

Erstellen einer Nexus 9000-VXLAN-Bereitstellung für gemeinsam genutzte Border Multisite mit DCNM

Inhalt

[Einführung](#)

[Topologie](#)

[Details zur Topologie](#)

[Verwendete Komponenten:](#)

[High Level Steps](#)

[Schritt 1: Erstellung von Easy Fabric für DC1](#)

[Schritt 2: Hinzufügen von Switches zur DC1-Fabric](#)

[Schritt 3: Konfiguration von Netzwerken/VRFs](#)

[Schritt 4: Wiederholen Sie die gleichen Schritte für DC2.](#)

[Schritt 5: Erstellung einer einfachen Struktur für gemeinsame Grenzen](#)

[Schritt 6: Erstellung von MSD und Verschieben von RZ1- und RZ2-Fabrics](#)

[Schritt 7: Erstellung externer Fabric](#)

[Schritt 8: eBGP-Underlay für Loopback-Erreichbarkeit zwischen BGWs \(auch iBGP zwischen gemeinsamen Grenzen\)](#)

[Schritt 9: Erstellung von Multisite-Overlays von BGWs zu gemeinsamen Grenzen](#)

[Schritt 10: Bereitstellung von Netzwerken/VRFs an beiden Standorten](#)

[Schritt 11: Erstellen von Downstream-Trunk-/Access-Ports auf Leaf-Switches/VTEP](#)

[Schritt 12: Für die gemeinsame Grenze erforderliche Freiheiten](#)

[Schritt 13: Loopback innerhalb von Tenant-VRFs auf BGWs](#)

[Schritt 14: VRFLITE-Erweiterungen von gemeinsamen Grenzen zu externen Routern](#)

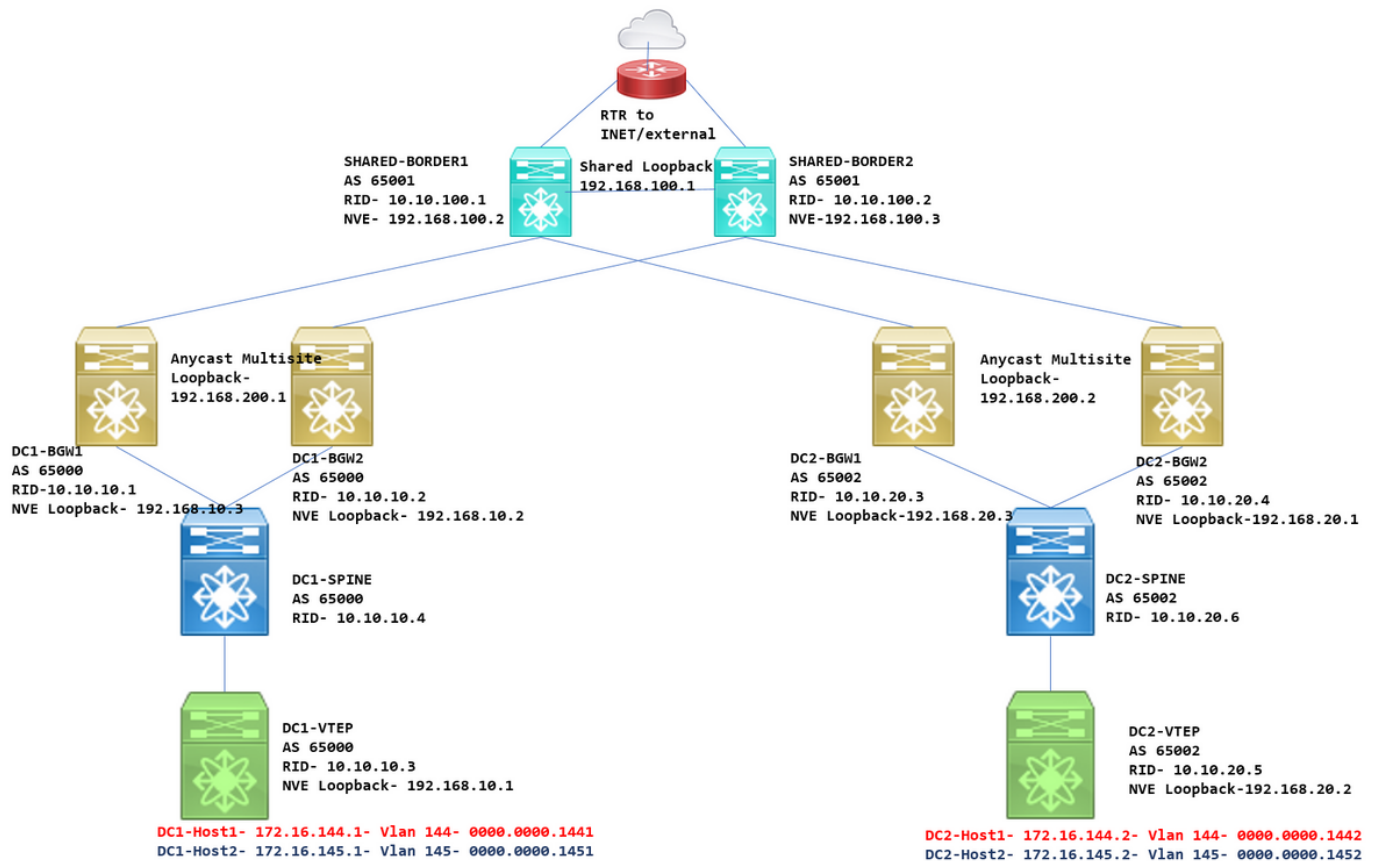
[a\) Hinzufügen von Fabric-übergreifenden Verbindungen zu externen Routern](#)

[b\) Hinzufügen von VRF-Erweiterungen](#)

Einführung

In diesem Dokument wird erläutert, wie eine Bereitstellung einer Cisco Nexus 9000 VXLAN Multisite-Bereitstellung mithilfe eines gemeinsamen Grenzmodells mit DCNM 11.2-Version bereitgestellt wird.

Topologie



Details zur Topologie

DC1 und DC2 sind zwei Rechenzentrumsstandorte, in denen VXLAN ausgeführt wird.

Border Gateways DC1 und DC2 verfügen über physische Verbindungen zu den gemeinsamen Grenzen.

Über gemeinsame Grenzen verfügen Sie über eine externe Verbindung (z. B. Internet); So werden die VRF-Lite-Verbindungen an gemeinsamen Grenzen terminiert, und an jedem Standort wird eine Standardroute über die gemeinsamen Grenzen zu Border Gateways eingespeist.

Gemeinsam genutzte Grenzen werden in vPC konfiguriert (dies ist erforderlich, wenn die Fabric mit DCNM bereitgestellt wird)

Border Gateways werden im Anycast-Modus konfiguriert.

Verwendete Komponenten:

Nexus 900 mit 9.3(2)

DCNM mit 11.2-Version

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

High Level Steps

- 1) Da dieses Dokument auf zwei Rechenzentren basiert, die eine VXLAN-Funktion für mehrere Standorte verwenden, müssen zwei Easy Fabrics erstellt werden.
- 2) Erstellen einer weiteren einfachen Fabric für die gemeinsame Grenze
- 3) MSD erstellen und RZ1 und RZ2 verschieben
- 4) Erstellen einer externen Fabric
- 5) Erstellen Sie Multisite Underlay und Overlay (für Ost/West).
- 6) Erstellen von VRF-Erweiterungsanhängen an gemeinsamen Grenzen

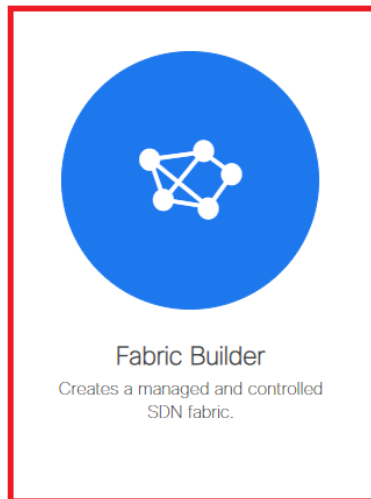
Schritt 1: Erstellung von Easy Fabric für DC1

- Melden Sie sich beim DCNM an, und wählen Sie im Dashboard die Option "Fabric Builder" aus.



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.

- Option "Create Fabric" auswählen



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

- Als Nächstes werden der Fabric-Name, die Vorlage und anschließend mehrere Registerkarten geöffnet, für die Details wie ASN, Fabric Interface Numbering (Nummerierung der Fabric-Schnittstellen) und Any Cast Gateway MAC (AGM) erforderlich sind.

Add Fabric

* Fabric Name : DC1

* Fabric Template : Easy_Fabric_11_1

General

Replication

vPC

Advanced

Resources

Manageability

Bootstrap

Configuration Backup

* BGP ASN 65000 ? 1-4294967295 | 1-65535[0-65535]

* Fabric Interface Numbering unnumbered ? Numbered(Point-to-Point) or Unnumbered

* Underlay Subnet IP Mask 30 ? Mask for Underlay Subnet IP Range

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

* Route-Reflectors 2 ? Number of spines acting as Route-Reflectors

* Anycast Gateway MAC 2020.2020.aaaa ? 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

Fabric-Schnittstellen (die Spine-/Leaf-Schnittstellen sind) können "unnummeriert" oder Punkt-zu-Punkt sein. Wenn nicht nummeriert wird, sind weniger IP-Adressen erforderlich (da die IP-Adresse die des nicht nummerierten Loopbacks ist).

Die AGM wird von den Hosts in der Fabric als MAC-Adresse des Standard-Gateways

verwendet. Dies ist für alle Leaf-Switches identisch, die die Standard-Gateways sind.

- Als Nächstes wird der Replikationsmodus festgelegt.

Add Fabric

* Fabric Name :

* Fabric Template :

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

* Replication Mode ? *Replication Mode for BUM Traffic*

* Multicast Group Subnet ? *Multicast address with prefix 16 to 30*

Enable Tenant Routed Multicast (TRM) ? *For Overlay Multicast Support In VXLAN Fabrics*

Default MDT Address for TRM VRFs ? *IPv4 Multicast Address*

* Rendezvous-Points ? *Number of spines acting as Rendezvous-Point (RP)*

* RP Mode ? *Multicast RP Mode*

* Underlay RP Loopback Id ? *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*

Der hier ausgewählte Replikationsmodus kann entweder Multicast- oder IR-Ingress-Replikation sein. IR repliziert jeden eingehenden BUM-Datenverkehr innerhalb eines VXLAN-VLAN unicast auf andere VTEPs, die auch als Head-End-Replikation bezeichnet werden. Der Multicast-Modus sendet den BUM-Datenverkehr mit einer äußeren Ziel-IP-Adresse, die der für jedes Netzwerk definierten Multicast-Gruppe entspricht, bis hin zum Spine, und Spines führt die Multicast-Replikation basierend auf der OIL-Adresse des äußeren VTEP durch. s

Multicast Group Subnet-> Erforderlich zur Replikation des BUM-Datenverkehrs (z. B. ARP-Anfrage von einem Host)

Wenn TRM aktiviert werden muss, aktivieren Sie das Kontrollkästchen neben derselben, und geben Sie die MDT-Adresse für die TRM-VRFs an.

- Die Registerkarte "vPC" bleibt standardmäßig leer. Falls Änderungen für das Backup-SVI/VLAN erforderlich sind, können diese hier definiert werden.
- Die Registerkarte Erweitert ist der nächste Abschnitt.

Add Fabric

* Fabric Name : DC1

* Fabric Template : Easy_Fabric_11_1

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

Die hier erwähnte Standort-ID wird automatisch in diese DCNM-Version übernommen, die von der ASN abgeleitet ist, die unter der Registerkarte "Allgemein" definiert ist.

Füllen/Ändern anderer relevanter Felder

- Die Registerkarte "Ressourcen" ist der nächste Bereich, der das IP-Adressierungsschema für Loopbacks, Underlays benötigt.

Add Fabric

* Fabric Name :

* Fabric Template :

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

VXLAN VNI-Bereich für Layer 2 -> Dies sind die VNIDs, die später VLANs zugeordnet werden (wird weiter unten angezeigt)

VXLAN-VNI-Bereich für Layer 3 -> Dies sind die Layer-3-VNIDs, die später auch dem VNI-VLAN für Layer 3 dem VN-Segment zugeordnet werden.

- Hier werden keine anderen Registerkarten angezeigt. Füllen Sie jedoch bei Bedarf die anderen Registerkarten aus.

Add Fabric ×

* Fabric Name :

* Fabric Template :

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. \(00:00 to 23:59\)](#)

- Nach dem Speichern zeigt die Fabric Builder-Seite den Fabric(From DCNM-> Control-> Fabric Builder an.

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, Administration, 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)' which contains a single fabric entry named 'DC1'. The entry details are: Type: Switch Fabric, ASN: 65000, Replication Mode: Multicast, and Technology: VXLAN Fabric. There are gear and close icons to the right of the entry name.

Dieser Abschnitt enthält die vollständige Liste der Fabrics, ASN und Replikationsmodi für die einzelnen Fabrics.

- Der nächste Schritt ist das Hinzufügen von Switches zur DC1-Fabric.

Schritt 2: Hinzufügen von Switches zur DC1-Fabric

Klicken Sie im obigen Diagramm auf DC1, um Switches hinzuzufügen.

The screenshot shows the 'Fabric Builder: DC1' interface. On the left is a blue navigation sidebar with the following items: Dashboard, Topology, Control, Monitor, Administration, and Applications. On the right, the 'Actions' menu is open, listing several options: Tabular view, Refresh topology, Save layout, Delete saved layout, a 'Random' dropdown menu, Restore Fabric, Re-sync Fabric, Add switches (highlighted with a red rounded rectangle), and Fabric Settings.

- Geben Sie die IP-Adressen und Anmeldeinformationen der Switches an, die in die DC1-Fabric importiert werden müssen(nach Topologie, die am Anfang dieses Dokuments aufgeführt ist, gehören DC1-VTEP, DC1-SPINE, DC1-BGW1 und DC1-BGW2 zu 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)

Da es sich um eine Greenfield-Bereitstellung handelt, beachten Sie, dass die Option "Keep Config" als "NO" ausgewählt ist. die alle Konfigurationen der Felder während des Importvorgangs löschen und die Switches neu laden.

Wählen Sie die "Start Discovery" aus, damit DCNM beginnt, die Switches anhand der IP-Adressen in der Spalte "Seed IP" zu ermitteln.

- Sobald der DCNM die Switches erkennt, werden die IP-Adressen und die Hostnamen in der Bestandsverwaltung aufgeführt.

Inventory Management

Discover Existing Switches | PowerOn Auto Provisioning (POAP)

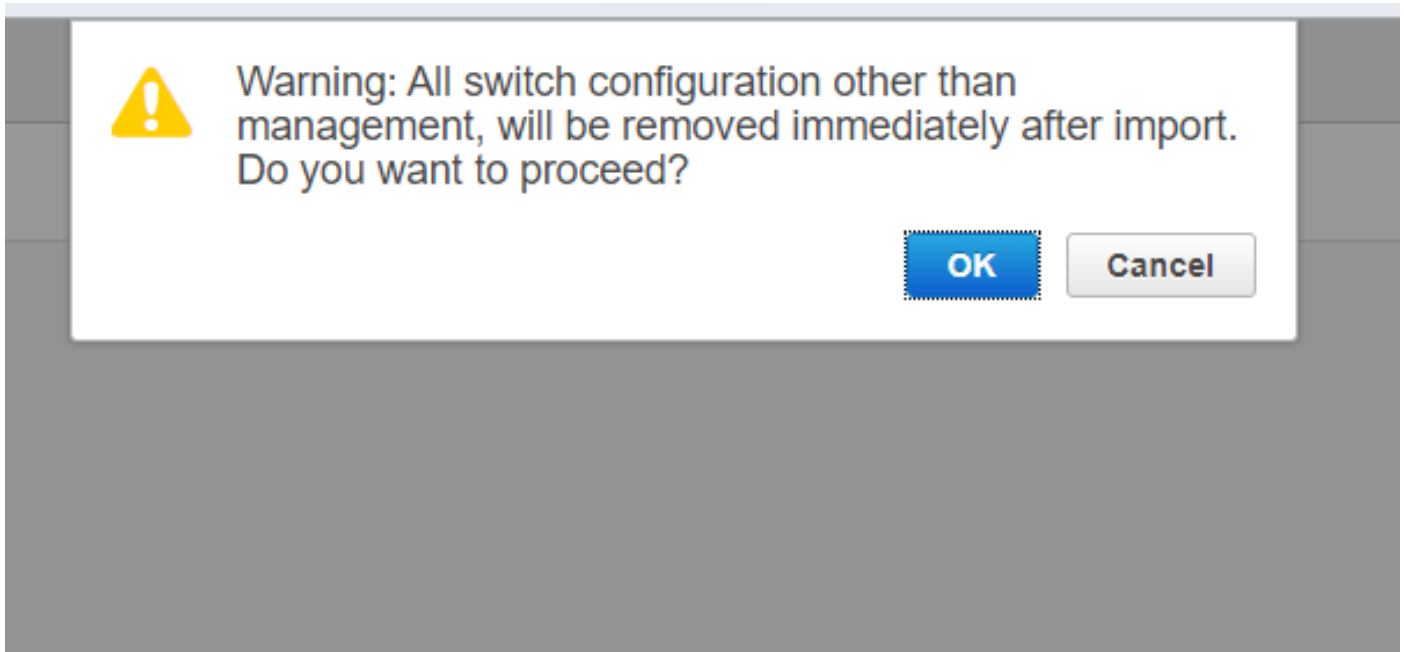
Discovery Information > Scan Details >

← 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	

Wählen Sie die entsprechenden Switches aus und klicken Sie dann auf "Importieren in 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

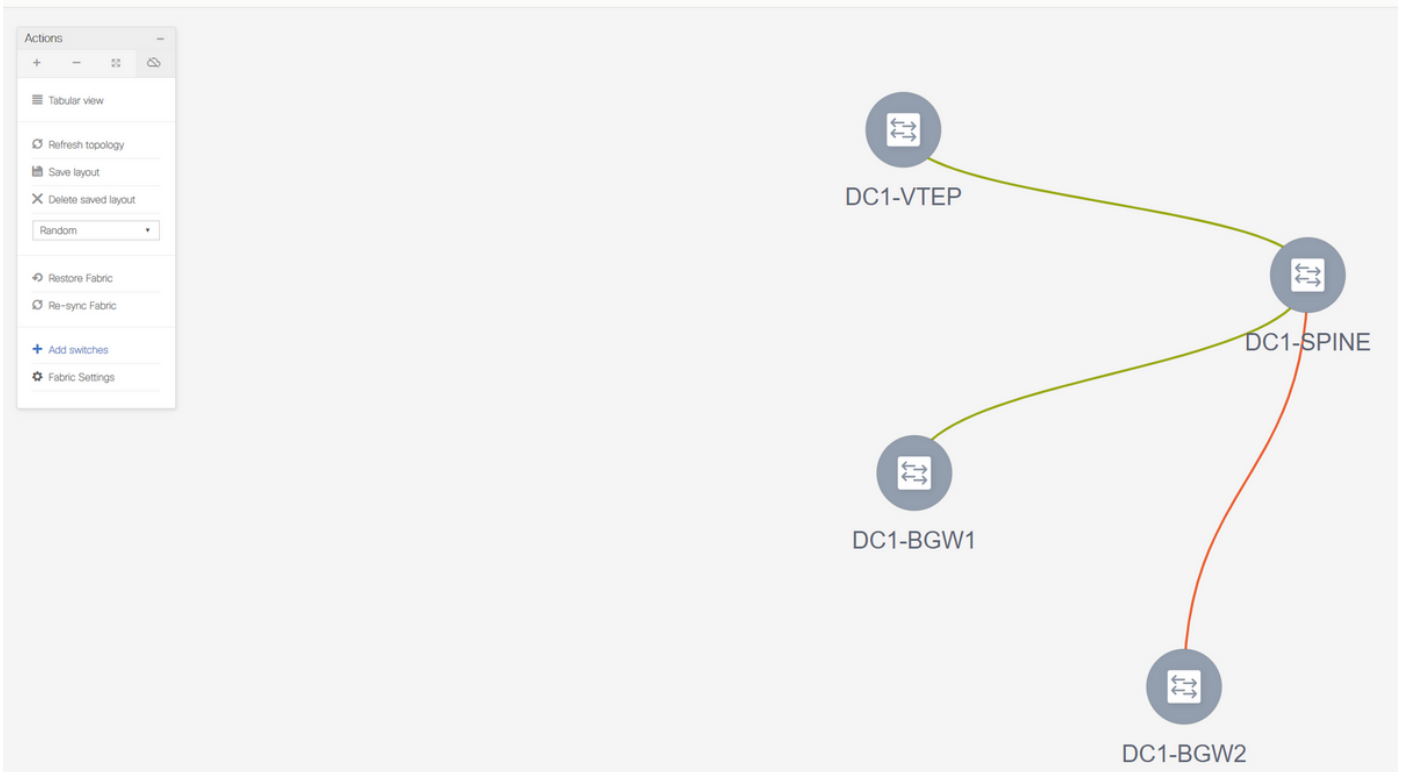
Show

Quick Filter

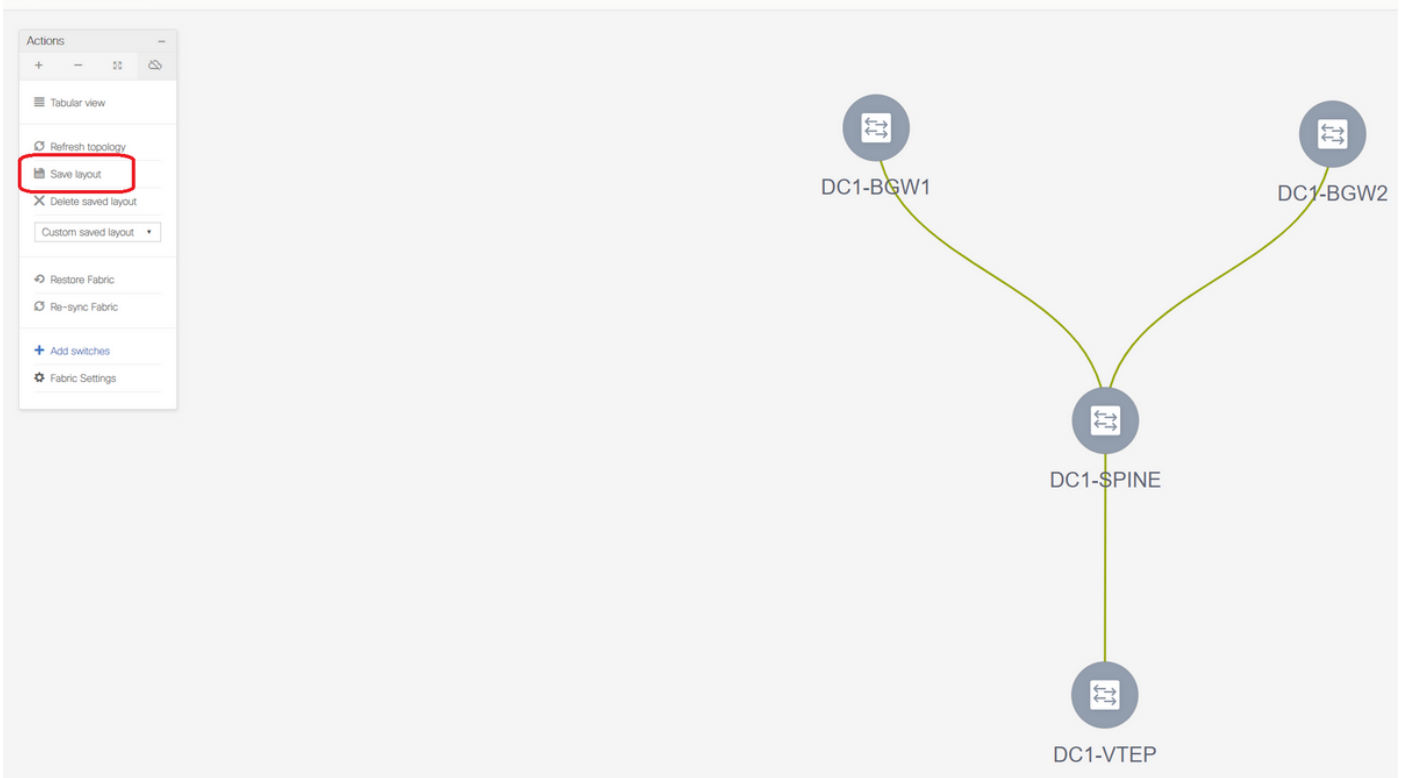


<input type="checkbox"/>	Name	IP Address	Model	Version	Status	Progress
<input type="checkbox"/>	DC1 <input type="text" value="x"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input checked="" type="checkbox"/>	DC1-SPINE	10.122.165.200	N9K-C933...	9.3(1)	manageable	<div style="width: 70%;"><div style="background-color: #76b82a; height: 10px;"></div></div> 70%
<input checked="" type="checkbox"/>	DC1-BGW1	10.122.165.187	N9K-C931...	9.3(1)	manageable	<div style="width: 70%;"><div style="background-color: #76b82a; height: 10px;"></div></div> 70%
<input checked="" type="checkbox"/>	DC1-BGW2	10.122.165.154	N9K-C931...	9.3(1)	manageable	<div style="width: 70%;"><div style="background-color: #76b82a; height: 10px;"></div></div> 70%
<input type="checkbox"/>	DC1-N3K	10.122.165.195	N3K-C317...	7.0(3)4(6)	manageable	<div style="width: 0%;"><div style="background-color: #76b82a; height: 10px;"></div></div>
<input checked="" type="checkbox"/>	DC1-VTEP	10.122.165.173	N9K-C9332C	9.3(1)	manageable	<div style="width: 70%;"><div style="background-color: #76b82a; height: 10px;"></div></div> 70%

Sobald der Import abgeschlossen ist, kann die Topologie unter Fabric Builder wie folgt aussehen:

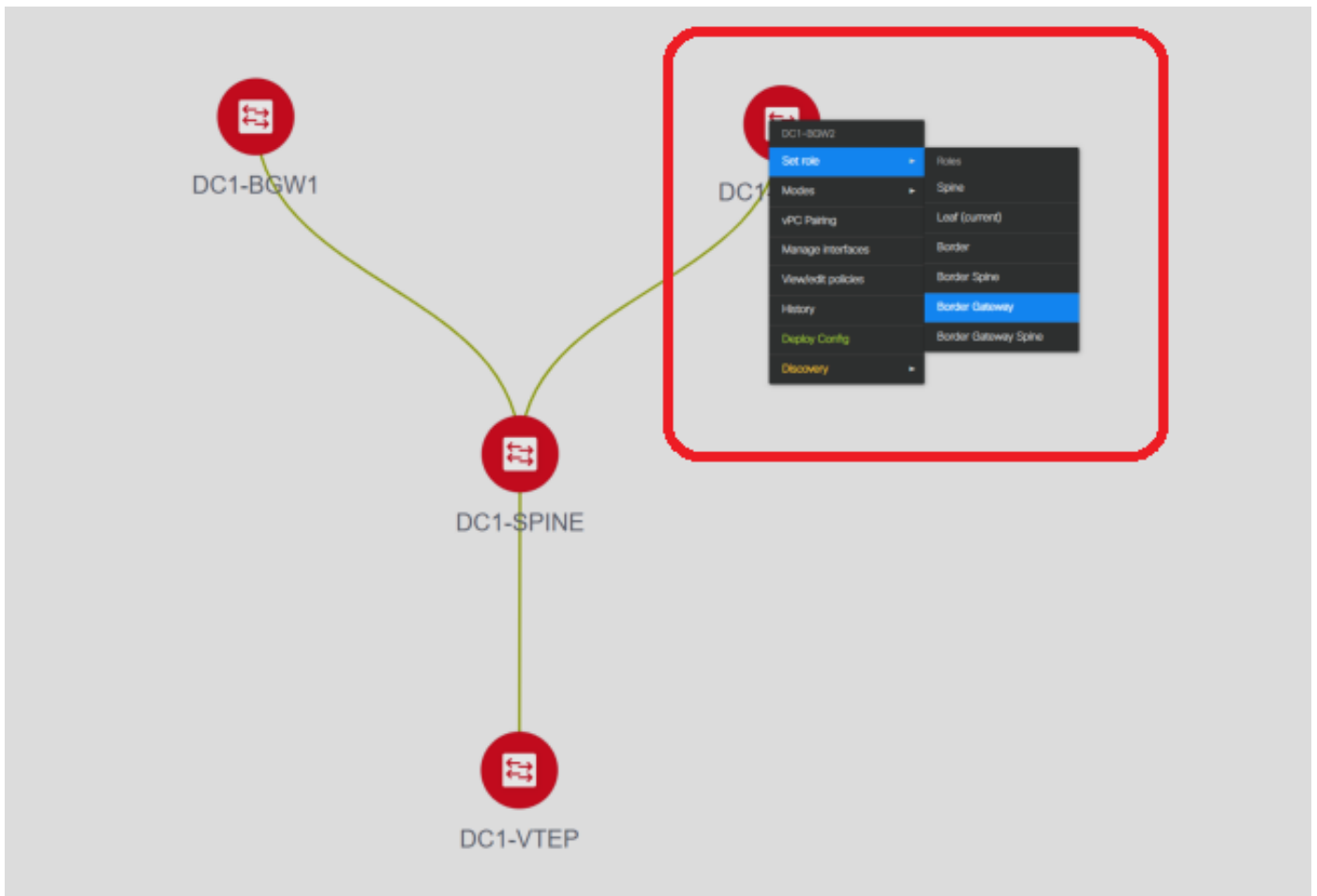


Die Switches können durch Klicken auf einen Switch verschoben werden, um ihn am richtigen Ort im Diagramm auszurichten.



Wählen Sie nach dem Umordnen der Switches in der Reihenfolge, in der das Layout benötigt wird, den Abschnitt "Layout speichern" aus.

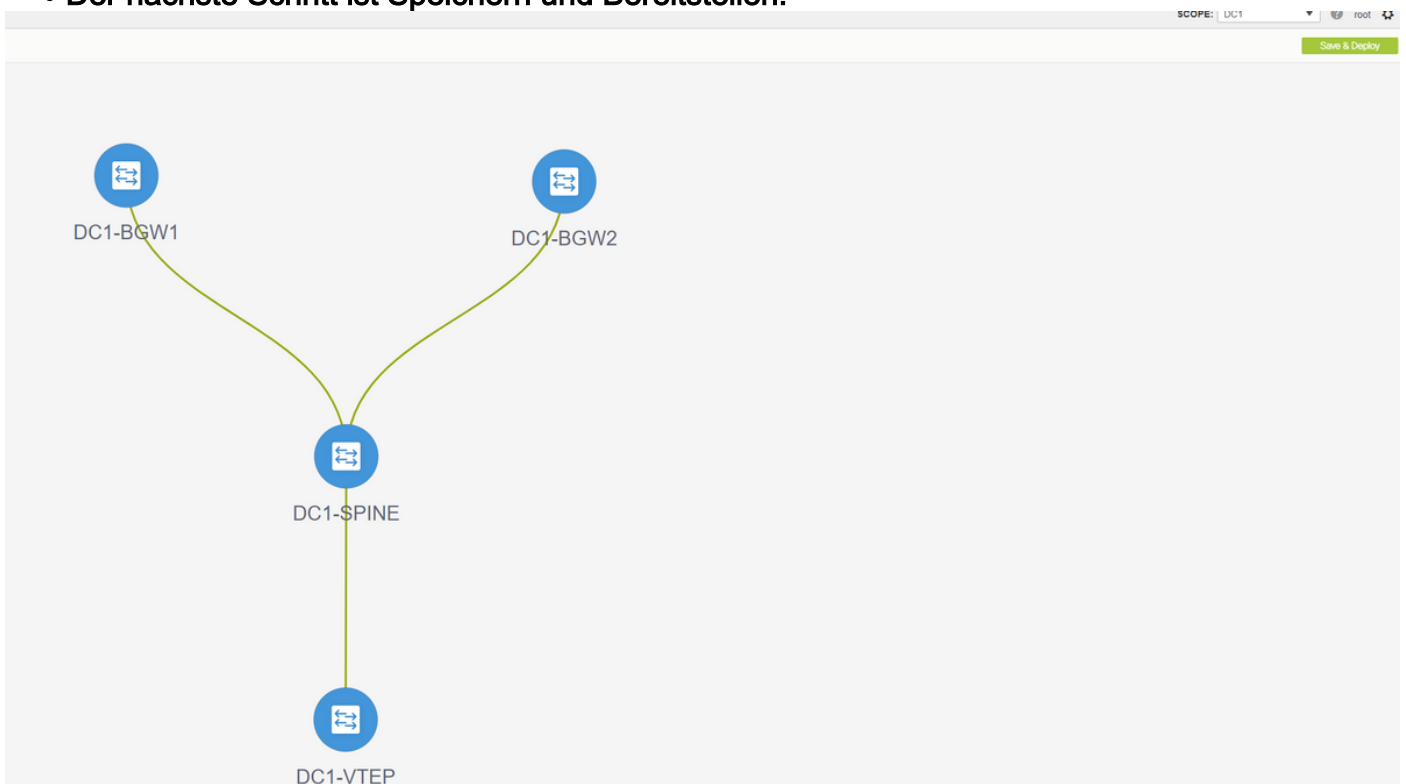
- Festlegen von Rollen für alle Switches



Klicken Sie mit der rechten Maustaste auf die einzelnen Switches, und legen Sie die richtige Rolle fest. Hier sind DC1-BGW1 und DC1-BGW2 die Grenz-Gateways.

DC1-SPINE-> wird auf role- spine, DC1-VTEP-> wird auf role-Leaf festgelegt.

- Der nächste Schritt ist Speichern und Bereitstellen.



DCNM listet jetzt die Switches auf und zeigt auch die Konfigurationen an, die DCNM an alle Switches übertragen wird.

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

Sobald der Status erfolgreich ist, wird er angezeigt, und die Switches werden grün angezeigt.

Config Deployment

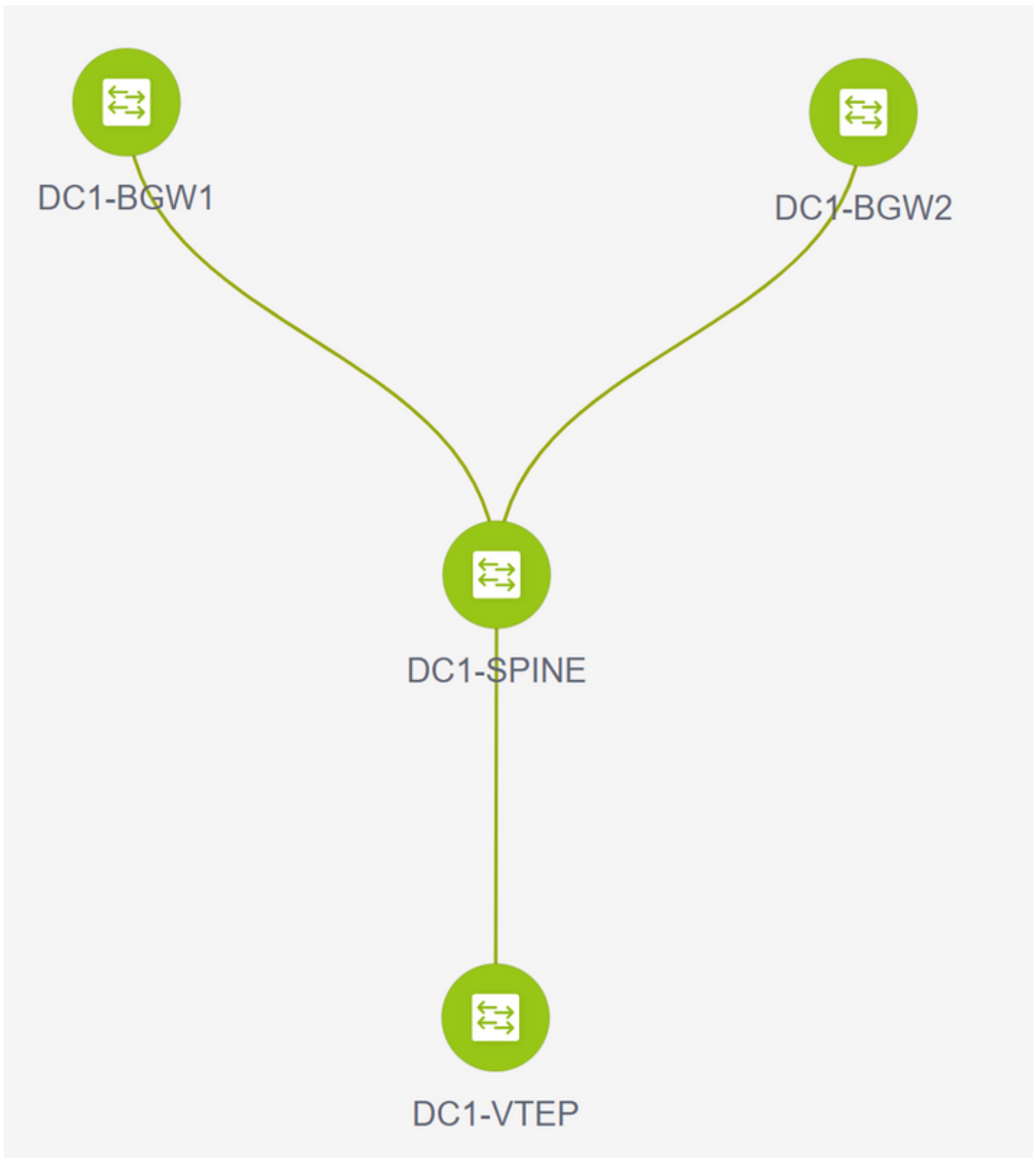


Step 1. Configuration Preview >

Step 2. Configuration Deployment Status >

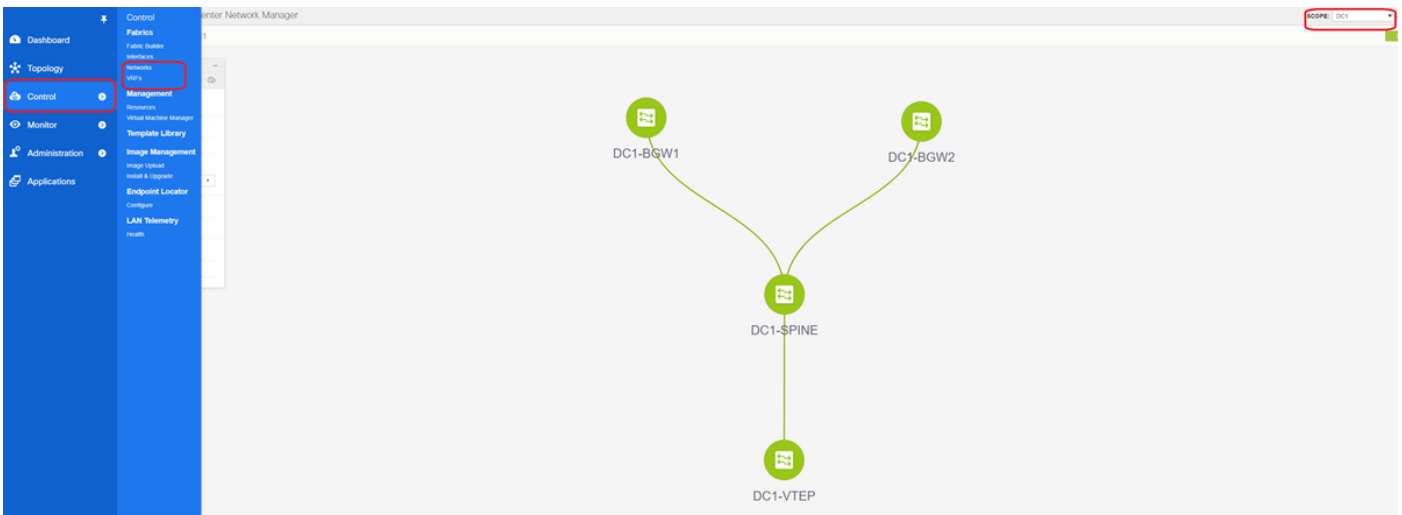
Switch Name	IP Address	Status	Status Description	Progress
DC1-VTEP	10.122.165.173	COMPLETED	Deployed successfully	100%
DC1-SPINE	10.122.165.200	COMPLETED	Deployed successfully	100%
DC1-BGW2	10.122.165.154	COMPLETED	Deployed successfully	100%
DC1-BGW1	10.122.165.187	COMPLETED	Deployed successfully	100%

Close



Schritt 3: Konfiguration von Netzwerken/VRFs

- Konfiguration von Netzwerken/VRFs
- # Wählen Sie DC1 Fabric (oben rechts) aus, Control > VRFs



Als Nächstes wird VRF erstellt.

11.2 DCNM-Version füllt die VRF-ID automatisch aus. Wenn der Unterschied besteht, geben Sie den gewünschten ein, und wählen Sie "Create VRF" (VRF erstellen) aus.

Hier wird als Layer-3-VNID 1001445 verwendet.

- Der nächste Schritt besteht in der Erstellung der Netzwerke

Networks

Network Name Network ID VRF Name IPv4 Gateway/Subnet IPv6 Gateway/Prefix Status VLAN ID

No data available

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

IPv4 Gateway/NetMask: 172.16.144.254/24 example 192.0.2.1/24

IPv6 Gateway/Prefix example 2001:db8::1/64

Vlan Name if > 32 chars enable: system vlan long-nan

Interface Description ?

MTU for L3 interface 68-9216

IPv4 Secondary GW1 example 192.0.2.1/24

IPv4 Secondary GW2 example 192.0.2.1/24

Create Network

Geben Sie die Netzwerk-ID an (dies ist die entsprechende VNID der Layer-2-VLANs).

Geben Sie die VRF-Instanz an, zu der die SVI gehören soll. Standardmäßig füllt DCNM 11.2 den VRF-Namen auf den zuvor erstellten Namen aus. Änderungen nach Bedarf

Die VLAN-ID ist Layer-2-VLAN, der dieser VNID zugeordnet ist.

IPv4-Gateway-> Dies ist die IP-Adresse des Anycast-Gateways, die auf der SVI konfiguriert wird und für alle VTEPs in der Fabric identisch ist.

- Die Registerkarte "Erweitert" verfügt über zusätzliche Zeilen, die bei Bedarf gefüllt werden müssen, z. B. DHCP Relay verwendet;

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

Wenn die Felder ausgefüllt sind, klicken Sie auf "Netzwerk erstellen".

Erstellen Sie alle anderen Netzwerke, die Teil dieser Fabric sein müssen.

- Derzeit sind VRF und Netzwerke nur in DCNM definiert. aber nicht von DCNM an die Switches in der Fabric weitergeleitet. Dies kann mithilfe der folgenden

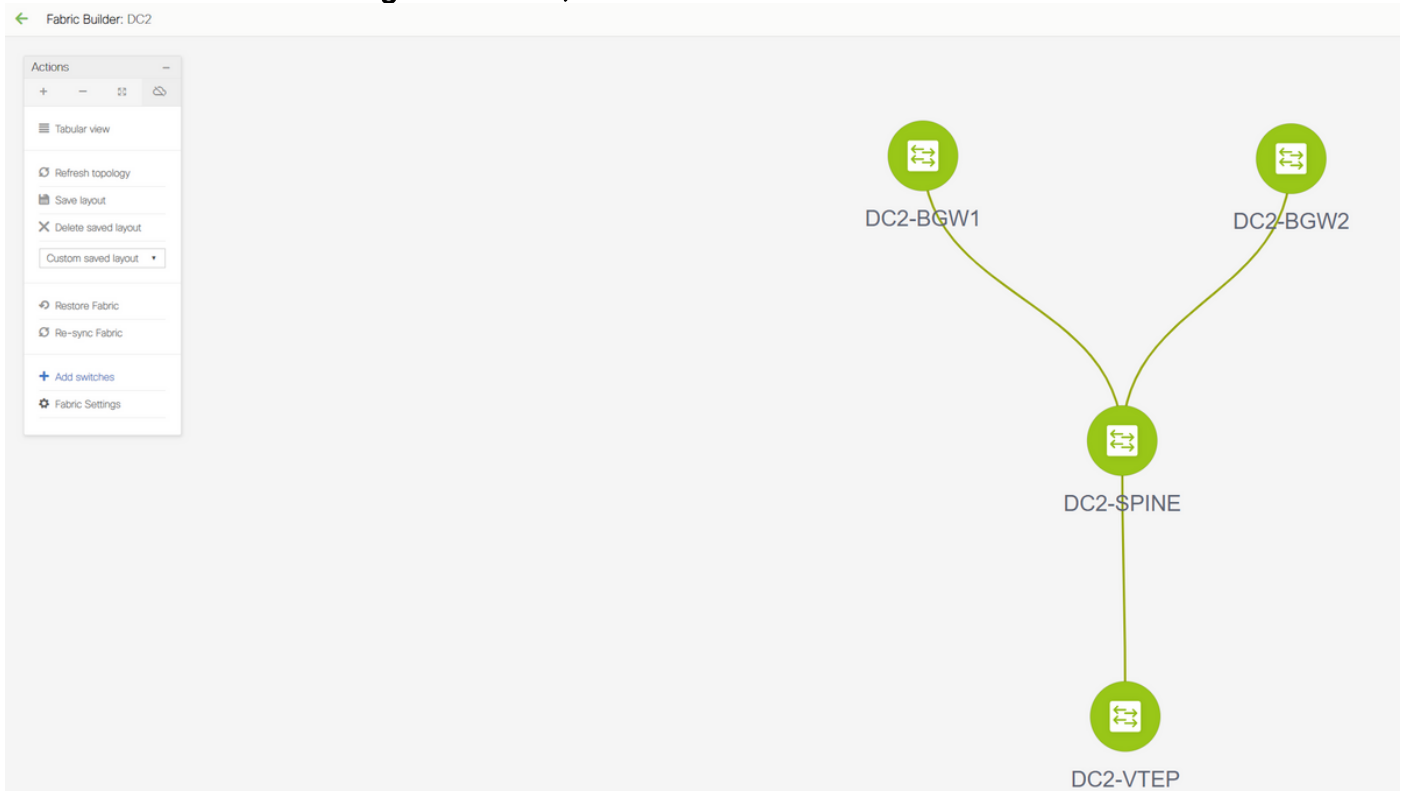
Network / VRF Selection > Network / VRF Deployment >

Networks							
	Network Name	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

Der Status wird in "NA" angezeigt, wenn dies NICHT auf den Switches bereitgestellt wird. Da es sich um einen Standort mit mehreren Standorten handelt und Border Gateways erforderlich sind, wird die Bereitstellung von Netzwerken/VRFs weiter unten besprochen.

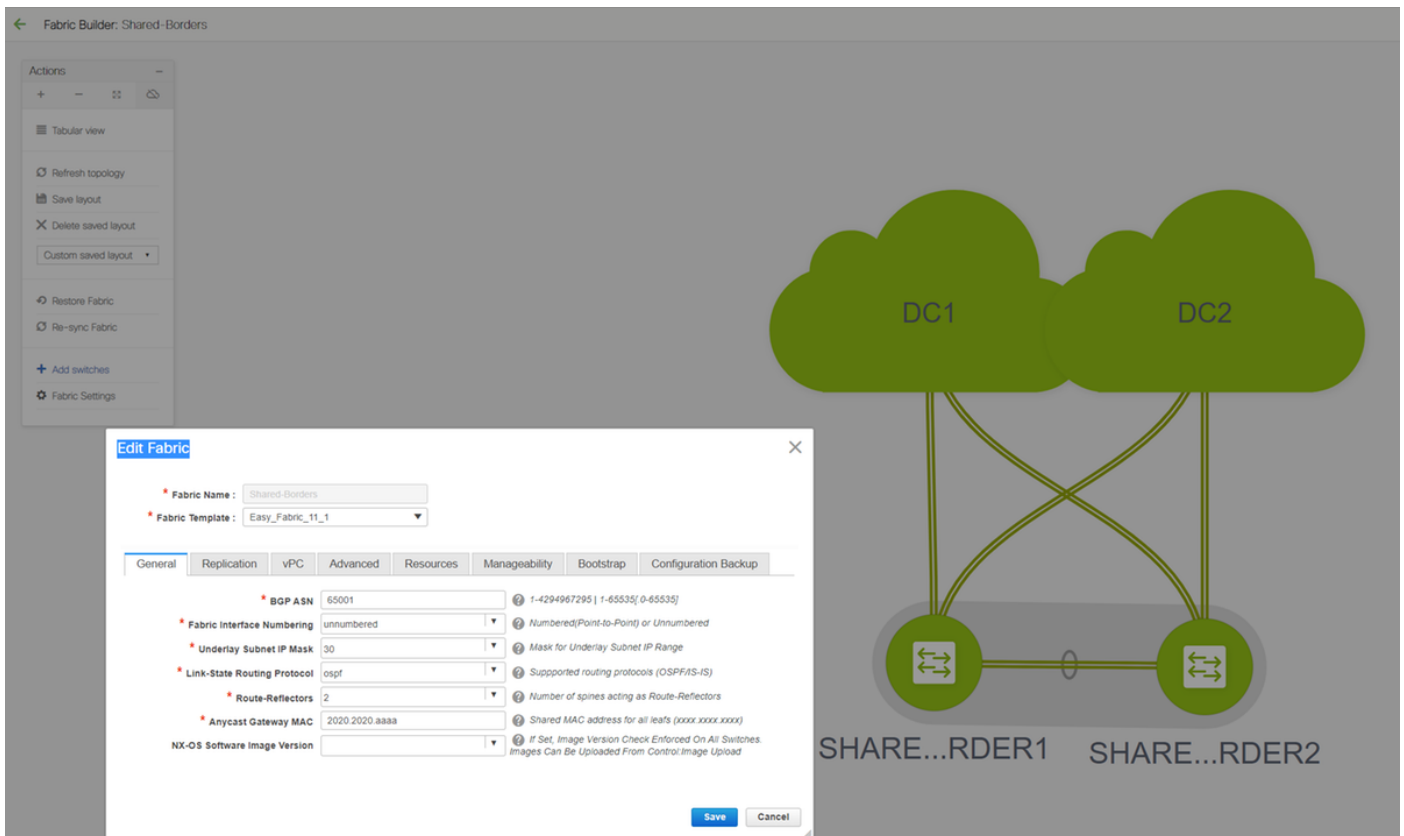
Schritt 4: Wiederholen Sie die gleichen Schritte für DC2.

- Nachdem DC1 vollständig definiert ist, wird das gleiche Verfahren auch für DC2 ausgeführt.
- Sobald DC2 vollständig definiert ist, sieht es wie unten aus.



Schritt 5: Erstellung einer einfachen Struktur für gemeinsame Grenzen

- Hier wird eine weitere einfache Fabric erstellt, die die gemeinsamen Grenzen enthält, die sich in vPC befinden.
- Beachten Sie, dass die gemeinsamen Grenzen bei der Bereitstellung über DCNM als vPC konfiguriert werden sollten. Andernfalls werden die Verbindungen zwischen den Switches geschlossen, nachdem ein "Re-Sync"-Vorgang auf DCNM ausgeführt wurde.
- Die Switches in gemeinsamen Grenzen müssen mit der Rolle "Border" (Grenze) festgelegt werden.

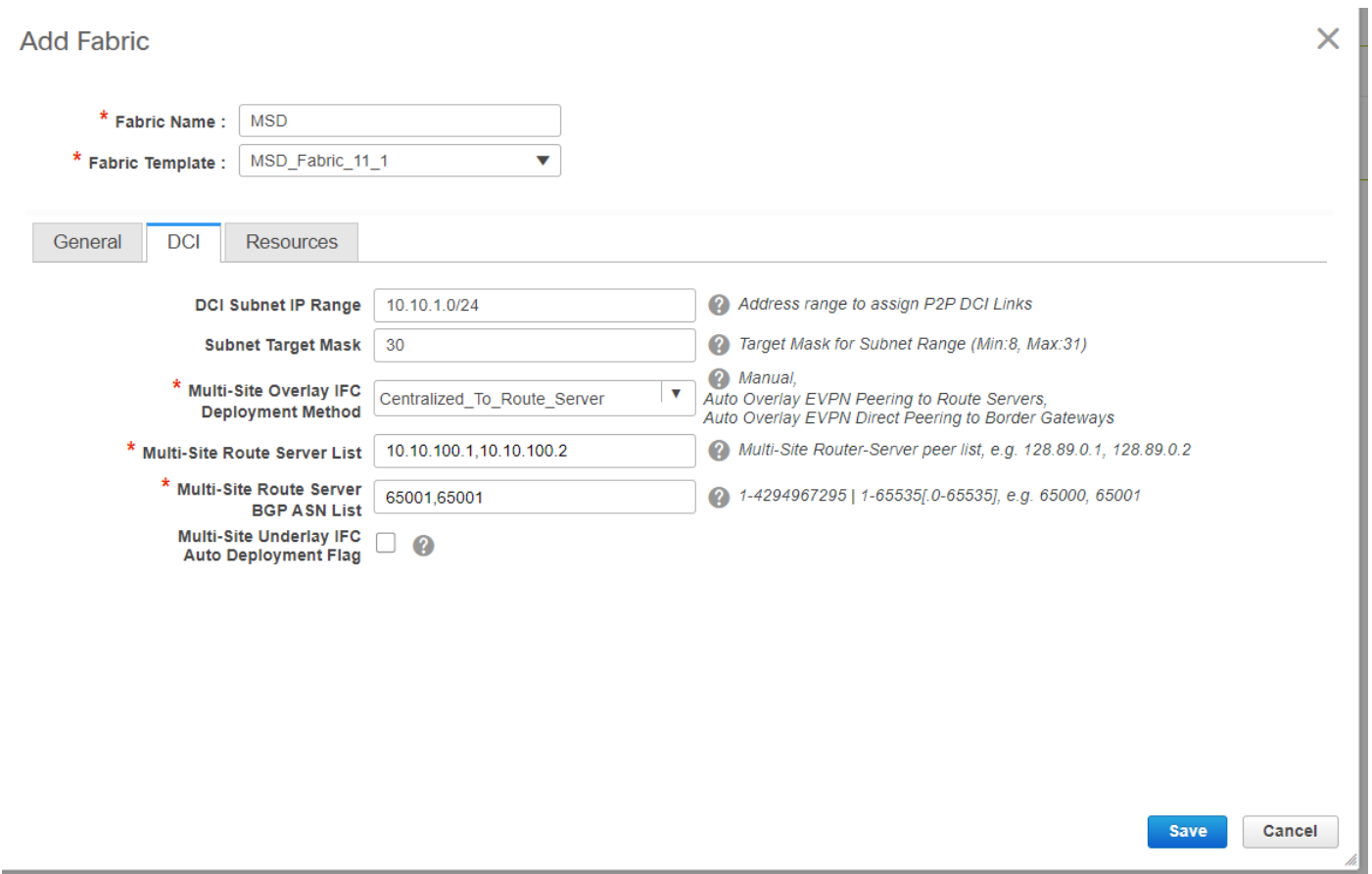
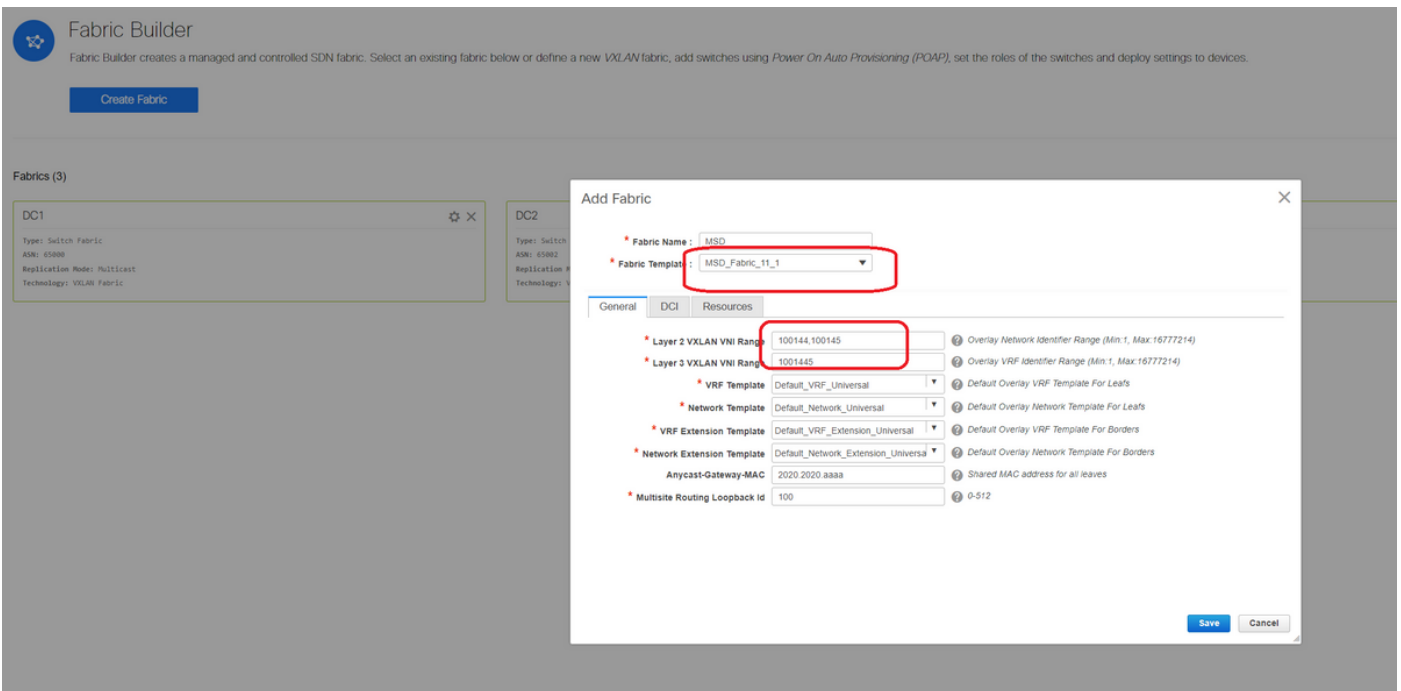


VRFs werden wie für DC1- und DC2-Fabrics erstellt.

Netzwerke sind an einer gemeinsamen Grenze nicht erforderlich, da an der gemeinsamen Grenze keine Layer-2-VLANs/VNIDs vorhanden sind. Gemeinsame Grenzen sind keine Tunnelterminierung für Ost-West-Datenverkehr von DC1 bis DC2. Nur die Border Gateways würden eine Rolle bei der VXLAN-Kapselung/Entkapselung für Ost-/West-DC1<>DC2-Datenverkehr spielen.

Schritt 6: Erstellung von MSD und Verschieben von RZ1- und RZ2-Fabrics

Wechseln Sie zum Fabric-Builder, erstellen Sie eine neue Fabric, und verwenden Sie die Vorlage -> MSD_Fabric_11_1



Beachten Sie, dass die IFC-Bereitstellungsmethode für mehrere Standorte **"centralized_To_Route_Server"** sein muss. Hier werden die gemeinsamen Grenzen als Routen-Server betrachtet. Diese Option wird daher von der Dropdown-Liste aus verwendet.

in der **"Liste der Routenserver für mehrere Standorte"**; Hier finden Sie die Loopback-IP-Adressen von Loopback0 (das Routing-Loopback) an der gemeinsamen Grenze, und füllen Sie es aus.

ASN ist die Nummer an der gemeinsamen Grenze (weitere Einzelheiten finden Sie im Diagramm oben in diesem Dokument). Im Rahmen dieses Dokuments werden beide

gemeinsamen Grenzen im gleichen ASN konfiguriert. Füllen Sie die Felder entsprechend aus.

- Auf der nächsten Registerkarte wird der IP-Bereich für Loopback an mehreren Standorten bereitgestellt (siehe unten).

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

Wenn alle Felder ausgefüllt sind, klicken Sie auf die Schaltfläche "Speichern", und eine neue Fabric wird mit der Vorlage erstellt -> MSD.

Als Nächstes verschieben Sie DC1- und DC2-Fabrics auf dieses MSD

Fabric Builder: MSD

Actions

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

Move Fabric

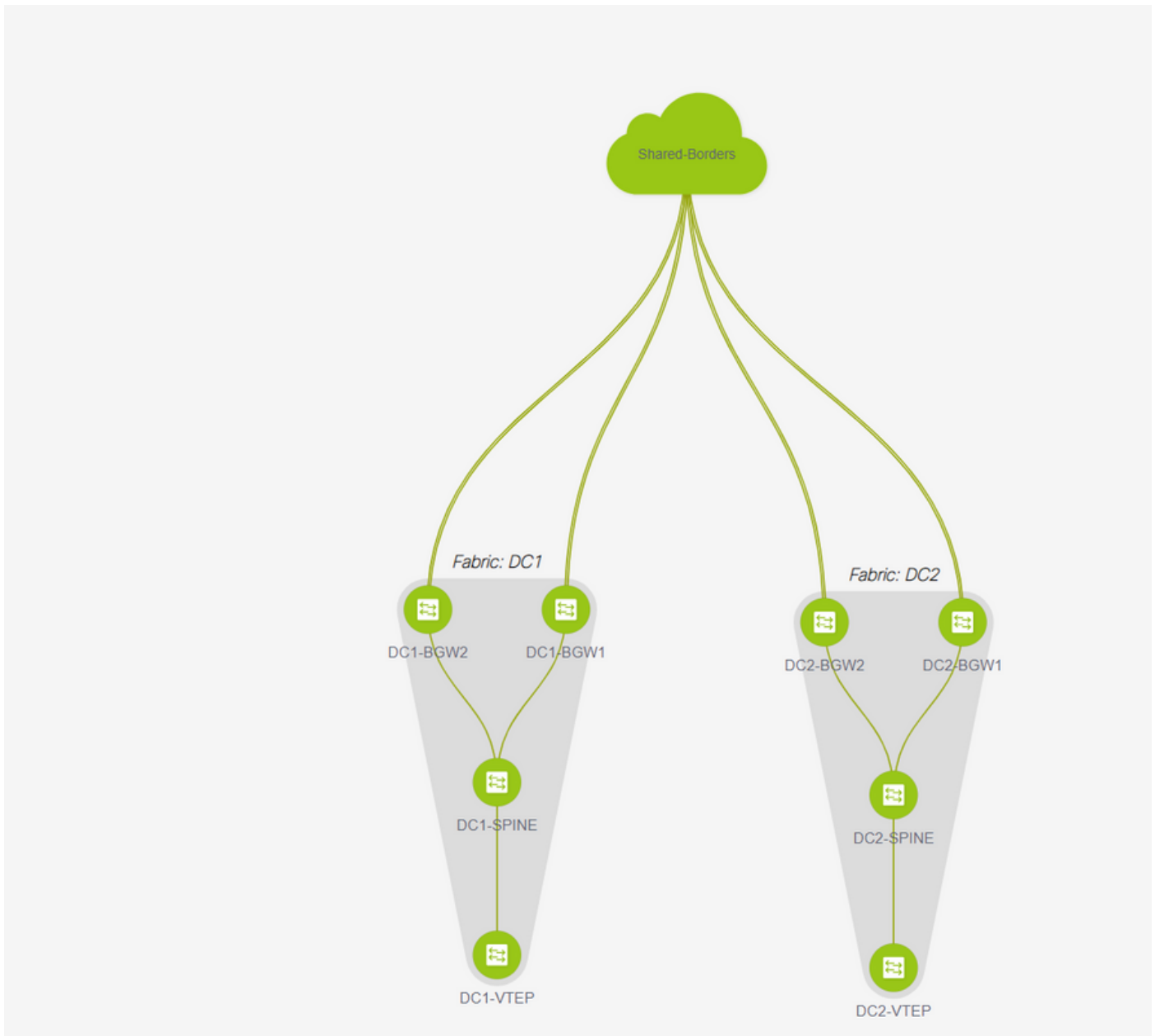
Please note that it may take a few minutes if there is a large number of VRFs/NWs in the fabrics!

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

Nach dem Umzug der Fabric sieht es wie unten aus.



Klicken Sie anschließend auf die Schaltfläche "Save&Deploy" (Speichern und Bereitstellen), um die erforderlichen Konfigurationen für mehrere Standorte an die Grenz-Gateways zu übertragen.

The screenshot shows the Fabric Builder MCO interface. A "Config Deployment" dialog box is open, displaying the deployment status of various switches. The dialog has two tabs: "Step 1: Configuration Preview" and "Step 2: Configuration Deployment Status". The "Step 2" tab is active, showing a table with the following data:

Switch Name	IP Address	Status	Status Description	Progress
DC2-BGW2	10.122.165.188	STARTED	Deployment in progress.	<div style="width: 100%;"></div>
DC2-BGW1	10.122.165.189	STARTED	Deployment in progress.	<div style="width: 100%;"></div>
DC1-BGW2	10.122.165.154	STARTED	Deployment in progress.	<div style="width: 100%;"></div>
DC1-BGW1	10.122.165.157	STARTED	Deployment in progress.	<div style="width: 100%;"></div>

The "Save & Deploy" button in the top right corner of the interface is highlighted with a red box.

Schritt 7: Erstellung externer Fabric

Erstellen Sie eine externe Fabric, und fügen Sie den externen Router wie unten gezeigt hinzu.

Add Fabric

* Fabric Name :

* Fabric Template :

General Advanced Resources DCI Configuration Backup Bootstrap

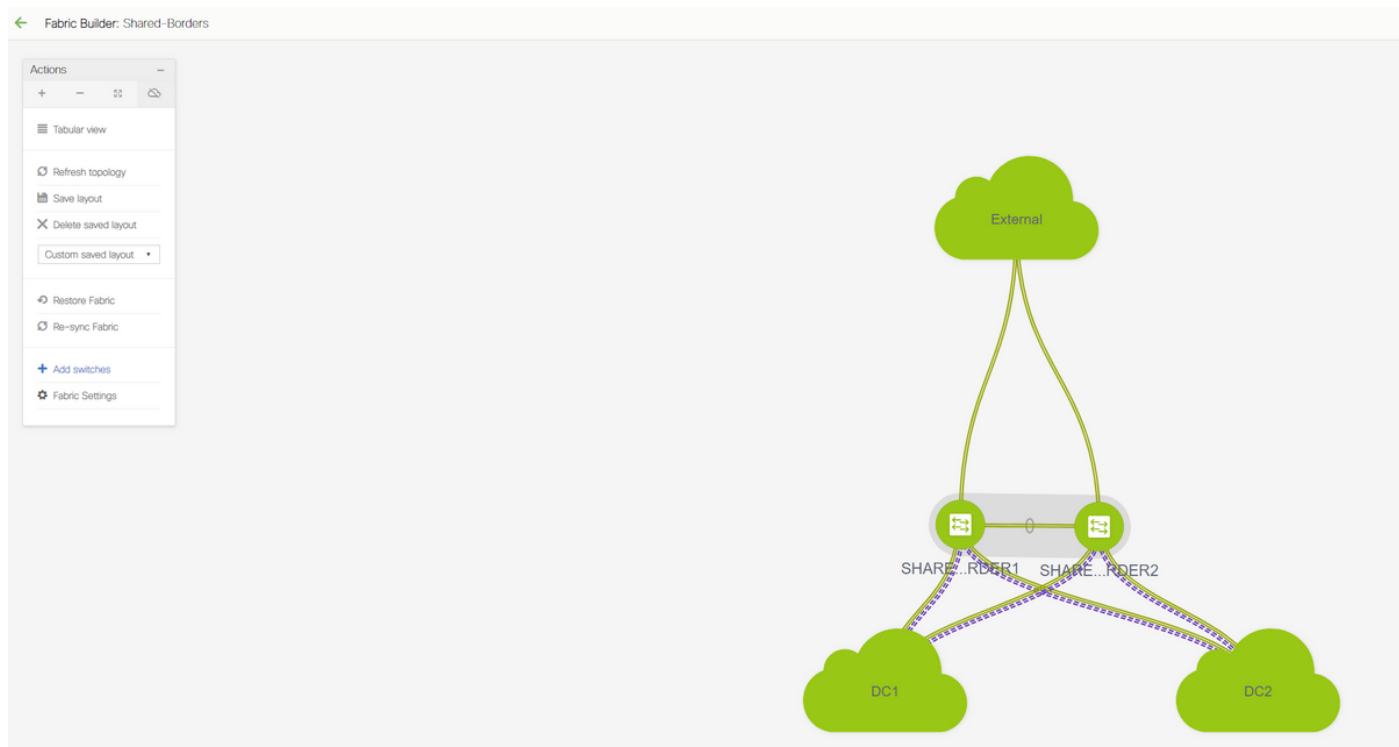
* BGP AS # 1-4294967295 | 1-65535[0-65535]

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

Nennen Sie die Fabric und verwenden Sie die Vorlage "External_Fabric_11_1";

Geben Sie das ASN

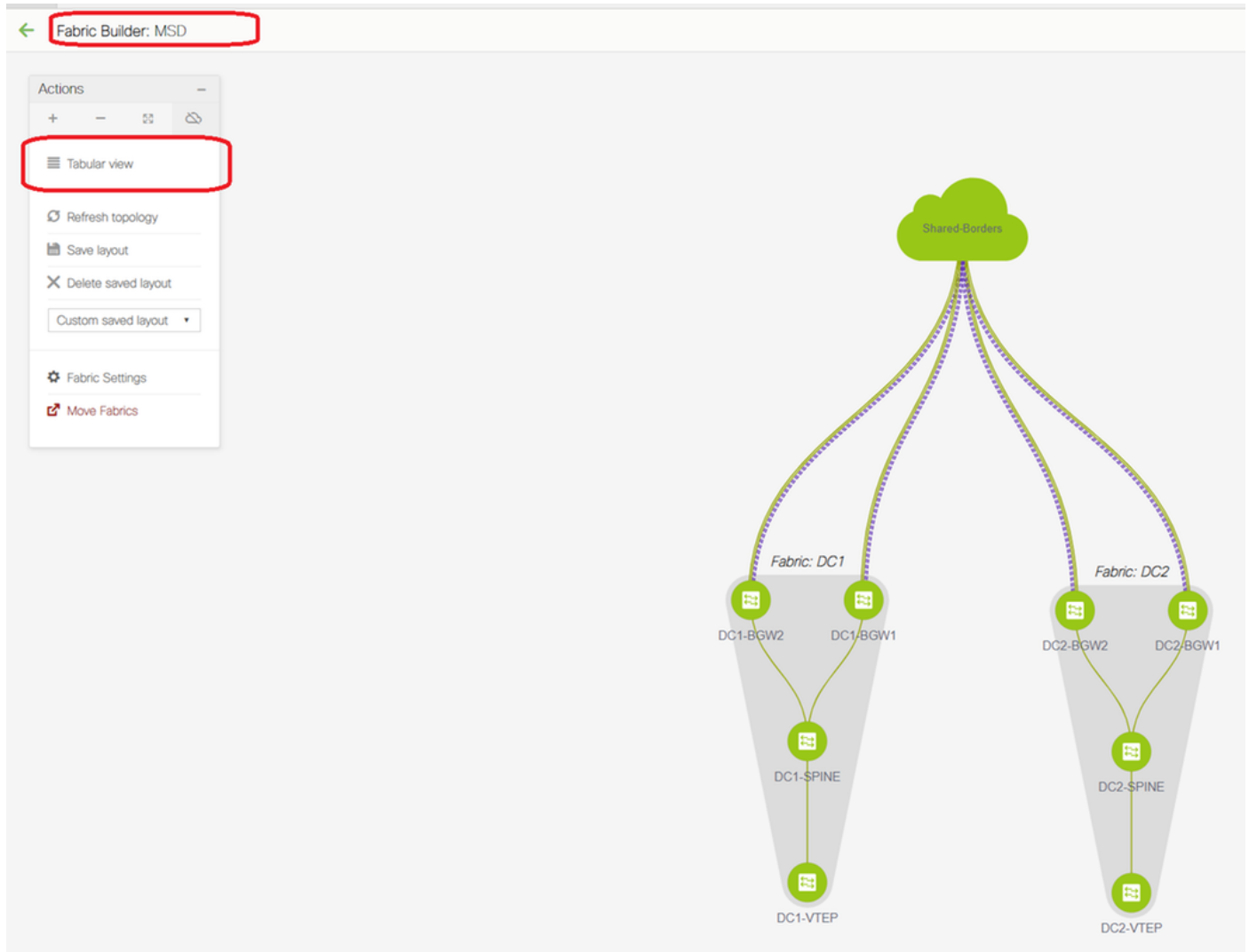
Am Ende sehen die verschiedenen Stoffe wie unten aus.



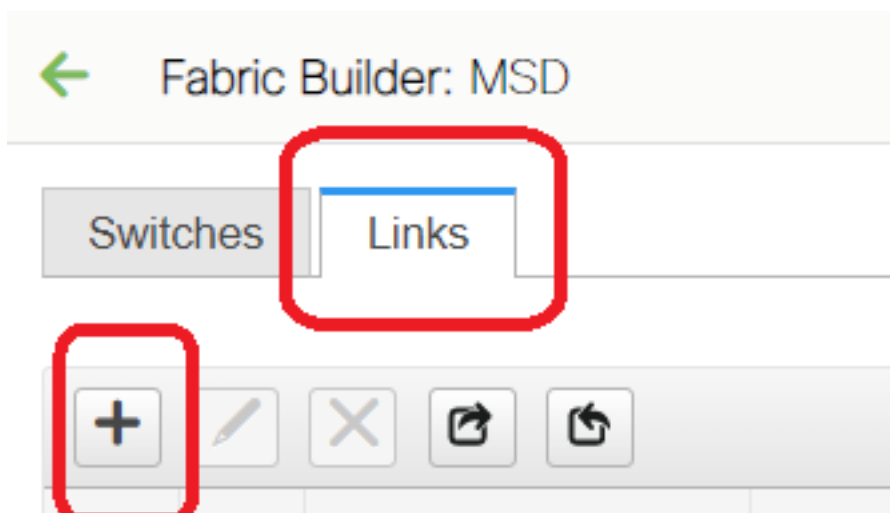
Schritt 8: eBGP-Underlay für Loopback-Erreichbarkeit zwischen BGWs (auch iBGP zwischen gemeinsamen Grenzen)

An gemeinsamen Grenzen wird eBGP I2vpn-Ereignis mit den Border Gateways und VRF-LITE-Verbindungen zum externen Router ausgeführt.

Bevor ein eBGP I2vpn-Ereignis mit den Loopbacks gebildet wird, muss sichergestellt werden, dass die Loopbacks auf irgendeine Weise erreichbar sind. In diesem Beispiel verwenden wir eBGP IPv4 AF von BGWs zu Shared Border und kündigen dann die Loopbacks an, um die I2vpn-Ereignisumgebung weiter zu bilden.



Wenn die MSD-Fabric ausgewählt ist, wechseln Sie zur "Tabellenansicht".



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 S

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

* BGP Neighbor IP Neighbor IP address

* BGP Neighbor ASN Neighbor BGP Autonomou

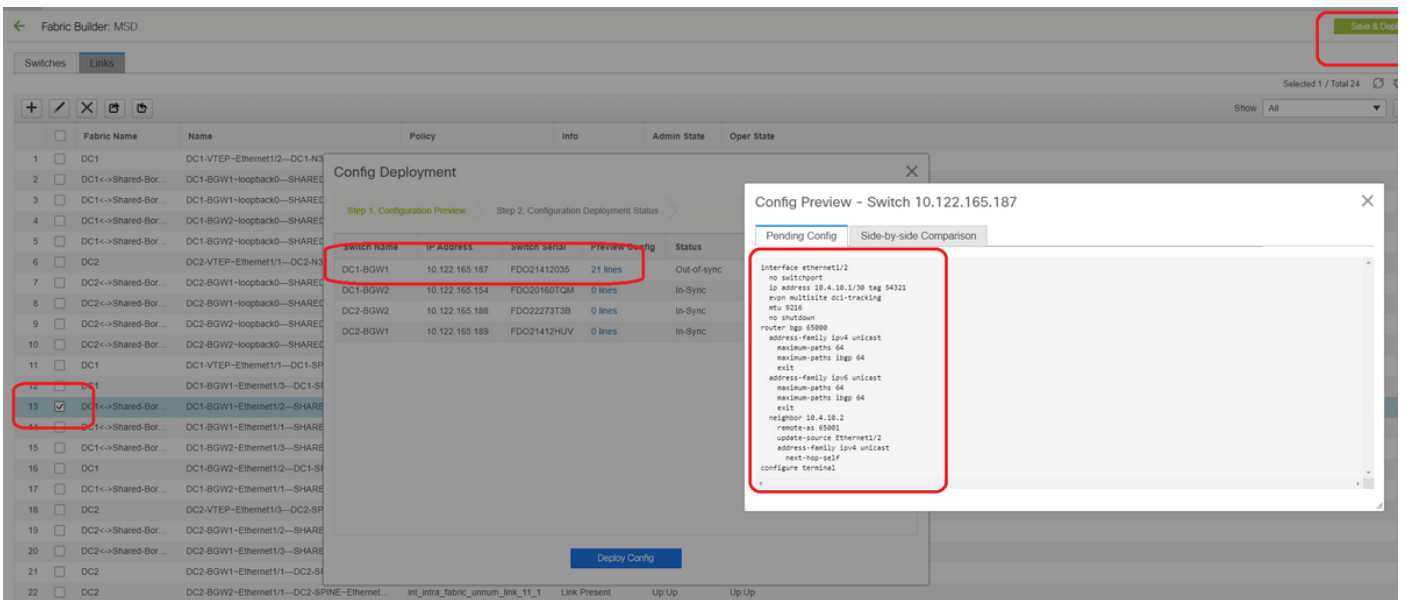
* BGP Maximum Paths Maximum number of IBGP,

* Routing TAG Routing tag associated with

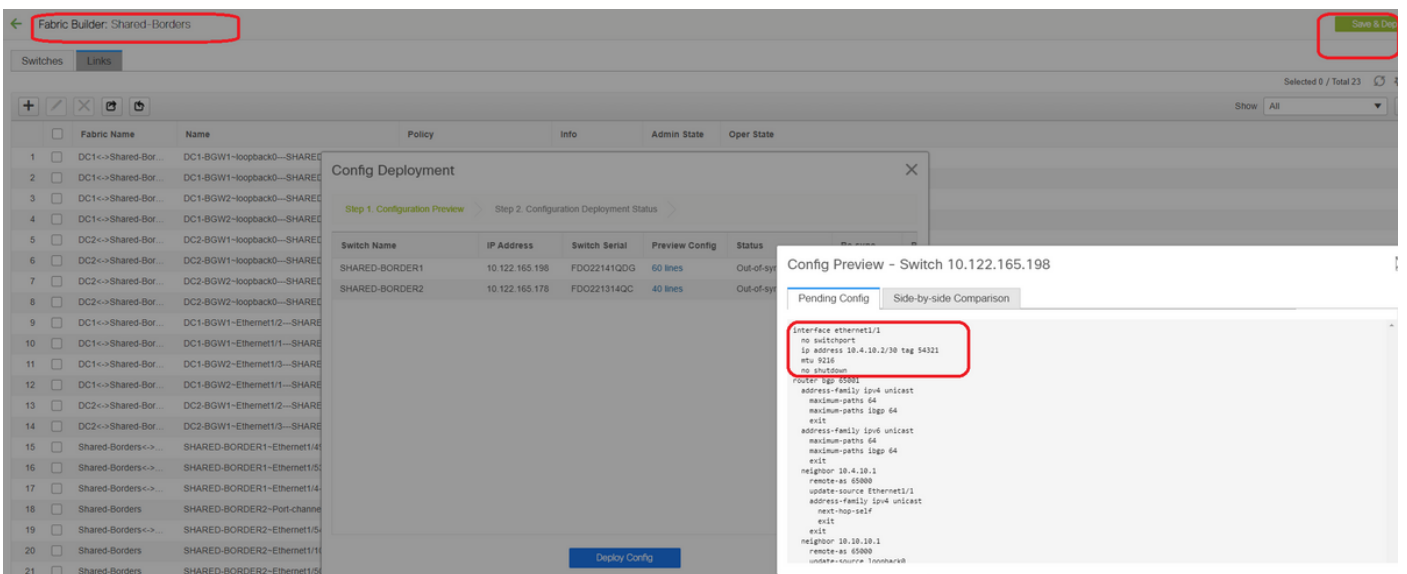
Wählen Sie die "Inter-Fabric" und verwenden Sie "Multisite_UNDERLAY".

Hier wird versucht, eine IPv4-BGP-Nachbarschaft mit dem Shared Border Router zu bilden. Wählen Sie die Switches und Schnittstellen entsprechend aus.

Beachten Sie, dass, wenn CDP den Nachbarn von DC1-BGW1 bis SB1 erkennt, es nur erforderlich ist, die IP-Adressen hier in diesem Abschnitt anzugeben und die IP-Adressen auf den entsprechenden Schnittstellen effektiv zu konfigurieren, nachdem "Save & Deploy" ausgeführt wurde.



Wenn Save and Deployment (Speichern und Bereitstellen) ausgewählt ist, werden die erforderlichen Konfigurationslinien für DC1-BGW1 propagiert. Derselbe Schritt muss auch nach der Auswahl der "Shared Border"-Fabric ausgeführt werden.



Von der CLI aus kann dies mit dem folgenden Befehl überprüft werden:

```

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
  
```

Beachten Sie, dass "save&Deploy" auch auf der DC1-Fabric ausgeführt werden muss (wählen Sie das Dropdown-Menü für DC1 aus, und führen Sie dann die gleichen aus), sodass die entsprechende IP-Adressierung BGP-Konfigurationen an die Switches in DC1 (die Border Gateways) propagiert werden.

Außerdem muss das Multisite-Underlay aus DC1-BGWs, DC2-BGWs zu Shared BGWs erstellt

werden. Daher müssen die gleichen Schritte wie oben auch für das gleiche ausgeführt werden.

Am Ende wird an den gemeinsamen Grenzen eine eBGP IPv4 AF-Nachbarschaft mit allen BGWs in DC1 und DC2 wie unten angezeigt.

```
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]
```

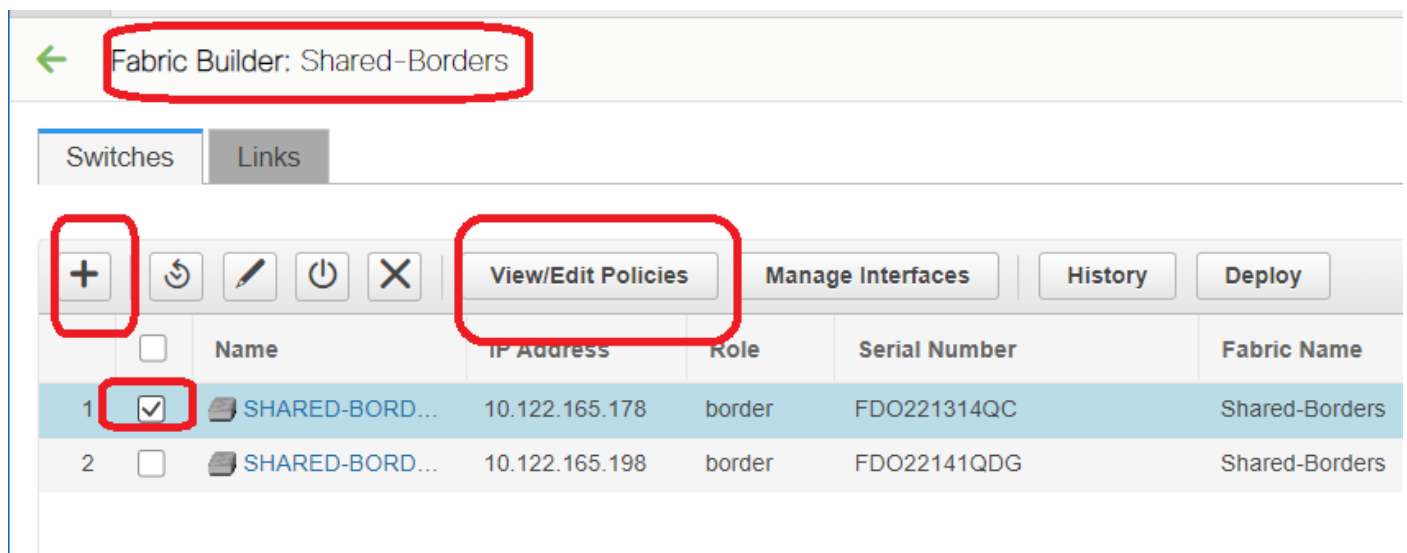
Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.4.10.1	4	65000	1715	1708	38	0	0	1d03h 5	
10.4.10.6	4	65000	1461	1458	38	0	0	1d00h 5	
10.4.10.18	4	65002	1459	1457	38	0	0	1d00h 5	
10.4.10.22	4	65002	1459	1457	38	0	0	1d00h 5	

```
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	

Oben ist die Voraussetzung für den Aufbau der I2vpn-Ereignisumgebung von BGWs zu gemeinsamen Grenzen (BGP muss nicht verwendet werden). jeder andere Mechanismus zum Austausch von Loopback-Präfixen würde dies tun); Letztlich müssen alle Loopbacks (von Shared BGWs) von allen BGWs erreichbar sein

Bitte beachten Sie auch, dass eine iBGP IPv4 AF-Nachbarschaft zwischen gemeinsamen Grenzen aufgebaut werden muss. Ab heute besteht für DCNM keine Option zum Erstellen eines iBGP zwischen gemeinsamen Rändern mithilfe einer Vorlage/Dropdown-Liste. Dazu muss eine Konfiguration für "Freeform" durchgeführt werden, die im Folgenden dargestellt ist.



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 Template Name: switch_freeform
 Entity Type: SWITCH 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

Suchen Sie die IP-Adressen, die auf der Backup-SVI der gemeinsamen Grenzen konfiguriert wurden. Wie oben gezeigt, wird Freeform auf dem Shared-Border1-Switch hinzugefügt, und der angegebene iBGP-Nachbarn entspricht dem Shared-Border2(10.100.100.2)

Beachten Sie, dass Sie, während Sie die Konfigurationen in der Freeform in DCNM bereitstellen, den richtigen Abstand nach jedem Befehl geben (es bleiben sogar Leerzeichen; d. h. nach Router bgp 65001 zwei Leerzeichen bereitstellen und dann den Befehl neighbor <> geben usw.)

Stellen Sie außerdem sicher, dass Sie eine Direktverteilung für die Direkttrouten(Loopback-Routen) im BGP oder in einer anderen Form durchführen, um Loopbacks anzukündigen. Im obigen Beispiel wird ein route-map direct erstellt, um alle direkten Routen abzugleichen. Anschließend wird die direkte Verteilung innerhalb des IPv4 AF-BGP durchgeführt.

Sobald die Konfiguration über DCNM "gespeichert und bereitgestellt" ist, wird die iBGP-Nachbarschaft wie unten gezeigt gebildet.

```

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

Mit oben Schritt ist das Multisite-Underlay vollständig konfiguriert.

Der nächste Schritt besteht darin, ein Overlay für mehrere Standorte zu erstellen.

Schritt 9: Erstellung von Multisite-Overlays von BGWs zu gemeinsamen Grenzen

Beachten Sie, dass hier Shared Bänder auch die Routenserver sind

Wählen Sie die MSD und gehen Sie dann zur "Tabellenansicht", wo ein neuer Link erstellt werden kann. Dort muss ein neuer Overlay-Link für mehrere Standorte erstellt werden, und die entsprechenden IP-Adressen müssen wie unten beschrieben mit dem richtigen ASN versehen werden. Dieser Schritt muss für alle l2vpn-Event-Nachbarn durchgeführt werden (d. h. von jedem BGW zu jeder gemeinsamen Grenze).

oben ist ein Beispiel. Führen Sie die gleiche Funktion für alle anderen Overlay-Links für mehrere Standorte durch, und am Ende sieht die CLI wie folgt aus:

```

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]

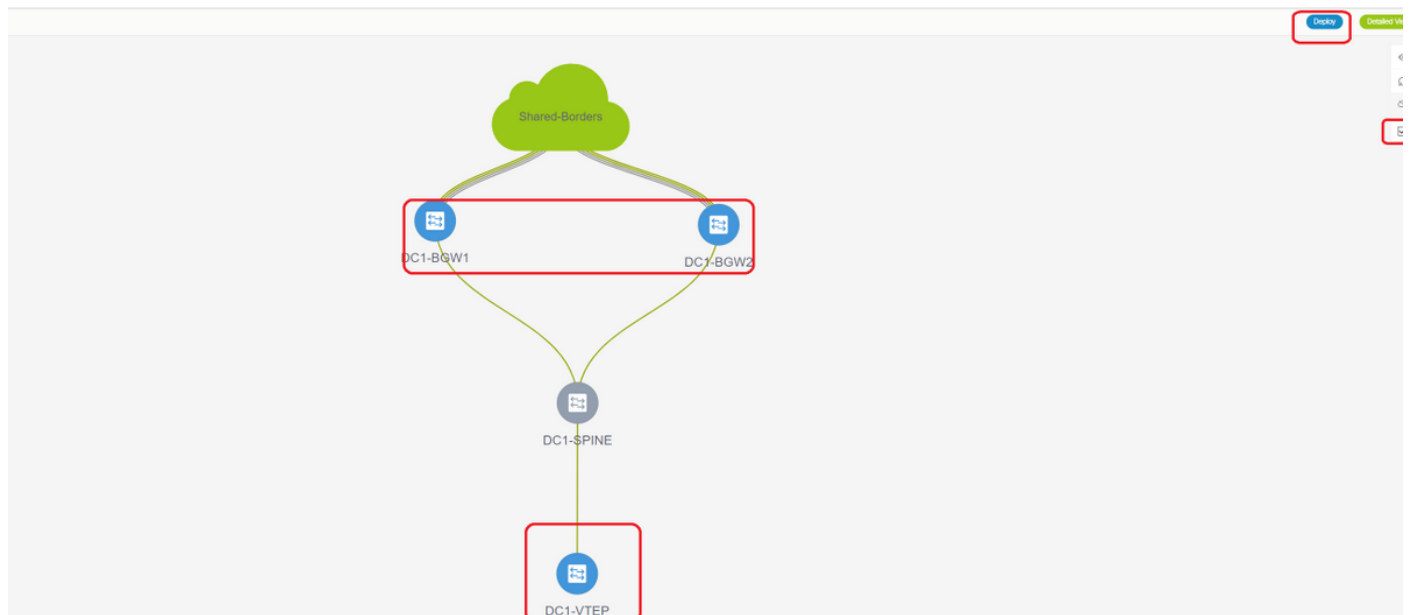
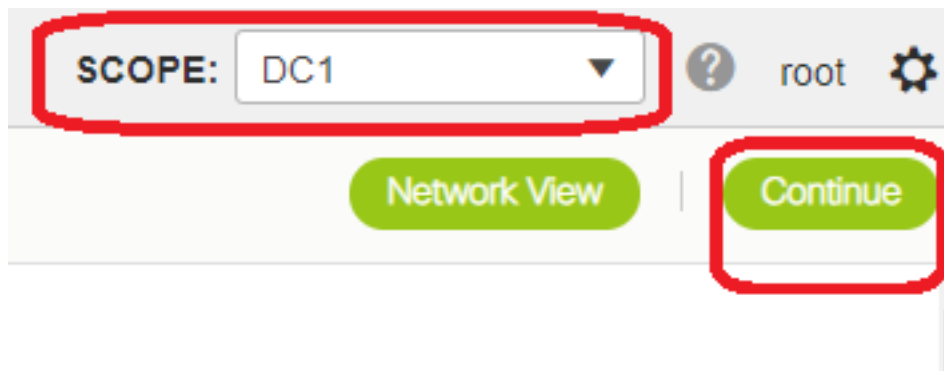
```

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

Schritt 10: Bereitstellung von Netzwerken/VRFs an beiden Standorten

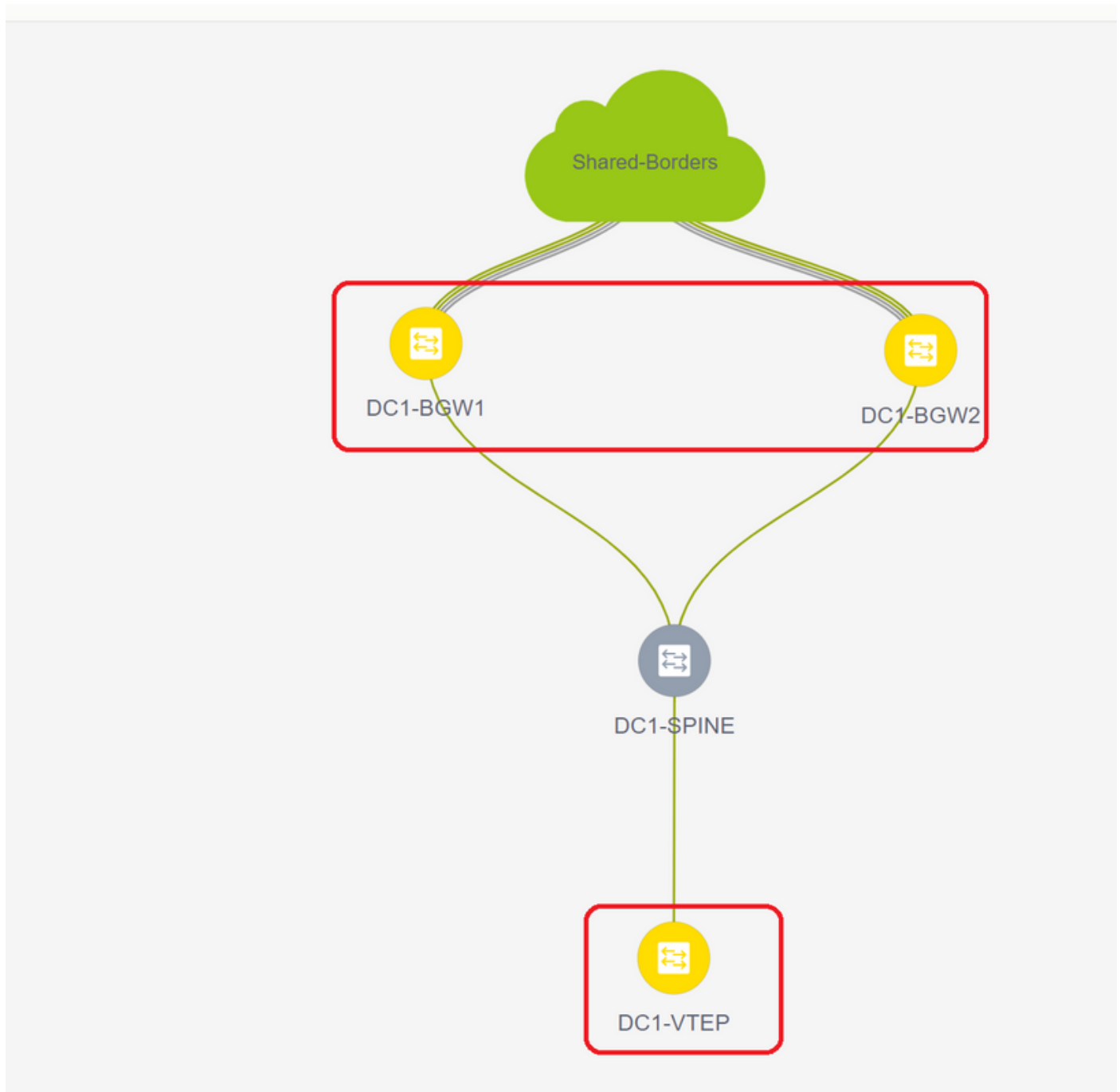
Nach Abschluss des Underlay und Overlay für mehrere Standorte besteht der nächste Schritt in der Bereitstellung der Netzwerke/VRFs auf allen Geräten.

Beginnend mit VRFs an Fabrics-> DC1-, DC2- und Shared-Rändern.



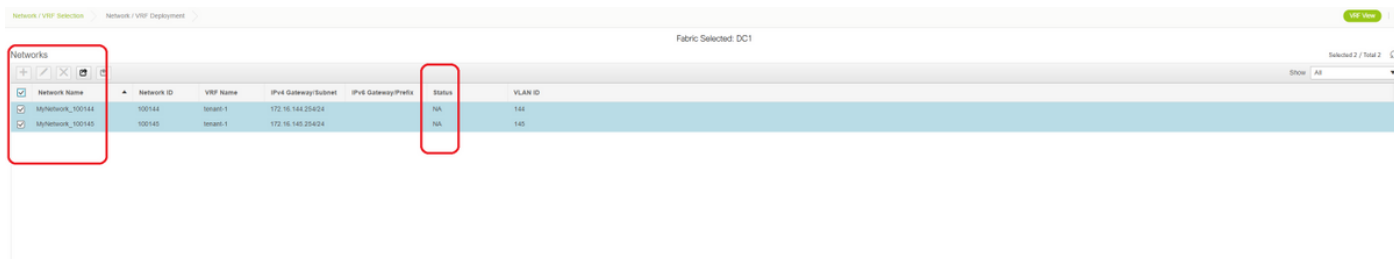
Wenn die VRF-Ansicht ausgewählt ist, klicken Sie auf "Weiter". Dadurch werden die Geräte in der Topologie aufgelistet.

Da die VRF-Instanz auf mehreren Switches bereitgestellt werden muss (einschließlich Border Gateways und Leaf), aktivieren Sie das Kontrollkästchen ganz rechts, und wählen Sie dann die Switches aus, die dieselbe Rolle gleichzeitig haben. z. B. DC1-BGW1 und DC1-BGW2 können gleichzeitig ausgewählt werden und dann beide Switches speichern. Wählen Sie anschließend die entsprechenden Leaf-Switches aus (hier: DC1-VTEP).



Wie oben gezeigt, wird bei Auswahl der Option "Bereitstellen" die Bereitstellung von allen zuvor ausgewählten Switches gestartet. Wenn die Bereitstellung erfolgreich war, leuchtet diese Option letztendlich grün.

Für die Bereitstellung von Netzwerken müssen dieselben Schritte ausgeführt werden.



Wenn mehrere Netzwerke erstellt werden, sollten Sie die folgenden Registerkarten verwenden, um die Netzwerke vor der Bereitstellung auszuwählen.



Der Status wechselt jetzt zu "DEPLOYED" (BEREITGESTELLT) von "NA", und die nachfolgende CLI des Switches kann zur Verifizierung der Bereitstellungen verwendet werden.

```
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]	

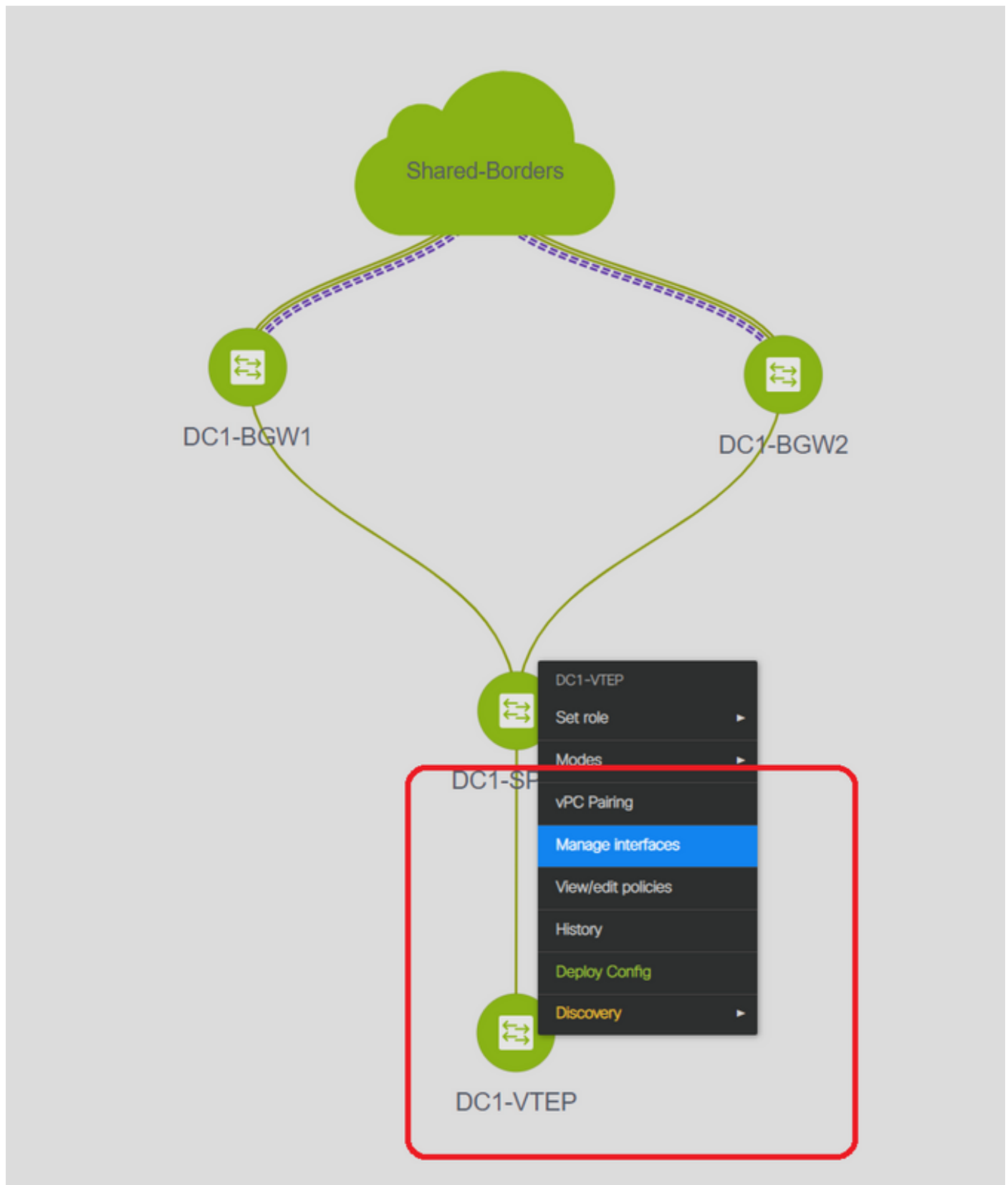
Oben ist auch von BGW. Kurz gesagt: Alle Switches, die wir zuvor im Schritt ausgewählt hatten, werden mit den Netzwerken und der VRF-Instanz bereitgestellt.

Dieselben Schritte müssen auch für Fabric DC2, Shared Border durchgeführt werden. Beachten Sie, dass für die gemeinsamen Grenzen KEINE Netzwerke oder Layer-2-VNIDs erforderlich sind.

Es ist nur L3-VRF erforderlich.

Schritt 11: Erstellen von Downstream-Trunk-/Access-Ports auf Leaf-Switches/VTEP

In dieser Topologie sind die Ports Eth1/2 und Eth1/1 von DC1-VTEP bzw. DC2-VTEP mit den Hosts verbunden. Verschieben Sie diese als Trunk-Ports in der DCNM-GUI, wie unten gezeigt.



Edit Configuration

Name: DC1-VTEP:Ethernet1/2

Policy: int_trunk_host_11_1

General

* Enable BPDU Guard no Enable spanning-tree bpduguard

Enable Port Type Fast Enable spanning-tree edge port behavior

* MTU jumbo MTU for the interface

* SPEED Auto Interface Speed

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

Interface Description Add description to the interface (Max Size 254)

Freeform Config

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

Wählen Sie die entsprechende Schnittstelle aus, und ändern Sie die "zulässigen VLANs" von "none" in "all" (oder nur die VLANs, die zugelassen werden müssen).

Schritt 12: Für die gemeinsame Grenze erforderliche Freiheiten

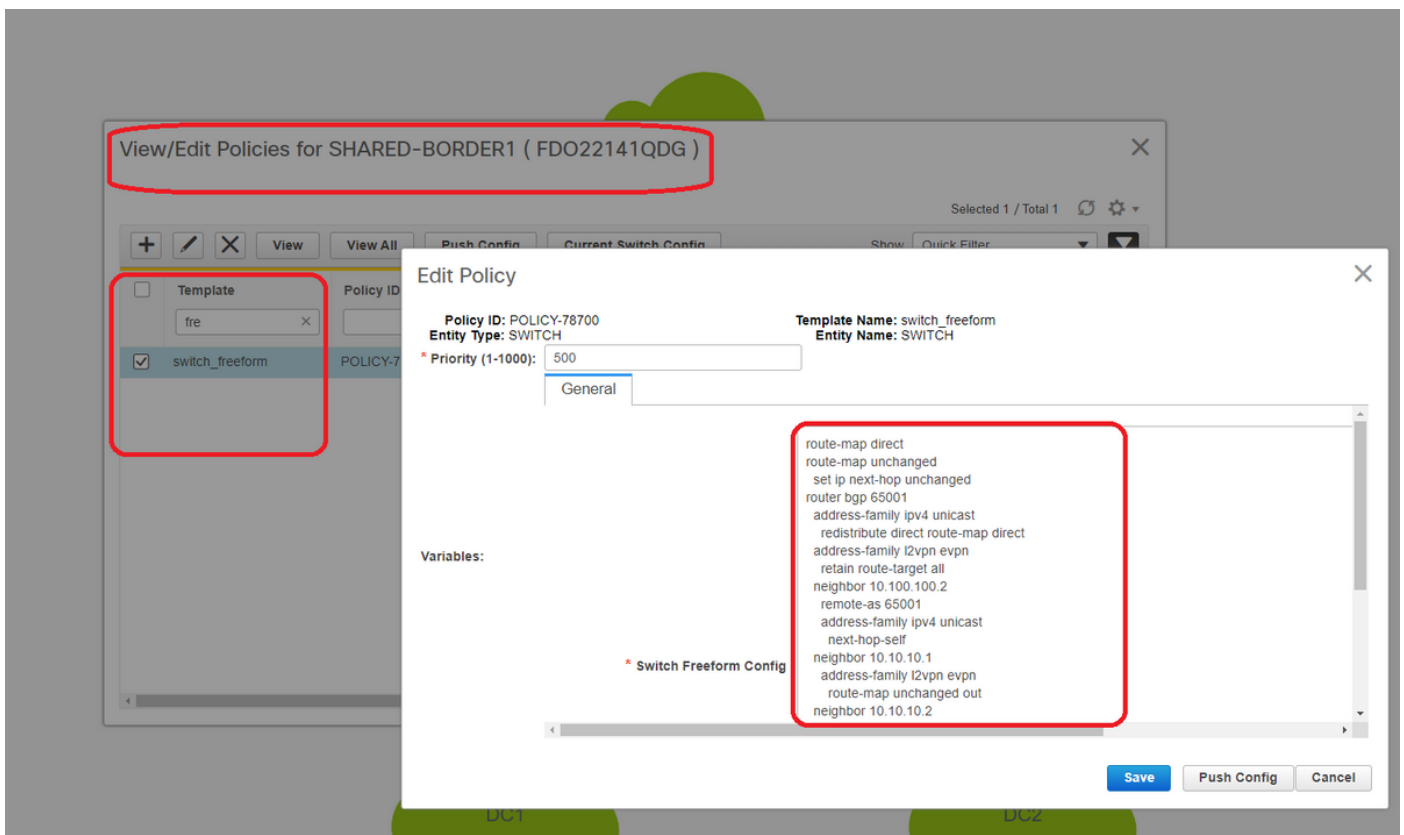
Da Shared Border Switches die Routing-Server sind, müssen einige Änderungen in Bezug auf die BGP I2vpn-evpn-Nachbarschaften vorgenommen werden.

Der standortübergreifende BUM-Datenverkehr wird mithilfe von Unicast repliziert. bedeutet, dass jeder BUM-Datenverkehr in VLAN 144 (eg) nach dem Eintreffen auf die BGWs vorhanden ist; Je nachdem, welcher BGW der designierte Forwarder (DF) ist, führt DF eine Unicast-Replikation für Remote-Standorte durch. Diese Replikation wird erreicht, nachdem der BGW eine Route vom Typ 3 vom Remote-BGW empfängt. Hier bilden die BGWs I2vpn-sogar-Peering nur mit gemeinsamen Grenzen. und die gemeinsamen Grenzen sollten keine Layer-2-VNIDs enthalten (falls diese erstellt werden, führt dies zu Blackholing des Ost-West-Datenverkehrs). Da Layer-2-VNIDs fehlen und der Routing-Typ 3 von BGWs pro VNID stammt, wird das von BGWs eingehende BGP-Update von den Shared BGP-Rändern nicht berücksichtigt. Um dies zu beheben, verwenden Sie das Feld "Keep-route-target all" unter dem AF-I2vpn-Ereignis.

Ein weiterer Punkt besteht darin sicherzustellen, dass die gemeinsamen Grenzen den Next HOP nicht ändern (BGP ändert standardmäßig den nächsten Hop für eBGP-Nachbarschaften); Hier sollte der standortübergreifende Tunnel für Unicast-Datenverkehr von Standort 1 bis 2 und umgekehrt vom BGW zum BGW sein (von dc1 zu dc2 und umgekehrt). Um dies zu erreichen, muss eine Route Map erstellt und für alle I2vpn-evpn-Nachbarschaften von der gemeinsamen Grenze zu den einzelnen BGWs angewendet werden.

Für beide oben genannten Punkte muss ein Freeform an gemeinsamen Grenzen wie unten verwendet werden.

```
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
```



Schritt 13: Loopback innerhalb von Tenant-VRFs auf BGWs

Für Nord-/Süd-Datenverkehr von Hosts, die mit den Leaf-Switches verbunden sind, verwenden die BGWs die äußere SRC-IP der IP-Adresse NVE Loopback1. Freigegebene Grenzen werden

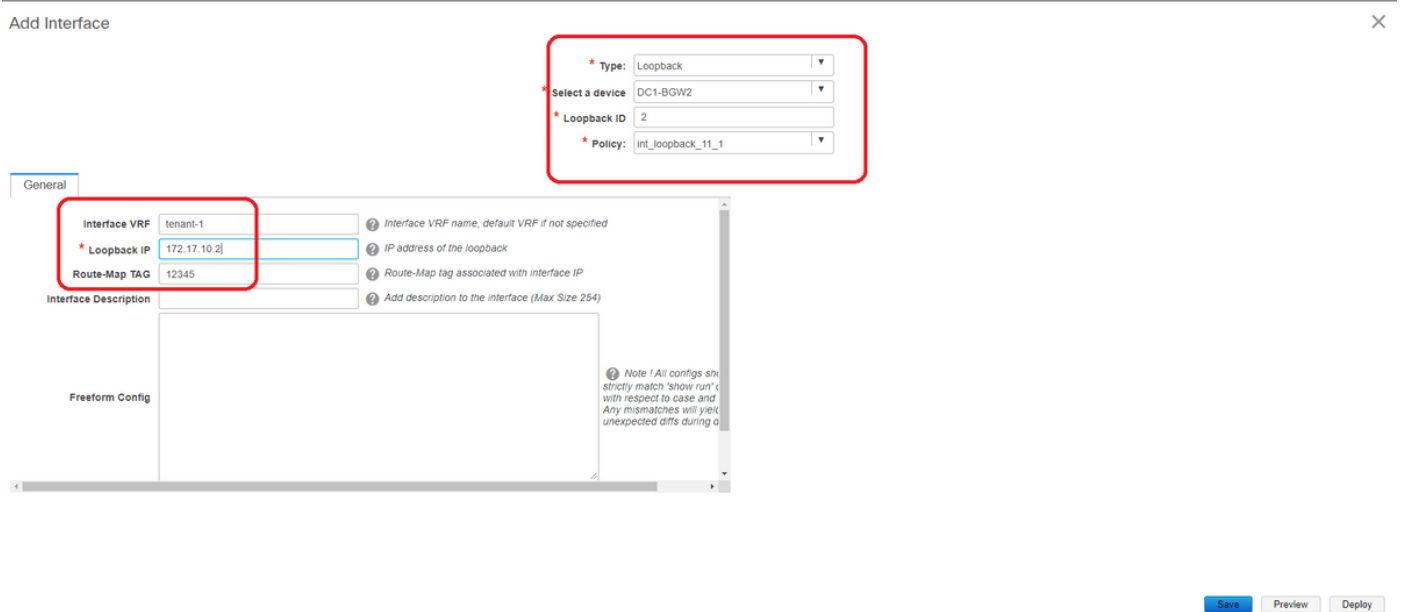
standardmäßig nur vom NVE-Peering mit der Loopback-IP-Adresse der BGWs für mehrere Standorte abgeleitet. Wenn ein VXLAN-Paket an die gemeinsame Grenze mit einer externen SRC-IP-Adresse des BGW-Loopback1 gelangt, wird das Paket aufgrund der SRCTEP-Miss verworfen. Um dies zu vermeiden, muss auf jedem BGW-Switch ein Loopback in Tenant-VRF erstellt und dann dem BGP angekündigt werden, sodass die Shared Bands dieses Update erhalten und dann das NVE-Peering mit der IP-Adresse des BGW Loopback1 bilden.

Anfänglich sieht das NVE-Peering wie unten an gemeinsamen Grenzen aus.

```

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

```



Wie oben gezeigt, wird das Loopback2 aus DCNM erstellt und in Tenant-1-VRF konfiguriert. Es erhält das Tag 12345, da dies der Tag ist, den die Route-Map verwendet, um das Loopback abzugleichen, während die Werbung geschaltet wird.

```

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-redist-subnet
  maximum-paths ibgp 2
  address-family ipv6 unicast
    advertise l2vpn evpn
  redistribute direct route-map fabric-rmap-redist-subnet
  maximum-paths ibgp 2

```

```

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

```

Nach diesem Schritt werden die NVE-Peerings für alle Loopback1-IP-Adressen zusammen mit der Loopback-IP-Adresse für mehrere Standorte angezeigt.

```

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

```

In diesem Stadium muss der Ost-West-Datenverkehr korrekt weitergeleitet werden.

Schritt 14: VRFLITE-Erweiterungen von gemeinsamen Grenzen zu externen Routern

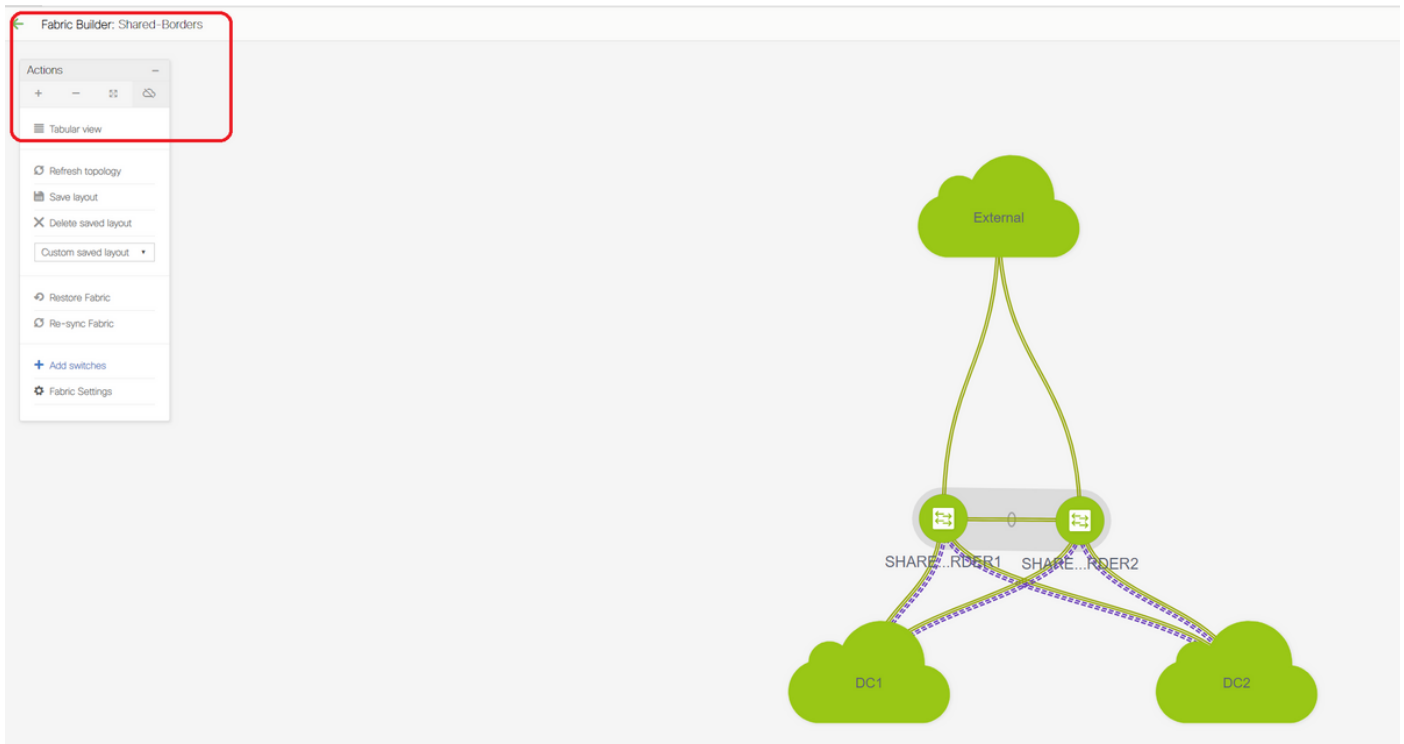
Es gibt Situationen, in denen Hosts außerhalb der Fabric mit Hosts innerhalb der Fabric kommunizieren müssen. In diesem Beispiel wird dies durch die gemeinsamen Grenzen ermöglicht.

Jeder Host, der in DC1 oder DC2 lebt, kann über die gemeinsamen Grenz-Switches mit externen Hosts kommunizieren.

Zu diesem Zweck enden gemeinsame Grenzen den VRF Lite; Hier in diesem Beispiel wird eBGP von den gemeinsamen Grenzen zu den externen Routern ausgeführt, wie im Diagramm am Anfang gezeigt.

Zum Konfigurieren von DCNM müssen **VRF-Erweiterungsanhänge** hinzugefügt werden. Im Folgenden werden Schritte zur Erreichung dieses Ziels beschrieben.

a) Hinzufügen von Fabric-übergreifenden Verbindungen zu externen Routern



Wählen Sie den Fabric Builder-Bereich auf "Shared Border" und Ändern in die Tabellenansicht.

The screenshot shows the 'Fabric Builder: Shared-Borders' interface. The 'Links' tab is selected and highlighted with a red box. Below the tabs is a toolbar with icons for adding (+), refreshing (circular arrow), editing (pencil), and deleting (power button), along with a 'View/Edit F' button. Below the toolbar is a table with two rows of links.

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

Wählen Sie die Links aus, und fügen Sie einen "Inter-Fabric"-Link hinzu (siehe unten).



* 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](#)

Aus dem Dropdown-Menü muss ein VRF-LITE-Subtyp ausgewählt werden.

Die Quell-Fabric ist eine gemeinsame Grenze, und die Ziel-Fabric ist extern, da es sich um eine VRF-LITE von SB zu Extern handelt.

Wählen Sie die relevanten Schnittstellen aus, die zum externen Router gehen

Geben Sie die IP-Adresse und -Maske sowie die IP-Adresse des Nachbarn an.

ASN wird automatisch ausgefüllt.

Klicken Sie anschließend auf Speichern

Gleiches für die gemeinsamen Grenzen und für alle externen Layer-3-Verbindungen, die sich in VRFLITE befinden

b) Hinzufügen von VRF-Erweiterungen

Gehen Sie zum Abschnitt "Shared Border VRF".

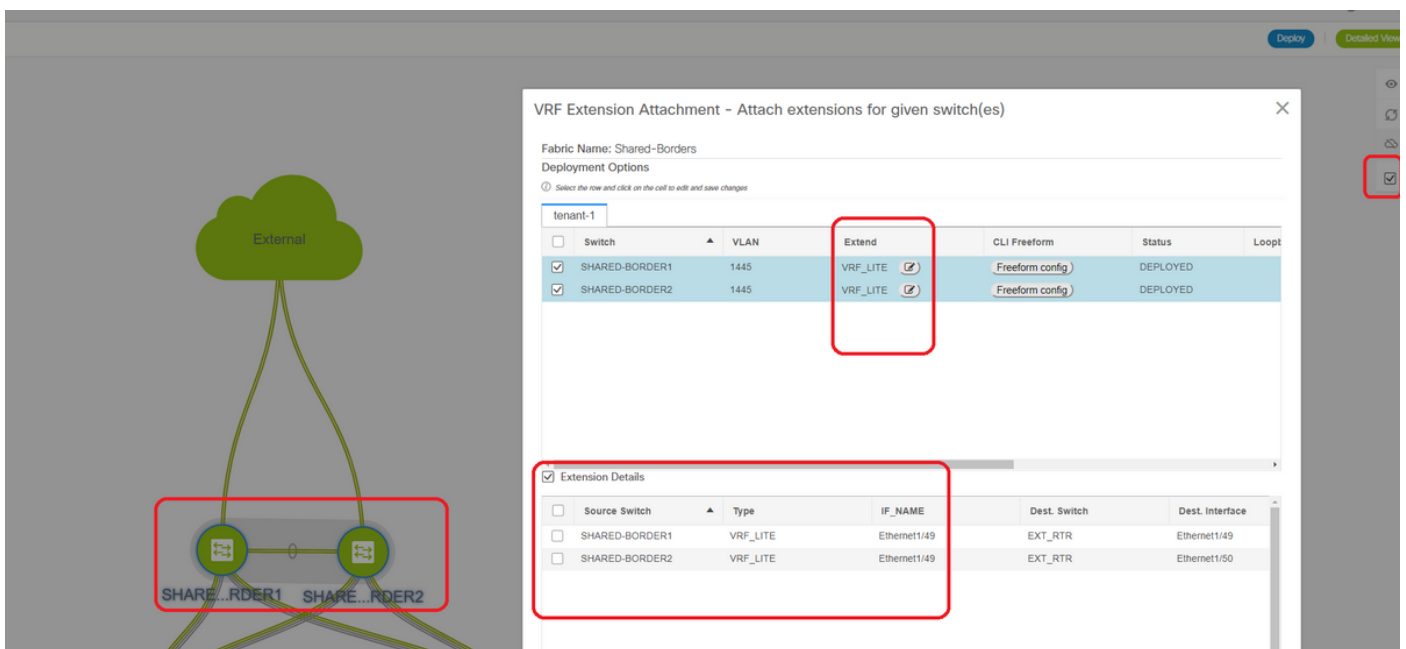
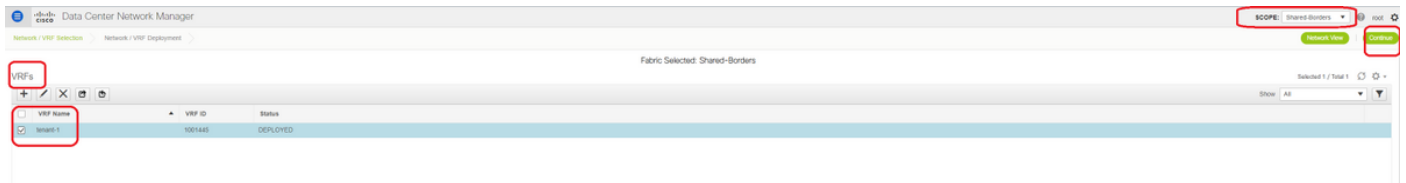
VRF ist im Bereitstellungsstatus. Aktivieren Sie das Kontrollkästchen rechts, damit mehrere Switches ausgewählt werden können.

Wählen Sie die freigegebenen Ränder aus, und das Fenster "VRF EXTension Attachment" wird geöffnet.

Ändern Sie unter "Erweitern" von "Keine" in "VRFLITE".

Gleiches für beide gemeinsam genutzten Grenzen

Danach werden mit "Extension Details" die VRF-LITE-Schnittstellen ausgefüllt, die zuvor in Schritt a) angegeben wurden.



VRF Extension Attachment - Attach extensions for given switch(es)

Fabric Name: Shared-Borders
Deployment Options

Select the row and click on the cell to edit and save changes

tenant-1

Switch	VLAN	Extend	CLI Freeform	Status	Loopback Id
<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	

Extension Details

Source Switch	Type	IF_NAME	Dest. Switch	Dest. Interface	DOT1Q ID	IP_MASK	NEIGHBOR_IP	NEIGHBOR_ASN	IPV6_MASK	IPV6_NEIGHBOR
<input checked="" type="checkbox"/> SHARED-BORDER1	VRF_LITE	Ethernet1/49	EXT_RTR	Ethernet1/49	2	172.16.22.1/24	172.16.22.2	65100		
<input checked="" type="checkbox"/> SHARED-BORDER2	VRF_LITE	Ethernet1/49	EXT_RTR	Ethernet1/50	2	172.16.22.1/24	172.16.22.2	65100		

Save

Die DOT1Q-ID wird automatisch auf 2 eingetragen.

Andere Felder werden ebenfalls automatisch ausgefüllt

Wenn IPv6-Nachbarschaft über VRFLITE eingerichtet werden muss, muss für IPv6 Schritt a durchgeführt werden.

Klicken Sie jetzt auf Speichern

Führen Sie schließlich die "Bereitstellen" oben rechts auf der Webseite.

Eine erfolgreiche Bereitstellung führt dazu, dass Konfigurationen an die gemeinsamen Grenzen verschoben werden. Dazu gehören die Einrichtung von IP-Adressen auf diesen Subschnittstellen und die Einrichtung von BGP IPv4-Nachbarschaften mit den externen Routern.

Beachten Sie, dass die Konfigurationen der externen Router (Einstellung von IP-Adressen auf Subschnittstellen und BGP Neighbourship-Anweisungen) in diesem Fall manuell von der CLI vorgenommen werden.

CLI Verifications können mithilfe der folgenden Befehle an beiden gemeinsamen Grenzen durchgeführt werden:

```
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
```

Bei allen oben genannten Konfigurationen wird die Nord-/Süd-Erreichbarkeit wie unten gezeigt festgelegt (Pings vom externen Router zu Hosts in 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
```

Traceroutes verweisen auch auf die richtigen Geräte im Paketpfad.

```
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#
```