VXLAN BGP-EVPN Null ルートの構成

この章は、次の内容で構成されています。

- EVPN null ルートについて （1 ページ）
- VXLAN BGP-EVPN null ルートの注意事項および制限事項 （2 ページ）
- スタティック MAC の構成 （3 ページ）
- ARP/ND の構成 （4 ページ）
- ローカル VTEP でのプレフィックス ヌル ルートの構成 （6 ページ）
- リモート VTEP での RPM ルート マップの構成 （8 ページ）
- Null ルートの構成例 （9 ページ）
- EVPN Null ルート構成の確認 （11 ページ）

EVPN null ルートについて

EVPN ファブリック内のホストに対する分散型サービス拒否（DDoS）攻撃は、ネットワーク帯域幅技術情報を消費し、他のホストへの正当なトラフィックに影響を与えます。

DDoS 攻撃は、次の設定のいずれかから発生する可能性があります：

- ローカル サイト内のリーフ スイッチに接続されたホスト
- リモート サイトのリーフ スイッチに接続されたホスト
- WAN などの外部ネットワーク

DDoS 攻撃は、サブネット内（MAC ベース）またはサブネット間（ホスト ベース – IPv4/IPv6）の可能性があります。

null ルート フィルタ処理は、特にサービス プロバイダ ネットワークで DDoS 攻撃を軽減するために伝統的に使用されてきました。

null ルートは、どこへも到達しないネットワーク ルート（ルーティング テーブル エントリ）です。このルートに一致したパケットは、転送されるのではなくドロップ（無視またはリダイレクト）されるので、このルートは一種の制限付きファイアウォールとして機能します。null ルートを使用する行為は、多くの場合、null ルート フィルタリングと呼ばれます。

NX-OS には、IPv4/IPv6/MAC の null/drop ルートを構成するメカニズムがすでにあります。null ルートは、ファブリック内のすべての VTEP で構成する必要があります。

IPv4/IPv6 ベースの攻撃の場合、次のコマンドを使用して、null インターフェイスで IPv4/IPv6 スタティック ルートを構成します：

- **ip route x.x.x.x/y Null0**
- **ipv6 route X:X:X::X/Y Null0**

MAC ベースの攻撃の場合、次のコマンドを使用して、パケットをドロップするように drop 隣接関係を持つ MAC アドレスを構成します。

- **mac address-table static xxxx.yyyy.zzzz vlan <VLAN-ID> drop**

多数の VTEP があり、複数のサイトにまたがるファブリックでは、Nexus Dashboard Fabric Controller（NDFC）や他の Orchestrator がない場合、すべての VTEP に手動で drop ルートを構成および管理するのは困難な作業です。

EVPN null ルーティング機能は、NDFC やその他のオーケストレータなど、中央の場所から null ルートを構成して挿入する方法がない場合に使用されます。

EVPN null ルーティング機能により、ネットワーク内の VTEP は、特定のコミュニティでタグ付けされたタイプ 2 およびタイプ 5 ルートを送信できます。

シングルサイトおよびマルチサイトの他のVTEP（ボーダーおよびリーフ）は、MACまたはIP（IPv4/IPv6）テーブルでエントリをインストールすることが可能で、個別に MAC または IP 宛てのトラフィックはエッジまたはリーフ スイッチでドロップされ、サイト内およびサイト全体の帯域幅の使用を防止します。

プログラムされた null ルート エントリは、ホスト IP（/32 または /128）、プレフィックス（VLSM）、または MAC です。

VXLAN BGP-EVPN null ルートの注意事項および制限事項

- null ルート（静的）MAC 構成には、一致する静的 ARP/ND 構成が必要です。つまり、MAC が null ルート MAC として構成されているダイナミック ARP/ND を使用してはなりません。
- L2 サービスのみを使用している場合（かつダイナミック ARP/ND 学習につながる構成がない場合）、「MAC ドロップ」構成のみが許可されます。他のすべての場合、「MAC ドロップ」構成とともに静的 ARP/ND 構成も必要になります。
- vPC の場合、null ルート（MAC、mac-ip、プレフィックス）を両方の vPC ボックス（VMCT と PMCT）で構成する必要があります。これが両方のボックスで構成されていない場合、動作は未定義です。同じことが、null ルートの構成解除中にも当てはまります。この機能の vPC 整合性チェッカーはサポートされていません。
- ルートマップは、リモート VTEP に適用する必要があります。この入力ルートマップは、タイプ 5 ルートにとって重要です。

- マルチキャスト トラフィックとの機能の相互作用はありません。
- VTEP でリモート スタティックが表示され、同じ MAC をローカル スタティック（有効なインターフェイスを持つ静的MAC、またはドロップ/null ルートMACに設定されたMAC）として構成する場合、修正する必要があるファブリックで構成の重複について警告する syslog が生成されます。ただし、構成は拒否されません。ローカルの静的構成は、その VTEP のリモートのスタティック構成よりも優先されます。
- 有効なインターフェイスを持つローカル静的 MAC が VTEP に構成されており、この静的 MAC を同じ VTEP 上の null ルートMAC に変換する場合、null ルート MAC が有効になります。
- リモート ダイナミック MAC ルートは、MAC-IP ルート スプリットから派生したリモート MAC ルートがエントリを上書きして MAC マネージャに伝播することを許可しますが、リモート静的 MAC ルートは、これらの派生 MAC によるエントリの上書きを尊重しません。その結果、リモート スタティック MAC が削除されるまで、MAC エントリは変更されません。
- null ルート MAC は、静的 MAC 構成のみの別の形式です。

スタティック MAC の構成

始める前に

スタティック ドロップ MAC アドレスを構成できます。これらのスタティック MAC アドレスは、インターフェイス上でダイナミックに学習された MAC アドレスを書き換えます。

手順の概要

1. **configure terminal**
2. **mac address-table static** *mac-address* **vlan** *vlan-id* {[**drop**| **interface**{*type slot/port*} | **port-channel** *number*]}
3. **exit**

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`
	`switch(config)#`
		グローバル構成モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**mac address-table static** *mac-address* **vlan** *vlan-id* {[**drop**| **interface**{*type slot/port*} | **port-channel** *number*]}
	例：
	`switch(config)# mac address-table static 3001.3010.99aa vlan 3001 drop`
	`switch(config)#`
		レイヤ 2 MAC アドレス テーブルに追加するスタティック MAC アドレスを指定します。

ステップ 3	**exit**
	例：
	`switch# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ARP/ND の構成

対応する SVI の IPv4/IPv6 ルートで ARP/ND ホストを構成できます。

始める前に

MAC がドロップ エントリとして構成されているスイッチで静的 MAC-IP 構成を構成してください。これにより、MAC-IP モビリティが回避され、DROP MAC と MAC-IP の両方が同じ VTEP から発信されます。

手順の概要

1. **configure terminal**
2. **interface** *vlan-number*
3. **vrf member** *vrf-name*
4. **no ip redirects**
5. **ip address** アドレスを取得
6. **ipv6 address** アドレスを取得
7. **ipv6 neighbor address** *ipv6address mac_addr*
8. **no ipv6 redirects**
9. **ip arp address** *ipaddr mac_addr*
10. **fabric forwarding mode anycast-gateway**

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：	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。

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**interface** *vlan-number*
	例：
	`switch(config)# interface Vlan 3001`
	`switch(config-if)#`
		VLAN インターフェイスを指定します。

ステップ 3	**vrf member** *vrf-name*
	例：
	`switch(config-if)# vrf member cgw_3001_3050`
	`switch(config-if)#`
		VLAN インターフェイスをテナント VRF に割り当てます。

ステップ 4	**no ip redirects**
	例：
	`switch(config-if)# no ip redirects`
	`switch(config-if)#`
		IPv4 リダイレクトを無効にします。

ステップ 5	**ip address** アドレスを取得
	例：
	`switch(config-if)# ip address 30.1.0.1/16`
	`switch(config-if)#`
		IP アドレスを指定します。

ステップ 6	**ipv6 address** アドレスを取得
	例：
	`switch(config-if)# ipv6 address 2001:3001::1/64`
	`switch(config-if)#`
		IPv6 アドレスを指定します。

ステップ 7	**ipv6 neighbor address** *ipv6address mac_addr*
	例：
	`switch(config-if)# ipv6 neighbor 2001:3001::99 3001.3010.99aa`
	`switch(config-if)#`
		静的 IPv6 ネイバーを構成します。

ステップ 8	**no ipv6 redirects**
	例：
	`switch(config-if)# no ipv6 redirects`
	`switch(config-if)#`
		IPv6 リダイレクトを無効にします。

ステップ 9	**ip arp address** *ipaddr mac_addr*
	例：
	`switch(config-if)# ip arp 30.1.0.99 3001.3010.99aa`
	`switch(config-if)#`
		IP アドレスを MAC アドレスにスタティック エントリとして関連付けます。

ステップ 10	**fabric forwarding mode anycast-gateway** 例：	VLAN 構成モードでエニーキャスト ゲートウェイと SVI を関連付けます。

	コマンドまたはアクション	目的
	`switch# fabric forwarding mode anycast-gateway` `switch#`	

ローカル VTEP でのプレフィックスヌル ルートの構成

Null ルートが構成されているローカル VTEP で、ルート マップを構成して、静的 ルートにブラックホール コミュニティを設定し、BGP に再配布します。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **ip route** {<*ip*>/*mask*} **Null0 tag** <*tag-number*> or **ip route** {<*ipv6*>/*mask*} **Null0 tag** <*tag-number*>
4. **route-map** *map-name* [**permit** | **deny**] [*seq*]
5. **match tag** <*tag-number*>
6. **set weight** *value*
7. **set community blackhole**
8. **router bgp** *as-number*
9. **vrf** *vrf-name*
10. **address-family ipv4/ipv6 unicast**
11. **redistribute static route-map** *route-map name*

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`
	`switch(config)#`
		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	**vrf context** *vrf-name*
	例：
	`switch(config)# vrf context tenant-0001`
	`switch(config-vrf)#`
		テナント VRF を構成します。

ステップ 3	**ip route** {<*ip*>/*mask*} **Null0 tag** <*tag-number*> or **ip route** {<*ipv6*>/*mask*} **Null0 tag** <*tag-number*> 例：	Null0 ネクストホップと一致するタグを使用して、接続先プレフィックスのスタティック ルートを設定します。

	コマンドまたはアクション	目的

	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-vrf)# ip route 50.1.0.0/24 Null0 tag 6666`
	`switch(config-vrf)#`
	IPv6 の場合
	`switch(config-vrf)# ipv6 route 50::1:0/120 Null0 tag 6666`
	`switch(config-vrf)#`	

ステップ 4	**route-map** *map-name* [**permit** | **deny**] [*seq*]
	例：
	`switch(config)# route-map SET_BHC permit 10`
	`switch(config-route-map)#`
		ルート マップを作成するか、または既存のルート マップに対応するルート マップ設定モードを開始します。seq を使用して、ルート マップ エントリを順序付けます。

ステップ 5	**match tag** <*tag-number*>
	例：
	`switch(config-route-map)# match tag 6666`
	`switch(config-route-map)#`
		構成されたタグを持つルートを照合します。

ステップ 6	**set weight** *value*
	例：
	`switch (config-route-map)# set weight 65535`
	`switch(config-route-map)#`
		ブラックホール コミュニティのある着信ルートの重みを設定します。**セット ウェイト**値を最大値に設定して、nullルートに最高の優先順位を与えることをお勧めします。**設定ウェイト**の最大値は65535です。

ステップ 7	**set community blackhole**
	例：
	`switch(config-route-map)# set community blackhole`
	`switch(config-route-map)#`
		コミュニティを Blackhole (well-known community) として設定します。

ステップ 8	**router bgp** *as-number*
	例：
	`switch(config)# router bgp 100`
	`switch(config-router)#`
		ルーティング プロセスをイネーブルにします。as-num の範囲は 1–65535 です。

ステップ 9	**vrf** *vrf-name*
	例：
	`switch(config-router)# vrf tenant-0001`
	`switch(config-router-vrf)#`
		テナント VRF を構成します。

ステップ 10	**address-family ipv4/ipv6 unicast**
	例：
	`switch(config-router-vrf)# address-family ipv4 unicast`
	`switch(config-router-vrf-af)#`
		IPv4/IPv6 アドレス ファミリを構成。この構成は、IPv4/IPv6 アンダーレイを使用した IPv4/IPv6 over VXLAN に必要です。

	コマンドまたはアクション	目的

ステップ 11	**redistribute static route-map** *route-map name*
	例：
	`switch(config-router-vrf-af)# redistribute static route-map SET_BHC`
	`switch(config-router-vrf-af)#`
		構成されたルート マップを使用して、prefix-null 静的 ルートを BGP に再配布します。

リモート VTEP での RPM ルート マップの構成

始める前に

リモート VTEP では、コミュニティ リストとルート マップを使用して null ルートに優先順位を付けます。

手順の概要

1. **configure terminal**
2. **ip community-list standard** <*community-list-name*> **seq** <*seq-number*> **permit blackhole**
3. **route-map** *map-name***[permit | deny]** <*seq-number*>
4. **match community** <*community-list*>
5. **set weight** *value*
6. **route-map** *map-name***permit** <*seq-number*>
7. **router bgp** *as-number*
8. **route-map** *route-map* {**in** | **out**}

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`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**ip community-list standard** <*community-list-name*> **seq** <*seq-number*> **permit blackhole**
	例：
	`switch (config)# ip community-list standard BH seq 10 permit blackhole`
	`switch(config)#`
		コミュニティ リストを設定し、よく知られた「ブラックホール」コミュニティ値を持つルートを許可します。
		Cisco NX-OS リリース 10.3（2）F 以降、ブラックホール（既知のコミュニティ）が既存の IP コミュニティ リストに追加されています。

	コマンドまたはアクション	目的

ステップ 3	**route-map** *map-name***[permit | deny]** <*seq-number*>
	例：
	`switch(config)# route-map PREFER_BHC permit 10`
	`switch(config-route-map)#`
		ルートマップ構成モードを開始します。

ステップ 4	**match community** <*community-list*>
	例：
	`switch(config-route-map)# match community BH`
	`switch(config-route-map)#`
		BGP ルートは、コミュニティ リストを使用して照合されます。

ステップ 5	**set weight** *value*
	例：
	`switch (config-route-map)# set weight 65535`
	`switch(config-route-map)#`
		ブラックホール コミュニティのある着信ルートの重みを設定します。**セット ウェイト**値を最大値に設定して、null ルートに最高の優先順位を与えることをお勧めします。**設定ウェイト**の最大値は 65535 です。

ステップ 6	**route-map** *map-name***permit** <*seq-number*>
	例：
	`switch(config-route-map)# route-map PREFER_BHC permit 20`
	`switch(config-route-map)#`
		他のルートを許可するフォールバック許可句を使用してルート マップを構成します。

ステップ 7	**router bgp** *as-number*
	例：
	`switch(config)# router bgp 100`
	`switch(config-router)#`
		ルーティング プロセスをイネーブルにします。
		as-num の範囲は 1 ～ 65535 です。

ステップ 8	**route-map** *route-map* {**in** | **out**} 例： `switch(config-router-neighbor-af)# route-map PREFER_BHC in`	構成された方向のネイバーにルート マップを適用します。

Null ルートの構成例

次の例は、プレフィックスヌルおよびMAC/MAC-IP ドロップ ルートにローカル/リモート構成を構成する方法を示しています：

構成 – プレフィックス Null

Type5 null ルートがアドバタイズされるローカル VTEP（ボーダー リーフ スイッチ）で、次の手順を実行します。

1. Null0 隣接で静的 IPv4/IPv6 アドレスを構成する

```
vrf context tenant-0001
  vni 3100001
```

```
  ip route 50.1.0.0/24 Null0 tag 6666
  ipv6 route 50::1:0/120 Null0 tag 6666
```

2. スタティック ルートに null ルート コミュニティを設定し、BGP に再配布するようにルート マップを構成します

```
route-map SET_BHC permit 10
  match tag 6666
  set community blackhole
router bgp 100
  router-id 10.1.0.21
  vrf tenant-0001
    address-family ipv4 unicast
      redistribute static route-map SET_BHC
    address-family ipv6 unicast
      redistribute static route-map SET_BHC
```

他のすべてのリモート VTEP で、次の手順を実行します。

1. null ルート コミュニティに一致するようにルート マップを構成し、重みを最大値に設定して、null ルートが常に優先されるようにします。

```
ip community-list standard BH seq 10 permit blackhole
route-map PREFER_BHC permit 10
  match community BH
  set weight 65535
route-map PREFER_BHC permit 20
router bgp 100
 router-id 10.1.0.13
 address-family l2vpn evpn
 template peer LEAF_to_FABRIC_IBGP_OVERLAY
    remote-as 100
    address-family l2vpn evpn
      send-community
      send-community extended
      route-map PREFER_BHC in
```

構成 – MAC/MAC-IP ドロップ

Type2 null ルートがアドバタイズされるローカル VTEP で、次の手順を実行します。

1. ドロップ隣接を使用して静的 MAC アドレスを構成します

```
mac address-table static 0013.e001.0001 vlan 2 drop
```

2. 同じアドレスの静的 ARP/ND ネイバーを構成する

```
interface Vlan2
  no shutdown
  vrf member tenant-0001
  ip address 5.0.63.254/18
  ipv6 address 5::3f7f/114
  ipv6 neighbor 5::17fe 0013.e001.0001
  no ipv6 redirects
  ip arp 5.0.23.254 0013.e001.0001
  fabric forwarding mode anycast-gateway
```

他のすべてのリモート VTEP で、次の手順を実行します：

1. ブラックホール コミュニティに一致するようにルート マップを構成し、重みを最大値に設定して、null ルートが常に優先されるようにします。

```
ip community-list standard BH seq 10 permit blackhole
route-map PREFER_BHC permit 10
  match community BH
  set weight 65535
route-map PREFER_BHC permit 20
router bgp 100
 router-id 10.1.0.13
 address-family l2vpn evpn
 template peer LEAF_to_FABRIC_IBGP_OVERLAY
    remote-as 100
    address-family l2vpn evpn
      send-community
      send-community extended
      route-map PREFER_BHC in
  neighbor 10.1.0.31
    inherit peer LEAF_to_FABRIC_IBGP_OVERLAY
```

EVPN Null ルート構成の確認

EVPN Null ルート構成情報を表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show bgp l2vpn evpn	ルーティング テーブルの情報を表示します。
show ip arp static vlan <*vlan-id*> **vrf** <*vrf-name*>	ローかつ ARP 情報を表示します。
<vlan-id> <vrf-name>　show ip arp static remote vlanvrf	リモート ARP 情報を表示します。
<vlan-id> <vrf-name>　show ip adjacency vlandetail vrf	ローカル隣接関係情報を表示します。
show ipv6 icmp neighbour static remote [*vlan* <*id*>] [*vrf* <*name*>]	リモートスタティック隣接情報を表示します。
show mac address-table static vlan <*vlan-id*>	ローカル/リモート MAC 情報を表示します。
show ip community-list *name*	IP コミュニティ リストに関する情報を表示します。
show route-map *name*	ルート マップの情報を表示します。

次の例では、**show bgp l2vpn evpn** コマンドの Type-2 EVPN ルート サンプル出力を表示します。

```
switch# show bgp l2vpn evpn 1111.1111.1111
BGP routing table information for VRF default, address family L2VPN EVPN
Route Distinguisher: 53.53.53.53:32769    (L2VNI 1000002)
BGP routing table entry for [2]:[0]:[0]:[48]:[1111.1111.1111]:[32]:[100.100.100.51]/272,
 version 23
Paths: (1 available, best #1)
Flags: (0x000102) (high32 00000000) on xmit-list, is not in l2rib/evpn
Multipath: eBGP iBGP
  Advertised path-id 1
  Path type: local, path is valid, is best path, no labeled nexthop, has esi_gw
  AS-Path: NONE, path locally originated
```

```
53.53.53.53 (metric 0) from 0.0.0.0 (53.53.53.53)
Origin IGP, MED not set, localpref 100, weight 32768
Received label 1000002 1000100
Community: Blackhole
Extcommunity: RT:23456:1000002 RT:23456:1000100 ENCAP:8
Router MAC:0476.b0f0.8157
Path-id 1 advertised to peers:
111.111.54.1
```

次の例では、**show bgp l2vpn evpn** コマンドの Type-5 EVPN ルート（送信）サンプル出力を表示します。

```
switch# sh bgp ipv4 uni 44.44.44.0 vrf 100
BGP routing table information for VRF 100, address family IPv4 Unicast
BGP routing table entry for 44.44.44.0/24, version 6
Paths: (1 available, best #1)
Flags: (0x80c0002) (high32 0x000020) on xmit-list, is not in urib, exported, has label
vpn: version 5, (0x00000000100002) on xmit-list
local label: 492287

Advertised path-id 1, VPN AF advertised path-id 1
Path type: redist, path is valid, is best path, no labeled nexthop, is extd
AS-Path: NONE, path locally originated
0.0.0.0 (metric 0) from 0.0.0.0 (44.44.44.44)
Origin incomplete, MED 0, localpref 100, weight 32768
Community: blackhole
Extcommunity: RT:23456:1000100

VRF advertise information:
Path-id 1 not advertised to any peer

VPN AF advertise information:
Path-id 1 not advertised to any peer

switch# sh bgp l2 e 44.44.44.0
BGP routing table information for VRF default, address family L2VPN EVPN
Route Distinguisher: 53.53.53.53:4 (L3VNI 1000100)
BGP routing table entry for [5]:[0]:[0]:[24]:[44.44.44.0]/224, version 5
Paths: (1 available, best #1)
Flags: (0x000002) (high32 00000000) on xmit-list, is not in l2rib/evpn
Multipath: eBGP iBGP

Advertised path-id 1
Path type: local, path is valid, is best path, no labeled nexthop, has esi_gw
Gateway IP: 0.0.0.0
AS-Path: NONE, path locally originated
53.53.53.53 (metric 0) from 0.0.0.0 (53.53.53.53)
Origin incomplete, MED 0, localpref 100, weight 32768
Received label 1000100
Community: blackhole
Extcommunity: RT:23456:1000100 ENCAP:8 Router MAC:0476.b0f0.8157

Path-id 1 advertised to peers:
111.111.54.1
```

次の例では、**show bgp l2vpn evpn** コマンドの Type-5 EVPN ルート（受信）サンプル出力を表示します。

```
switch# sh bgp l2 e 44.44.44.0
BGP routing table information for VRF default, address family L2VPN EVPN
Route Distinguisher: 53.53.53.53:4
BGP routing table entry for [5]:[0]:[0]:[24]:[44.44.44.0]/224, version 2
Paths: (1 available, best #1)
Flags: (0x000002) (high32 00000000) on xmit-list, is not in l2rib/evpn, is not in HW
```

```
Multipath: eBGP iBGP

Advertised path-id 1
Path type: external, path is valid, is best path, no labeled nexthop, has esi_gw
Imported to 2 destination(s)
Imported paths list: 100 L3-1000100
Gateway IP: 0.0.0.0
AS-Path: 4241653625 , path sourced external to AS
53.53.53.53 (metric 2) from 111.111.53.1 (53.53.53.53)
Origin incomplete, MED 0, localpref 100, weight 0
Received label 1000100
Community: blackhole
Extcommunity: RT:11000:1000100 Route-Import:53.53.53.53:100
Source AS:4241653625:0 SOO:50529024:00000000 ENCAP:8
Router MAC:0476.b0f0.8157
Path-id 1 not advertised to any peer

switch# show bgp ipv4 uni 44.44.44.0 vrf 100
BGP routing table information for VRF 100, address family IPv4 Unicast
BGP routing table entry for 44.44.44.0/24, version 3
Paths: (1 available, best #1)
Flags: (0x8008001a) (high32 00000000) on xmit-list, is in urib, is best urib route, is
in HW
vpn: version 3, (0x00000000100002) on xmit-list

Advertised path-id 1, VPN AF advertised path-id 1
Path type: external, path is valid, is best path, no labeled nexthop, in rib, has esi_gw

Imported from 53.53.53.53:4:[5]:[0]:[0]:[24]:[44.44.44.0]/224
AS-Path: 4241653625 , path sourced external to AS
53.53.53.53 (metric 2) from 111.111.53.1 (53.53.53.53)
Origin incomplete, MED 0, localpref 100, weight 0
Received label 1000100
Community: blackhole
Extcommunity: RT:11000:1000100 Route-Import:53.53.53.53:100
Source AS:4241653625:0 SOO:50529024:00000000 ENCAP:8
Router MAC:0476.b0f0.8157

VRF advertise information:
Path-id 1 not advertised to any peer
```

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。