Configurer la multidiffusion de couche 2 dans l'ACI

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Informations générales Configuration Topologie du réseau Configurations Étape 1 : Configurer les stratégies d'accès au fabric pour la connectivité du serveur multidiffusion et de l'hôte client Étape 2 : Créez l'EPG, le BD et le VRF pour le récepteur et la source de multidiffusion Étape 3 : Fixer un domaine physique au groupe de terminaux et configurer le port statique Étape 4 : Configurer la file d'attente IGMP Vérification Explication du flux de paquets multicast de couche 2 **Requête IGMP requise** Dépannage Informations connexes

Introduction

Ce document décrit comment configurer et vérifier la multidiffusion de couche 2 (L2) dans le même groupe de terminaux (EPG) sur un fabric ACI (Application Centric Infrastructure) unique.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Prise en charge de la multidiffusion de couche 2 dans l'ACI toujours prise en charge
- Surveillance IGMP (Internet Group Management Protocol) dans ACI activée par défaut

Note: Pour plus d'informations sur la surveillance IGMP, consultez le document <u>Cisco APIC</u> <u>et IGMP Snoop Layer 2 Multicast Configuration</u>.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- N9K-C93180YC-FX
- Version 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La multidiffusion de couche 2 désigne les paquets de multidiffusion IP transmis sur un segment de réseau de couche 2 (domaine de pont (BD)/sous-réseau), et non les paquets de multidiffusion de couche 2 qui sont des paquets de multidiffusion avec une adresse MAC de multidiffusion de destination sans en-tête IP. La multidiffusion de couche 2 exclut également la multidiffusion link-local (224.0.0.0/24). La multidiffusion locale de liaison est toujours transmise à tous les ports du BD.

La multidiffusion de couche 2 dans l'ACI n'est transmise que dans le BD. Si vous avez plusieurs groupes de terminaux qui utilisent le même BD, le trafic de multidiffusion inonde tous les groupes de terminaux indépendamment des contrats en place entre les groupes de terminaux.

L'ACI Cisco transmet les trames de multidiffusion sur l'arborescence multicast de superposition qui est construite entre les commutateurs leaf et spine. Le trafic de couche 2 utilise des arborescences FTAG (Forwarding Tag) pour fournir un équilibrage de charge efficace sur plusieurs liaisons redondantes de même coût. Pour plus d'informations sur les détails de l'arborescence FTAG, consultez le document <u>Fondamentaux ACI</u>.

Remarque : Nous vous recommandons de ne pas désactiver IGMP Snoop sur le BD. Si vous désactivez IGMP Snoop, les performances de multidiffusion risquent d'être réduites en raison d'une inondation erronée excessive au sein du BD.

Configuration

Topologie du réseau



Configurations

Voici un résumé des étapes de configuration. Il n'y a pas beaucoup de configuration pour la multidiffusion de couche 2 sauf pour activer un interrogateur IGMP.

- Étape 1 : Configurer les stratégies d'accès au fabric pour la connectivité du serveur multidiffusion et de l'hôte client
- Étape 2 : Créez l'EPG, le BD et le VRF pour le récepteur et la source de multidiffusion
- Étape 3 : Fixer un domaine physique au groupe de terminaux et configurer le port statique
- Étape 4 : Configurer le serveur de requêtes IGMP

Cette section décrit les étapes de configuration détaillées.

Étape 1 : Configurer les stratégies d'accès au fabric pour la connectivité du serveur multidiffusion et de l'hôte client

Les images montrent l'approche de haut niveau de la configuration. Des détails supplémentaires sur les politiques d'accès sont disponibles dans le document <u>ACI Initial Deployment</u>.

Vous pouvez ignorer cette étape si les stratégies d'accès sont déjà en place.

• Cette image montre les stratégies de matrice de ports du serveur de multidiffusion.



• Cette image montre les stratégies de fabric du port du récepteur de multidiffusion (client).



Étape 2 : Créez l'EPG, le BD et le VRF pour le récepteur et la source de multidiffusion



Par défaut, un BD utilise la stratégie IGMP Snoop par défaut prédéfinie dans le service partagé.

Le demandeur IGMP n'est pas activé par défaut sous le sous-réseau BD, ce qui est également le cas pour un déploiement NXOS ou Cisco IOS® hérité.

 Afin de vérifier la stratégie IGMP Snoop par défaut, choisissez le 'locataire commun > Politiques > Protocole > IGMP Snoop > default pour voir que la case Activer le demandeur n'est pas activée pour la stratégie IGMP par défaut.



APIC

System	Tenants	Fabric	Virtual Networking	L4-L7 Se	ervices	Admin	Operations	s Ap	ps Inte	egrations
ALL TENANT	S Add T	enant Ten	ant Search: name or descr	1	common	I TN_D	l mgmt l	infra	Test1_Aks	
common			(I	IGMP S	inoop Pol	icy - default			
> C Quick St	art			^						
commor	ı									
> 🧮 Appli	ication Profiles									
> 🚞 Netw	vorking				Proper	ties				
> 🚞 IP Ad	Idress Pools						Name	: default		
> 🚞 Cont	racts						Description	: optiona	1	
🗸 🚞 Polic	ies									
~ 🚞 P	rotocol						Admin State	: Disabl	ed Enabl	ed
> 🖿	BFD						Control	: 🗌 Fast le	ave	
> 🖿	BGP							Enable	e querier	
> 🖿	Custom QOS	5			Last	Member Qu	ery Interval (sec)	: 1		\Diamond
> 🖿	DHCP					Que	ery Interval (sec)	125		\Diamond
> 🖿	Data Plane P	Policing			Q	uery Respor	nse Interval (sec)	: 10		\Diamond
> 🖿	EIGRP					S	tart Query Count	2		\Diamond
> 🖿	End Point Re	etention				Start Qu	ery Interval (sec)	31		\bigcirc
> 🖿	First Hop Se	curity								
> 🖿	HSRP									
> 🖿	IGMP Interfa	ce								
~ 🖿	IGMP Snoop									
	= default									

• Cette image présente le résumé de la configuration EPG, BD et VRF (vue logique).



Étape 3 : Fixer un domaine physique au groupe de terminaux et configurer le port statique

• Cette image montre un domaine physique attaché à un EPG.

cisco APIC											adr	nin 🔇 😍	• •	
System Tenants Fabric	Virtual Networking L4-L7 S	ervices Admin	Operations	Apps Int	tegrations									
ALL TENANTS Add Tenant Tenan	t Search: name or descr I	common TN_D	I mgmt I	infra Test1_Aks										
TN_D	©90	Domains (V)	Ms and Bare-	Metals)									Q	0
O Quick Start													0 ± %	t-
V III TN_D V III Application Profiles		 Domain 	Туре	Deployment	Resolution	Allow Micro- Segmentation	Primary VLAN	Port Encap	Switching Mode	Encap Mode	Cos Value	Enhanced Lag Policy	Custom EPG Name	
V 🛞 Multicast_Servers		TN_D_PhysDom	Physical Domain	n					native	Auto	Cos0			
V 🔛 Application EPGs														
V 12_Meast_EPG														
Domains (VMs and Ban	e-Metals)													

• Cette image montre un port statique configuré sous un 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 i	ntra Test1_Aks					
TN_D (P.)	 Static Ports 						0.0
⇒ O+ Quick Start	L F						0 ± %-
V Application Profiles	Path	Primary VLAN for Micro-Seg	Port Encap (or Secondary VLAN for Micro-Seg)	Deployment Immediacy	Mode	PTP	
✓	@ Node: Pod-1						
V 🚞 Application EPGs	Pod-1/Node-101/eth1/47	unknown	vlan-1900	Immediate	Access (Untagged)	Disabled	
V St L2_Mcast_EPG	Pod-1/Node-102/eth1/47	unknown	vlan-1900	Immediate	Access (Untagged)	Disabled	
Constants (vinis and sare - Metals) EPG Members							
> 🚍 Static Ports							

• Cette image montre que les points d'extrémité du serveur de multidiffusion (source) et du client de multidiffusion (récepteur) sont tous deux acquis (connectés) sous le même EPG.

CEPG - L2_Mca	st_EPG											00
						Summary	Policy	Operational	Stats	Health	Faults	History
			Client End-Points	Configured Access	Policies	Contracts	Controlle	er End-Points	Deployed	d Leaves	Learned End	-Points
♥Healthy 🛞 👽	🕐 🕔 Ι τ											0 <u>+</u>
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-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	Stream[Server] MAC: .100.0.10 : 239.100.0.10	Eth1/47	Eth1/49 Leaf-101 N9K-C93180Y 4.2(7q)	′C-FX		Leaf N9K-C93 4.2(th1/49 -102 180YC-FX (7q)	Eth1/47	J	Multicast IP:1 Ioin Grou	Receiver[0 0.100.0.20 p: 239.100	[lient]).0.10

Étape 4 : Configurer la file d'attente IGMP

Le demandeur IGMP doit être activé à deux endroits, sous la stratégie IGMP Snoop respective et sous le sous-réseau BD.

Note: Étant donné que la stratégie de surveillance IGMP avec **Enable querier** activé nécessite une adresse IP source pour envoyer la requête IGMP, il est nécessaire de configurer l'activation de l'**IP** IGMP **Querier** sous le sous-réseau BD. Sinon, le commutateur leaf n'enverra pas la requête IGMP au récepteur de multidiffusion.

Il est toujours recommandé de configurer une nouvelle stratégie IGMP Snooping avec le demandeur IGMP activé au lieu d'utiliser une stratégie IGMP Snooping par défaut. Notez que la stratégie de surveillance IGMP par défaut n'a pas de demandeur IGMP activé par défaut et qu'elle est associée par défaut à chaque BD. Une modification de toute configuration sous la stratégie de surveillance IGMP par défaut affecte chaque BD associé à la stratégie de surveillance IGMP par défaut. Il n'est donc pas recommandé de modifier les paramètres de stratégie de surveillance IGMP par défaut dans l'ACI.

• Afin de créer une nouvelle stratégie de surveillance IGMP, choisissez le locataire TN_D >

Politiques > Protocoles, puis cliquez avec le bouton droit sur IGMP Snoop et cliquez sur Créer une stratégie de surveillance IGMP.