegment (Bridge Domain(BD)/Subnetz) weitergeleitet werden, nicht auf L2-Nicht-IP-Multicast-Pakete, bei denen es sich um Multicast-Pakete mit einer Ziel-Multicast-MAC-Adresse ohne IP-Header handelt. L2-Multicast beinhaltet auch kein lokales Link-Multicast (224.0.0.0/24). Link Local Multicast wird immer an alle Ports im BD weitergeleitet.

L2-Multicast in der ACI wird nur innerhalb des BD weitergeleitet. Wenn Sie mehrere EPGs haben, die dasselbe BD verwenden, wird der Multicast-Datenverkehr in allen EPGs überflutet, unabhängig davon, welche Verträge zwischen EPGs bestehen.

Die Cisco ACI leitet Multicast-Frames über den Overlay-Multicast-Tree weiter, der zwischen Leafund Spine-Switches erstellt wurde. Für den L2-Datenverkehr werden Forwarding Tag (FTAG)-Trees verwendet, um einen effizienten Lastenausgleich über mehrere redundante Links mit denselben Kosten zu ermöglichen. Weitere Informationen zu den Details der FTAG-Struktur finden Sie im Dokument <u>zu den ACI-Grundlagen</u>.

**Hinweis**: Wir empfehlen, IGMP-Snoop auf dem BD nicht zu deaktivieren. Wenn Sie IGMP-Snoop deaktivieren, kann die Multicast-Leistung aufgrund übermäßiger falscher Überflutung im BD beeinträchtigt werden.

## Konfigurieren

### Netzwerktopologie



### Konfigurationen

Dies ist eine Zusammenfassung der Konfigurationsschritte. Für L2-Multicast gibt es nur wenige Konfigurationen, außer zum Aktivieren eines IGMP-Abfragers.

- Schritt 1: Konfigurieren der Fabric-Zugriffsrichtlinien für die Verbindung von Multicast-Server und Client-Host
- Schritt 2: Erstellen Sie EPG, BD und VRF für den Multicast Receiver und die Quelle.
- Schritt 3: Anfügen einer physischen Domäne an die EPG und Konfigurieren des statischen Ports
- Schritt 4: Konfigurieren des IGMP Querier

In diesem Abschnitt werden die einzelnen Konfigurationsschritte beschrieben.

# Schritt 1: Konfigurieren der Fabric-Zugriffsrichtlinien für die Verbindung von Multicast-Server und Client-Host

Die Bilder zeigen den allgemeinen Ansatz für die Konfiguration. Weitere Details zu Zugriffsrichtlinien finden Sie im Dokument <u>zur</u> ersten <u>ACI-Bereitstellung</u>.

Sie können diesen Schritt überspringen, wenn die Zugriffsrichtlinien bereits vorhanden sind.

• Dieses Image zeigt die Fabric-Richtlinien für Multicast-Server-Ports.



• Dieses Bild zeigt die Fabric-Richtlinien für den Multicast-Receiver-Port (Client).



#### Schritt 2: Erstellen Sie EPG, BD und VRF für den Multicast Receiver und die Quelle.



Ein BD verwendet standardmäßig die IGMP-Snoop-Standardrichtlinie, die im "Common" Tenant vordefiniert ist.

Der IGMP Querier ist im BD-Subnetz standardmäßig nicht aktiviert. Dies ist auch bei älteren NXOS- oder Cisco IOS®-basierten Bereitstellungen der Fall.

Um die IGMP-Snoop-Standardrichtlinie zu aktivieren, wählen Sie "Common' Tenant > Policies
 > Protocol > IGMP Snoop > default, um zu sehen, dass das Kontrollkästchen Enable querier nicht für die IGMP-Standardrichtlinie aktiviert ist.



#### APIC

System	Tenants	Fabric	Virtual Networking	L4-L7 Se	ervices	Admin	Operations	s App	s Integrations
ALL TENANT	S   Add	Tenant   Ten	ant Search: name or descr	1	common	I TN_D	l mgmt l	infra   1	Test1_Aks
common			Ē	$\bigcirc$	IGMP S	noop Pol	icy - default		
> C Quick St	art			<b>^</b>					
common	ı								
> 🧮 Appli	cation Profile	25							
> 🚞 Netw	orking				Proper	rties			
> 🚞 IP Ad	Idress Pools						Name	: default	
> 🚞 Cont	racts						Description	optional	
🗸 🚞 Polic	ies								
~ 🚞 P	rotocol						Admin State	: Disabled	Enabled
> 🚞	BFD						Control	: 🗌 Fast leav	/e
> 🖿	BGP							Enable o	querier
> 🖿	Custom QC	os			Last	Member Qu	ery Interval (sec)	: 1	$\Diamond$
> 🖿	DHCP					Qu	ery Interval (sec)	125	$\bigcirc$
> 🖿	Data Plane	Policing			Q	uery Respor	nse Interval (sec)	: 10	$\Diamond$
> 🖿	EIGRP					S	tart Query Count	2	$\Diamond$
> 🖿	End Point F	Retention				Start Qu	ery Interval (sec)	31	$\Diamond$
> 🖿	First Hop S	ecurity							
> 🖿	HSRP								
> 🖿	IGMP Inter	face							
~ 🖿	IGMP Snoc	q							
	= default								

• Dieses Bild zeigt die Zusammenfassung der EPG-, BD- und VRF-Konfiguration (logische Ansicht).



Schritt 3: Anfügen einer physischen Domäne an die EPG und Konfigurieren des statischen Ports

• Dieses Bild zeigt eine physische Domäne, die an eine EPG angeschlossen ist.

-duala cusco	APIC	
CISCO		

System Tenants Fabric Virtual Networking L4	L7 Services	Admin Operations	s Apps In	tegrations								
ALL TENANTS   Add Tenant   Tenant Search: name or descr	I common	TN_D   mgmt	infra   Test1_Aks									
TN_D (P)()	Dom	ains (VMs and Bare-	Metals)									0.0
O• Quick Start												0 ± %-
✓ III TN_D     ✓ III Application Profiles	🔺 Doma	n Type	Deployment	Resolution	Allow Micro- Segmentation	Primary VLAN	Port Encap	Switching Mode	Encap Mode	Cos Value	Enhanced Lag Policy	Custom EPG Name
V 🛞 Mutticast_Servers	TN_D_Pt	sDom Physical Domai	n					native	Auto	Cos0		
V Application EPGs												
V Statust_EPG												
Domains (VMs and Bare-Metals)												

admin 💽 😍 🔟 🔕

• Dieses Bild zeigt einen konfigurierten statischen Port unter einer EPG.

cisco APIC						admin 🔇 😍	• •
System Tenants Fabric Virtual Networking L4-L7	Services Admin Operations	Apps Integrations					
ALL TENANTS   Add Tenant   Tenant Search: name or descr.	common   TN_D   mgmt   in	ntra   Test1_Aks					
™_D (D (G) (O)	<ul> <li>Static Ports</li> </ul>						00
⇒Ore Opeick Start ∨⊞TN D	A F						○ ± **-
V E Application Profiles	Path	Primary VLAN for Micro-Seg	Port Encap (or Secondary VLAN for Micro-Seg)	Deployment Immediacy	Mode	PTP	
✓ ⊕ Multicast_Servers	@ Node: Pod-1						
V 🚞 Application [POs	Pod-1/Node-101/eth1/47	unknown	vlan-1900	Immediate	Access (Untagged)	Disabled	
V % L2_Mcast_EPG Domains (VMs and Bare-Metals) EPG Members	Pod-1/Node-102/eth1/47	unknown	vlan-1900	Immediate	Access (Untagged)	Disabled	
> 🖿 Static Ports							

• Dieses Bild zeigt, dass die Endpunkte des Multicast-Servers (Quelle) und des Multicast-Clients (Empfänger) beide unter demselben EPG erfasst (verbunden) werden.

EPG - L2_Mcast_EPG											00	
						Summary	Policy	Operational	Stats	Health	Faults	History
			Client End-Points	Configured Access	Policies	Contracts	Controlle	er End-Points	Deploye	d Leaves	Learned End	J-Points
🗢 Healthy 🙁 🕥	🕚 🕕 Τ											0 ±
End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controlle	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-10	1/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-10	2/eth1/47 (learned)			vlan-1900	
Multicast S N IP:10. Join Group	tream[Server] /AC: 100.0.10 : 239.100.0.10	Eth1/47	Eth1/49 Leaf-101 N9K-C93180Y 4.2(7q)	IC-FX		Leaf N9K-C93 4.2	th <b>1/49</b> -102 180YC-FX (7q)	Eth1/47		Multicast IP:1 Join Grou	Receiver[( 0.100.0.20 ip: 239.10(	Client] ) ).0.10

Schritt 4: Konfigurieren von IGMP Querier

Der IGMP Querier muss an zwei Stellen aktiviert werden, unter der jeweiligen IGMP-Snoop-Richtlinie und unter dem BD-Subnetz.

Anmerkung: Da für die IGMP-Snooping-Richtlinie mit aktiviertem Enable Querier eine Quell-IP-Adresse zum Senden der IGMP-Abfrage erforderlich ist, muss die IGMP Querier-IP unter dem BD-Subnetz konfiguriert werden. Andernfalls sendet der Leaf-Switch die IGMP-Abfrage nicht an den Multicast-Empfänger.

Es wird immer empfohlen, eine neue IGMP-Snooping-Richtlinie mit aktiviertem IGMP Querier zu konfigurieren, anstatt eine standardmäßige IGMP-Snooping-Richtlinie zu verwenden. Beachten Sie, dass die IGMP-Snooping-Standardrichtlinie standardmäßig keinen IGMP-Abfrager aktiviert hat und standardmäßig jedem BD zugeordnet ist. Eine Änderung einer Konfiguration unter der IGMP-Snooping-Standardrichtlinie wirkt sich auf jedes BD aus, das mit der IGMP-Snoop-Standardrichtlinie verknüpft ist. Daher wird nicht empfohlen, die IGMP-Snooping-Standardrichtlinienparameter in der ACI zu ändern.

• Um eine neue IGMP-Snooping-Richtlinie zu erstellen, wählen Sie **TN\_D-Tenant > Policies > Protocols**, klicken Sie mit der rechten Maustaste auf **IGMP-Snoop** und klicken Sie auf **Create IGMP Snoop Policy**.