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 <u>Cisco APIC e IGMP Snoop Layer 2 Multicast Configuration</u>.

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 <u>Fundamentos da ACI</u>.

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 <u>Implantação inicial da ACI</u>.

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



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' locatário > Políticas > Protocolo > IGMP Snoop > default para ver se a política IGMP padrão não tem a caixa Ativar consulta marcada.



APIC

System	Tenants	Fabric	Virtual Networking	L4-L7 Se	ervices	Admin	Operati	ons	App)S	Integratio	ns
ALL TENANT	S AddT	enant Ten	ant Search: name or descr	1	common	I TN_D	l mgmt	l infi	ra	Test1_/	Aks	
common			(06	IGMP S	Snoop Pol	icy - defa	ult				
> C Quick St	art			^								
commor	ı											
> 🚞 Appl	ication Profiles	3										
> 🚞 Netw	orking				Proper	rties						
> 🚞 IP Ad	Idress Pools						Na	ame: de	fault			
> 🚞 Cont	racts						Descrip	tion: 0	ptional			
🗸 🚞 Polic	ies											
~ 🚞 P	rotocol						Admin S	tate: 🤇	Disable	d	Enabled	
> 🚞	BFD						Cor	ntrol: 🗌	Fast lea	ive		
> 🚞	BGP								Enable	querier		
> 🚞	Custom QO	S			Last	Member Qu	ery Interval (sec): 1			\Diamond	
> 🚞	DHCP					Qu	ery Interval (sec): 1	25		\Diamond	
> 🚞	Data Plane F	Policing			Q	uery Respor	nse Interval (s	sec): 1	0		\bigcirc	
> 🚞	EIGRP			4		S	tart Query Co	ount: 2			\bigcirc	
> 🖿	End Point Re	etention				Start Qu	ery Interval (sec): 3	1		\Diamond	
> 🚞	First Hop Se	curity										
> 🖿	HSRP											
> 🖿	IGMP Interfa	ice										
~ 🖿	IGMP Snoop)										
	= default											

• 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.

diale APIC											adm		0	•	0
System Tenants Fabric Virt.	ual Networking L4-L7 S	ervices Admin	Operations	Apps In	tegrations										
ALL TENANTS Add Tenant Tenant Sear	ch: name or descr	common TN_D	I mgmt I i	nfra Test1_Aks											
TN_D	000	Domains (V)	Ms and Bare-M	Aetals)											0.0
> O Quick Start														0.	· *-
✓ III TN_D. ✓ III Application Profiles		 Domain 	Туре	Deployment	Resolution	Allow Micro- Segmentation	Primary VLAN	Port Encap	Switching Mode	Encap Mode	Cos Value	Enhane Policy	sed Lag	Custor Name	m EPG
V 🚯 Multicast_Servers		TN_D_PhysDom	Physical Domain						native	Auto	Cos0				
Application EPGs															
✓ State L2_Moist_EPG															
Domains (VMs and Bare-Meta	als)														

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

cisco APIC						admin 🔮 😈	
System Tenants Fabric Virtual Networking L4-L7 S	Services Admin Operations	Apps Integrations					
ALL TENANTS Add Tenant Tenant Search: name or descr	common TN_D mgmt ir	ıfra Test1_Aks					
TN_D (P.9)(0)	Static Ports						0.0
> Or Quick Start √ Ⅲ TN D	A F						○ ± %-
V 🔛 Application Profiles	Path	Primary VLAN for Micro-Seg	Port Encap (or Secondary VLAN for Micro-Seg)	Deployment Immediacy	Mode	PTP	
Witcast_Servers	Node: Pod-1						
V Application EPGs	Pod-1/Node-101/eth1/47	unknown	vlan-1900	Immediate	Access (Untagged)	Disabled	
V 🎇 L2_Mcast_EPG	Pod-1/Node-102/eth1/47	unknown	vlan-1900	Immediate	Access (Untagged)	Disabled	
Domains (VMs and Bare-Metals)							
> 🧮 EPG Members							
> 🚞 Static Ports							

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

EPG - L2_Mcast_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 🛞 😗	🕚 🕐 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	tream[Server] //AC: 100.0.10 : 239.100.0.10	Eth1/47	Eth1/49 Leaf-101 N9K-C93180Y 4.2(7q)	'C-FX		Leaf V9K-C93: 4.2(th 1/49 -102 180YC-FX 7q)	Eth1/47	٦ د	Лulticast IP:1 oin Grou	Receiver[0 0.100.0.20 p: 239.100	Client]).0.10

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.

Ésempre 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 a cada BD 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, portanto 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.