MPLS VPN sur ATM : avec OSPF côté client (sans zone 0)

Contenu

Introduction

Ce document fournit une configuration d'échantillon d'un Commutation multiprotocole par étiquette (MPLS) VPN au-dessus d'atmosphère quand le Protocole OSPF (Open Shortest Path First) est présent du côté client, sans zone 0.

La caractéristique du réseau privé virtuel (VPN), une fois utilisée avec le MPLS, permet à plusieurs sites pour interconnecter d'une manière transparente par le réseau d'un fournisseur de services. Un réseau du fournisseur de service peut prendre en charge plusieurs VPN d'IP différents. Chacun de ces derniers apparaît à ses utilisateurs en tant que réseau privé, séparé de tous les autres réseaux. Dans un VPN, chaque site peut envoyer des paquets IP à n'importe quel autre site dans le même VPN.

Conditions préalables

Conditions requises

Chaque VPN est associé avec un ou plusieurs VPN de routage ou instances de transmission (VRF). UN VRF se compose d'une table de Routage IP, d'un Technologie Cisco Express Forwarding (CEF) dérivé, de la table et d'un ensemble d'interfaces qui utilisent cette table d'expédition.

Le routeur conserve un routage distinct et la table CEF pour chaque VRF. Avec ceci, les informations ne peuvent pas être envoyées en dehors du VPN mais le même sous-réseau peut être utilisé dans plusieurs VPN sans problèmes d'adresse IP en double.

Le routeur qui utilise le Protocole BGP (Border Gateway Protocol) distribue les informations de routage VPN avec les communautés BGP étendues.

Le pour en savoir plus en vue de la propagation des mises à jour par un VPN, se rapportent ces à l'URLs :

- Les communautés cibles de la route VPN
- Distribution par BGP d'informations de routage de VPN
- Transmission MPLS

Matériel et versions de logiciel

Ces lettres représentent les différents types des Routeurs et de Commutateurs utilisés :

- **P** : Principal routeur de fournisseur
- **PE** : Routeur de Provider Edge
- **CE** : Routeur de Customer Edge
- **C** : Routeur client

Nous avons développé et avons testé la configuration avec des ces logiciel et versions de matériel :

- **Routeurs de PE** :**Logiciel** : Version de logiciel 12.1(3)T de Cisco IOS®. Les caractéristiques MPLS VPN apparaissent dans la release 12.0(5)T. L'OSPF comme protocole de routage PE-CE apparaît dans la release 12.0(7)T.**Matériel** : Le Cisco 3660 ou 7206 Routeurs. Pour des détails de l'autre matériel que vous pouvez utiliser, référez-vous au MPLS concevant pour le guide atmosphère.
- **Routeurs de la CE** : Utilisez n'importe quel routeur qui peut permuter les informations de routage avec son routeur PE.
- **Routeurs et Commutateurs P** : La fonction d'intégration MPLS VPN réside seulement au bord du réseau MPLS, ainsi utilisez n'importe quel commutateur MPLS-capable. Dans la configuration d'échantillon, le nuage MPLS se compose de 8540 MSR et un LightStream 1010. Si vous utilisez le LightStream 1010, nous recommandons que vous utilisiez la version de logiciel WA4.8d ou plus élevé. Vous pouvez également utiliser d'autres Commutateurs ATM, tels que le BPX 8650 de Cisco ou MGX 8850 dans le réseau de noyau atmosphère.

Conventions

Ce diagramme affiche une configuration typique qui utilise ces conventions :

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

L'information générale OSPF

Traditionnellement, un réseau élaboré OSPF se compose d'une zone fédératrice (la zone 0) et un

certain nombre de zones connectées à ce circuit principal par une zone encadrent le routeur (ABR).

Avec un circuit principal MPLS pour le VPN avec l'OSPF sur le site client, vous pouvez introduire un niveau dans la hiérarchie du modèle OSPF. Ce niveau s'appelle le circuit principal superbe MPLS VPN.

Dans des cas simples, le circuit principal superbe MPLS VPN est combiné avec le circuit principal traditionnel de la zone 0. Ceci signifie qu'il n'y a aucun circuit principal de la zone 0 sur le réseau client puisque le circuit principal superbe MPLS VPN joue le même rôle que le circuit principal de la zone 0. Ceci est montré dans le schéma suivant :

Ce diagramme montre ces informations :

- Les Routeurs de Provider Edge (PE) sont des Routeurs d'ABR et de routeur ASBR (Autonomous System Boundary Router).
- Les Routeurs de Customer Edge (CE) sont les Routeurs simples OSPF.
- Les informations VPN sont transportées par les communautés BGP étendues du siège potentiel d'explosion à l'autre siège potentiel d'explosion et sont réinjectées dans les zones OSPF en tant que réseau récapitulatif (annonces d'état de lien de type 3) (LSAs).

Le circuit principal superbe MPLS VPN permet également à des clients d'utiliser des circuits principaux de la plusieurs zone 0 sur leurs sites. Chaque site peut avoir une zone distincte 0 tant que il est connecté au circuit principal superbe MPLS VPN. Le résultat est identique qu'avec un circuit principal divisé de la zone 0. Ceci est montré dans le schéma suivant :

Dans ce cas, ces choses se produisent :

- Les Routeurs de PE sont des Routeurs d'ABR et ASBR.
- Les Routeurs de la CE sont des Routeurs d'ABR.
- Le LSAs qui contiennent les informations VPN sont transportés avec les communautés BGP étendues du siège potentiel d'explosion à l'autre siège potentiel d'explosion. En résumé réseau (le type 3) LSAs, les informations est transporté entre le siège potentiel d'explosion et le ces.

Cette configuration d'échantillon est basée sur la première installation affichée. Vous pouvez trouver une configuration d'échantillon qui utilise la deuxième installation dans MPLS VPN au-dessus d'atmosphère : avec l'OSPF du côté client (avec zone 0).

Les informations OSPF sont transportées avec les attributs de la communauté BGP étendue (qui incluent un qui identifie le réseau OSPF). Chaque VPN doit avoir son propre processus OSPF. Afin de spécifier ceci, vous pouvez utiliser cette commande :

```
router ospf <process ID> vrf <VPN routing/forwarding instance name>
```

Procédure de configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

La documentation Cisco IOS (réseaux privés virtuels MPLS) décrit également cette procédure de configuration.

Partie I de procédure de configuration

Assurez-vous que l'ip cef est activé. Si vous utilisez un routeur de Cisco 7500, vous devez s'assurer que l'ip cef distribué est activé. Sur le siège potentiel d'explosion, une fois que le MPLS est installé, effectuez ces tâches :

1. Créez un VRF pour chaque VPN lié à la commande de **name> de routage/instance de transfert du vrf <VPN d'IP**. Quand vous faites ceci :Spécifiez le moteur de distinction de route correct utilisé pour ce VPN. Ceci est utilisé pour étendre l'adresse IP de sorte que vous puissiez identifier le VPN auquel elle appartient.
   `rd <VPN route distinguisher>` Installez les propriétés d'importation et d'exportation pour les communautés BGP étendues. Ceux-ci sont utilisés pour filtrer le processus d'importation et d'exportation.
   `route-target [export|import|both] <target VPN extended community>`
2. Configurez les détails de transfert pour les interfaces de respectives avec cette commande : **`ip vrf forwarding <table name>`** Souvenez-vous pour installer l'adresse IP après que vous fassiez ceci.
3. Personne à charge sur le protocole de routage PE-CE que vous utilisation, vous devez maintenant faire un ou plusieurs de ces derniers :Configurez les artères statiques : **`ip route vrf vrf-name prefix mask [next-hop-address] [interface {interface-number}]`**Configurez le RIP avec cette commande :
   `address-family ipv4 vrf <VPN routing/forwarding instance name>` Une fois que vous avez fait la présente partie, sélectionnez les commandes normales de configuration RIP.**Remarque:** Ceci est seulement appliqué aux interfaces de transfert pour le VRF en cours.**Remarque:** Vous devez redistribuer le BGP correct dans le RIP. Quand vous faites ceci, souvenez-vous également pour spécifier la mesure qui est utilisée.Déclarez les informations sur les voisins BGP.Configurez l'OSPF avec la nouvelle commande IOS : **`router ospf <process ID> vrf <VPN routing/forwarding instance name>`** **Remarque:** Ceci est seulement appliqué aux interfaces de transfert pour le VRF en cours.**Remarque:** Vous devez redistribuer le BGP correct dans l'OSPF. Quand vous faites ceci, souvenez-vous également pour spécifier la mesure qui est utilisée.**Remarque:** Une fois que vous attribuez le processus OSPF à un VRF, ce nombre de processus est toujours utilisé pour ce VRF particulier. Ceci s'applique même si vous ne le spécifiez pas dans la ligne de commande.

Partie II de procédure de configuration

Configurez le BGP entre les Routeurs de PE. Il y a plusieurs manières de configurer le BGP, tel que l'utilisation des méthodes de réflecteur ou de confédération d'artère. La méthode utilisée ici – configuration de voisinage directe – est la plus simple et moins extensible.

1. Déclarez les différents voisins.
2. Écrivez le **name> de routage/instance de transfert du vrf <VPN d'ipv4 d'address-family** pour

chaque VPN actuel à ce routeur PE. Effectuez un ou plusieurs de ces étapes, selon les besoins :Redistribuez les informations de routage statiques.Redistribuez les informations de routage de RIP.Redistribuez les informations de routage OSPF.Lancez les voisins BGP avec les Routeurs de la CE.

3. Entrez le mode d'**address-family vpnv4**, et effectuez ces tâches :Activez les voisins.Spécifiez que la communauté étendue doit être utilisée. Ceci est obligatoire.

Configurations

Remarque: Seulement les éléments pertinents de la sortie sont inclus ici.

Alcazaba

```
ip cef
!
ip vrf vpn1
 rd 1:101
 route-target export 1:101
 route-target import 1:101
!
interface Loopback0
 ip address 223.0.0.3 255.255.255.255
!
interface Loopback1
 ip vrf forwarding vpn1
 ip address 222.0.0.10 255.255.255.255
!
interface Ethernet1/1
 ip vrf forwarding vpn1
 ip address 150.150.0.1 255.255.255.0
 no ip mroute-cache
!
interface ATM4/0
 no ip address
 no ip mroute-cache
 atm sonet stm-1
 no atm ilmi-keepalive
!
interface ATM4/0.1 tag-switching
 ip address 10.0.0.13 255.255.255.252
 tag-switching atm vpi 2-4
 tag-switching ip
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 150.150.0.0 0.0.0.255 area 0
 network 223.0.0.3 0.0.0.0 area 0
!
router ospf 2 vrf vpn1
 log-adjacency-changes
 redistribute bgp 1 metric-type 1 subnets
 network 150.150.0.0 0.0.0.255 area 1
 network 222.0.0.0 0.0.0.255 area 1
!
router bgp 1
 neighbor 223.0.0.21 remote-as 1
 neighbor 223.0.0.21 update-source Loopback0
 !
```

```
 address-family ipv4 vrf vpn1
 redistribute ospf 2
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 223.0.0.21 activate
 neighbor 223.0.0.21 send-community extended
 exit-address-family
!
```

Kozel

```
!
ip cef
!
ip vrf vpn1
 rd 1:101
 route-target export 1:101
 route-target import 1:101
!
interface Loopback0
 ip address 223.0.0.21 255.255.255.255
!
interface Loopback1
 ip vrf forwarding vpn1
 ip address 222.0.0.30 255.255.255.255
!
interface Ethernet1/1
 ip vrf forwarding vpn1
 ip address 69.69.0.1 255.255.255.252
 no ip mroute-cache
 tag-switching ip
!
interface ATM4/0
 no ip address
 no atm scrambling cell-payload
 no atm ilmi-keepalive
 pvc qsaal 0/5 qsaal
 !
 pvc ilmi 0/16 ilmi
 !
!
interface ATM4/0.1 tag-switching
 ip address 11.0.0.6 255.255.255.252
 tag-switching atm vpi 2-4
 tag-switching ip
!
router ospf 1
 log-adjacency-changes
 network 11.0.0.0 0.0.0.255 area 0
 network 223.0.0.21 0.0.0.0 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
router ospf 2 vrf vpn1
 log-adjacency-changes
 redistribute bgp 1 metric-type 1 subnets
 network 69.69.0.0 0.0.0.255 area 3
 network 222.0.0.0 0.0.0.255 area 3
!
router bgp 1
 neighbor 223.0.0.3 remote-as 1
```

```
 neighbor 223.0.0.3 update-source Loopback0
 neighbor 223.0.0.11 remote-as 1
 neighbor 223.0.0.11 update-source Loopback0
 !
 address-family ipv4 vrf vpn1
 redistribute ospf 2
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 223.0.0.3 activate
 neighbor 223.0.0.3 send-community extended
 neighbor 223.0.0.11 activate
 neighbor 223.0.0.11 send-community extended
 exit-address-family
!
```

Rapide

```
!
interface Loopback0
 ip address 222.0.0.1 255.255.255.255
!
interface Loopback2
 ip address 7.7.7.7 255.255.255.0
!
interface FastEthernet0/1
 ip address 150.150.0.2 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 network 7.7.7.7 0.0.0.0 area 1
 network 150.150.0.0 0.0.0.255 area 1
 network 222.0.0.1 0.0.0.0 area 1
!
```

Pivrnec

```
!
interface Loopback0
 ip address 222.0.0.3 255.255.255.255
!
interface Loopback1
 ip address 6.6.6.6 255.255.255.255
!
interface FastEthernet0/1
 ip address 69.69.0.2 255.255.255.252
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 6.6.6.6 0.0.0.0 area 3
 network 69.69.0.0 0.0.0.255 area 3
 network 222.0.0.3 0.0.0.0 area 3
!
```

Vérifiez

Commandes show

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- routage du show ip route vrf <VPN ou name> d'instance de transfert
- routage du vrf <VPN de show ip bgp vpnv4 ou name> <A.B.C.D> d'instance de transfert
- number> d'ID de <process de show ip ospf
- interface de number> d'ID de <process de show ip ospf
- base de données de number> d'ID de <process de show ip ospf
- affichez le routage du vrf <VPN d'expédition-table de balise-commutation ou le name> d'instance de transfert

Cette commande montre le VRF pour un VPN particulier au routeur PE :

```
Alcazaba#show ip route vrf vpn1 Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external
type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate
default, U - per-user static route, o - ODR P - periodic downloaded static route Gateway of last
resort is not set 69.0.0.0/30 is subnetted, 1 subnets B 69.69.0.0 [200/0] via 223.0.0.21,
00:19:39 222.0.0.0/32 is subnetted, 4 subnets B 222.0.0.30 [200/0] via 223.0.0.21, 00:19:39 C
222.0.0.10 is directly connected, Loopback1 B 222.0.0.3 [200/11] via 223.0.0.21, 00:20:39 O
222.0.0.1 [110/11] via 150.150.0.2, 00:20:59, Ethernet1/1 6.0.0.0/32 is subnetted, 1 subnets B
6.6.6.6 [200/11] via 223.0.0.21, 00:20:39 7.0.0.0/32 is subnetted, 1 subnets O 7.7.7.7 [110/11]
via 150.150.0.2, 00:21:00, Ethernet1/1 150.150.0.0/24 is subnetted, 1 subnets C 150.150.0.0 is
directly connected, Ethernet1/1
```

Vous pouvez également afficher les informations BGP pour un VRF particulier avec la commande de **vrf de show ip bgp vpnv4**. Les résultats PE-PE du BGP interne (IBGP) sont indiqués par un I.

```
Alcazaba#show ip bgp vpnv4 vrf vpn1 BGP table version is 21, local router ID is 223.0.0.3 Status
codes: s suppressed, d damped, h history, * valid, > best, i - internal Origin codes: i - IGP, e
- EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path Route Distinguisher: 1:101
(default for vrf vpn1) *>i6.6.6.6/32 223.0.0.21 11 100 0 ? *> 7.7.7.7/32 150.150.0.2 11 32768 ?
*>i69.69.0.0/30 223.0.0.21 0 100 0 ? *> 150.150.0.0/24 0.0.0.0 0 32768 ? *> 222.0.0.1/32
150.150.0.2 11 32768 ? *>i222.0.0.3/32 223.0.0.21 11 100 0 ? *> 222.0.0.10/32 0.0.0.0 0 32768 ?
*>i222.0.0.30/32 223.0.0.21 0 100 0 ?
```

Vous pouvez vérifier les détails d'une entrée. Afin d'afficher ceci, le moteur de distinction de route est "1:101."

```
Alcazaba#show ip bgp vpnv4 vrf vpn1 6.6.6.6 BGP routing table entry for 1:101:6.6.6.6/32,
version 28 Paths: (1 available, best #1, table vpn1) Not advertised to any peer Local 223.0.0.21
(metric 4) from 223.0.0.21 (223.0.0.21) Origin incomplete, metric 11, localpref 100, valid,
internal, best Extended Community: RT:1:101 OSPF RT:3:2:0 Alcazaba#show ip bgp vpnv4 vrf vpn1
7.7.7.7 BGP routing table entry for 1:101:7.7.7.7/32, version 20 Paths: (1 available, best #1,
table vpn1) Advertised to non peer-group peers: 223.0.0.21 Local 150.150.0.2 from 0.0.0.0
(223.0.0.3) Origin incomplete, metric 11, localpref 100, weight 32768, valid, sourced, best
Extended Community: RT:1:101 OSPF RT:1:2:0
```

La commande de **show ip route** sur un routeur CE est le principal moyen pour vérifier les tables de routage :

```
rapid#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-
IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 69.0.0.0/30 is subnetted, 1 subnets O IA 69.69.0.0 [110/11] via 150.150.0.1, 00:20:25,
FastEthernet0/1 222.0.0.0/32 is subnetted, 4 subnets O IA 222.0.0.30 [110/11] via 150.150.0.1,
00:20:25, FastEthernet0/1 O 222.0.0.10 [110/11] via 150.150.0.1, 00:21:46, FastEthernet0/1 O IA
222.0.0.3 [110/21] via 150.150.0.1, 00:21:25, FastEthernet0/1 C 222.0.0.1 is directly connected,
Loopback0 6.0.0.0/32 is subnetted, 1 subnets O IA 6.6.6.6 [110/21] via 150.150.0.1, 00:21:25,
```

FastEthernet0/1 7.0.0.0/24 is subnetted, 1 subnets C 7.7.7.0 is directly connected, Loopback2 10.0.0.0/22 is subnetted, 1 subnets C 10.200.8.0 is directly connected, FastEthernet0/0 150.150.0.0/24 is subnetted, 1 subnets C 150.150.0.0 is directly connected, FastEthernet0/1 S 158.0.0.0/8 is directly connected, Null0

Commandes d'OSPF-particularité

Vous pouvez utiliser toutes les commandes de **show ip ospf**. Quand vous faites ceci, souvenez-vous pour indiquer l'ID de processus. Nous avons marqué les la plupart des parties importantes de la sortie ci-dessous en texte *en italiques*.

OSPF LSAs du type 9, 10 et 11 (également connu en tant que LSAs opaque) sont utilisés pour machiner le trafic.

Commandes pour un routeur PE

Alcazaba#**show ip ospf 2** Routing Process "ospf 2" with ID 222.0.0.10 Supports only single TOS(TOS0) routes Supports opaque LSA Connected to *MPLS VPN super backbone* It is an area border and *autonomous system boundary router Redistributing* External Routes from, *bgp 1*, includes subnets in redistribution SPF schedule delay 5 secs, Hold time between two SPFs 10 secs Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs Number of external LSA 0. Checksum Sum 0x0 Number of opaque AS LSA 0. Checksum Sum 0x0 Number of DCbitless external and opaque AS LSA 0 Number of DoNotAge external and opaque AS LSA 0 Number of areas in this router is 1. 1 normal 0 stub 0 nssa External flood list length 0 Area 1 Number of interfaces in this area is 2 Area has no authentication SPF algorithm executed 4 times Area ranges are Number of LSA 7. Checksum Sum 0x420BE Number of opaque link LSA 0. Checksum Sum 0x0 Number of DCbitless LSA 0 Number of indication LSA 0 Number of DoNotAge LSA 0 Flood list length 0 Alcazaba#**show ip ospf 2 interface** Loopback1 is up, line protocol is up Internet Address 222.0.0.10/32, Area 1 Process ID 2, Router ID 222.0.0.10, Network Type LOOPBACK, Cost: 1 Loopback interface is treated as a stub Host Ethernet1/1 is up, line protocol is up Internet Address 150.150.0.1/24, Area 1 Process ID 2, Router ID 222.0.0.10, Network Type BROADCAST, Cost: 10 Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 222.0.0.10, Interface address 150.150.0.1 Backup Designated router (ID) 222.0.0.1, Interface address 150.150.0.2 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:07 Index 1/1, flood queue length 0 Next 0x0(0)/0x0(0) Last flood scan length is 2, maximum is 3 Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 1, Adjacent neighbor count is 1 Adjacent with neighbor 222.0.0.1 (Backup Designated Router) Suppress hello for 0 neighbor(s) Alcazaba#**show ip ospf 2 database** OSPF Router with ID (222.0.0.10) (Process ID 2) Router Link States (Area 1) Link ID ADV Router Age Seq# Checksum Link count 222.0.0.1 222.0.0.1 1364 0x80000013 0x7369 3 222.0.0.10 222.0.0.10 1363 0x80000002 0xFEFE 2 Net Link States (Area 1) Link ID ADV Router Age Seq# Checksum 150.150.0.1 222.0.0.10 1363 0x80000001 0xEC6D Summary Net Link States (Area 1) Link ID ADV Router Age Seq# Checksum 6.6.6.6 222.0.0.10 1328 0x80000001 0x4967 69.69.0.0 222.0.0.10 1268 0x80000001 0x2427 222.0.0.3 222.0.0.10 1328 0x80000001 0xEEF7 222.0.0.30 222.0.0.10 1268 0x80000001 0x7B5A

Commandes pour un routeur CE

rapid#**show ip ospf interface** FastEthernet0/1 is up, line protocol is up Internet Address 150.150.0.2/24, Area 1 Process ID 1, Router ID 222.0.0.1, Network Type BROADCAST, Cost: 10 Transmit Delay is 1 sec, State BDR, Priority 1 Designated Router (ID) 222.0.0.10, Interface address 150.150.0.1 Backup Designated router (ID) 222.0.0.1, Interface address 150.150.0.2 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:04 Index 2/2, flood queue length 0 Next 0x0(0)/0x0(0) Last flood scan length is 1, maximum is 2 Last flood scan time is 0 msec, maximum is 0 msec Neighbor Count is 1, Adjacent neighbor count is 1 Adjacent with neighbor 222.0.0.10 (Designated Router) Suppress hello for 0 neighbor(s) Loopback0 is up, line protocol is up Internet Address 222.0.0.1/32, Area 1 Process ID 1, Router ID 222.0.0.1, Network Type LOOPBACK, Cost: 1 Loopback interface is treated as a stub Host Loopback2 is up, line protocol is up Internet Address 7.7.7.7/24, Area 1 Process ID 1, Router ID 222.0.0.1, Network Type LOOPBACK, Cost: 1 Loopback interface is treated as a stub Host rapid#**show ip ospf database** OSPF Router with ID (222.0.0.1) (Process ID 1) Router Link States (Area 1) Link ID ADV Router Age Seq# Checksum Link count 222.0.0.1 222.0.0.1 1350 0x80000013 0x7369 3 222.0.0.10 222.0.0.10 1350 0x80000002 0xFEFE 2 Net Link States (Area 1) Link ID ADV

```
Router Age Seq# Checksum 150.150.0.1 222.0.0.10 1351 0x80000001 0xEC6D Summary Net Link States
(Area 1) Link ID ADV Router Age Seq# Checksum 6.6.6.6 222.0.0.10 1316 0x80000001 0x4967
69.69.0.0 222.0.0.10 1256 0x80000001 0x2427 222.0.0.3 222.0.0.10 1316 0x80000001 0xEEF7
222.0.0.30 222.0.0.10 1256 0x80000001 0x7B5A Alcazaba#show tag-switching forwarding-table vrf
vpn1 Local Outgoing Prefix Bytes tag Outgoing Next Hop tag tag or VC or Tunnel Id switched
interface 24 Aggregate 222.0.0.10/32[V] 0 25 Aggregate 150.150.0.0/24[V] 0 27 Untagged
7.7.7.7/32[V] 1710 Et1/1 150.150.0.2 28 Untagged 222.0.0.1/32[V] 0 Et1/1 150.150.0.2
```

Mpls label

Vous pouvez vérifier la pile d'étiquette utilisée pour une artère particulière :

```
Alcazaba#show tag-switching forwarding-table vrf vpn1 6.6.6.6 detail Local Outgoing Prefix Bytes
tag Outgoing Next Hop tag tag or VC or Tunnel Id switched interface None 2/41 6.6.6.6/32 0
AT4/0.1 point2point MAC/Encaps=4/12, MTU=4466, Tag Stack{2/41(vcd=10) 16} 000A8847
0000A00000010000
```

Sortie de débogage

Voici un extrait des informations de débogage d'échange d'artère. Ceci affiche comment une artère particulière est importée.

```
Alcazaba#debug ip bgp vpnv4 import Tag VPN import processing debugging is on *Aug 5
05:10:09.283: vpn: Start import processing for: 1:101:222.0.0.3 *Aug 5 05:10:09.283: vpn: Import
check for vpn1; flags mtch, impt *Aug 5 05:10:09.283: vpn: Import for vpn1 permitted; import
flags mtch, impt *Aug 5 05:10:09.283: vpn: Same RD import for vpn1 *Aug 5 05:10:09.283: vpn:
1:101:222.0.0.3 (ver 29), imported as: *Aug 5 05:10:09.283: vpn: 1:101:222.0.0.3 (ver 29) *Aug 5
05:10:09.287: VPN: Scanning for import check is done.
```

Sortie de test

Vous pouvez maintenant employer le **ping** pour tester que tout est bien :

```
Pivrnec#ping 7.7.7.7 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 7.7.7.7,
timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

La commande traceroute affiche cette sortie :

```
Pivrnec#traceroute 7.7.7.7 Type escape sequence to abort. Tracing the route to 7.7.7.7 1
69.69.0.1 0 msec 0 msec 0 msec 2 150.150.0.1 0 msec 0 msec 20 msec 3 150.150.0.2 0 msec 0 msec *
```

Les hôtes MLPS ne sont pas ici parce qu'ils ne voient pas l'en-tête IP. Les hôtes MPLS vérifient seulement l'étiquette ou l'interface et puis en avant lui d'arrivée.

L'exécution sur le champ du Time to Live IP (TTL) est seulement effectuée sur la périphérie LSR. Le compte de saut affiché est moins que le compte réel de saut.

Informations connexes

- Pages de support technologique atmosphère
- Support et documentation techniques - Cisco Systems