

Nexus 7000 シリーズ スイッチでのレイヤ 2 vPC Data Center Interconnect の設定

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[FHRP 分離](#)

[デュアル L2/L3 POD 相互接続](#)

[集約と DCI のためのマルチレイヤ vPC](#)

[分離のその他の設定](#)

[MACSec 暗号化](#)

[確認](#)

[FHRP 分離](#)

[その他の分離](#)

[MACSec 暗号化](#)

[トラブルシューティング](#)

[警告](#)

[関連情報](#)

概要

このドキュメントでは、仮想 Port-Channel (vPC) を使用したレイヤ 2 (L2) データセンター相互接続 (DCI) を設定する方法について説明します。

前提条件

このドキュメントに記載されている例で使用されるデバイスに、vPC および Hot Standby Router Protocol (HSRP) があらかじめ設定されていることを前提とします。

注: DCI として機能する vPC リンク上では、Link Aggregation Control Protocol (LACP) を使用する必要があります。

ヒント : MACsec の暗号化には、バージョン 6.1(1) より前のバージョンの LAN アドバンスド サービス ライセンスが必要で、ラインカード固有の制限事項があります。 詳細について

は、『Cisco Nexus 7000 シリーズ NX-OS セキュリティの設定ガイド リリース 6.x』の「[Cisco TrustSec のガイドラインおよび制限事項](#)」の項を参照してください。

要件

次の項目に関する知識が推奨されます。

- vPC
- HSRP
- スパニング ツリー プロトコル (STP)
- MACSec 暗号化 (オプション)

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 6.2(8b) が稼働する Cisco Nexus 7000 シリーズ スイッチに基づくものです。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

DCI の目的は、遠く離れたサーバとネットワークアタッチドストレージ (NAS) デバイスについて L2 隣接関係を提供するような、異なるデータセンター間で特定の VLAN を拡張することです。

vPC は、2 つのサイト間での STP 分離 (DCI vPC を横断するブリッジ プロトコル データ ユニット (BPDU) なし) のメリットを示すので、データセンターで何かしらのシステム停止が発生しても、データセンター間で冗長なリンクが提供され続けるので、リモート データセンターにはシステム停止の影響が及びません。

注: vPC を使用して、最大 2 つのデータセンターを相互接続できます。2 つを超えるデータセンターを相互接続する必要がある場合、オーバーレイトランスポート仮想化 (OTV) を使用することをお勧めします。

DCI vPC イーサチャネルは、通常この情報を念頭に設定されています。

- First Hop Redundancy Protocol (FHRP) 分離 : 各データセンター専用のゲートウェイを使用した最適でないルーティングを防止します。構成は、VRRP ゲートウェイの場所によって異なります。
- STP 分離 : これにより、前述したように、あるデータセンターから別のデータセンターにシステム停止の影響が伝播しなくなります。

- ブロードキャスト ストーム制御：これは、データセンター間でブロードキャスト トラフィックの量を最小化するのに使用されます。
- MACsec 暗号化 (オプション)：これにより、2 つの施設の間に侵入されるのを防ぐために、トラフィックが暗号化されます。

設定

vPC を使用して L2 DCI を設定するには、この項に記載されている情報を活用してください。

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

FHRP 分離

この項では、FHRP 分離を実装できる 2 つのシナリオについて説明します。

デュアル L2/L3 POD 相互接続

これは、このシナリオで使用されるトポロジです。

このシナリオでは、同じ vPC のペアでレイヤ 3 (L3) ゲートウェイが設定され、DCI として機能します。HSRP を分離するには、DCI ポート チャンネルでポート アクセス コントロール リスト (PACL) を設定し、DCI を横断して移動する VLAN 用のスイッチ仮想インターフェイス (SVI) 上で HSRP Gratuitous Address Resolution Protocol (ARP) (GARP) を無効にする必要があります。

次に設定例を示します。

```
ip access-list DENY_HSRP_IP
 10 deny udp any 224.0.0.2/32 eq 1985
 20 deny udp any 224.0.0.102/32 eq 1985
 30 permit ip any any

interface <DCI-Port-Channel>
 ip port access-group DENY_HSRP_IP in

interface Vlan <x>
 no ip arp gratuitous hsrp duplicate
```

注: Nexus 9000 スイッチでは以前の設定を使用できます。

集約と DCI のためのマルチレイヤ vPC

これは、このシナリオで使用されるトポロジです。

このシナリオでは、DCI は独自の L2 仮想デバイス コンテキスト (VDC) で分離され、L3 ゲート

ウェイはアグリゲーションレイヤデバイス上にあります。HSRPを分離するには、HSRPコントロールトラフィックをブロックするVLANアクセスコントロールリスト(VACL)と、HSRPGARPをブロックするARP検査フィルタを設定する必要があります。

次に設定例を示します。

```
ip access-list ALL_IPs
 10 permit ip any any
mac access-list ALL_MACs
 10 permit any any
ip access-list HSRP_IP
 10 permit udp any 224.0.0.2/32 eq 1985
 20 permit udp any 224.0.0.102/32 eq 1985
mac access-list HSRP_VMAC
 10 permit 0000.0c07.ac00 0000.0000.00ff any
 20 permit 0000.0c9f.f000 0000.0000.0fff any
vlan access-map HSRP_Localization 10
 match ip address HSRP_IP
 match mac address HSRP_VMAC
 action drop
 statistics per-entry
vlan access-map HSRP_Localization 20
 match ip address ALL_IPs
 match mac address ALL_MACs
 action forward
 statistics per-entry
vlan filter HSRP_Localization vlan-list <DCI_Extended_VLANs>

feature dhcp

arp access-list HSRP_VMAC_ARP
 10 deny ip any mac 0000.0c07.ac00 ffff.ffff.ff00
 20 deny ip any mac 0000.0c9f.f000 ffff.ffff.f000
 30 permit ip any mac any

ip arp inspection filter HSRP_VMAC_ARP vlan <DCI_Extended_VLANs>
```

分離のその他の設定

この項では、次のような設定例を示します。

- リモート データセンターで必要とされている VLAN のみを延長できます。
- 各データセンターで STP を分離します。
- 総リンク速度の 1% を超えるブロードキャストトラフィックをドロップします。

次に設定例を示します。

```
interface <DCI-Port-Channel>
 switchport trunk allowed vlan <DCI_Extended_VLANs>
 spanning-tree port type edge trunk
 spanning-tree bpdudfilter enable
 storm-control broadcast level 1.0
```

注: マルチキャストトラフィックのストーム制御も設定できますが、ブロードキャストトラフィックと同じパーセンテージである必要があります。

MACsec 暗号化

注: この項で説明する設定は任意です。

MACSec の設定には次の情報を使用します。

```
feature dot1x
feature cts

! MACSec requires 24 additional bytes for encapsulation.
interface <DCI-Port-Channel>
  mtu 1524

interface <DCI-Physical-Port>
  cts manual
  no propagate-sgt
  sap pmk <Preshared-Key>
```

注: MACsec の認証が行われるようにするには、インターフェイスをフラップする必要があります。

確認

この項で説明されている情報を活用し、設定が適切に機能することを確認してください。

FHRP 分離

CLI に **show hsrp br** コマンドを入力し、HSRP ゲートウェイが両方のデータセンターでアクティブであるか確認します。

```
!DC-1
N7K-A# show hsrp br
*:IPv6 group   #:group belongs to a bundle
                P indicates configured to preempt.
                |
Interface      Grp  Prio P State      Active addr      Standby addr      Group addr
Vlan10         10  120  Active local      10.1.1.3          10.1.1.5
(conf)
```

```
!DC-2
N7K-C# show hsrp br
*:IPv6 group   #:group belongs to a bundle
                P indicates configured to preempt.
                |
Interface      Grp  Prio P State      Active addr      Standby addr      Group addr
Vlan10         10  120  Active local      10.1.1.3          10.1.1.5
(conf)
```

CLI に次のコマンドを入力し、ARP フィルタを検証します。

```
N7K-D# show log log | i DUP_VADDR
```

```
2015 Apr 10 21:16:45 N7K-A %ARP-3-DUP_VADDR_SRC_IP: arp [7915] Source address of
packet received from 0000.0c9f.f00a on Vlan10(port-channel102) is duplicate of local
virtual ip, 10.1.1.5
```

ここに示すような出力が表示された場合は、2つのアクティブなゲートウェイ間で GARP 適切に分離されていません。

その他の分離

CLI に `show spanning-tree root` コマンドを入力し、STP ルートが DVI ポート チャネルのほうをポイントしていないことを検証します。

```
N7K-A# show spanning-tree root
```

```

          Root  Hello Max Fwd
Vlan          Root ID      Cost  Time  Age Dly  Root Port
-----
VLAN0010      4106 0023.04ee.be01      0    2   20  15  This bridge is root
```

CLI に次のコマンドを入力し、ストーム制御が適切に設定されているか検証します。

```
N7K-A# show interface <DCI-Port-Channel> counters storm-control
```

```
-----
Port          UcastSupp %      McastSupp %      BcastSupp %      TotalSuppDiscards
-----
Po103          100.00           100.00            1.00                0
```

MACsec 暗号化

CLI に次のコマンドを入力し、MACsec の暗号化が適切に設定されていることを検証します。

```
N7K-A# show cts interface <DCI-Physical-Port>
```

```
CTS Information for Interface Ethernet3/41:
```

```
...
```

```
SAP Status:          CTS_SAP_SUCCESS
  Version: 1
  Configured pairwise ciphers: GCM_ENCRYPT
  Replay protection: Enabled
  Replay protection mode: Strict
  Selected cipher: GCM_ENCRYPT
  Current receive SPI: sci:e4c7220b98dc0000 an:0
  Current transmit SPI: sci:e4c7220b98d80000 an:0
```

```
...
```

トラブルシューティング

FHRP またはその他の分離設定に関して利用できるような、具体的なトラブルシューティング情報は現在ありません。

MACSec 設定の場合、リンクの両側で事前共有キーが合意されていないと、`show interface <DCI-Physical-Port>` コマンドを CLI に入力すると、次のような出力が表示されます。

```
N7K-A# show interface <DCI-Physical-Port>
Ethernet3/41 is down (Authorization pending)
admin state is up, Dedicated Interface
```

注: キーは、接続の両側で同じにする必要があります。

警告

注: 関連製品の注意事項は含まれていません。

次の注意事項は、Cisco Nexus 7000 シリーズ スイッチ上で DCI を使用する場合に関連します。

- Cisco Bug ID [CSCur69114](#) : HSRP PACL フィルタの破損 - パケットがレイヤ 2 ドメインにフラッピングしている。この不具合は、ソフトウェア バージョン 6.2(10) でのみ発生します。
- Cisco Bug ID [CSCut75457](#) : HSRP VACL フィルタの破損。この不具合は、ソフトウェア バージョン 6.2(10) および 6.2(12) でのみ発生します。
- Cisco Bug ID [CSCut43413](#) : DCI: HSRP 仮想 MAC が FHRP 分離 PACL 経由でフラッピングする。この不具合は、ハードウェアの制限が原因です。

関連情報

- [データセンター デザイン: データセンターの相互接続ページ](#)
- [OTV 技術の概要と導入の考慮事項ページ](#)
- [Cisco 仮想化ワークロード モビリティ デザインの考慮事項ページ](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)