

Creación de una implementación multisitio de borde compartido de VXLAN Nexus 9000 mediante DCNM

Contenido

[Introducción](#)

[Topología](#)

[Detalles de la topología](#)

[Componentes Utilizados:](#)

[Pasos de alto nivel](#)

[Paso 1: Creación de un fabric sencillo para DC1](#)

[Paso 2: Agregar switches al fabric DC1](#)

[Paso 3: Configuración de Redes/VRF](#)

[Paso 4: Repita los mismos pasos para DC2](#)

[Paso 5: Creación de un fabric sencillo para las fronteras compartidas](#)

[Paso 6: Creación de MSD y desplazamiento de fabric DC1 y DC2](#)

[Paso 7: Creación de fabric externo](#)

[Paso 8: eBGP Underlay para loopback reacty entre BGW\(iBGP entre fronteras compartidas también\)](#)

[Paso 9: Creación de superposición multisitio de BGW a fronteras compartidas](#)

[Paso 10: Implementación de redes/VRF en ambos sitios](#)

[Paso 11: Creación de puertos troncales/de acceso descendentes en switches hoja/VTEP](#)

[Paso 12: Se requieren formularios libres en el borde compartido](#)

[Paso 13: Loopback dentro de los VRF de arrendatarios en los BGW](#)

[Paso 14: Extensiones VRFLITE de los bordes compartidos a los routers externos](#)

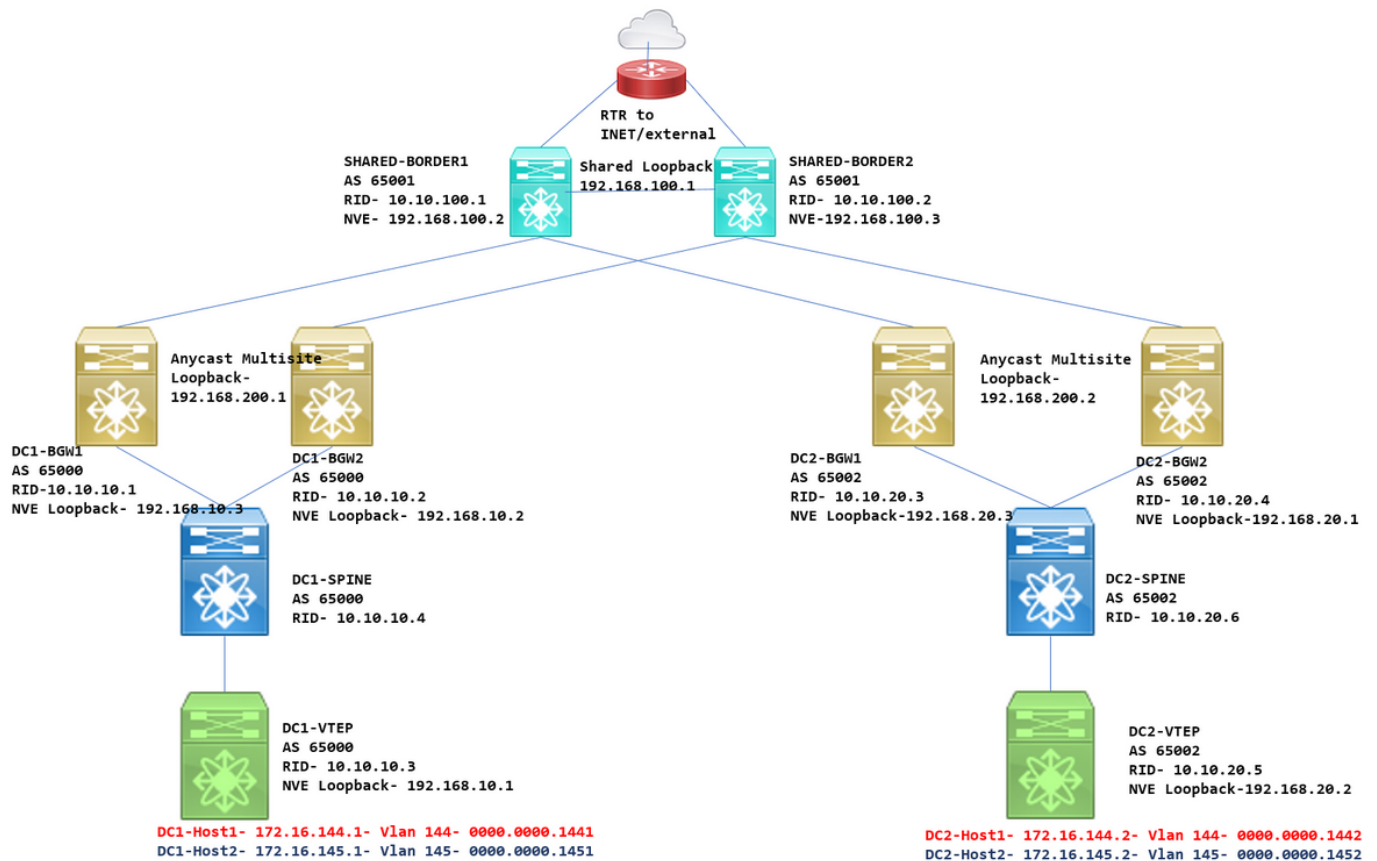
[a\) Adición de links entre estructuras desde fronteras compartidas a routers externos](#)

[b\) Adición de extensiones VRF](#)

Introducción

Este documento explica cómo implementar una implementación multisitio de Cisco Nexus 9000 VXLAN mediante un modelo de borde compartido utilizando la versión 11.2 de DCNM.

Topología



Detalles de la topología

DC1 y DC2 son dos ubicaciones de Data Center que ejecutan vxlan;

Los gateways de frontera DC1 y DC2 tienen conexiones físicas a los bordes compartidos;

Los bordes compartidos tienen la conectividad externa (por ejemplo; Internet); de modo que las conexiones de la lista VRF se terminan en los bordes compartidos y los bordes compartidos inyectan una ruta predeterminada a los Gateways de borde en cada sitio

Los bordes compartidos se configuran en vPC (Se trata de un requisito cuando el fabric se implementa mediante DCNM)

Los gateways de borde se configuran en modo de difusión

Componentes Utilizados:

Nexus 9ks con 9.3(2)

DCNM ejecutando la versión 11.2

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, make sure that you understand the potential impact of any command.

Pasos de alto nivel

- 1) Teniendo en cuenta que este documento se basa en dos Data Centers que utilizan la función vxlan multisite, se deben crear dos estructuras sencillas
- 2) Crear otro fabric sencillo para el borde compartido
- 3) Crear MSD y mover DC1 y DC2
- 4) Creación de fabric externo
- 5) Crear superposición y superposición multisitio (para Oriente/Occidente)
- 6) Crear adjuntos de extensión VRF en bordes compartidos

Paso 1: Creación de un fabric sencillo para DC1

- Inicie sesión en DCNM y, desde Panel, seleccione la opción -> "Fabric Builder"



DCNM Licenses

License this copy of DCNM for each managed switch to unlock Performance Collection.



Fabric Builder

Creates a managed and controlled SDN fabric.



Networks & VRFs

Simple network overlay provisioning for N9K VXLAN EVPN Fabrics.



Documentation

Access cisco.com from documentation on configuration, maintenance and operation.

- Seleccione la opción "Crear fabric"



Fabric Builder

Fabric Builder creates a managed and controlled SDN fabric. Select an existing fabric below or define a new *VXLAN* fabric, add switches using *Power On Auto Provisioning (POAP)*, set the roles of the switches and deploy settings to devices.

Create Fabric

- A continuación, se proporciona el nombre del fabric, la plantilla y, a continuación, se abrirán varias fichas que necesitarán detalles como ASN, Fabric Interface Numering, Any Cast Gateway MAC(AGM)

Add Fabric

* Fabric Name :

* Fabric Template :

General

Replication

vPC

Advanced

Resources

Manageability

Bootstrap

Configuration Backup

* BGP ASN 1-4294967295 | 1-65535[0-65535]

* Fabric Interface Numering Numbered(Point-to-Point) or Unnumbered

* Underlay Subnet IP Mask Mask for Underlay Subnet IP Range

* Link-State Routing Protocol Supported routing protocols (OSPF/IS-IS)

* Route-Reflectors Number of spines acting as Route-Reflectors

* Anycast Gateway MAC Shared MAC address for all leafs (xxxx.xxxx.xxxx)

NX-OS Software Image Version If Set, Image Version Check Enforced On All Switches. Images Can Be Uploaded From Control:Image Upload

Las interfaces de fabric (que son interfaces de columna/hoja) se pueden "sin numerar" o punto a punto; Si se utiliza sin numerar, las direcciones IP requeridas son menores (ya que la dirección IP es la del loopback sin numerar)

AGM es utilizado por los hosts en el fabric como la dirección MAC de gateway predeterminada;

Esto será igual en todos los switches de hoja que son las puertas de enlace predeterminadas

- A continuación, se establece el modo de replicación

Add Fabric

* Fabric Name :

* Fabric Template :

General | **Replication** | vPC | Advanced | Resources | Manageability | Bootstrap | Configuration Backup

* Replication Mode	Multicast	? Replication Mode for BUM Traffic
* Multicast Group Subnet	239.1.1.0/25	? Multicast address with prefix 16 to 30
Enable Tenant Routed Multicast (TRM)	<input checked="" type="checkbox"/> ? For Overlay Multicast Support In VXLAN Fabrics	
Default MDT Address for TRM VRFs	239.100.100.100	? IPv4 Multicast Address
* Rendezvous-Points	2	? Number of spines acting as Rendezvous-Point (RP)
* RP Mode	asm	? Multicast RP Mode
* Underlay RP Loopback Id	254	? 0-512
Underlay Primary RP Loopback Id		? 0-512, Primary Loopback Bidir-PIM Phantom RP
Underlay Backup RP Loopback Id		? 0-512, Fallback Loopback Bidir-PIM Phantom RP
Underlay Second Backup RP Loopback Id		? 0-512, Second Fallback Loopback Bidir-PIM Phantom RP
Underlay Third Backup RP Loopback Id		? 0-512, Third Fallback Loopback Bidir-PIM Phantom RP

El modo de replicación seleccionado aquí puede ser multicast o IR-Ingress Replication; IR replicará cualquier tráfico BUM entrante dentro de una vlan vxlan de manera unicast a otros VTEP que también se denomina replicación de cabecera mientras que el modo de multidifusión enviará el tráfico BUM con una dirección IP de destino externa como la del grupo de multidifusión definido para cada red hasta la columna y Spines hará la replicación multicast basada en la dirección IP de destino exterior OIL a otros VTEP.

Multicast Group subnet-> Obligatorio para replicar el tráfico BUM (como solicitud ARP de un host)

Si se requiere que TRM esté habilitado, active la casilla de verificación contra la misma y proporcione la dirección MDT para los VRF TRM.

- La pestaña "vPC" se deja de forma predeterminada; Si se requiere algún cambio para la SVI/VLAN de respaldo, se pueden definir aquí
- La ficha Opciones avanzadas es la siguiente sección

Add Fabric

* Fabric Name :

* Fabric Template :

General	Replication	vPC	Advanced	Resources	Manageability	Bootstrap	Configuration Backup
			* VRF Template	<input type="text" value="Default_VRF_Universal"/>	<input type="button" value="?"/> Default Overlay VRF Template For Leafs		
			* Network Template	<input type="text" value="Default_Network_Universal"/>	<input type="button" value="?"/> Default Overlay Network Template For Leafs		
			* VRF Extension Template	<input type="text" value="Default_VRF_Extension_Universal"/>	<input type="button" value="?"/> Default Overlay VRF Template For Borders		
			* Network Extension Template	<input type="text" value="Default_Network_Extension_Universa"/>	<input type="button" value="?"/> Default Overlay Network Template For Borders		
			Site Id	<input type="text" value="65000"/>	<input type="button" value="?"/> For EVPN Multi-Site Support (Min:1, Max: 281474976710655). Defaults to Fabric ASN		
			* Underlay Routing Loopback Id	<input type="text" value="0"/>	<input type="button" value="?"/> 0-512		
			* Underlay VTEP Loopback Id	<input type="text" value="1"/>	<input type="button" value="?"/> 0-512		
			* Link-State Routing Protocol Tag	<input type="text" value="UNDERLAY"/>	<input type="button" value="?"/> Routing Process Tag (Max Size 20)		
			* OSPF Area Id	<input type="text" value="0.0.0.0"/>	<input type="button" value="?"/> OSPF Area Id in IP address format		
			Enable OSPF Authentication	<input type="checkbox"/>	<input type="button" value="?"/>		
			OSPF Authentication Key ID	<input type="text"/>	<input type="button" value="?"/> 0-255		
			OSPF Authentication Key	<input type="text"/>	<input type="button" value="?"/> 3DES Encrypted		
			Enable IS-IS Authentication	<input type="checkbox"/>	<input type="button" value="?"/>		
			IS-IS Authentication Keychain Name	<input type="text"/>	<input type="button" value="?"/>		
			IS-IS Authentication Key ID	<input type="text"/>	<input type="button" value="?"/> 0-65535		
			IS-IS Authentication Key	<input type="text"/>	<input type="button" value="?"/> Cisco Type 7 Encrypted		
			* Power Supply Mode	<input type="text" value="ps-redundant"/>	<input type="button" value="?"/> Default Power Supply Mode For The Fabric		
			* CoPP Profile	<input type="text" value="strict"/>	<input type="button" value="?"/> Fabric Wide CoPP Policy. Customized CoPP policy should be provided when 'manual' is selected		
			Enable VXLAN OAM	<input checked="" type="checkbox"/>	<input type="button" value="?"/> For Operations, Administration, and Management Of VXLAN Fabrics		
			Enable Tenant DHCP	<input checked="" type="checkbox"/>	<input type="button" value="?"/>		
			Enable BFD	<input type="checkbox"/>	<input type="button" value="?"/>		
			* Greenfield Cleanup Option	<input type="text" value="Disable"/>	<input type="button" value="?"/> Switch Cleanup Without Reload When PreserveConfig=no		
			Enable BGP Authentication	<input type="checkbox"/>	<input type="button" value="?"/>		

El ID del sitio mencionado aquí se rellena automáticamente en esta versión de DCNM que se deriva del ASN definido debajo de la ficha "General".

Rellene/modifique otros campos que sean relevantes

- La pestaña Recursos es la siguiente que necesitaría el esquema de direccionamiento IP para loopbacks, Underlots

Add Fabric

* Fabric Name : DC1

* Fabric Template : Easy_Fabric_11_1

General Replication vPC Advanced Resources Manageability Bootstrap Configuration Backup

Manual Underlay IP Address Allocation Checking this will disable Dynamic Underlay IP Address Allocations

* Underlay Routing Loopback IP Range	10.10.10.0/24	? Typically Loopback0 IP Address Range
* Underlay VTEP Loopback IP Range	192.168.10.0/24	? Typically Loopback1 IP Address Range
* Underlay RP Loopback IP Range	10.100.100.0/24	? Anycast or Phantom RP IP Address Range
* Underlay Subnet IP Range	10.4.10.0/24	? Address range to assign Numbered and Peer Link SVI IPs
* Layer 2 VXLAN VNI Range	100144,100145	? Overlay Network Identifier Range (Min:1, Max:16777214)
* Layer 3 VXLAN VNI Range	1001445	? Overlay VRF Identifier Range (Min:1, Max:16777214)
* Network VLAN Range	144,145	? Per Switch Overlay Network VLAN Range (Min:2, Max:3967)
* VRF VLAN Range	1445	? Per Switch Overlay VRF VLAN Range (Min:2, Max:3967)
* Subinterface Dot1q Range	2-511	? Per Border Dot1q Range For VRF Lite Connectivity (Min:2, Max:511)
* VRF Lite Deployment	Manual	? VRF Lite Inter-Fabric Connection Deployment Options
* VRF Lite Subnet IP Range	10.10.33.0/24	? Address range to assign P2P DCI Links
* VRF Lite Subnet Mask	30	? Mask for Subnet Range (Min:8, Max:31)

Intervalo VXLAN VNI de Capa 2 -> Estos son los VNID que se mapearán posteriormente a Vlan(lo mostrará más abajo)

VXLAN VNI Range de Capa 3-> Estos son los VNID de Capa 3 que también se mapearán posteriormente a VNI de Capa 3 a Vn-Segmento

- No se muestran otras fichas aquí; pero rellene las demás fichas si es necesario;

Add Fabric ✕

* Fabric Name : DC1

* Fabric Template : Easy_Fabric_11_1

General Replication vPC Advanced Resources Manageability Bootstrap Configuration Backup

Hourly Fabric Backup Backup Only when a Fabric is modified

Scheduled Fabric Backup Backup at Specified Scheduled Time

Scheduled Time Time in 24hr format. (00:00 to 23:59)

Save Cancel

- Una vez guardado, la página Fabric Builder mostrará el Fabric(From DCNM-> Control-> Fabric Builder

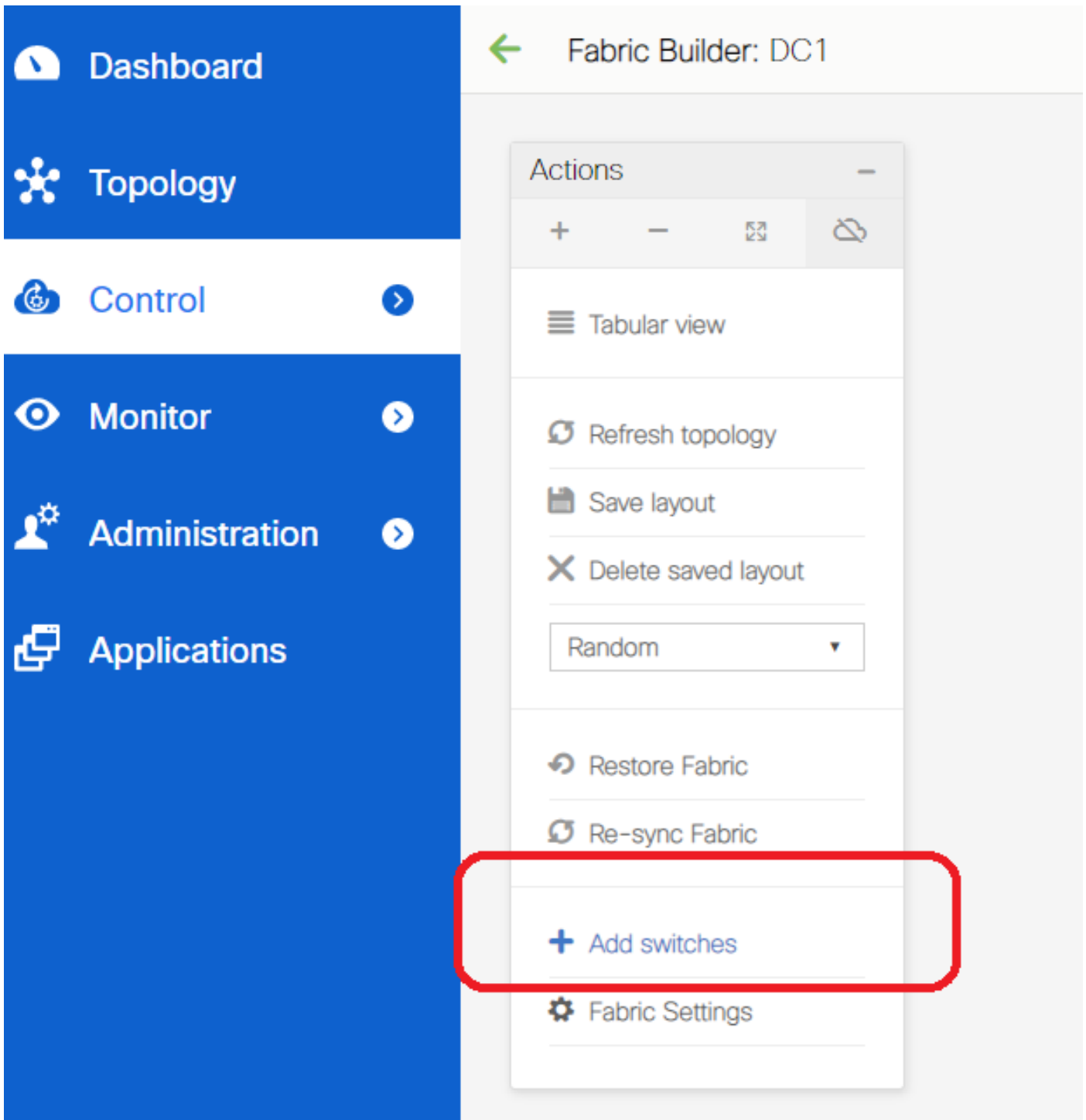
The screenshot shows the Fabric Builder interface. On the left is a blue navigation sidebar with the following menu items: Dashboard, Topology, Control (highlighted with a right arrow), Monitor (with a right arrow), Administration (with a right arrow), and Applications. The main content area has a header with the 'Fabric Builder' logo and the text 'Fabric Builder creates a managed and controlled SDN fabric. Select an existing fabric below or def'. Below this is a blue 'Create Fabric' button. A red rectangular box highlights a section titled 'Fabrics (1)'. Inside this box is a card for 'DC1' with a settings gear icon and a close 'X' icon. The card details are: Type: Switch Fabric, ASN: 65000, Replication Mode: Multicast, and Technology: VXLAN Fabric.

Esta sección muestra la lista completa de modos de fabric, ASN y replicación para cada uno de los fabric.

- El siguiente paso es agregar switches al fabric DC1

Paso 2: Agregar switches al fabric DC1

Haga clic en DC1 en el diagrama anterior y eso daría la opción de agregar switches.



- Proporcione direcciones IP y credenciales de los switches que deben importarse al fabric DC1(Por topología enumerada al principio de este documento, DC1-VTEP, DC1-SPINE, DC1-BGW1 y DC1-BGW2 forman parte de DC1)

Inventory Management

Discover Existing Switches | PowerOn Auto Provisioning (POAP)

Discovery Information > Scan Details >

Seed IP:
Ex: "2.2.2.20"; "10.10.10.40-60"; "2.2.2.20, 2.2.2.21"

Authentication Protocol:

Username:

Password:

Max Hops: hop(s)

Preserve Config: no yes
Selecting 'no' will clean up the configuration on switch(es)

Dado que se trata de una implementación Greenfield, tenga en cuenta que la opción "conservar configuración" está seleccionada como "NO"; que eliminará todas las configuraciones de los cuadros mientras realiza la importación y también recargará los switches

Seleccione el "Start discovery" para que DCNM comience a descubrir los switches en función de las direcciones IP proporcionadas en la columna "seed IP".

- Una vez que el DCNM termine de detectar los switches, las direcciones IP junto con los nombres de host se enumerarán en la administración del inventario

Inventory Management

Discover Existing Switches | PowerOn Auto Provisioning (POAP)

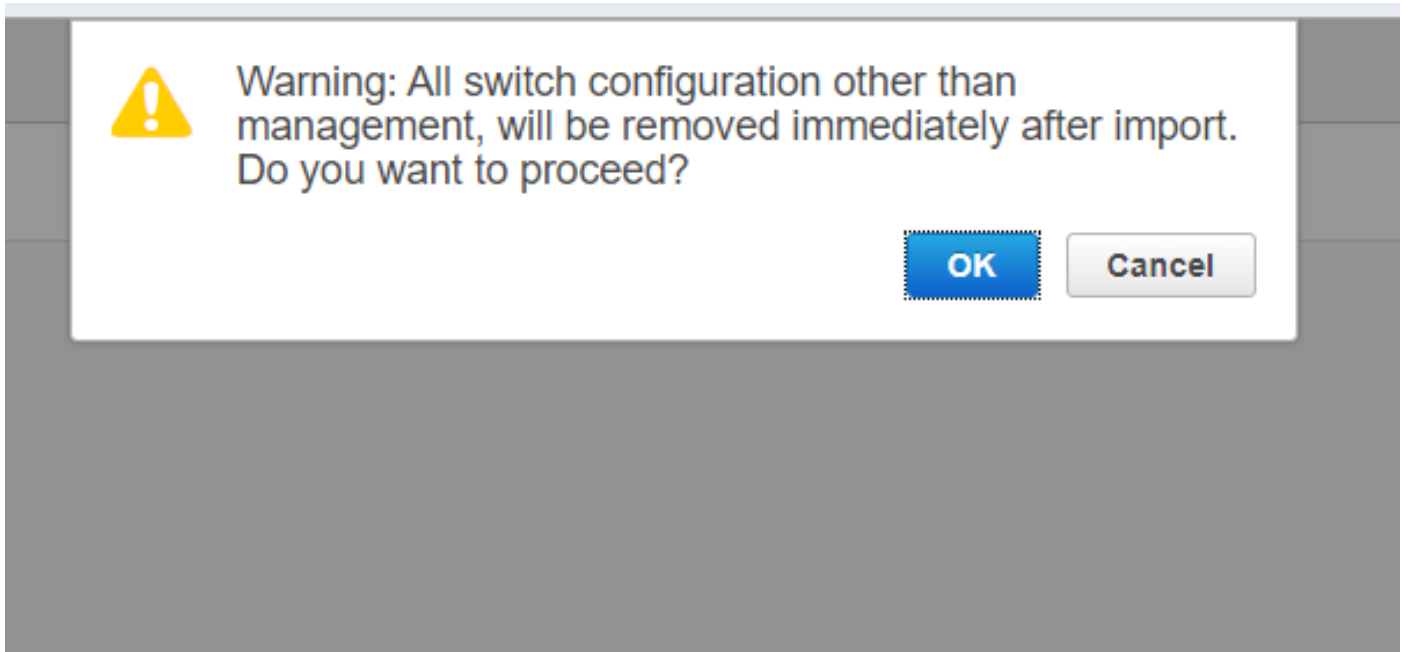
Discovery Information > Scan Details >

← Back Note: Preserve Config selection is 'no'. Switch configuration will be erased. Import into fabric

Show Quick Filter

<input type="checkbox"/>	Name	IP Address	Model	Version	Status	Progress
<input checked="" type="checkbox"/>	DC1-SPINE	10.122.165.200	N9K-C933...	9.3(1)	manageable	
<input checked="" type="checkbox"/>	DC1-BGW1	10.122.165.187	N9K-C931...	9.3(1)	manageable	
<input checked="" type="checkbox"/>	DC1-BGW2	10.122.165.154	N9K-C931...	9.3(1)	manageable	
<input type="checkbox"/>	DC1-N3K	10.122.165.195	N3K-C317...	7.0(3)I4(6)	manageable	
<input checked="" type="checkbox"/>	DC1-VTEP	10.122.165.173	N9K-C9332C	9.3(1)	manageable	

Seleccione los switches pertinentes y, a continuación, haga clic en "Importar al fabric".



Inventory Management

Discover Existing Switches | PowerOn Auto Provisioning (POAP)

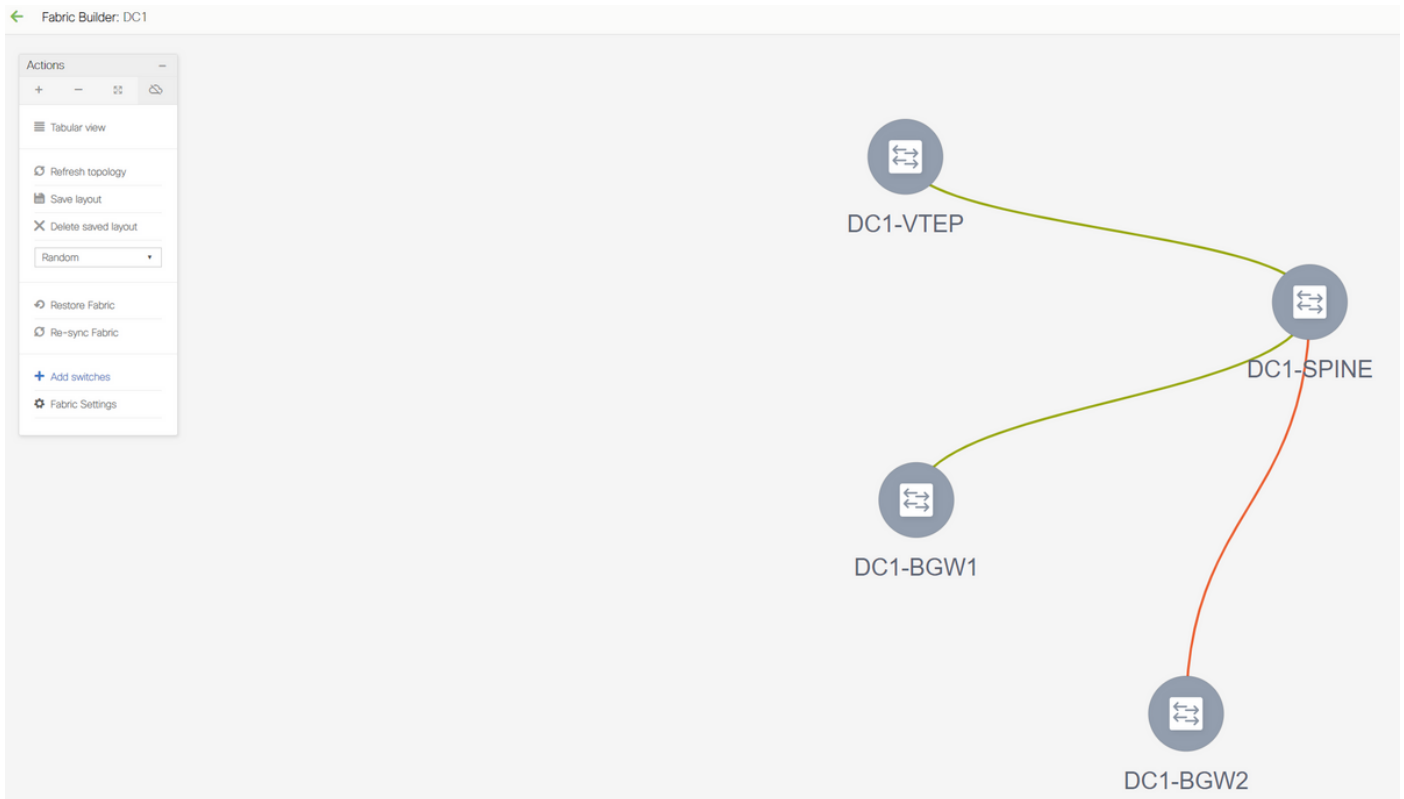
Discovery Information > Scan Details >

← Back *Note: Preserve Config selection is 'no'. Switch configuration will be erased.* Import into fabric

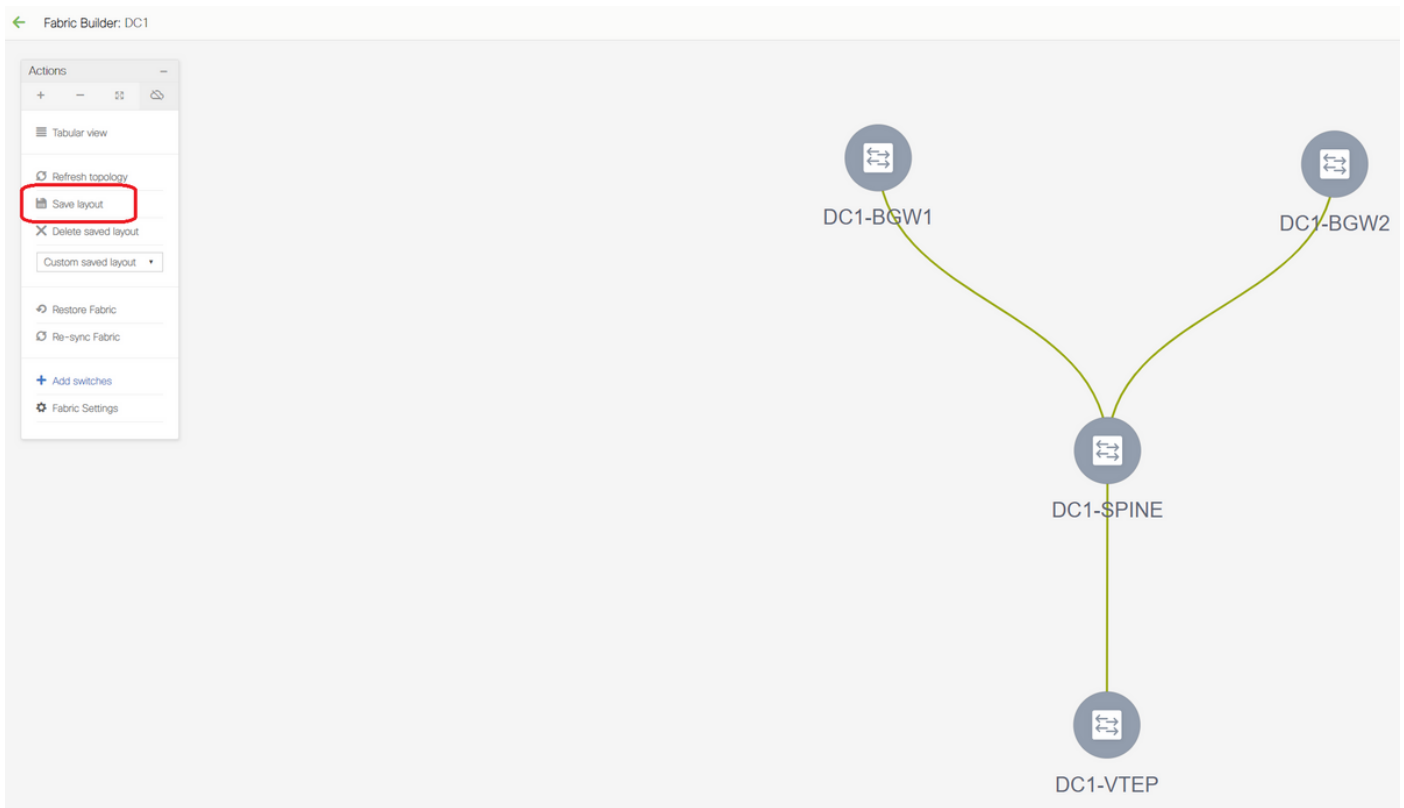
Show Quick Filter

<input type="checkbox"/>	Name	IP Address	Model	Version	Status	Progress
<input type="checkbox"/>	DC1					
<input checked="" type="checkbox"/>	DC1-SPINE	10.122.165.200	N9K-C933...	9.3(1)	manageable	70%
<input checked="" type="checkbox"/>	DC1-BGW1	10.122.165.187	N9K-C931...	9.3(1)	manageable	70%
<input checked="" type="checkbox"/>	DC1-BGW2	10.122.165.154	N9K-C931...	9.3(1)	manageable	70%
<input type="checkbox"/>	DC1-N3K	10.122.165.195	N3K-C317...	7.0(3)4(6)	manageable	
<input checked="" type="checkbox"/>	DC1-VTEP	10.122.165.173	N9K-C9332C	9.3(1)	manageable	70%

Una vez realizada la importación, la topología en el fabric builder puede ser similar a la siguiente;

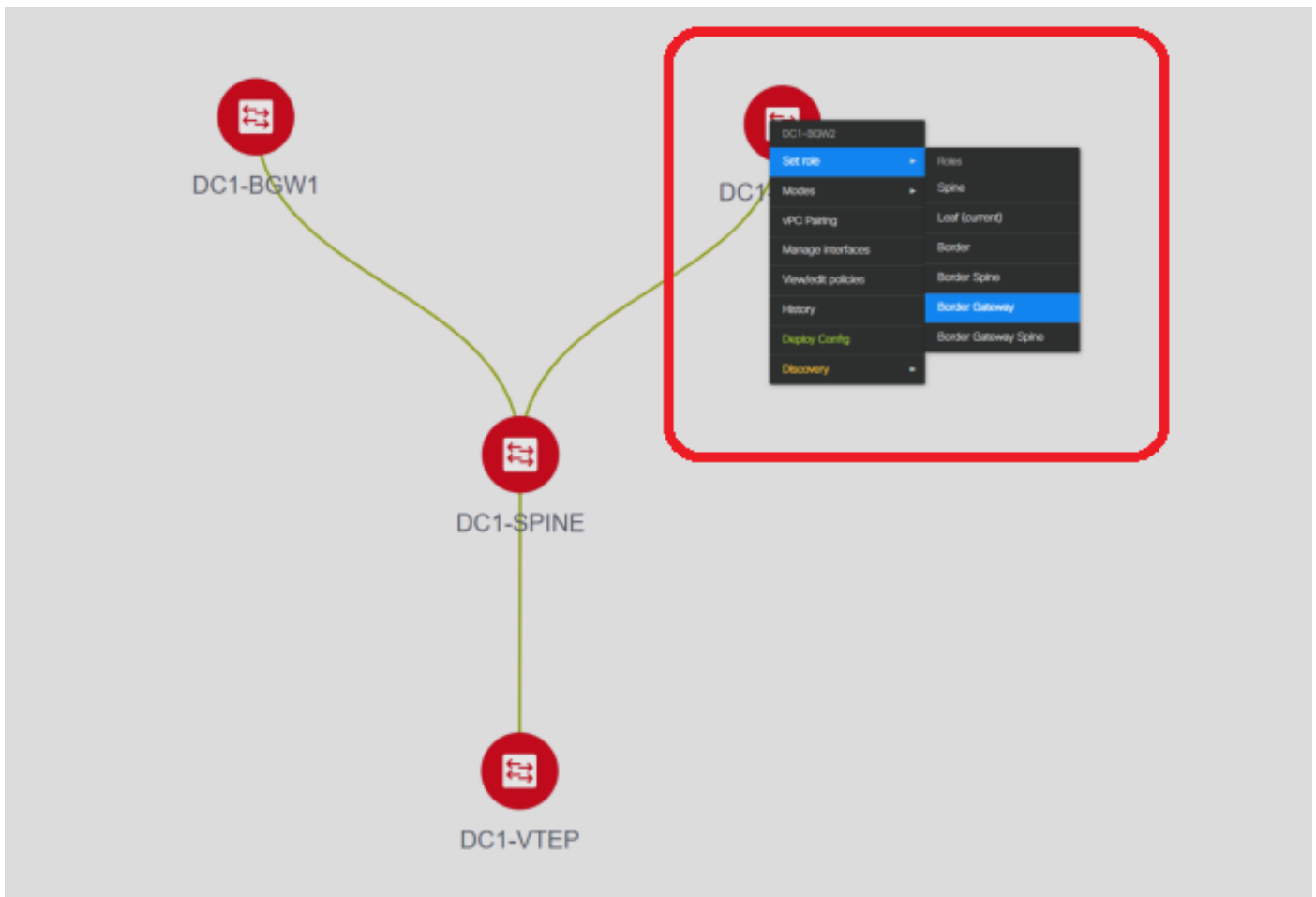


Los switches se pueden mover haciendo clic en un switch y alineándolo con la ubicación correcta dentro del diagrama



Seleccione la sección "Guardar diseño" después de reorganizar los switches en el orden en que se necesita el diseño

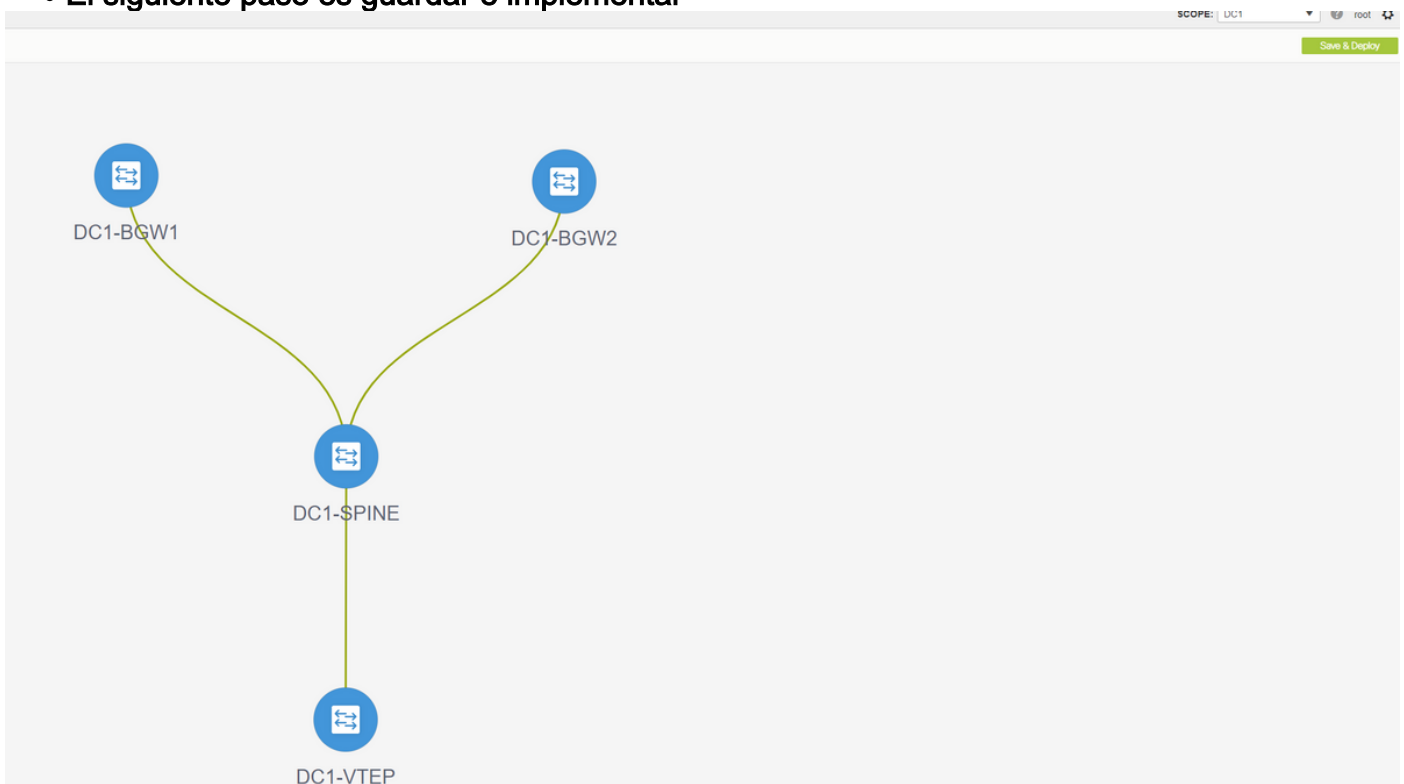
- Configuración de roles para todos los switches



Right (N.º derecho) Haga clic en cada uno de los switches y establezca la función adecuada; Aquí, DC1-BGW1 y DC1-BGW2 son las puertas de enlace de frontera

DC1-SPINE-> Se establecerá en role-Spine, DC1-VTEP-> se establecerá en role-Leaf

- El siguiente paso es guardar e implementar



DCNM ahora enumerará los switches y también tendrá la vista previa de las configuraciones que DCNM va a enviar a todos los switches.

The screenshot displays the 'Config Deployment' window in DCNM. It features two steps: 'Step 1. Configuration Preview' (active) and 'Step 2. Configuration Deployment Status'. A table lists four switches with their respective IP addresses, serial numbers, preview configurations, and deployment status. All switches are currently 'Out-of-sync' with 100% progress. A red box highlights the 'Deploy Config' button at the bottom of the window.

Switch Name	IP Address	Switch Serial	Preview Config	Status	Re-sync	Progress
DC1-VTEP	10.122.165.173	FDO22260MFQ	301 lines	Out-of-sync		100%
DC1-SPINE	10.122.165.200	FDO2313001T	520 lines	Out-of-sync		100%
DC1-BGW1	10.122.165.187	FDO21412035	282 lines	Out-of-sync		100%
DC1-BGW2	10.122.165.154	FDO20160TQM	282 lines	Out-of-sync		100%

Deploy Config

Config Deployment ×

Step 1. Configuration Preview > Step 2. Configuration Deployment Status >

Switch Name	IP Address	Status	Status Description	Progress
DC1-VTEP	10.122.165.173	STARTED	Deployment in progress.	30%
DC1-SPINE	10.122.165.200	STARTED	Deployment in progress.	23%
DC1-BGW2	10.122.165.154	STARTED	Deployment in progress.	31%
DC1-BGW1	10.122.165.187	STARTED	Deployment in progress.	29%

[Close](#)

DC1-VTEP

Una vez que se haya realizado correctamente, el estado reflejará y también los switches se mostrarán en verde

Config Deployment

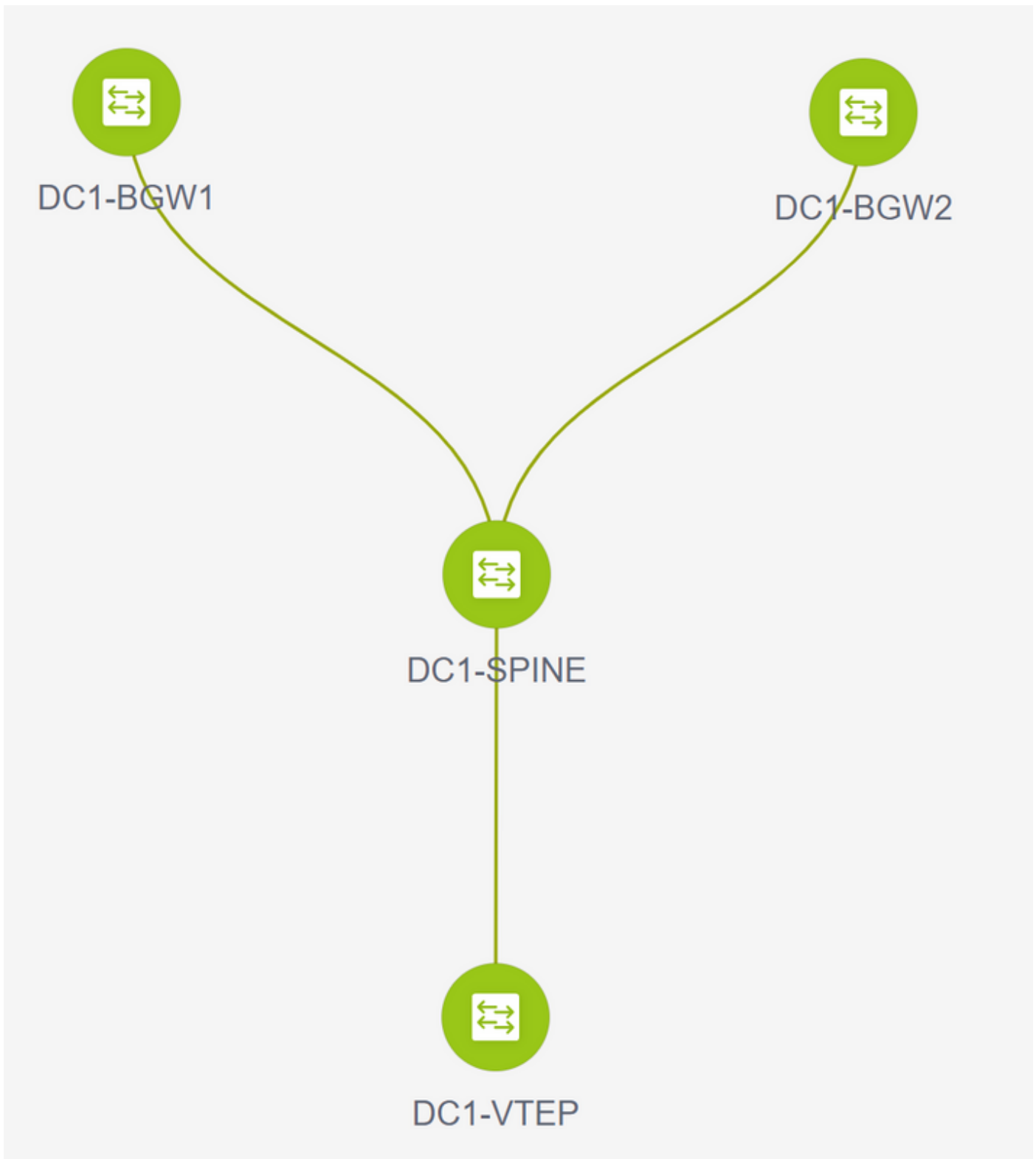


Step 1. Configuration Preview >

Step 2. Configuration Deployment Status >

Switch Name	IP Address	Status	Status Description	Progress
DC1-VTEP	10.122.165.173	COMPLETED	Deployed successfully	100%
DC1-SPINE	10.122.165.200	COMPLETED	Deployed successfully	100%
DC1-BGW2	10.122.165.154	COMPLETED	Deployed successfully	100%
DC1-BGW1	10.122.165.187	COMPLETED	Deployed successfully	100%

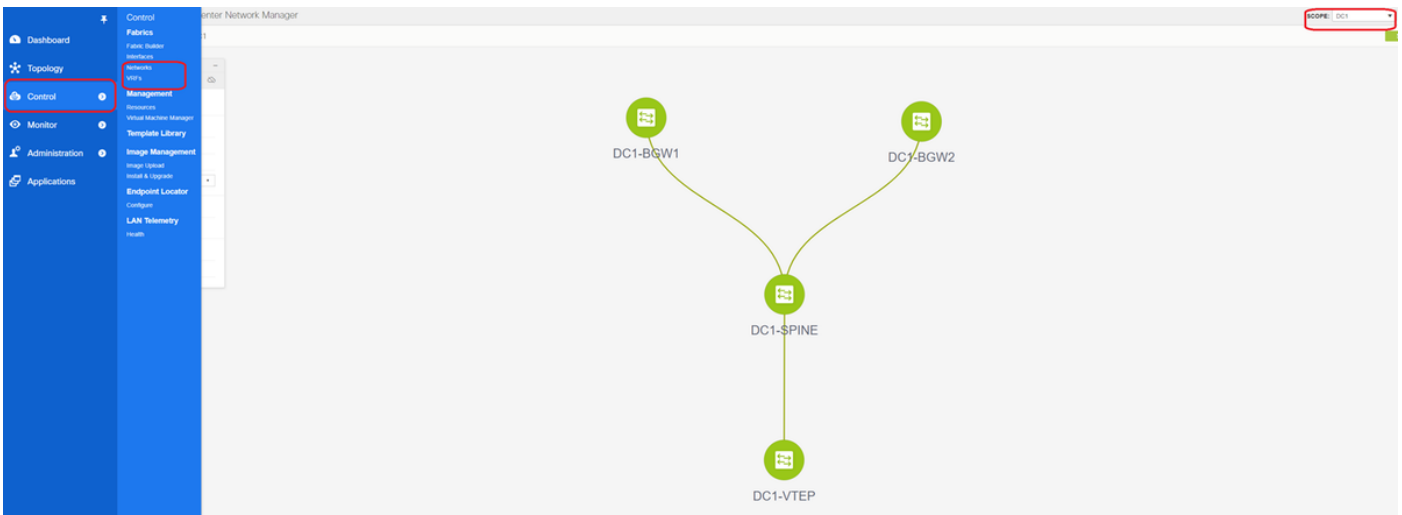
Close



Paso 3: Configuración de Redes/VRF

- Configuración de Redes/VRF

Seleccione DC1 Fabric (del menú desplegable superior derecha), Control > VRF



Lo siguiente es crear VRF

11.2 La versión de DCNM está relleno automáticamente el ID de VRF; Si es Diferente, escriba el que necesita y seleccione el botón "Crear VRF"

Aquí, el VNID de capa 3 utilizado es 1001445

- El siguiente paso es crear las redes

Proporcione el ID de red (que es el VNID correspondiente de VLAN de Capa 2)

Proporcione el VRF del que el SVI debe formar parte; De forma predeterminada, DCNM 11.2 rellena el nombre VRF en el creado anteriormente; Cambie según sea necesario

El ID de VLAN será Vlan de Capa 2 que se mapea a este VNID particular

IPv4 Gateway-> Esta es la dirección IP de la gateway de difusión que se configurará en la SVI y será la misma para todos los VTEP del fabric.

- La ficha Avanzado tiene filas adicionales que se deben rellenar si, por ejemplo, DHCP Relay está usando;

Create Network

Network Information

* Network ID: 100144

* Network Name: MyNetwork_100144

* VRF Name: tenant-1

Layer 2 Only:

* Network Template: Default_Network_Universal

* Network Extension Template: Default_Network_Extension_Univer

VLAN ID: 144 Propose VLAN ?

Network Profile

Generate Multicast IP *Please click only to generate a New Multicast Group Address and override the default value!*

General

Advanced

ARP Suppression ?

Ingress Replication ? *Read-only per network, Fabric-wide setting*

Multicast Group Address: 239.1.1.0 ?

DHCPv4 Server 1: ? *DHCP Relay IP*

DHCPv4 Server 2: ? *DHCP Relay IP*

DHCPv4 Server VRF: ?

Loopback ID for DHCP Relay interface (Min:0, Max:1023): ?

Create Network

Una vez rellenos los campos, haga clic en "Crear red".

Cree cualquier otra red que deba formar parte de este fabric;

- En este momento, VRF y Redes se acaban de definir en DCNM; pero no se transfieren de DCNM a los switches del fabric. Esto se puede verificar utilizando lo siguiente

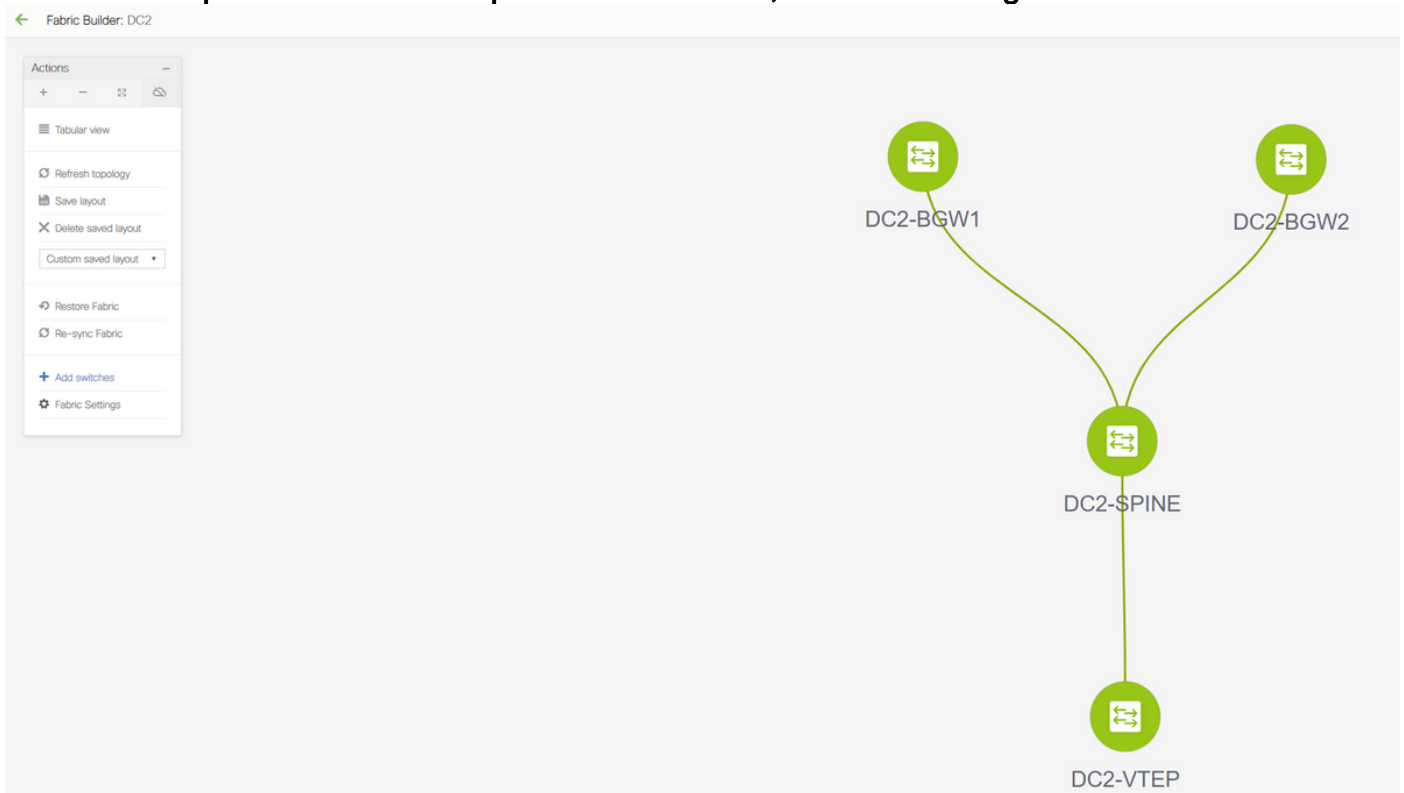
Network / VRF Selection > Network / VRF Deployment >

Networks		Network ID	VRF Name	IPv4 Gateway/Subnet	IPv6 Gateway/Prefix	Status	VLAN ID
<input type="checkbox"/>	MyNetwork_100144	100144	tenant-1	172.16.144.254/24		NA	144
<input checked="" type="checkbox"/>	MyNetwork_100145	100145	tenant-1	172.16.145.254/24		NA	145

El estado estará en "NA" si NO se implementa en los switches. Dado que se trata de un sitio múltiple que incluye los gateways de frontera, la implementación de redes/VRF se analizará más a fondo.

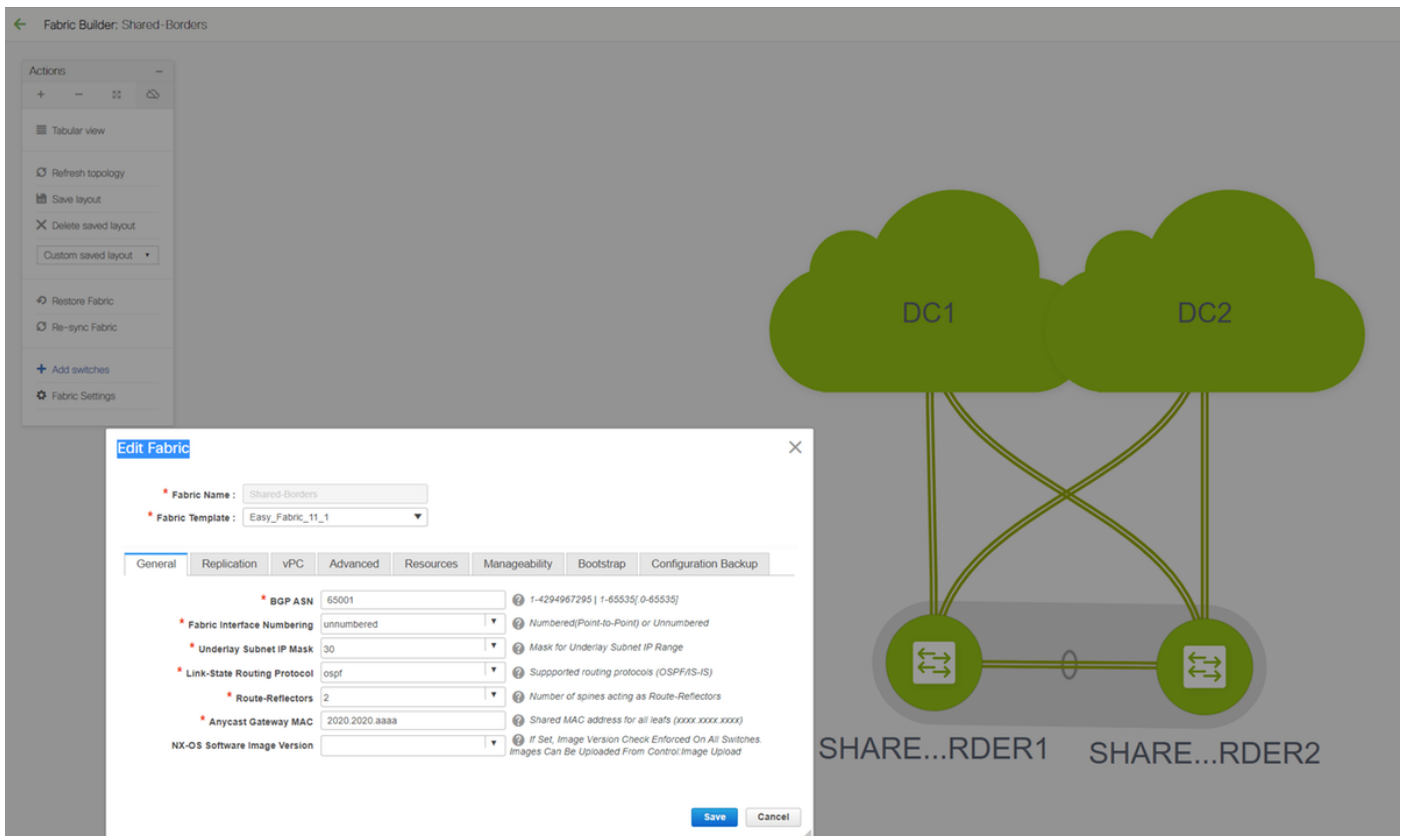
Paso 4: Repita los mismos pasos para DC2

- Ahora que el DC1 está completamente definido, también realizará el mismo procedimiento para el DC2
- Una vez que el DC2 esté completamente definido, será como el siguiente



Paso 5: Creación de un fabric sencillo para las fronteras compartidas

- Aquí es donde se crea otro fabric sencillo que incluirá los bordes compartidos que se encuentran en vPC
- Tenga en cuenta que los bordes compartidos mientras se implementa a través de DCNM Se deben configurar como vPC de otra manera, los links entre switches se apagarán después de que se realice una operación de "resincronización" en DCNM
- Los switches de las fronteras compartidas deben configurarse con la función de "borde"

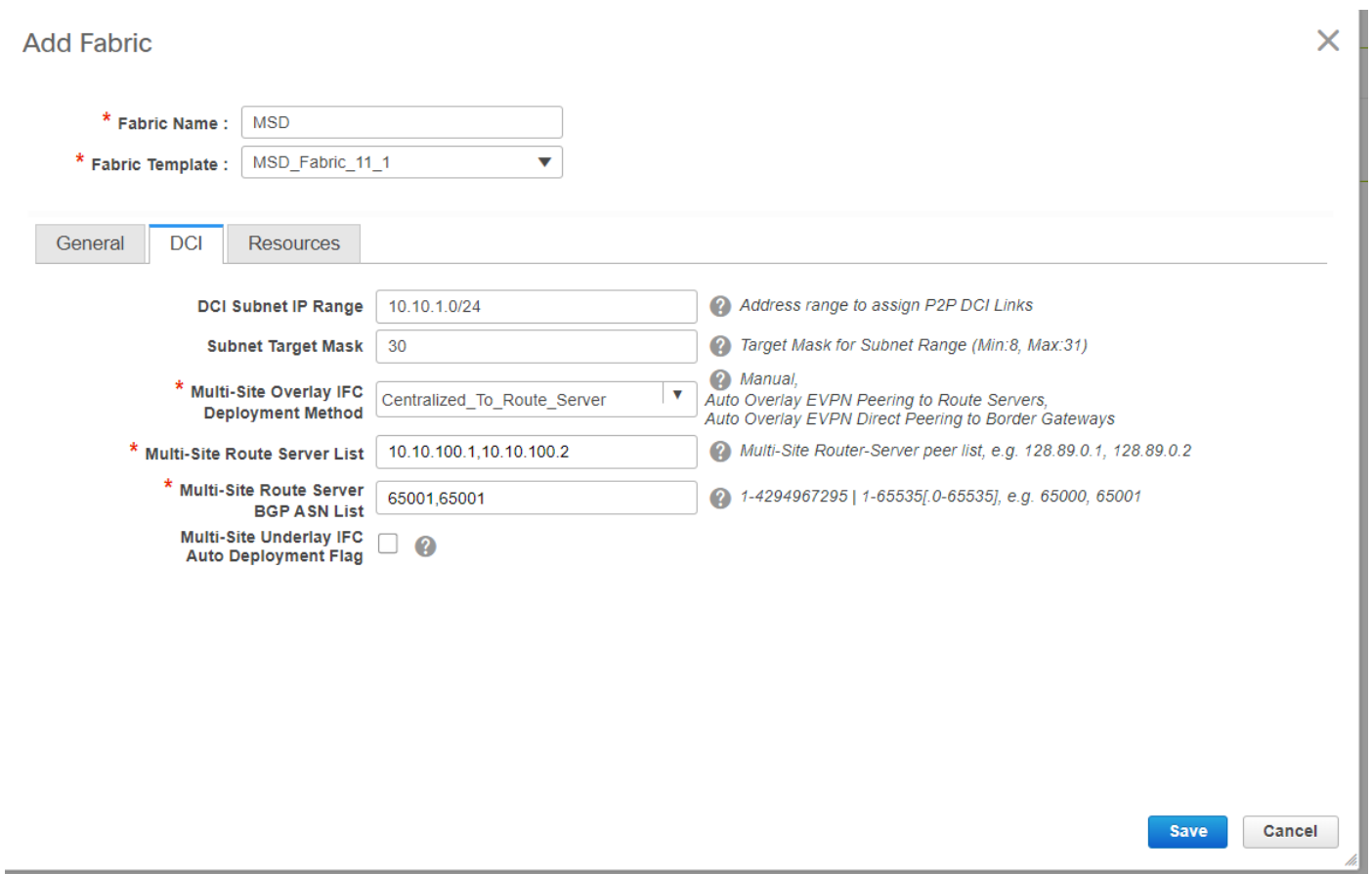
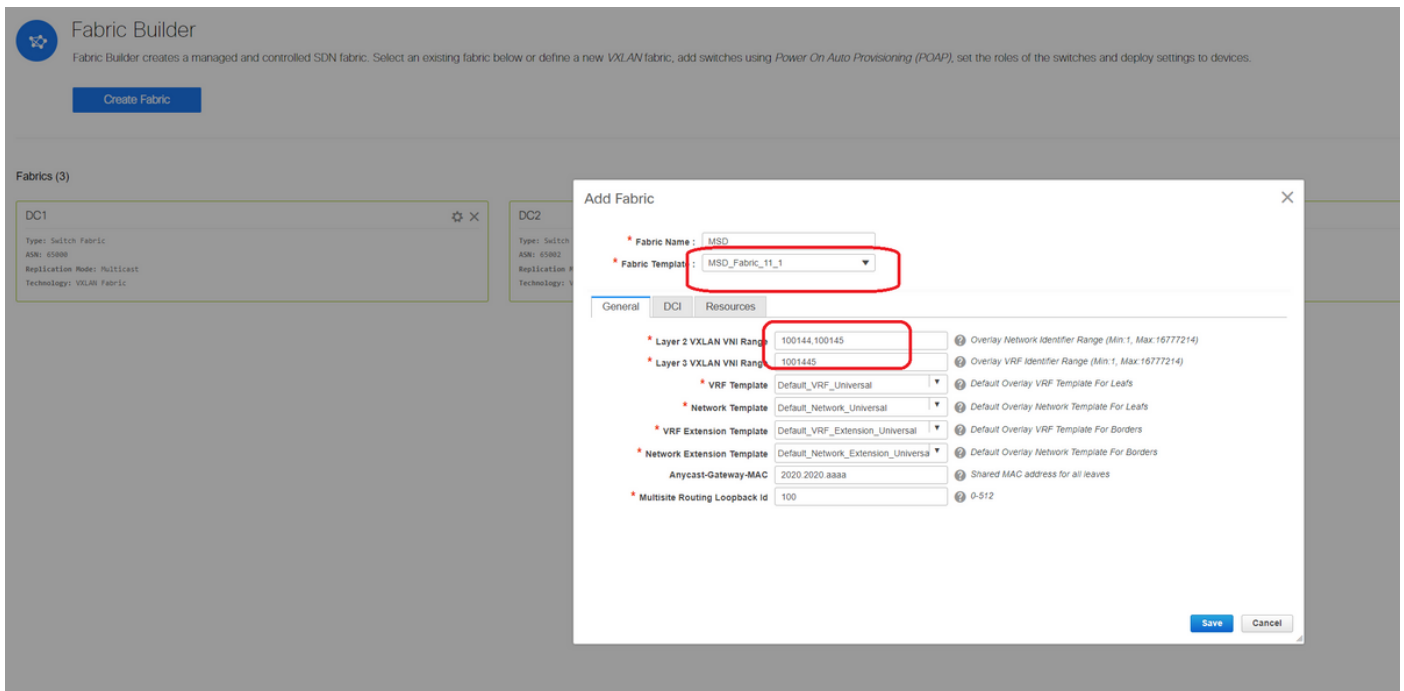


Los VRF también se crean como lo fueron para los fabrics DC1 y DC2

Las redes no son necesarias en un borde compartido porque el borde compartido no tendrá ninguna VLAN/VNID de Capa 2; Los bordes compartidos no son una terminación de túnel para cualquier tráfico Este/Oeste de DC1 a DC2; Sólo los gateways de frontera desempeñarían un papel en términos de encapsulación/desencapsulación de vxlan para el tráfico DC1 Este/Oeste<>DC2

Paso 6: Creación de MSD y desplazamiento de fabric DC1 y DC2

Vaya a Fabric Builder y cree un nuevo Fabric y utilice la plantilla -> MSD_Fabric_11_1



Tenga en cuenta que el método de implementación de IFC superpuesta de varios sitios debe ser **"centralizado_en_servidor_de_ruta"**; Aquí, los bordes compartidos se consideran servidores de ruta, por lo que esta opción se utiliza desde la lista desplegable.

Dentro de la **"Lista de Servidor de Ruta Multisitio"**; A continuación, descubra las direcciones IP de bucle invertido de Loopback0 (que es el loopback de routing) en el borde compartido y llénalo

ASN es el que se encuentra en el borde compartido(consulte el diagrama de la parte superior de este documento para obtener más detalles); A los efectos de este documento, ambos bordes compartidos se configuran en el mismo ASN; Rellenar en consecuencia

- La siguiente pestaña es donde se proporciona el rango de IP de loopback multisitio como se muestra a continuación

Add Fabric

* Fabric Name : MSD

* Fabric Template : MSD_Fabric_11_1

General DCI Resources

* Multi-Site Routing Loopback IP Range 10.222.222.0/24 ? Typically Loopback100 IP Address Range

Save Cancel

Una vez rellenados todos los campos, haga clic en el botón "guardar" y se creará un nuevo fabric con la plantilla-> MSD

Lo siguiente es mover los fabrics DC1 y DC2 a este MSD

Fabric Builder: MSD

Actions

- Tabular view
- Refresh topology
- Save layout
- Delete saved layout
- Random
- Fabric Settings
- Move Fabrics**

Move Fabric

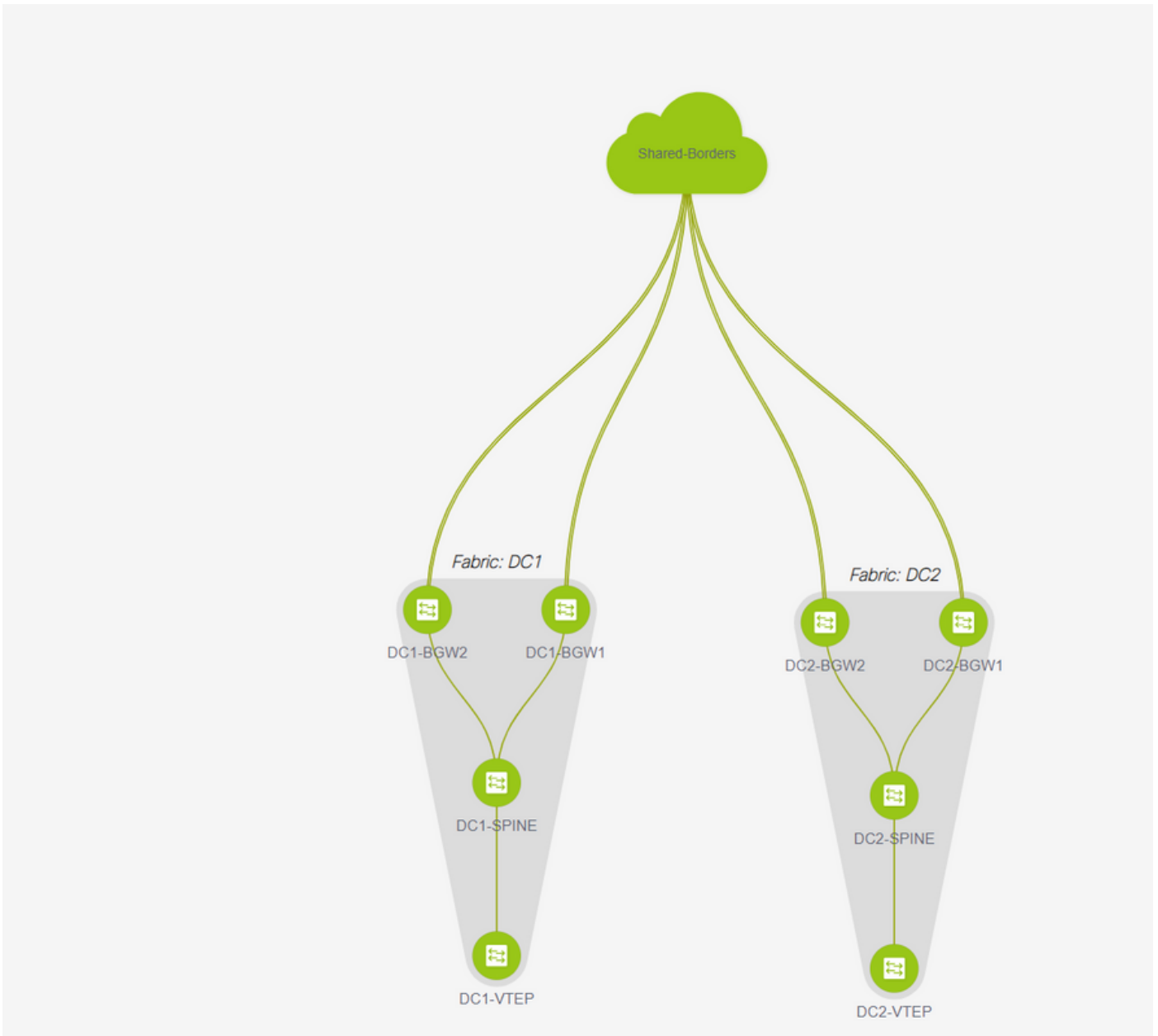
Please note that it may take a few minutes if there is a large number of VRFs/NWs in the fabrics!

Selected 0 / Total 3

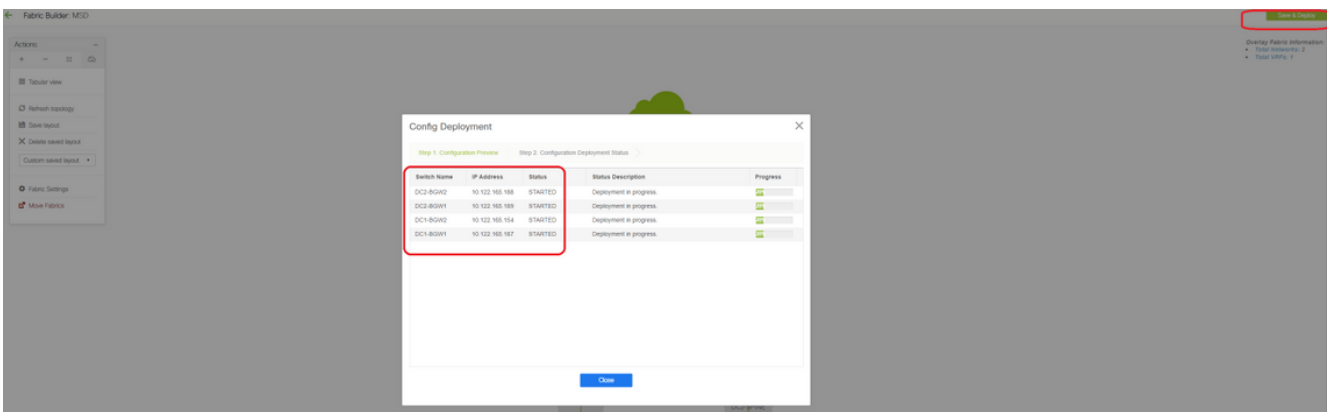
Fabric Name	Fabric State
<input type="radio"/> DC1	standalone
<input type="radio"/> DC2	standalone
<input type="radio"/> Shared-Borders	standalone

Add Remove Cancel

Después de mover el fabric, se ve como abajo



Una vez hecho esto, haga clic en el botón "Save&Deploy" (Guardar y implementar), que llevará las configuraciones necesarias en lo que respecta a los Gateways de borde a varios sitios.



Paso 7: Creación de fabric externo

Cree un entramado externo y añada el router externo como se muestra a continuación;

Add Fabric

* Fabric Name : External

* Fabric Template : External_Fabric_11_1

General Advanced Resources DCI Configuration Backup Bootstrap

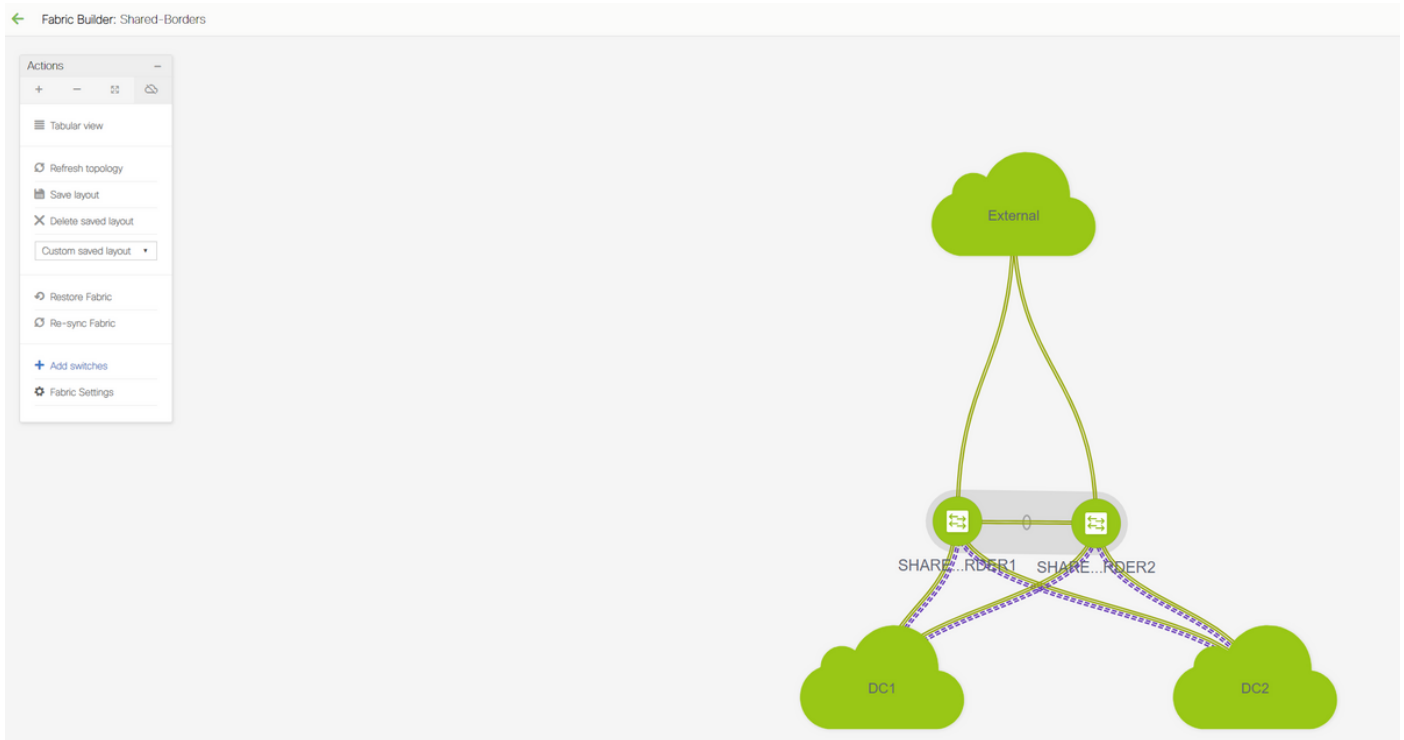
* BGP AS # 65100 ? 1-4294967295 | 1-65535[.0-65535]

Fabric Monitor Mode ? If enabled, fabric is only monitored. No configuration will be deployed

Asigne un nombre al fabric y utilice la plantilla-> "External_Fabric_11_1";

Proporcione el ASN

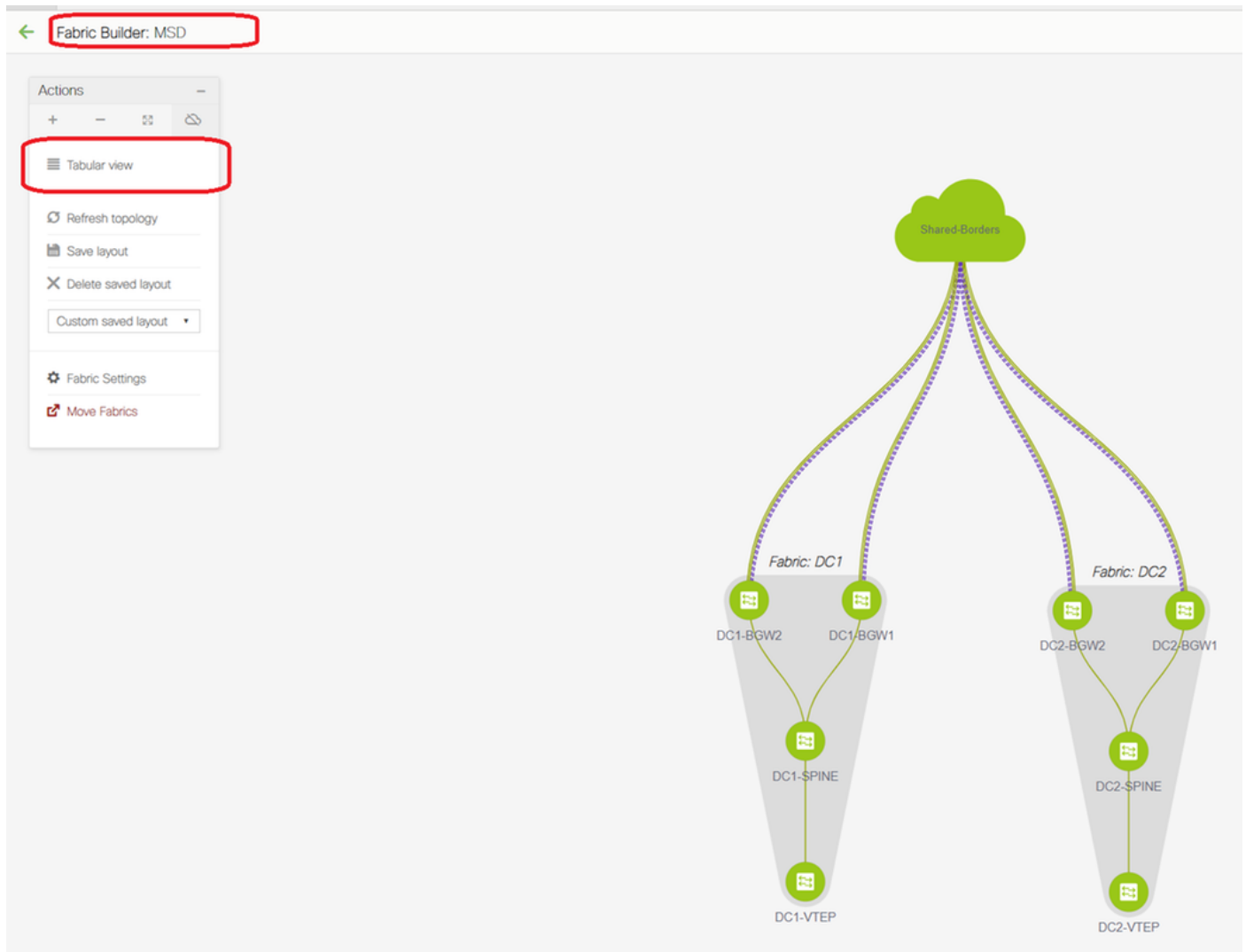
Al final, los distintos tejidos serán como los que se muestran a continuación



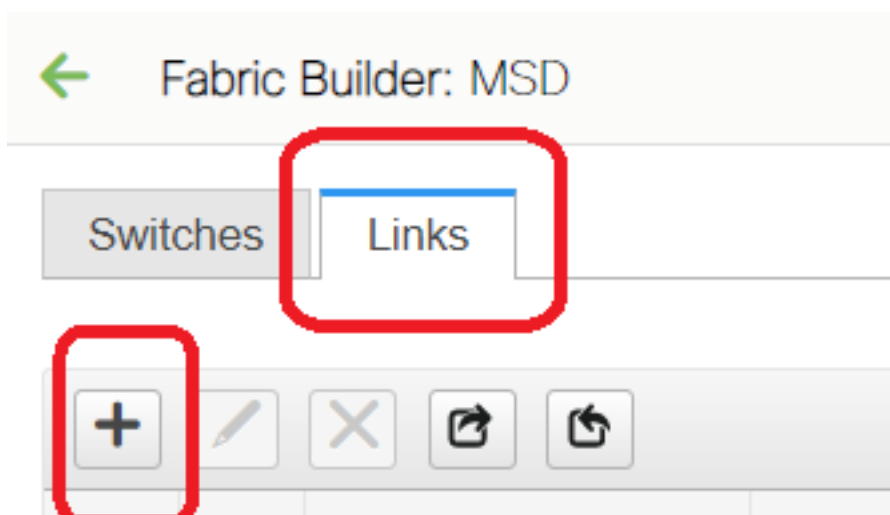
Paso 8: eBGP Underlay para loopback reacty entre BGW(iBGP entre fronteras compartidas también)

Los bordes compartidos ejecutan el evpn eBGP I2vpn con los Gateways de Borde y las conexiones VRF-LITE hacia el router externo

Antes de formar eBGP I2vpn evpn con los loopbacks, se debe asegurarse de que los loopbacks sean accesibles a través de algún método; En este ejemplo, estamos utilizando eBGP IPv4 AF de BGW a los bordes compartidos y luego anunciamos los loopbacks para formar más la vecindad del evpn I2vpn.



Una vez seleccionado el fabric MSD, cambie a la "vista tabular"



Link Management - Add Link ✕

* Link Type

* Link Sub-Type

* Link Template

* Source Fabric

* Destination Fabric

* Source Device

* Source Interface

* Destination Device

* Destination Interface

▼ Link Profile

General

Advanced

* BGP Local ASN Local BGP Autonomous System

* IP Address/Mask IP address with mask (e.g. 10.4.10.1/24)

* BGP Neighbor IP Neighbor IP address

* BGP Neighbor ASN Neighbor BGP Autonomous System

* BGP Maximum Paths Maximum number of iBGP neighbors

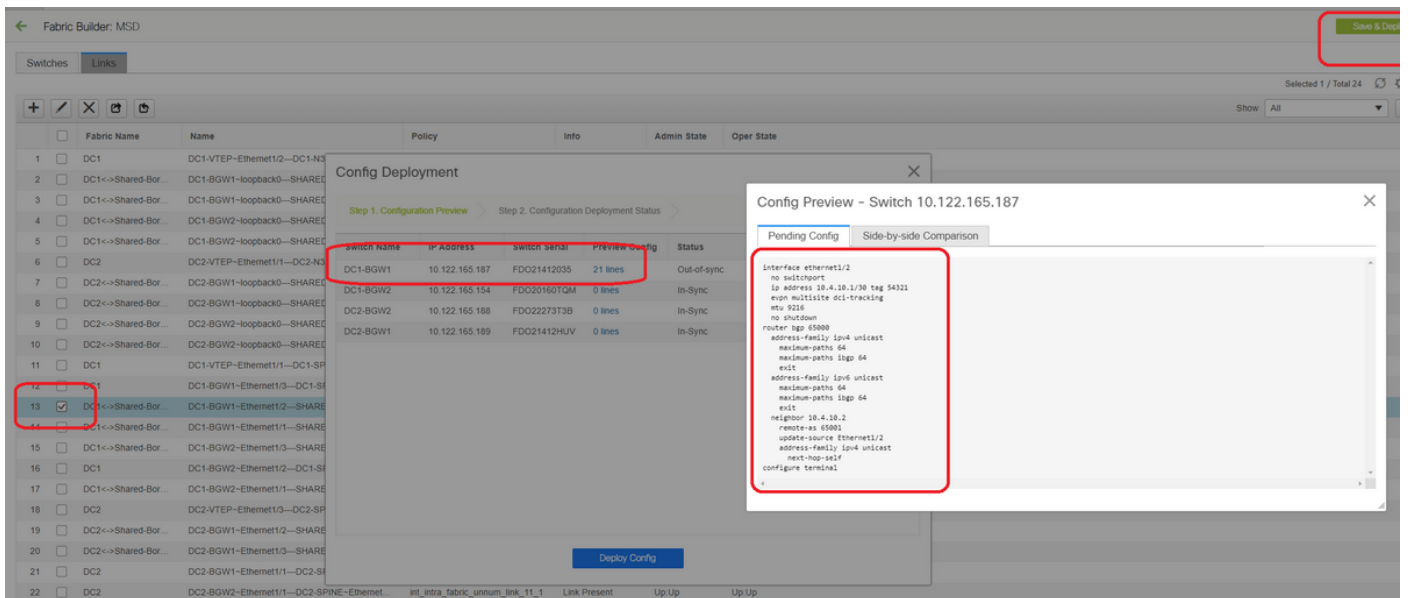
* Routing TAG Routing tag associated with this link

[Save](#)

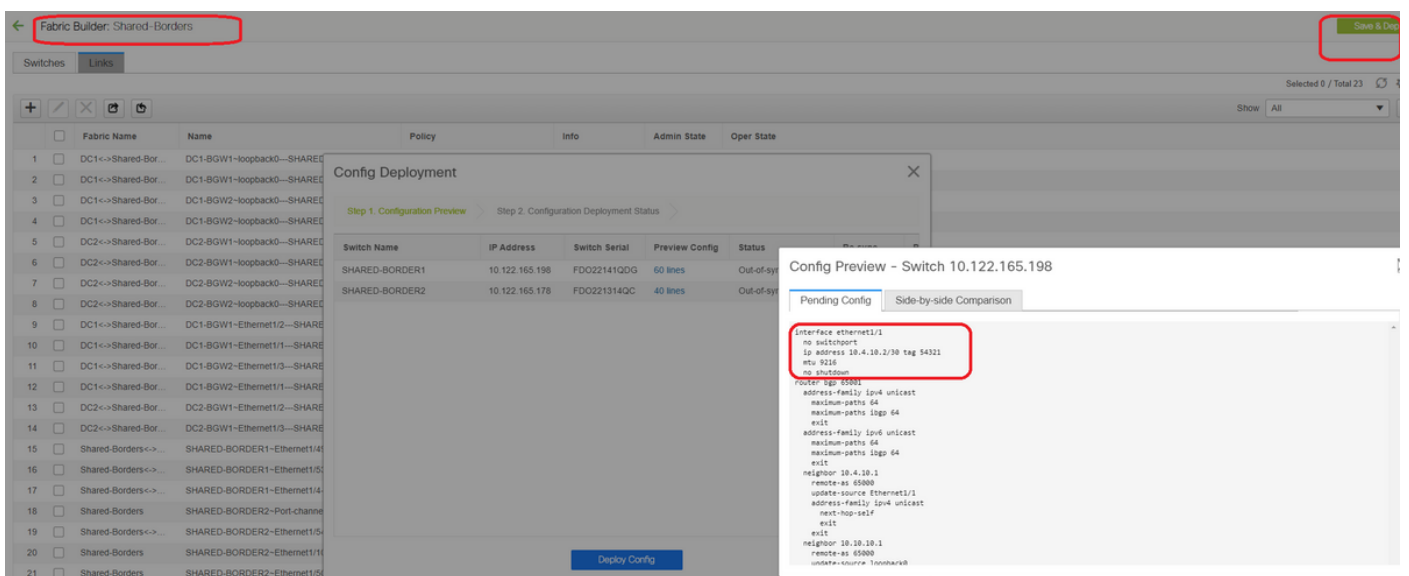
Seleccione "Inter-Fabric" y utilice "Multisite_UNDERLAY"

Estamos aquí tratando de formar un Vecindario BGP IPv4 con el router de borde compartido; Seleccione los switches e interfaces en consecuencia.

Tenga en cuenta que si CDP está detectando al vecino de DC1-BGW1 a SB1, sólo es necesario proporcionar las direcciones IP aquí en esta sección y eso configurará de manera efectiva las direcciones IP en las interfaces relevantes después de realizar "guardar e implementar"



Una vez que se selecciona Guardar e implementar, las líneas de configuración necesarias se propagan para DC1-BGW1; El mismo paso tendrá que llevarse a cabo después de seleccionar también el fabric de "borde compartido".



Desde CLI, se puede verificar lo mismo con el siguiente comando;

```

DC1-BGW1# show ip bgp sum
BGP summary information for VRF default, address family IPv4 Unicast
BGP router identifier 10.10.10.1, local AS number 65000
BGP table version is 11, IPv4 Unicast config peers 1, capable peers 1
2 network entries and 2 paths using 480 bytes of memory
BGP attribute entries [1/164], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [0/0]
  
```

```

Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.4.10.2     4 65001      6       7      11    0    0 00:00:52 0
  
```

Tenga en cuenta que también se debe realizar el "save&Deploy" en el fabric DC1 (seleccione el desplegable para DC1 y luego realice lo mismo) de modo que el direccionamiento IP relevante, las configuraciones BGP se propaguen a los switches en DC1(que son los Gateways de borde);

Además, la capa subyacente multisitio debe crearse desde DC1-BGW, DC2-BGW hasta los bordes compartidos; por lo tanto, también hay que hacer lo mismo con los pasos anteriores.

Al final, los bordes compartidos tendrán vecindad AF IPv4 eBGP con todos los BGW en DC1 y DC2 como se muestra a continuación;

```
SHARED-BORDER1# sh ip bgp sum
BGP summary information for VRF default, address family IPv4 Unicast
BGP router identifier 10.10.100.1, local AS number 65001
BGP table version is 38, IPv4 Unicast config peers 4, capable peers 4
18 network entries and 20 paths using 4560 bytes of memory
BGP attribute entries [2/328], BGP AS path entries [2/12]
BGP community entries [0/0], BGP clusterlist entries [0/0]
```

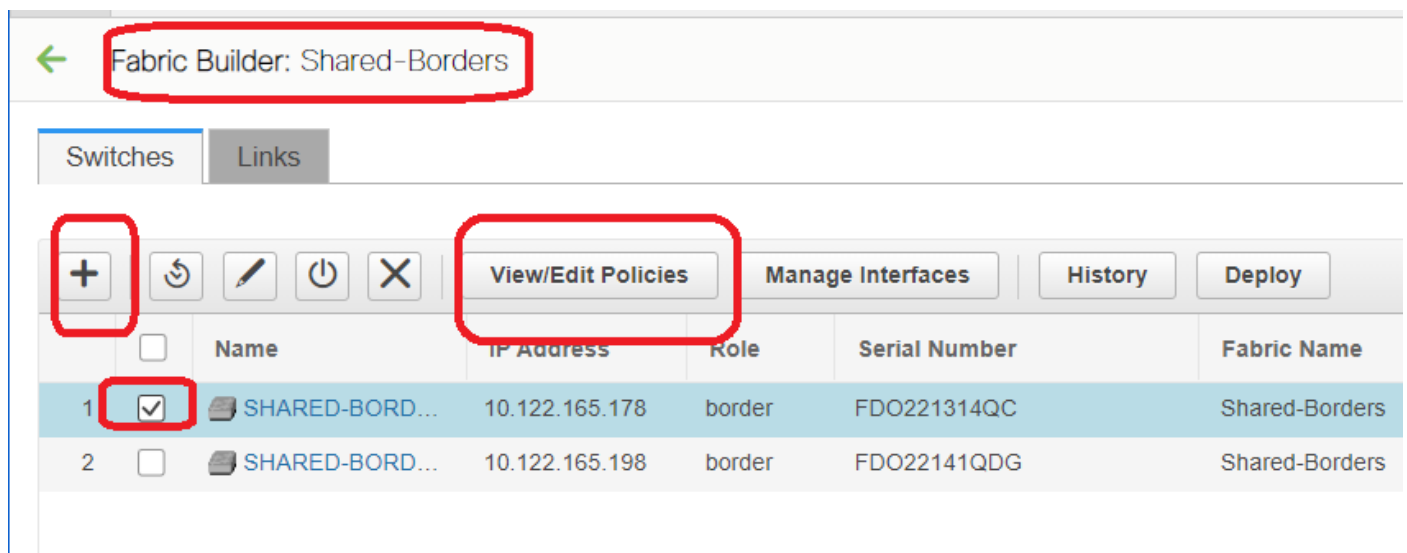
Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.4.10.1	4	65000	1715	1708	38	0	0	1d03h 5	
10.4.10.6	4	65000	1461	1458	38	0	0	1d00h 5	
10.4.10.18	4	65002	1459	1457	38	0	0	1d00h 5	
10.4.10.22	4	65002	1459	1457	38	0	0	1d00h 5	

```
SHARED-BORDER2# sh ip bgp sum
BGP summary information for VRF default, address family IPv4 Unicast
BGP router identifier 10.10.100.2, local AS number 65001
BGP table version is 26, IPv4 Unicast config peers 4, capable peers 4
18 network entries and 20 paths using 4560 bytes of memory
BGP attribute entries [2/328], BGP AS path entries [2/12]
BGP community entries [0/0], BGP clusterlist entries [0/0]
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.4.10.10	4	65000	1459	1458	26	0	0	1d00h 5	
10.4.10.14	4	65000	1461	1458	26	0	0	1d00h 5	
10.4.10.26	4	65002	1459	1457	26	0	0	1d00h 5	
10.4.10.30	4	65002	1459	1457	26	0	0	1d00h 5	

Anteriormente es el requisito previo previo para construir la vecindad l2vpn evpn de BGW a los bordes compartidos(Tenga en cuenta que no es obligatorio utilizar BGP; cualquier otro mecanismo para intercambiar prefijos de loopback lo haría); Al final, el requisito básico es que todos los loopbacks (de fronteras compartidas, BGW) deben ser accesibles desde todos los BGW.

Tenga en cuenta también que es necesario establecer una vecindad AF IPv4 de iBGP entre las fronteras compartidas; A partir de hoy, DCNM no tiene la opción de construir un iBGP entre los bordes compartidos usando una plantilla/desplegable; Para ello, se debe realizar una configuración de forma libre que se muestra a continuación;



View/Edit Policies for SHARED-BORDER1 (FDO22141QDG)

Selected 1 / Total 1

View All Push Config Current Switch Config Show Quick Filter

Template	Policy ID	Fabric Name	Serial Number	Editable	Entity Type	Entity Name
fre						
<input checked="" type="checkbox"/> switch_freeform	POLICY-78700	Shared-Borders	FDO22141QDG	true	SWITCH	SWITCH

Edit Policy

Policy ID: POLICY-78700
Entity Type: SWITCH

Template Name: switch_freeform
Entity Name: SWITCH

* Priority (1-1000): 500

General

* Switch Freeform Config

```

route-map direct
router bgp 65001
address-family ipv4 unicast
redistribute direct route-map direct
neighbor 10.100.100.2
remote-as 65001
address-family ipv4 unicast
next-hop-self

```

Variables:

Save Push Config Cancel

Busque las direcciones IP configuradas en la SVI de Respaldo de los bordes compartidos; Como se muestra arriba, la forma libre se agrega en el switch Shared-border1 y el vecino iBGP especificado es el de Shared-border2(10.100.100.2)

Tenga en cuenta que mientras proporciona las configuraciones dentro de la forma libre en DCNM, proporcione el espaciado correcto después de cada comando (deje el número par de espacios; es decir, después del router bgp 65001, proporcione dos espacios y luego el comando neighbor <>, etc)

Asegúrese también de realizar una redistribución directa para las rutas directas (rutas de loopback) en BGP o en algún otro formulario para anunciar los loopbacks; en el ejemplo anterior, se crea un route-map direct para que coincida con todas las rutas directas y luego se redistribuye direct dentro del BGP AF IPv4

Una vez que la configuración se "guarda e implementa" desde DCNM, la vecindad iBGP se forma como se muestra a continuación;

```

SHARED-BORDER1# sh ip bgp sum
BGP summary information for VRF default, address family IPv4 Unicast
BGP router identifier 10.10.100.1, local AS number 65001
BGP table version is 57, IPv4 Unicast config peers 5, capable peers 5
18 network entries and 38 paths using 6720 bytes of memory
BGP attribute entries [4/656], BGP AS path entries [2/12]
BGP community entries [0/0], BGP clusterlist entries [0/0]

```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.4.10.1	4	65000	1745	1739	57	0	0	1d04h	5
10.4.10.6	4	65000	1491	1489	57	0	0	1d00h	5
10.4.10.18	4	65002	1490	1487	57	0	0	1d00h	5
10.4.10.22	4	65002	1490	1487	57	0	0	1d00h	5
10.100.100.2	4	65001	14	6	57	0	0	00:00:16	18 # iBGP neighborship from shared border1 to shared border2

Con el paso anterior, la base multisitio está completamente configurada.

El siguiente paso es crear la superposición de varios sitios;

Paso 9: Creación de superposición multisitio de BGW a fronteras compartidas

Tenga en cuenta que aquí los bordes compartidos son también los servidores de ruta

Seleccione el MSD y, a continuación, vaya a la "vista tabular" donde se puede crear un nuevo enlace; A partir de ahí, se debe crear un nuevo link de superposición multisitio y las direcciones IP relevantes tendrán que proporcionar el ASN correcto como se muestra a continuación; Este paso debe hacerse para todos los vecinos evpn l2vpn (que es de cada BGW a cada borde compartido)

Arriba es un ejemplo; Realice lo mismo para todos los otros links superpuestos multisitio y, al final, la CLI será similar a la siguiente;

```
SHARED-BORDER1# sh bgp l2vpn evpn summary
BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 10.10.100.1, local AS number 65001
BGP table version is 8, L2VPN EVPN config peers 4, capable peers 4
1 network entries and 1 paths using 240 bytes of memory
BGP attribute entries [1/164], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [0/0]
```


Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.10.10.1	4	65000	21	19	8	0	0	00:13:52	0
10.10.10.2	4	65000	22	20	8	0	0	00:14:14	0
10.10.20.1	4	65002	21	19	8	0	0	00:13:56	0
10.10.20.2	4	65002	21	19	8	0	0	00:13:39	0

```

SHARED-BORDER2# sh bgp l2vpn evpn summary
BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 10.10.100.2, local AS number 65001
BGP table version is 8, L2VPN EVPN config peers 4, capable peers 4
1 network entries and 1 paths using 240 bytes of memory
BGP attribute entries [1/164], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [0/0]

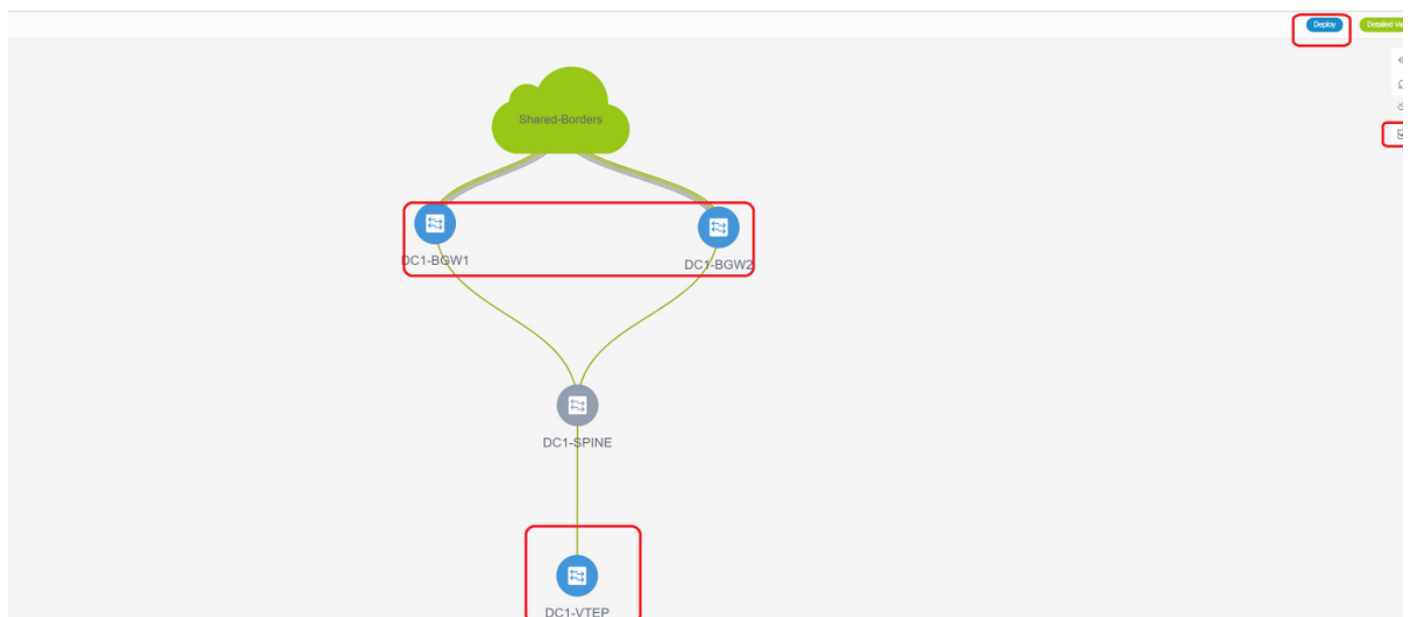
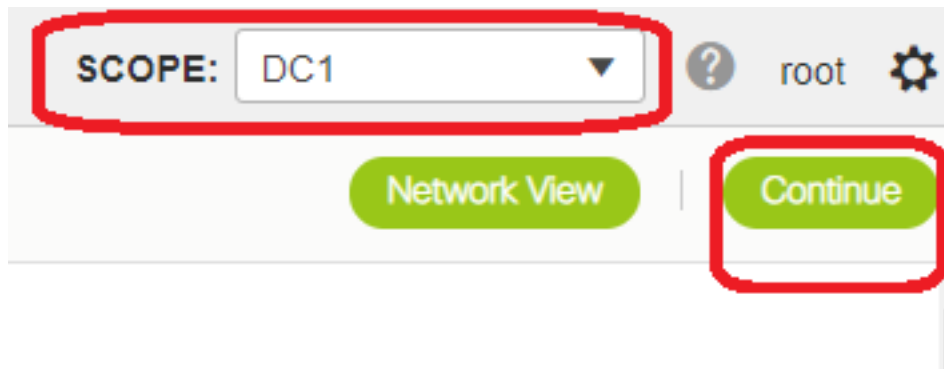
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.10.10.1	4	65000	22	20	8	0	0	00:14:11	0
10.10.10.2	4	65000	21	19	8	0	0	00:13:42	0
10.10.20.1	4	65002	21	19	8	0	0	00:13:45	0
10.10.20.2	4	65002	22	20	8	0	0	00:14:15	0

Paso 10: Implementación de redes/VRF en ambos sitios

A medida que hemos terminado la superposición y la superposición multisitio, el siguiente paso es implementar las redes/VRF en todos los dispositivos;

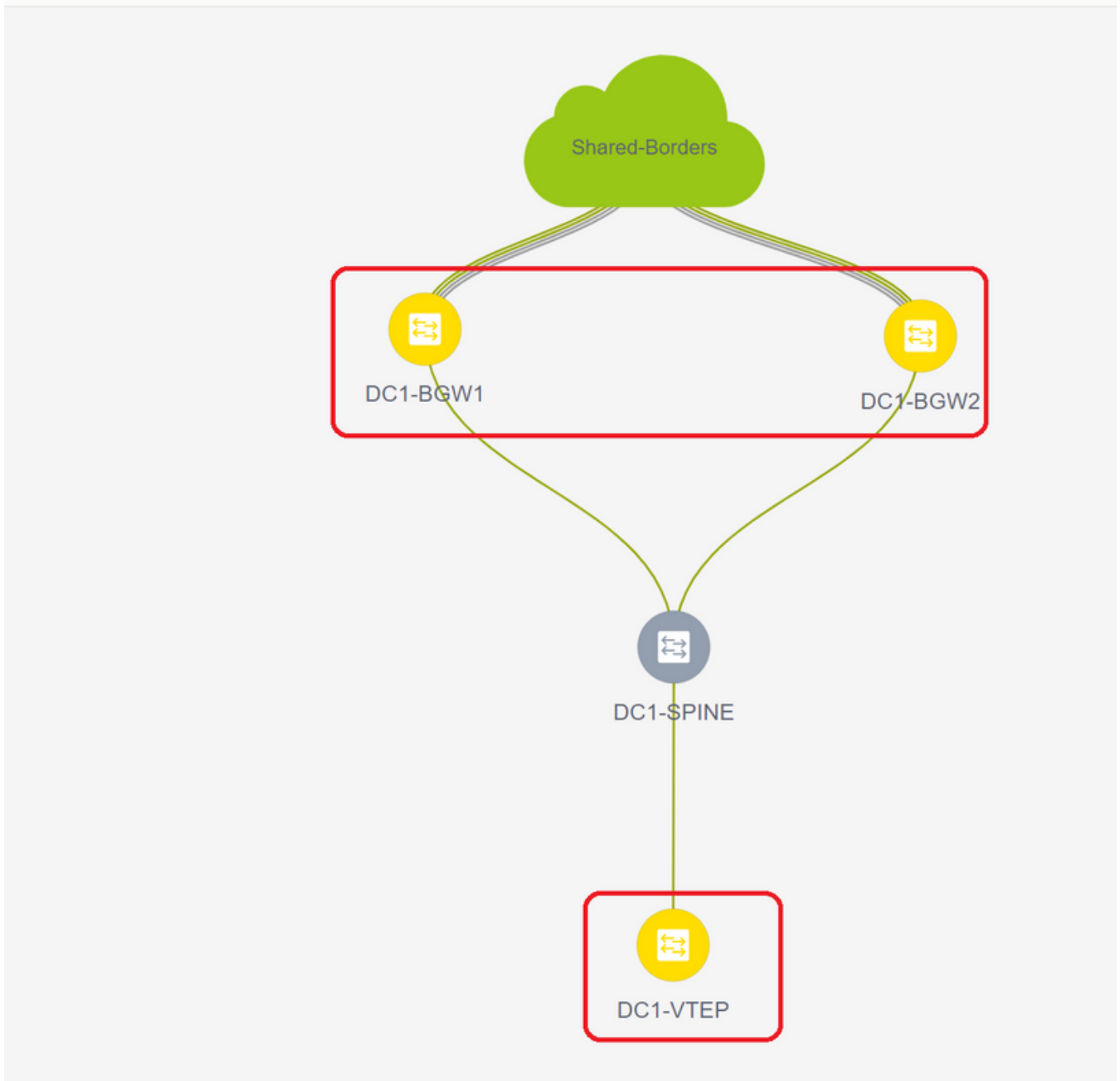
Comenzando con los VRF en los Fabric-> DC1, DC2 y bordes compartidos.



Una vez seleccionada la vista VRF, haga clic en "continuar"; Esto mostrará los dispositivos en la

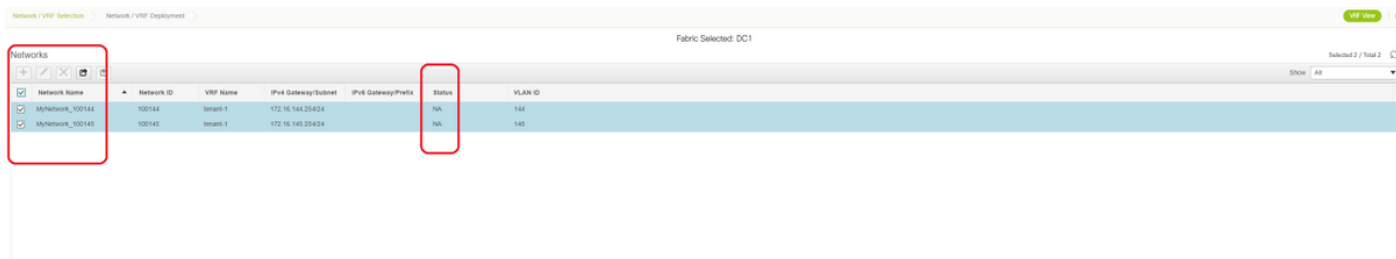
topología

Dado que el VRF debe implementarse en varios switches (incluidos los Gateways de borde y la hoja), seleccione la casilla de verificación en el extremo derecho y y, a continuación, seleccione los switches que tienen la misma función al mismo tiempo; por ejemplo: DC1-BGW1 y DC1-BGW2 se pueden seleccionar al mismo tiempo y, a continuación, guardar ambos switches; Después de esto, seleccione los switches de hoja que sean aplicables(aquí sería DC1-VTEP)



Como se ha visto anteriormente, cuando se selecciona la opción "Implementar", todos los switches que se seleccionaron anteriormente iniciarán la implementación y finalmente se volverán verdes si la implementación se realizó correctamente.

Tendrán que realizarse los mismos pasos para implementar las redes;



Si se crean varias redes, tenga en cuenta navegar a las fichas siguientes para seleccionar las redes antes de implementar



El estado pasará ahora a "IMPLEMENTADO" desde "NA" y la CLI del switch que aparece a continuación se puede utilizar para verificar las implementaciones

```
DC1-VTEP# sh nve vni
Codes: CP - Control Plane          DP - Data Plane
       UC - Unconfigured           SA - Suppress ARP
       SU - Suppress Unknown Unicast
       Xconn - Crossconnect
       MS-IR - Multisite Ingress Replication
```

```
Interface VNI      Multicast-group    State Mode Type [BD/VRF]      Flags
-----
nve1      100144            239.1.1.144        Up   CP   L2 [144]           # Network1 which is VLAN
144 mapped to VNID 100144
nve1      100145            239.1.1.145        Up   CP   L2 [145]           # Network2 Which is VLAN
145 mapped to VNID 100145
nve1      1001445           239.100.100.100    Up   CP   L3 [tenant-1]      # VRF- tenant1 which is
mapped to VNID 1001445
```

```
DC1-BGW1# sh nve vni
Codes: CP - Control Plane          DP - Data Plane
       UC - Unconfigured           SA - Suppress ARP
       SU - Suppress Unknown Unicast
       Xconn - Crossconnect
       MS-IR - Multisite Ingress Replication
```

```
Interface VNI      Multicast-group    State Mode Type [BD/VRF]      Flags
-----
nve1      100144            239.1.1.144        Up   CP   L2 [144]           MS-IR
nve1      100145            239.1.1.145        Up   CP   L2 [145]           MS-IR
nve1      1001445           239.100.100.100    Up   CP   L3 [tenant-1]
```

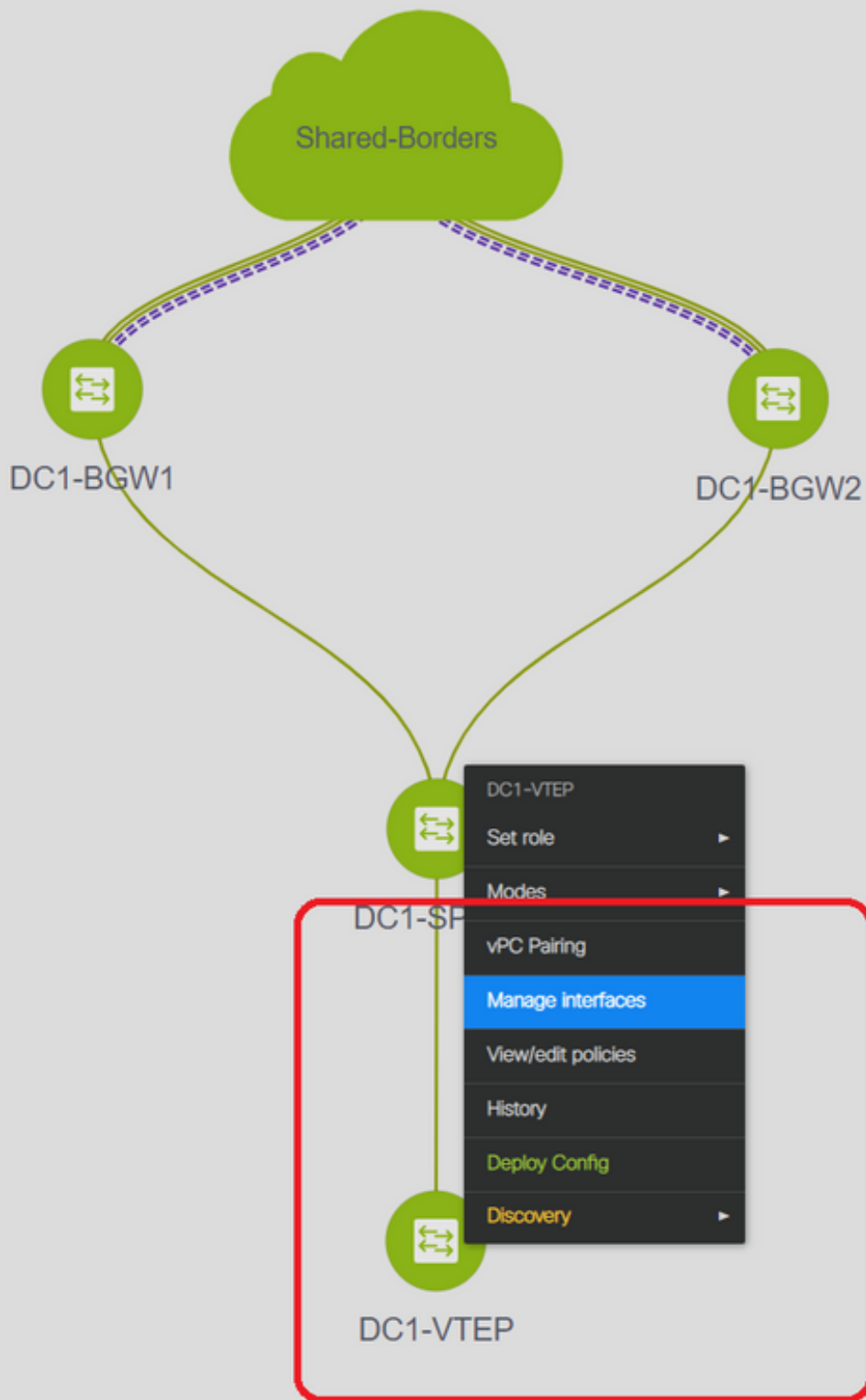
Arriba también es de BGW; en resumen, todos los switches que hemos seleccionado anteriormente en el paso se implementarán con las redes y el VRF

También se deben realizar los mismos pasos para el Fabric DC2, borde compartido. Tenga en cuenta que los bordes compartidos NO necesitan redes ni VNID de capa 2; sólo se requiere el

VRF L3.

Paso 11: Creación de puertos troncales/de acceso descendentes en switches hoja/VTEP

En esta topología, los puertos Eth1/2 y Eth1/1 de DC1-VTEP y DC2-VTEP respectivamente están conectados a los hosts; de modo que se mueven como puertos troncales en la GUI de DCNM como se muestra a continuación



Edit Configuration

Name: DC1-VTEP:Ethernet1/2

Policy: int_trunk_host_11_1

General

* Enable BPDU Guard ? Enable spanning-tree bpduguard

Enable Port Type Fast ? Enable spanning-tree edge port behavior

* MTU ? MTU for the interface

* SPEED ? Interface Speed

* Trunk Allowed Vlans ? Allowed values: 'none', 'all', or vlan ranges (ex: 1-200,500-2000,3000)

Interface Description

Freeform Config

Note ! All configs shu strictly match 'show run' c with respect to case and Any mismatches will yield unexpected diffs during o

Seleccione la interfaz relevante y cambie las "vlan permitidas" de ninguna a "todas" (o sólo las vlan que necesitan ser permitidas)

Paso 12: Se requieren formularios libres en el borde compartido

Debido a que los switches de borde compartidos son los servidores de ruta, se requiere realizar algunos cambios en términos de los vecindarios BGP I2vpn evpn

El tráfico BUM entre sitios se replica usando Unicast; Significa, cualquier tráfico BUM en Vlan 144(eg) después de que llegue en los BGW; dependiendo de qué BGW es el reenviador designado (DF), DF realizará una replicación de unidifusión en el sitio remoto; Esta replicación se logra después de que el BGW recibe una ruta de tipo 3 del BGW remoto; Aquí, los BGW están formando I2vpn evpn peering solamente con los bordes compartidos; y los bordes compartidos no deben tener ningún VNID de capa 2 (si se crea, se producirá una retención en negro del tráfico este/oeste). Dado que faltan VNID de capa 2 y que los BGWs originan el tipo de ruta 3 por VNID, los bordes compartidos no honrarán la actualización de BGP que viene de los BGWs; Para corregir esto, utilice el comando "keep route-target all" en el elevpn AF I2vpn

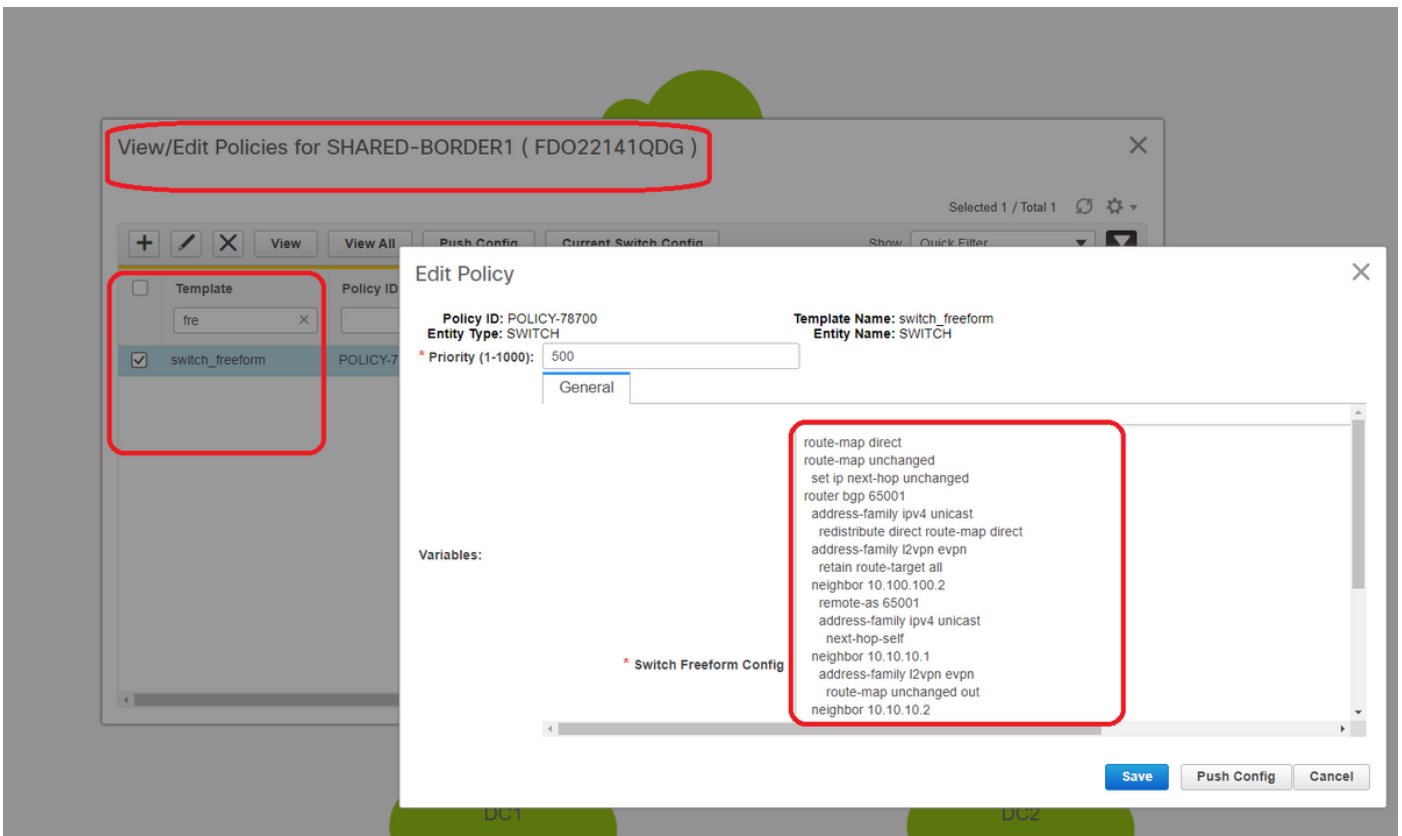
Otro punto es asegurarse de que los bordes compartidos no cambien el siguiente salto (BGP de forma predeterminada cambia el siguiente salto para los vecinos eBGP); Aquí, el túnel entre sitios para el tráfico de unidifusión del sitio 1 al 2 y viceversa debe ser de BGW al BGW (de dc1 a dc2 y viceversa); Para lograr esto, se debe crear un route-map y aplicarlo para cada vecino de EVPN I2VPN desde el borde compartido a cada BGW

Para los dos puntos anteriores, se debe utilizar una forma libre en los bordes compartidos como los siguientes

```

route-map direct
route-map unchanged
  set ip next-hop unchanged
router bgp 65001
  address-family ipv4 unicast
    redistribute direct route-map direct
  address-family l2vpn evpn
    retain route-target all
  neighbor 10.100.100.2
    remote-as 65001
  address-family ipv4 unicast
    next-hop-self
  neighbor 10.10.10.1
    address-family l2vpn evpn
    route-map unchanged out
  neighbor 10.10.10.2
    address-family l2vpn evpn
    route-map unchanged out
  neighbor 10.10.20.1
    address-family l2vpn evpn
    route-map unchanged out
  neighbor 10.10.20.2
    address-family l2vpn evpn
    route-map unchanged out

```



Paso 13: Loopback dentro de los VRF de arrendatarios en los BGW

para el tráfico Norte/Sur de los hosts conectados dentro de los switches de hoja, los BGW utilizan la IP SRC exterior de la dirección IP de Loopback1 de NVE; Los bordes compartidos sólo de forma predeterminada formarán el NVE Peering con la dirección Ip de loopback multisitio de los BGW; así, si un paquete vxlan llega al borde compartido con una dirección IP SRC externa del

Loopback BGW1, el paquete se descartará debido a la pérdida SRCTEP; Para evitar esto, se debe crear un loopback en el arrendatario-VRF en cada switch BGW y luego anunciar al BGP para que los bordes compartidos reciban esta actualización y luego formen el Peering NVE con la dirección IP de Loopback1 BGW ;

Inicialmente, el Peering de NVE será similar al de abajo en los bordes compartidos

```
SHARED-BORDER1# sh nve pee
```

Interface	Peer-IP	State	LearnType	Uptime	Router-Mac	
nve1	10.222.222.1	Up	CP	01:20:09	0200.0ade.de01	#
Multisite Loopback 100 IP address of DC1-BGWs						
nve1	10.222.222.2	Up	CP	01:17:43	0200.0ade.de02	#
Multisite Loopback 100 IP address of DC2-BGWs						



Como se muestra arriba, el loopback2 se crea a partir de DCNM y se configura en el VRF del arrendatario 1 y se le da la etiqueta 12345 ya que ésta es la etiqueta que el route-map utiliza para hacer coincidir el loopback mientras hace el anuncio.

```
DC1-BGW1# sh run vrf tenant-1

!Command: show running-config vrf tenant-1
!Running configuration last done at: Tue Dec 10 17:21:29 2019
!Time: Tue Dec 10 17:24:53 2019

version 9.3(2) Bios:version 07.66

interface Vlan1445
 vrf member tenant-1

interface loopback2
 vrf member tenant-1
 vrf context tenant-1
 vni 1001445
 ip pim rp-address 10.49.3.100 group-list 224.0.0.0/4
 ip pim ssm range 232.0.0.0/8
 rd auto
 address-family ipv4 unicast
```



```

route-target both auto
route-target both auto mvpn
route-target both auto evpn
address-family ipv6 unicast
route-target both auto
route-target both auto evpn
router bgp 65000
vrf tenant-1
address-family ipv4 unicast
advertise l2vpn evpn
redistribute direct route-map fabric-rmap-redis-subnet
maximum-paths ibgp 2
address-family ipv6 unicast
advertise l2vpn evpn
redistribute direct route-map fabric-rmap-redis-subnet
maximum-paths ibgp 2

```

```

DC1-BGW1# sh route-map fabric-rmap-redis-subnet
route-map fabric-rmap-redis-subnet, permit, sequence 10
Match clauses:
tag: 12345
Set clauses:

```

Después de este paso, los pares NVE mostrarán para todas las direcciones Ip Loopback1 junto con la dirección IP de loopback multisitio.

```

SHARED-BORDER1# sh nve pee
Interface Peer-IP                               State LearnType Uptime   Router-Mac
-----
nve1      192.168.20.1                                   Up      CP        00:00:01 b08b.cfdc.2fd7
nve1      10.222.222.1                                   Up      CP        01:27:44 0200.0ade.de01
nve1      192.168.10.2                                   Up      CP        00:01:00 e00e.daa2.f7d9
nve1      10.222.222.2                                   Up      CP        01:25:19 0200.0ade.de02
nve1      192.168.10.3                                   Up      CP        00:01:43 6cb2.aeee.0187
nve1      192.168.20.3                                   Up      CP        00:00:28 005d.7307.8767

```

En esta etapa, el tráfico Este/Oeste debe reenviarse correctamente

Paso 14: Extensiones VRFLITE de los bordes compartidos a los routers externos

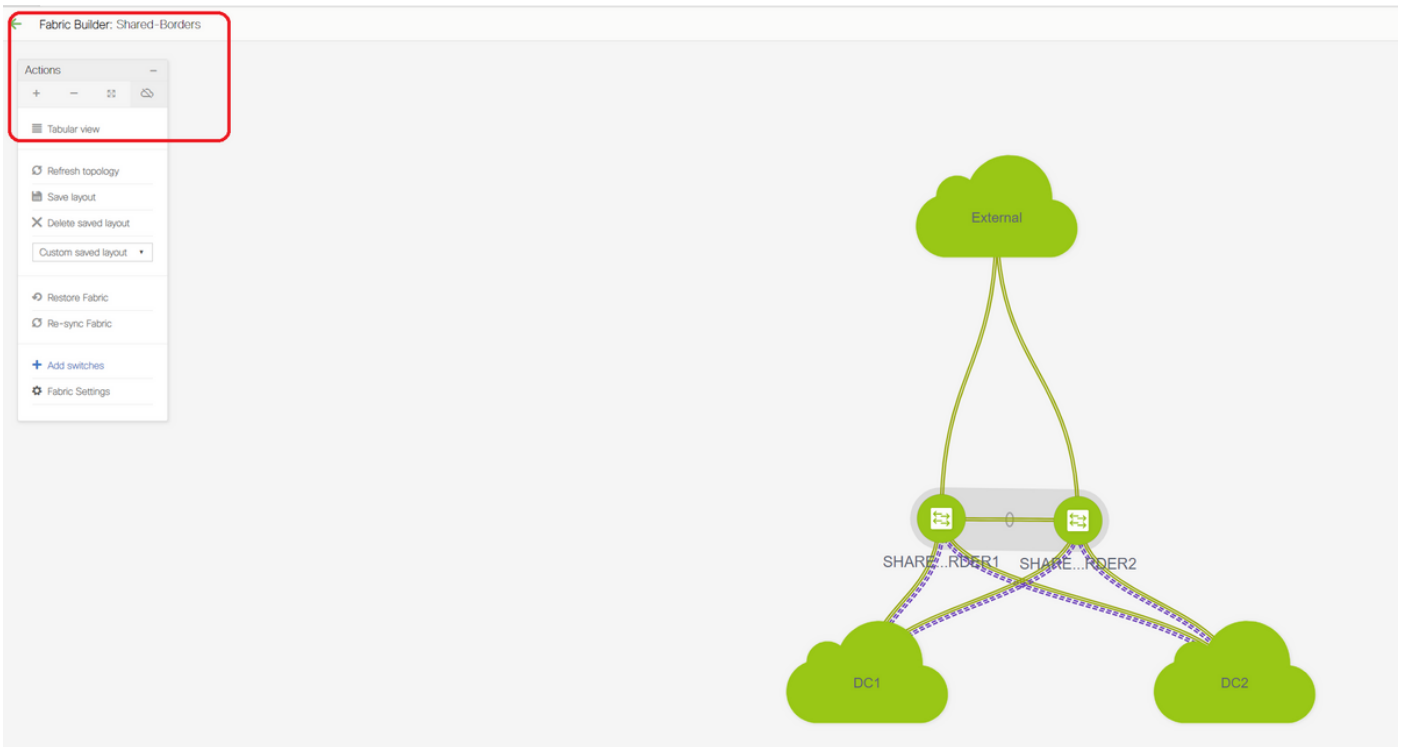
Habrá situaciones en las que los hosts fuera del fabric tendrán que comunicarse con los hosts dentro del fabric. En este ejemplo, las fronteras compartidas permiten lo mismo;

Cualquier host que viva en DC1 o DC2 podrá comunicarse con hosts externos a través de los switches de borde compartidos.

Para ello, los bordes compartidos terminan el VRF Lite; Aquí en este ejemplo, eBGP se ejecuta desde los bordes compartidos a los routers externos como se muestra en el diagrama al principio.



Para configurar esto desde DCNM, es necesario **agregar adjuntos de extensión vrf**. A continuación se indican las medidas que se han de adoptar para lograr lo mismo.

a) Adición de links entre estructuras desde fronteras compartidas a routers externos



Seleccione el ámbito del Fabric Builder para "borde compartido" y cambie a la vista tabular

The screenshot shows the 'Fabric Builder: Shared-Borders' interface with the 'Links' tab selected. The 'Links' tab is highlighted with a red box. Below the tabs, there is a toolbar with icons for adding, refreshing, editing, and deleting links, along with a 'View/Edit Fabric' button. A table below the toolbar lists the links:

	<input type="checkbox"/>	Name
1	<input type="checkbox"/>	 SHARED-BORDER2
2	<input type="checkbox"/>	 SHARED-BORDER1

Seleccione los enlaces y agregue un enlace "Inter-Fabric" como se muestra a continuación

Link Management - Edit Link



* Link Type	Inter-Fabric
* Link Sub-Type	VRF_LITE
* Link Template	ext_fabric_setup_11_1
* Source Fabric	Shared-Borders
* Destination Fabric	External
* Source Device	SHARED-BORDER2
* Source Interface	Ethernet1/49
* Destination Device	EXT_RTR
* Destination Interface	Ethernet1/50

Link Profile

General	
Advanced	

* BGP Local ASN	65001	? Local BGP Autonomous System Number
* IP Address/Mask	172.16.222.1/24	? IP address for sub-interface in each VRF
* BGP Neighbor IP	172.16.222.2	? Neighbor IP address in each VRF
* BGP Neighbor ASN	65100	? Neighbor BGP Autonomous System Number

Save

Se debe seleccionar un subtipo VRF LITE en el menú desplegable

El fabric de origen son bordes compartidos y el fabric de destino es externo, ya que será un VRF LITE de SB a externo

Seleccione las interfaces relevantes que van hacia el router externo

Proporcione la dirección IP y la máscara y la dirección IP vecina

ASN se rellenará automáticamente.

Una vez hecho esto, haga clic en el botón Save (Guardar)

Realice lo mismo para los bordes compartidos y para todas las conexiones de capa 3 externas que se encuentran en VRFLITE

b) Adición de extensiones VRF

Vaya a la sección VRF de borde compartido

El VRF estará en estado de implementación; Seleccione la casilla de verificación de la derecha para que se puedan seleccionar varios switches

Seleccione los bordes compartidos y se abrirá la ventana "Conexión VRF EXTension".

En "extender", cambie de "Ninguno" a "VRFLITE"

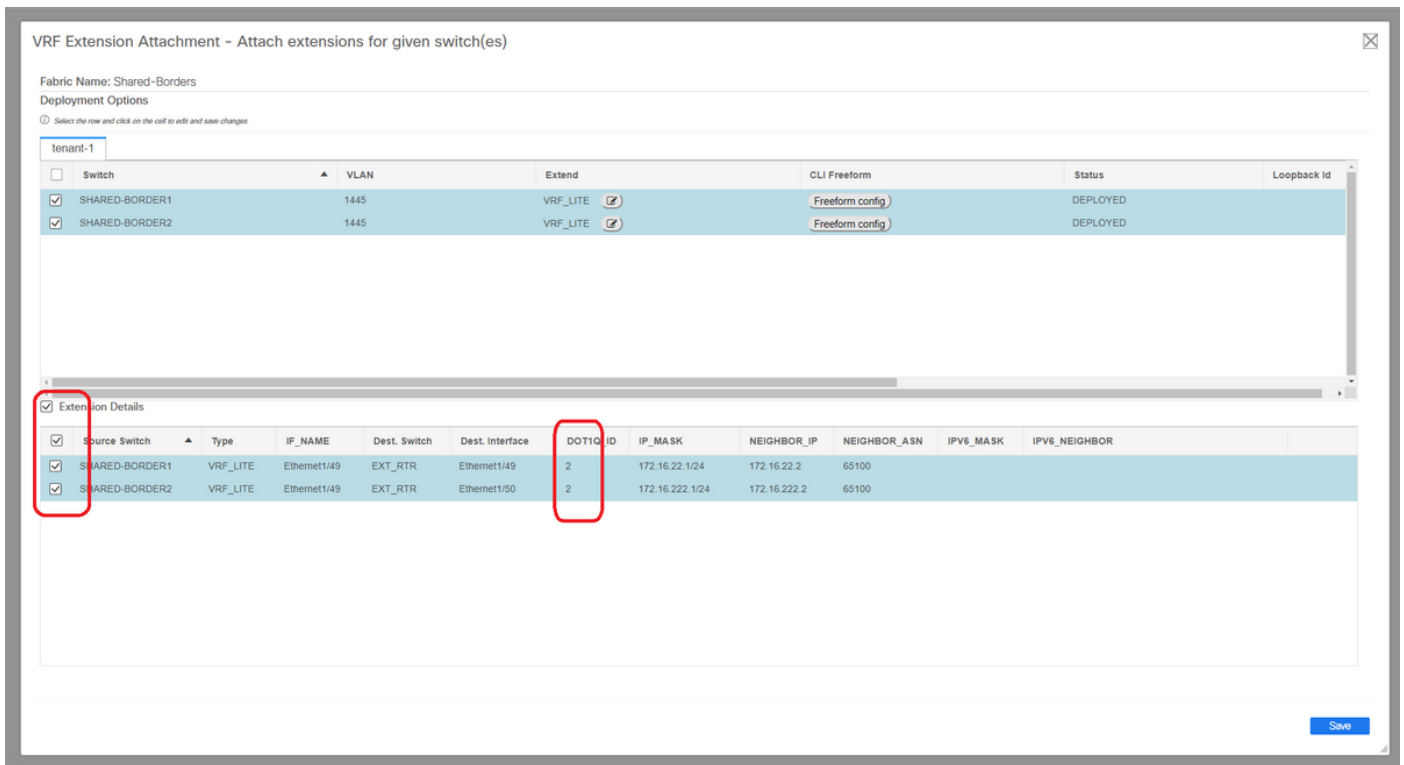
Haga lo mismo para ambos bordes compartidos

Una vez hecho esto, "Detalles de la extensión" completará las interfaces LITE VRF que se dieron previamente en el paso a) anterior.

The screenshot shows the Data Center Network Manager interface. At the top, the 'SCOPE' is set to 'Shared-Borders'. Below, a table lists VRFs, with 'Shared-1' selected. The main area displays a network diagram with an 'External' cloud and two switches, 'SHARE...RDER1' and 'SHARE...RDER2', which are highlighted with a red box. A modal window titled 'VRF Extension Attachment - Attach extensions for given switch(es)' is open, showing configuration options for 'tenant-1'. The 'Extend' column is set to 'VRF_LITE' for both switches, and the 'Extension Details' table shows the corresponding interface configurations.

Switch	VLAN	Extend	CLI Freeform	Status	Loop
<input checked="" type="checkbox"/> SHARED-BORDER1	1445	VRF_LITE <input checked="" type="checkbox"/>	Freeform config	DEPLOYED	
<input checked="" type="checkbox"/> SHARED-BORDER2	1445	VRF_LITE <input checked="" type="checkbox"/>	Freeform config	DEPLOYED	

Source Switch	Type	IF_NAME	Dest. Switch	Dest. Interface
<input type="checkbox"/> SHARED-BORDER1	VRF_LITE	Ethernet1/49	EXT_RTR	Ethernet1/49
<input type="checkbox"/> SHARED-BORDER2	VRF_LITE	Ethernet1/50	EXT_RTR	Ethernet1/50



DOT1Q ID se rellena automáticamente en 2

Otros campos también se rellenan automáticamente

Si la vecindad de IPv6 debe establecerse a través de VRFLITE, el paso a) debe hacerse para IPv6

Ahora haga clic en Save (Guardar)

Por último, realice la implementación en la parte superior derecha de la página web.

Una implementación exitosa dará como resultado que las configuraciones se trasladen a los bordes compartidos, lo que incluye establecer direcciones IP en esas subinterfaces y establecer Vecindades BGP IPv4 con los routers externos

Tenga en cuenta que las configuraciones de router externo (configuración de direcciones IP en subinterfaces y sentencias de Vecindad BGP) se realizan manualmente por CLI en este caso.

Las verificaciones de CLI se pueden realizar mediante los siguientes comandos en ambos bordes compartidos;

```
SHARED-BORDER1# sh ip bgp sum vr tenant-1
```

```
BGP summary information for VRF tenant-1, address family IPv4 Unicast
BGP router identifier 172.16.22.1, local AS number 65001
BGP table version is 18, IPv4 Unicast config peers 1, capable peers 1
9 network entries and 11 paths using 1320 bytes of memory
BGP attribute entries [9/1476], BGP AS path entries [3/18]
BGP community entries [0/0], BGP clusterlist entries [0/0]
```

```
Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
172.16.22.2   4 65100    20     20     18    0    0 00:07:59 1
```

```
SHARED-BORDER2# sh ip bgp sum vr tenant-1
```

BGP summary information for VRF tenant-1, address family IPv4 Unicast
BGP router identifier 172.16.222.1, local AS number 65001
BGP table version is 20, IPv4 Unicast config peers 1, capable peers 1
9 network entries and 11 paths using 1320 bytes of memory
BGP attribute entries [9/1476], BGP AS path entries [3/18]
BGP community entries [0/0], BGP clusterlist entries [0/0]

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
172.16.222.2	4	65100	21	21	20	0	0	00:08:02	1

Con todas las configuraciones anteriores, también se establecerá la disponibilidad Norte/Sur como se muestra a continuación(pings del router externo a los hosts en el fabric)

EXT_RTR# ping 172.16.144.1 **# 172.16.144.1 is Host in DC1 Fabric**

PING 172.16.144.1 (172.16.144.1): 56 data bytes
64 bytes from 172.16.144.1: icmp_seq=0 ttl=251 time=0.95 ms
64 bytes from 172.16.144.1: icmp_seq=1 ttl=251 time=0.605 ms
64 bytes from 172.16.144.1: icmp_seq=2 ttl=251 time=0.598 ms
64 bytes from 172.16.144.1: icmp_seq=3 ttl=251 time=0.568 ms
64 bytes from 172.16.144.1: icmp_seq=4 ttl=251 time=0.66 ms
^[[A^[[A

--- 172.16.144.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.568/0.676/0.95 ms

EXT_RTR# ping 172.16.144.2 **# 172.16.144.2 is Host in DC2 Fabric**

PING 172.16.144.2 (172.16.144.2): 56 data bytes
64 bytes from 172.16.144.2: icmp_seq=0 ttl=251 time=1.043 ms
64 bytes from 172.16.144.2: icmp_seq=1 ttl=251 time=6.125 ms
64 bytes from 172.16.144.2: icmp_seq=2 ttl=251 time=0.716 ms
64 bytes from 172.16.144.2: icmp_seq=3 ttl=251 time=3.45 ms
64 bytes from 172.16.144.2: icmp_seq=4 ttl=251 time=1.785 ms

--- 172.16.144.2 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.716/2.623/6.125 ms

Los traceroutes también apuntan a los dispositivos correctos en la trayectoria del paquete

EXT_RTR# traceroute 172.16.144.1

traceroute to 172.16.144.1 (172.16.144.1), 30 hops max, 40 byte packets

```
 1 SHARED-BORDER1 (172.16.22.1) 0.914 ms 0.805 ms 0.685 ms
 2 DC1-BGW2 (172.17.10.2) 1.155 ms DC1-BGW1 (172.17.10.1) 1.06 ms 0.9 ms
 3 ANYCAST-VLAN144-IP (172.16.144.254) (AS 65000) 0.874 ms 0.712 ms 0.776 ms
 4 DC1-HOST (172.16.144.1) (AS 65000) 0.605 ms 0.578 ms 0.468 ms
```

EXT_RTR# traceroute 172.16.144.2 traceroute to 172.16.144.2 (172.16.144.2), 30 hops max, 40 byte packets
1 SHARED-BORDER2 (172.16.222.1) 1.137 ms 0.68 ms 0.66 ms
2 DC2-BGW2 (172.17.20.2) 1.196 ms
DC2-BGW1 (172.17.20.1) 1.193 ms 0.903 ms
3 ANYCAST-VLAN144-IP (172.16.144.254) (AS 65000) 1.186 ms 0.988 ms 0.966 ms
4 172.16.144.2 (172.16.144.2) (AS 65000) 0.774 ms 0.563 ms 0.583 ms

EXT_RTR#