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

内容

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。

DCIとして機能するvPCリンクでLink Aggregation Control Protocol(LACP)を使用します。

ヒント: MACSec暗号化には、バージョン6.1(1)より前のバージョンのLAN Advanced Servicesライセンスが必要で、ラインカード固有の制限があります。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あることが推奨されます。

- vPC
- HSRP
- Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）
- 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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

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。

vPCを使用して、最大2つのデータセンターを相互接続します。2つ以上のデータセンターを相互接続する必要がある場合は、Overlay Transport Virtualization(OTV)を使用します。

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：各データセンターに専用のゲートウェイを使用することで、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の分離：前述したように、これにより、あるデータセンターから別のデータセンターへの停止の伝播が防止されます。
- ブロードキャストストーム制御：これは、データセンター間のブロードキャストトラフィックの量を最小限に抑えるために使用されます。
- MACSec暗号化（オプション）:2つのファシリティ間の侵入を防ぐために、トラフィックを暗号化します。

設定

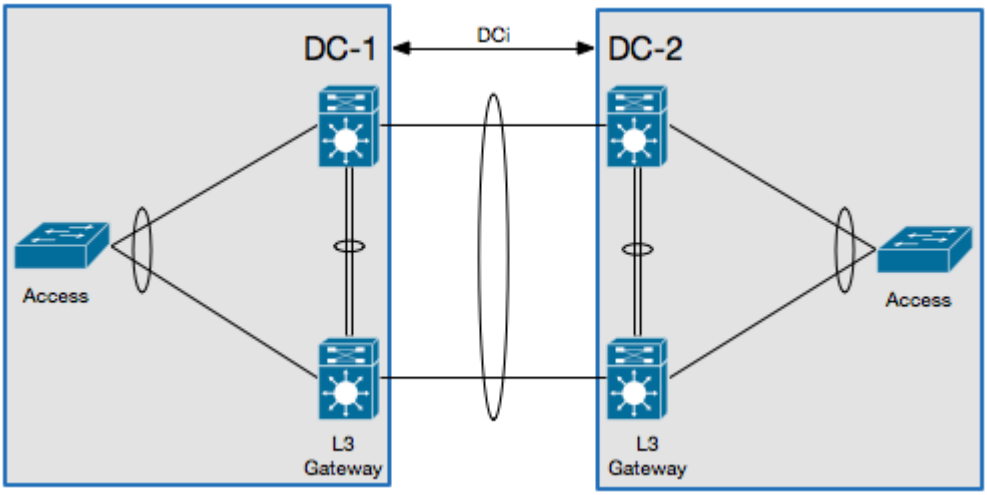
このセクションで説明する情報を使用して、vPCを使用するL2 DCIを設定します。登録ユーザは、Command Lookup Tool（登録ユーザ専用）を使用して、ここで使用されているコマンドの詳細を取得できます。

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ポートチャネル上にポートアクセスコントロールリスト(PACL)を設定し、DCIを移動するVLANのスイッチ仮想インターフェイス(SVI)上でHSRP Gratuitousアドレス解決プロトコル(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。

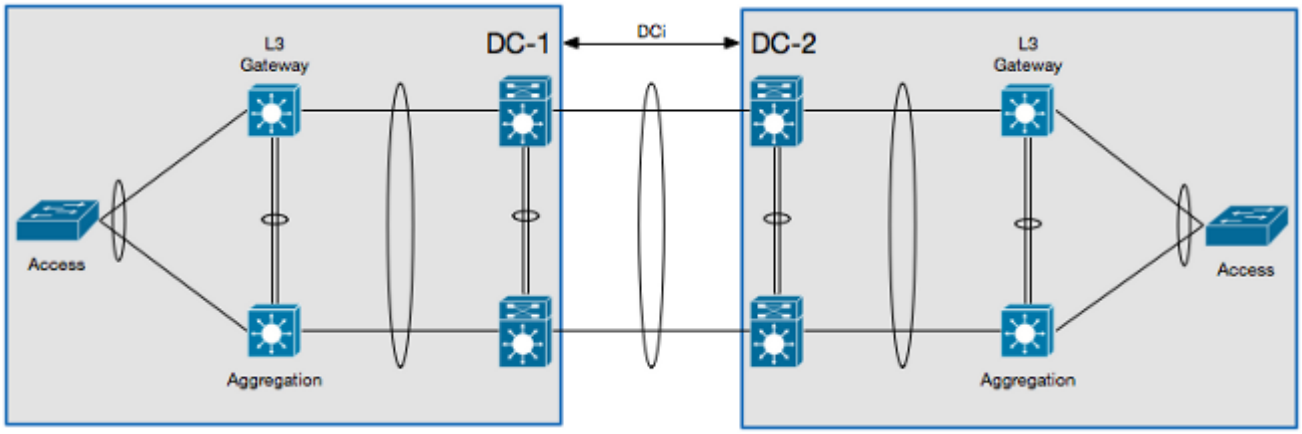
```
ip access-list DENY_HSRP_IP
  10 deny udp any 224.0.0.2/32 eq 1985
  20 deny udp any 224.0.0.102/32 eq 1985
  30 permit ip any any

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

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

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を隔離するには、HSRP制御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、L2 DCI VDC上のHSRP GARPをブロックするARPインスペクションフィルタを設定します。設定例：

```
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なVLANだけを拡張できる
- 各データセンターでSTPを分離
- 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する

設定例：

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

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

このセクションで説明する設定はオプションです。

次の情報を使用して、MACSec暗号化を設定します。

```
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>
```

MACSec許可が発生するようにインターフェイスをフラップします。

確認

このセクションで説明されている情報を使用して、設定が正しく動作していることを確認します。

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。

<#root>

```
!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フィルタを確認します。

<#root>

```
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DCIポートチャネルをポイントしていないことを確認します。

<#root>

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、ストーム制御が正しく設定されていることを確認します。

<#root>

N7K-A#

show interface

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暗号化が正しく設定されていることを確認します。

<#root>

N7K-A#

show cts interface

```
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。

<#root>

N7K-A#

show interface

```
Ethernet3/41 is down (Authorization pending)
admin state is up, Dedicated Interface
```

キーは、接続の両側で同じにする必要があります。

警告

これらの警告は、Cisco Nexus 7000シリーズスイッチでのDCIの使用に関連するものです。関連製品に関する警告は含まれていません。

- Cisco Bug ID CSCur69114 : HSRP PACL フィルタの破損 - パケットがレイヤ 2 ドメインにフラッディングしている。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

- Cisco ソリューション
- 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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。