vPC ファブリック ピアリングの設定

この章は、次の内容で構成されています。

- vPC ファブリック ピアリングの詳細 （1 ページ）
- vPC ファブリック ピアリングの注意事項と制約事項 （2 ページ）
- vPC ファブリック ピアリングの設定 （5 ページ）
- vPCから vPC ファブリック ピアリング への移行 （9 ページ）
- vPC ファブリック ピアリング 設定の確認 （12 ページ）

vPC ファブリック ピアリングの詳細

vPC ファブリック ピアリング は、vPC ピア リンクの物理ポートを無駄にすることなく、拡張デュアル ホーミング アクセス ソリューションを提供します。この機能は、従来の vPC のすべての特性を保持します。

vPC ファブリック ピアリング ソリューションを次に示します。

- 仮想メンバー（トンネル）を含む vPC ファブリック ピアリング ポートチャネル。
- vPC ファブリック ピアリング （トンネル）、物理ピアリンク要件の削除。
- vPC ファブリック ピアリング アップ/ダウン イベントは、ルートの更新とファブリックのアップ/ダウンに基づいてトリガーされます。
- 拡張障害カバレッジのアップリンク トラッキング。
- vPC ファブリック ピアリング ルーティングされたネットワーク（スパインなど）を介した到達可能性。
- vPC コントロール プレーン over TCP-IP（CFSoIP）の復元力の向上。
- VXLAN トンネル上のデータ プレーン トラフィック。
- vPC メンバー スイッチ間の通信では、VXLAN カプセル化が使用されます。
- ノード上のすべてのアップリンクに障害が発生すると、そのスイッチの vPC ポートがダウンします。このシナリオでは、vPC ピアがプライマリ ロールを引き受け、トラフィックを転送します。

- vPC のステート依存性とアップ/ダウンシグナリングによるアップリンク トラッキング。
- ポジティブ アップリンク ステート トラッキングにより、vPC プライマリ ロールの選択が促進されます。
- ボーダー リーフおよびスパインの場合、ネットワーク通信はファブリックを使用するため、VRF 単位のピアリングは必要ありません。
- VIP/PIP 機能をタイプ 2 ルートに拡張することにより、孤立したホストへの転送を強化します。
- インフラ VLAN は、vPC ファブリック ピアリングには必要ありません。

（注） 1 つの VTEP としてカウントされる通常の vPC とは異なり、vPC ファブリック ピアリング は 3 つの VTEP としてカウントされます。

vPC ファブリック ピアリングの注意事項と制約事項

次に、vPC ファブリック ピアリングの注意事項と制限事項を示します。

- Cisco Nexus 9332C、9364C、および 9300-EX/FX/FXP/FX2/FX3/GX/GX2/H2R/H1 プラットフォーム スイッチは、vPC ファブリック ピアリングをサポートします。Cisco Nexus 9200 および 9500 プラットフォーム スイッチは、vPC ファブリック ピアリングをサポートしていません。

（注） Cisco Nexus 9300-EX スイッチでは、混合モードのマルチキャストと入力レプリケーションはサポートされていません。VNI はマルチキャストまたは IR アンダーレイのいずれかで設定する必要があります。

- vPC ファブリック ピアリングでは、リージョンの **ing-flow-redirect** の TCAM カービングが必要です。TCAM カービングでは、機能を使用する前に設定を保存し、スイッチをリロードする必要があります。

（注） この要件、Cisco Nexus 9300-EX、9300-FX、9300-FX2、および 9364C プラットフォーム スイッチには適用されません。

- vPC ファブリック ピアリングの送信元および宛先 IP を再設定する前に、vPC ドメインをシャットダウンする必要があります。vPC ファブリック ピアリングの送信元と宛先のIPを調整したら、vPCドメインを有効にできます（**no shutdown**）。

- **virtual peer-link destination** コマンドでサポートされる送信元および接続先 IP は、クラス A、B、および C です。クラス D および E は、vPC ファブリック ピアリングではサポートされません。
- vPC ファブリック ピアリング ピアリンクは、トランスポート ネットワーク（ファブリックのスパイン層）を介して確立されます。vPC ピア間の通信がこのように行われると、ポート ステート情報、VLAN 情報、VLAN-to-VNI マッピング、ホスト MAC アドレスの同期に使用されるコントロール プレーン情報 CFS メッセージがファブリック経由で送信されます。CFS メッセージは、トランスポート ネットワークで保護する必要がある適切な DSCP 値でマーキングされます。次の例は、Cisco Nexus 9000 シリーズ スイッチのスパイン レイヤでの QoS 設定の例を示しています。

  DSCP 値を照合してトラフィックを分類します（DSCP 56 がデフォルト値です）。

  ```
  class-map type qos match-all CFS
    match dscp 56
  ```

  適切なスパイン スイッチの完全プライオリティ キューに対応する qos-group にトラフィックを設定します。この例では、スイッチは完全プライオリティ キュー（キュー 7）に対応する qos-group 7にトラフィックを送信します。異なる Cisco Nexus プラットフォームでは、キューイング構造が異なる場合があることに注意してください。

  ```
  policy-map type qos CFS
    class CFS
      Set qos-group 7
  ```

  VTEP（ネットワークのリーフ層）に向かうすべてのインターフェイスに分類サービス ポリシーを割り当てます。

  ```
  interface Ethernet 1/1
    service-policy type qos input CFS
  ```

- Cisco NX-OS リリース 10.1（1）以降、FEX サポートは Cisco Nexus 9300-EX/FX/FX2/FX3 プラットフォーム スイッチ IPv4 アンダーレイのために vMCT と一緒に提供されてます。
- Cisco NX-OS リリース 10.2（2）F 以降、この機能は Cisco Nexus 9300-GX プラットフォーム スイッチでサポートされます。
- vPC ファブリック ピアリング ドメインは、マルチサイト vPC BGW のロールではサポートされません。
- VIP/PIP 機能をタイプ 2 ルートに拡張して、孤立ホストへの転送を強化します。
- レイヤ 3 テナント ルーテッド マルチキャスト（TRM）はサポートされていません。レイヤ 2/レイヤ 3 TRM（混合モード）はサポートされていません。
- この機能でタイプ 5 ルートを使用する場合、この **advertise-pip** コマンドは必須設定です。
- vPC ポートの背後にある VTEP はサポートされません。これは、仮想ピアリンクピアが vPC ポートの背後にある VTEP の中継ノードとして機能できないことを意味します。
- SVI およびサブインターフェイス アップリンクはサポートされていません。

- 孤立したタイプ 2 ホストは、PIP を使用してアドバタイズされます。vPC タイプ 2 ホストは、VIP を使用してアドバタイズされます。これはタイプ 2 ホストのデフォルトの動作です。

  PIP を使用して孤立したタイプ 5 ルートをアドバタイズするには、BGP で PIP をアドバタイズする必要があります。

- リモート VTEP から孤立したホストへのトラフィックは、孤立した実際のノードに到達します。トラフィックのバウンスが回避されます。

（注） vPC レッグがダウンしている場合でも、vPC ホストは VIP IP でアドバタイズされます。

- Cisco NX-OS リリース 10.2（F）以降、ND-ISSU と LXC-ISSU は Cisco Nexus 9300-EX/FX/FXP/FX2/FX3/GX/GX2 ToR スイッチ上の IPv4 アンダーレイのために vMCT と一緒にサポートされています。
- Cisco NX-OS リリース 10.3(2)F 以降、vPC ファブリック ピアリングは Cisco Nexus 9300-EX/FX/FXP/FX2/FX3/GX/GX2 ToR スイッチの IP6 アンダーレイに対してサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、vPC ファブリック ピアリングは、Cisco Nexus 9332D-H2R スイッチの IPv6 アンダーレイでサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、vPC ファブリック ピアリングは、Cisco Nexus 93400LD-H1 スイッチの IPv6 アンダーレイでサポートされます。
- Cisco NX-OS リリース 10.4(3)F 以降、vPC ファブリック ピアリングは、Cisco Nexus 9364C-H1 スイッチの IPv6 アンダーレイでサポートされます。
- Cisco NX-OS リリース 10.3(2)F 以降、ND-ISSU と LXC-ISSU は Cisco Nexus 9300-EX/FX/FXP/FX2/FX3/GX/GX2 ToR スイッチ上の IPv6 アンダーレイに対して vMCT と一緒にサポートされます。
- IPv6 アンダーレイの vMCT は、FEX の接続をサポートしていません。
- ファブリック ピアリングから物理ピア リンクに変換した直後に、両方のピアで次の変更を行います。

  1. **hardware access-list tcam region ing-flow-redirect 0** コマンドを使用して、TCAM リージョンをグローバルに設定します。
  2. 必要に応じて、空き領域を他のクラスに割り当てます。詳細については、Nexus 9000 TCAM スペースの切り分け方法を理解するを参照してください。
  3. **copy running-config startup-config** コマンドを使用して、実行コンフィギュレーションを保存します。
  4. スイッチをリロードします。

- 孤立ポートの vPC ファブリック ピアリングと物理ピア リンクでは、ARP の動作が異なります。 vPC ファブリック ピアリングは、物理ピア リンクの場合のように ARP エントリを同期しません。孤立したタイプ 2 ホストは、PIP を使用して vPC ファブリック ピアリングでアドバタイズされます。
- 孤立したポートについては、NVE 障害シナリオにおけるトラフィックの中断を回避するために、両方の vPC ノードで **vpc orphan-port suspend** コマンドを実行しておくことを強くお勧めします。

vPC ファブリック ピアリングの設定

両方の vPC メンバー スイッチで vPC ファブリック ピアリング DSCP 値が一致していることを確認します。対応する QoS ポリシーが vPC ファブリック ピアリング DSCP マーキングと一致することを確認します。

vPC ファブリック ピアリング を通過する通信を必要とするすべての VLAN は、VXLAN を有効にする必要があります（vn-segment）。これにはネイティブ VLAN が含まれます。

（注） MSTP では、ピアリンクと vPC レッグにデフォルトのネイティブ VLAN 設定がある場合、VLAN 1 は vPC ファブリック ピアリング全体に拡張する必要があります。この動作は、VLAN 1 を VXLAN（vn-segment）経由で拡張することで実現できます。ピアリンクおよび vPC レッグにデフォルト以外のネイティブ VLAN がある場合は、VLAN を VXLAN（vn-segment）に関連付けることによって、それらの VLAN を vPC ファブリック ピアリング全体に拡張する必要があります。

show vpc virtual-peerlink vlan consistency コマンドを使用して、vPC ファブリック ピアリングに使用する既存の VLAN-to-VXLAN マッピングを確認します。

vPC ファブリック ピアリング の **peer-keepalive** コマンドは、次のいずれかの設定でサポートされます。

- 管理インターフェイス
- デフォルトまたは非デフォルト VRF の専用レイヤ 3 リンク
- スパイン経由で到達可能なループバック インターフェイス。

機能の設定

例では、アンダーレイ ルーティング プロトコルとして OSPF を使用しています。

```
configure terminal
nv overlay evpn
feature ospf
feature bgp
feature pim
feature interface-vlan
feature vn-segment-vlan-based
```

```
feature vpc

feature nv overlay
```

vPC の設定

（注） vPC ファブリック ピアリング 送信元または宛先 IP を変更するには、変更前に vPC ドメインをシャットダウンする必要があります。vPC ドメインは、**no shutdown** コマンドを使用して変更後に動作に戻すことができます。

TCAM カービングの設定

```
hardware access-list tcam region ing-racl 0
hardware access-list tcam region ing-sup 768
hardware access-list tcam region ing-flow-redirect 512
```

（注）

- ファブリック vPC ピアリングを設定する場合、Ingress-Flow-redirect TCAM リージョン サイズの最小サイズは 512 です。また、TCAM リージョン サイズが常に 512 の倍数で構成されていることを確認します。
- **ing-flow-redirect** リージョン の TCAM カービングは、Cisco Nexus 9300-FX3/GX/GX2/H2R/H1 プラットフォーム スイッチではサポートされません。
- TCAM カービングを有効にするには、スイッチのリロードが必要です。

vPC ドメインの設定

インターネット ユーザに商品やサービスを提供する IPv4

```
vpc domain 100
peer-keepalive destination 192.0.2.1
virtual peer-link destination 192.0.2.100 source 192.0.2.20/32 [dscp <dscp-value>]
Warning: Appropriate TCAM carving must be configured for virtual peer-link vPC
peer-switch
peer-gateway
ip arp synchronize
ipv6 nd synchronize
exit
```

IPv6 の場合

```
vpc domain 100
peer-keepalive destination 192:0:2::1
virtual peer-link destination 192:0:2::100 source 192:0:2::20/32 [dscp <dscp-value>]
Warning: Appropriate TCAM carving must be configured for virtual peer-link vPC
peer-switch
peer-gateway
ipv6 arp synchronize
ipv6 nd synchronize
exit
```

（注） オプションの **dscp** キーワード。範囲は 1 ～ 63 です。デフォルト値は 56 です。

vPC ファブリック ピアリング ポート チャネルの設定

次のポート チャネルのメンバーを設定する必要はありません。

```
interface port-channel 10
switchport
switchport mode trunk
vpc peer-link
```

interface loopback0

（注） このループバックは、NVE 送信元インターフェイス ループバック（VTEP IP アドレスに使用されるインターフェイス）ではありません。

インターネット ユーザに商品やサービスを提供する IPv4

```
interface loopback 0
ip address 192.0.2.20/32
ip router ospf 1 area 0.0.0.0
```

IPv6 の場合

```
interface loopback 0
ipv6 address 192:0:2::20/32
ipv6 router ospfv3 1 area 0.0.0.0
```

（注） BGP ピアリングまたは専用ループバックにループバックを使用できます。このルックバックは、ピアのキープ アライブとは異なる必要があります。

アンダーレイ インターフェイスの設定

L3 物理チャネルと L3 ポート チャネルの両方がサポートされます。SVI およびサブインターフェイスはサポートされていません。

インターネット ユーザに商品やサービスを提供する IPv4

```
router ospf 1
interface Ethernet1/16
port-type fabric
ip address 192.0.2.2/24
ip router ospf 1 area 0.0.0.0
no shutdown
interface Ethernet1/17
port-type fabric
ip address 192.0.2.3/24
ip router ospf 1 area 0.0.0.0
no shutdown
interface Ethernet1/40
port-type fabric
ip address 192.0.2.4/24
```

```
ip router ospf 1 area 0.0.0.0
no shutdown
interface Ethernet1/41
port-type fabric
ip address 192.0.2.5/24
ip router ospf 1 area 0.0.0.0
no shutdown
```

IPv6 の場合

```
router ospfv3 1
interface Ethernet1/16
port-type fabric
ipv6 address 192:0:2::2/24
ipv6 router ospfv3 1 area 0.0.0.0
no shutdown
interface Ethernet1/17
port-type fabric
ipv6 address 192:0:2::3/24
ipv6 router ospfv3 1 area 0.0.0.0
no shutdown
interface Ethernet1/40
port-type fabric
ipv6 address 192:0:2::4/24
ipv6 router ospfv3 1 area 0.0.0.0
no shutdown
interface Ethernet1/41
port-type fabric
ipv6 address 192:0:2::5/24
ipv6 router ospfv3 1 area 0.0.0.0
no shutdown
```

（注） スパインに接続されるすべてのポートは、ポートタイプのファブリックである必要があります。

VXLAN 設定

（注） **advertise virtual-rmac**（NVE）と **advertise-pip**（BGP）の設定は必須の手順です。詳細については、vPC マルチホーミングの構成 の章を参照してください。

SVI および VLAN の設定

```
vlan 10
vn-segment 10010
vlan 101
vn-segment 10101

interface Vlan101
no shutdown
mtu 9216
vrf member vxlan-10101
no ip redirects
ip forward
ipv6 address use-link-local-only
no ipv6 redirects
interface vlan10
```

```
no shutdown
mtu 9216
vrf member vxlan-10101
no ip redirects
ip address 192.0.2.102/24
ipv6 address 2001:DB8:0:1::1/64
no ipv6 redirects
fabric forwarding mode anycast-gateway
```

仮想ポート チャネルの設定

```
interface Ethernet1/3
switchport
switchport mode trunk
channel-group 100
no shutdown
exit
interface Ethernet1/39
switchport
switchport mode trunk
channel-group 101
no shutdown
interface Ethernet1/46
switchport
switchport mode trunk
channel-group 102
no shutdown
interface port-channel100
vpc 100
interface port-channel101
vpc 101
interface port-channel102
vpc 102
exit
```

vPCから vPC ファブリック ピアリング への移行

この手順には、通常の vPC から vPC ファブリック ピアリング への移行手順が含まれています。

vPC ピア間の直接レイヤ 3 リンクは、ピアキープ アライブにのみ使用する必要があります。このリンクは、vPC ファブリック ピアリング ループバックのパスをアドバタイズするために使用しないでください。

（注） この移行は中断を伴います。

始める前に

移行前に、vPC ピア間のすべての物理レイヤ 2 リンクをシャットダウンすることを推奨します。また、移行前または移行後に VLAN を vn-segment にマッピングすることを推奨します。

手順の概要

1. **configure terminal**
2. **show vpc**
3. **show port-channel summary**
4. **interface ethernet** *slot/port*
5. **no channel-group**
6. インターフェイスごとにステップ 4 と 5 を繰り返します。
7. **show running-config vpc**
8. **vpc domain** *domain-id*
9. **virtual peer-link destination** *dest-ip* **source** *source-ip*
10. **interface {ethernet | port-channel}** *value*
11. **port-type fabric**
12. （任意） **show vpc fabric-ports**
13. **virtual peer-link destination** *dest-ip* | *dest_ipv6* **source** *source-ip* | *source_ipv6* **dhcp** *dhcp_val*
14. **hardware access-list tcam region ing-flow-redirect** *tcam-size*
15. **copy running-config startup-config**
16. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**show vpc** 例： `switch(config)# show vpc`	ポート チャネルのメンバー数を決定します。
ステップ 3	**show port-channel summary** 例： `switch(config)# show port-channel summary`	メンバーの数を決定します。
ステップ 4	**interface ethernet** *slot/port* 例： `switch(config)# interface ethernet 1/4`	設定するインターフェイスを指定します。 （注） これは、ピアリンク ポート チャネルです。
ステップ 5	**no channel-group** 例： `switch(config-if)# no channel-group`	vPC ピアリンク ポート チャネル メンバーを削除します。 （注） このステップの後に中断が発生します。

	コマンドまたはアクション	目的
ステップ 6	インターフェイスごとにステップ 4 と 5 を繰り返します。 例： `switch(config-if)# show running-config vpc`	
ステップ 7	**show running-config vpc** 例： `switch(config-if)# show running-config vpc`	vPC ドメインを決定します。
ステップ 8	**vpc domain** *domain-id* 例： `switch(config-if)# vpc domain 100`	vPC ドメイン コンフィギュレーション モードを入力します。
ステップ 9	**virtual peer-link destination** *dest-ip* **source** *source-ip* 例： `switch(config-vpc-domain)# virtual peer-link destination 192.0.2.1 source 192.0.2.100`	vPC ファブリック ピアリングの宛先および送信元 IP アドレスを指定します。
ステップ 10	**interface {ethernet | port-channel}** *value* 例： `switch(config-if)# interface Ethernet1/17`	構成する L3 アンダーレイ インターフェイスを指定します。
ステップ 11	**port-type fabric** 例： `switch(config-if)# port-type fabric`	アンダーレイ インターフェイスのポート タイプ ファブリックを設定します。 （注） スパインに接続されるすべてのポートは、ポートタイプのファブリックである必要があります。
ステップ 12	（任意） **show vpc fabric-ports** 例： `switch# show vpc fabric-ports`	スパインに接続されているファブリック ポートを表示します。
ステップ 13	**virtual peer-link destination** *dest-ip* | *dest_ipv6* **source** *source-ip* | *source_ipv6* **dhcp** *dhcp_val* 例： インターネット ユーザに商品やサービスを提供する IPv4 `switch(config-vpc-domain)# virtual peer-link destination 192.0.2.1 source 192.0.2.100 dhcp 56` 例： IPv6 の場合	vPC ファブリック ピアリングの宛先および送信元 IPv4/IPv6 アドレスを指定します。 （注） IPv4 vPC ファブリック ピアリング構成は IPv4 VXLAN アンダーレイでのみ機能し、IPv6 vPC ファブリック ピアリング構成は IPv6 VXLAN アンダーレイでのみ機能します。

	コマンドまたはアクション	目的
	`switch(config-vpc-domain)# virtual peer-link destination 6001:aaa::11 source 6001:aaa::22 dhcp 56`	
ステップ 14	**hardware access-list tcam region ing-flow-redirect** *tcam-size* 例： `switch(config-vpc-domain)# hardware access-list tcam region ing-flow-redirect 512`	TCAM カービングを実行します。 入力フローリダイレクト TCAM リージョン サイズの最小サイズは 512 です。また、512 の倍数で構成されていることを確認します。
ステップ 15	**copy running-config startup-config** 例： `switch(config-vpc-domain)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 16	**reload** 例： `switch(config-vpc-domain)# reload`	スイッチをリブートします。

vPC ファブリック ピアリング 設定の確認

vPC ファブリック ピアリング 設定のステータスを表示するには、次のコマンドを入力します。

表 *1 : vPC* ファブリック ピアリング 検証コマンド

コマンド	目的
show vpc fabric-ports	ファブリック ポートの状態を表示します。
show vpc	vPC ファブリック ピアリング モードに関する情報を表示します。
show vpc virtual-peerlink vlan consistency	vn-segment に関連付けられていない VLAN を表示します。

show vpc fabric-ports コマンドの例

```
switch# show vpc fabric-ports
Number of Fabric port : 9
Number of Fabric port active : 9

Fabric Ports State
-------------------------------------
Ethernet1/9 UP
Ethernet1/19/1 ( port-channel151 ) UP
Ethernet1/19/2 ( port-channel151 ) UP
Ethernet1/19/3 UP
Ethernet1/19/4 UP
```

```
Ethernet1/20/1 UP
Ethernet1/20/2 ( port-channel152 ) UP
Ethernet1/20/3 ( port-channel152 ) UP
Ethernet1/20/4 ( port-channel152 ) UP
```

show vpc コマンドの例

```
switch# show vpc
Legend:
                 (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 3
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 1
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled, timer is off.(timeout = 240s)
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Disabled
Virtual-peerlink mode             : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id    Port   Status Active vlans
--    ----   ------ -------------------------------------------------
1     Po100  up     1,56,98-600,1001-3401,3500-3525

vPC status
----------------------------------------------------------------------------
Id    Port          Status Consistency Reason                Active vlans
--    ------------  ------ ----------- ------                ---------------
101   Po101         up     success     success               98-99,1001-280
                                                             0

Please check "show vpc consistency-parameters vpc <vpc-num>" for the
consistency reason of down vpc and for type-2 consistency reasons for
any vpc.

ToR_B1#
```

show vpc virtual-peerlink vlan 整合性コマンドの例

```
switch# show vpc virtual-peerlink vlan consistency
Following vlans are inconsistent
23
switch#
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。