

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

Contenu

[Introduction](#)

[Avant de commencer](#)

[Conventions](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Théorie générale](#)

[Utilisant l'OSPF](#)

[Configurez](#)

[Diagramme du réseau](#)

[Procédure de configuration](#)

[Configurations](#)

[Vérifiez](#)

[Commandes d'OSPF-particularité](#)

[Mpls label](#)

[Commandes de test](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

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

[Avant de commencer](#)

[Conventions](#)

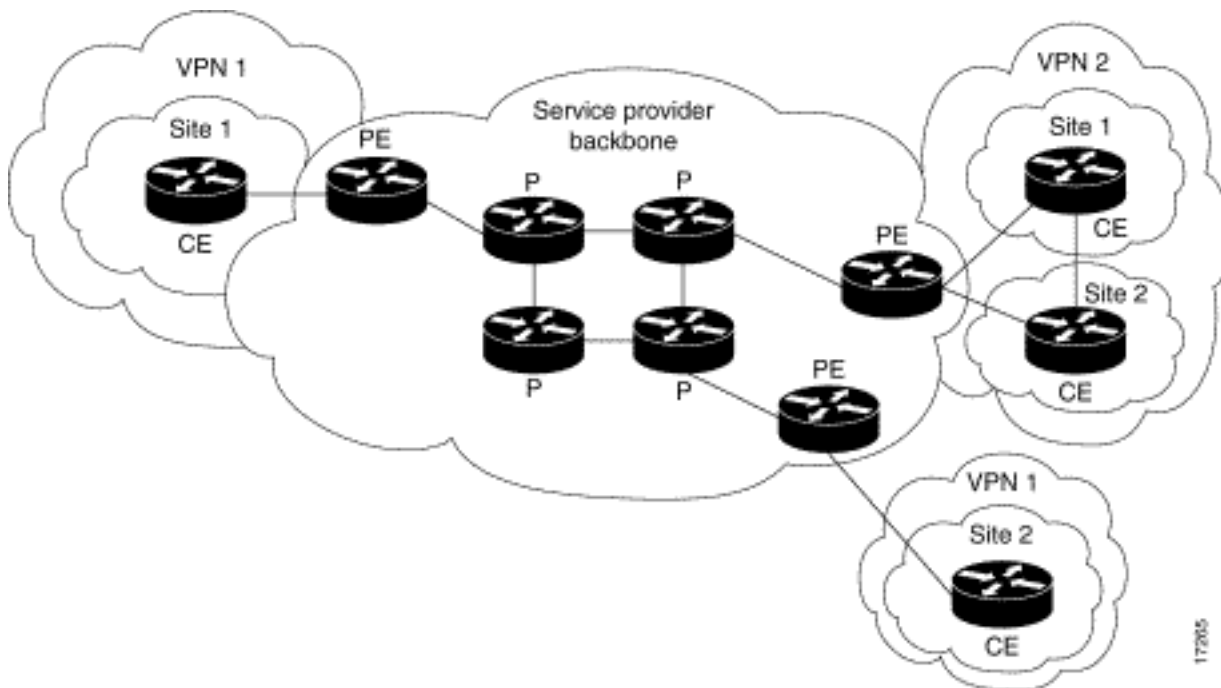
Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

Les lettres ci-dessous représentent les différents types des Routeurs et de Commutateurs utilisés :

- P : Le principal routeur du fournisseur
- PE : Routeur de la périphérie du fournisseur

- CE : Routeur de la périphérie du client
- C : Le routeur du client

Ce diagramme affiche une configuration typique utilisant ces conventions :



Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- **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** : N'importe quel routeur capable permuter les informations de routage avec son routeur PE peut être utilisé.
- **Routeurs et Commutateurs P** : La fonction d'intégration MPLS VPN réside seulement au bord du réseau MPLS, ainsi n'importe quel commutateur MPLS-capable peut être utilisé. Dans cette configuration d'échantillon, le nuage MPLS se compose de commutateur-routeur ATM 8540 interarmées (MSR) et de LightStream 1010. Si vous utilisez le LightStream 1010 de Cisco, nous recommandons que vous utilisiez la version de logiciel WA4.8d ou plus tard. Vous pouvez également utiliser d'autres Commutateurs ATM comme le BPX 8650 de Cisco ou MGX 8850 dans le réseau de noyau atmosphère.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de

l'utiliser.

[Théorie générale](#)

La caractéristique VPN, une fois utilisée avec le MPLS, permet à plusieurs sites pour interconnecter d'une manière transparente par 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.

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'une table (E-F) dérivée de Cisco Express Forwarding et d'un ensemble d'interfaces qui utilisent cette table d'expédition.

Le routeur met à jour un routage distinct et une table E-F de Cisco pour chaque VRF. Ceci empêche l'information d'être envoyée en dehors du VPN et permet au même sous-réseau d'être utilisé dans plusieurs VPN sans causer de problèmes d'adresse IP en double.

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

Pour plus d'informations sur la propagation des mises à jour par un VPN, voyez l'URLs suivant :

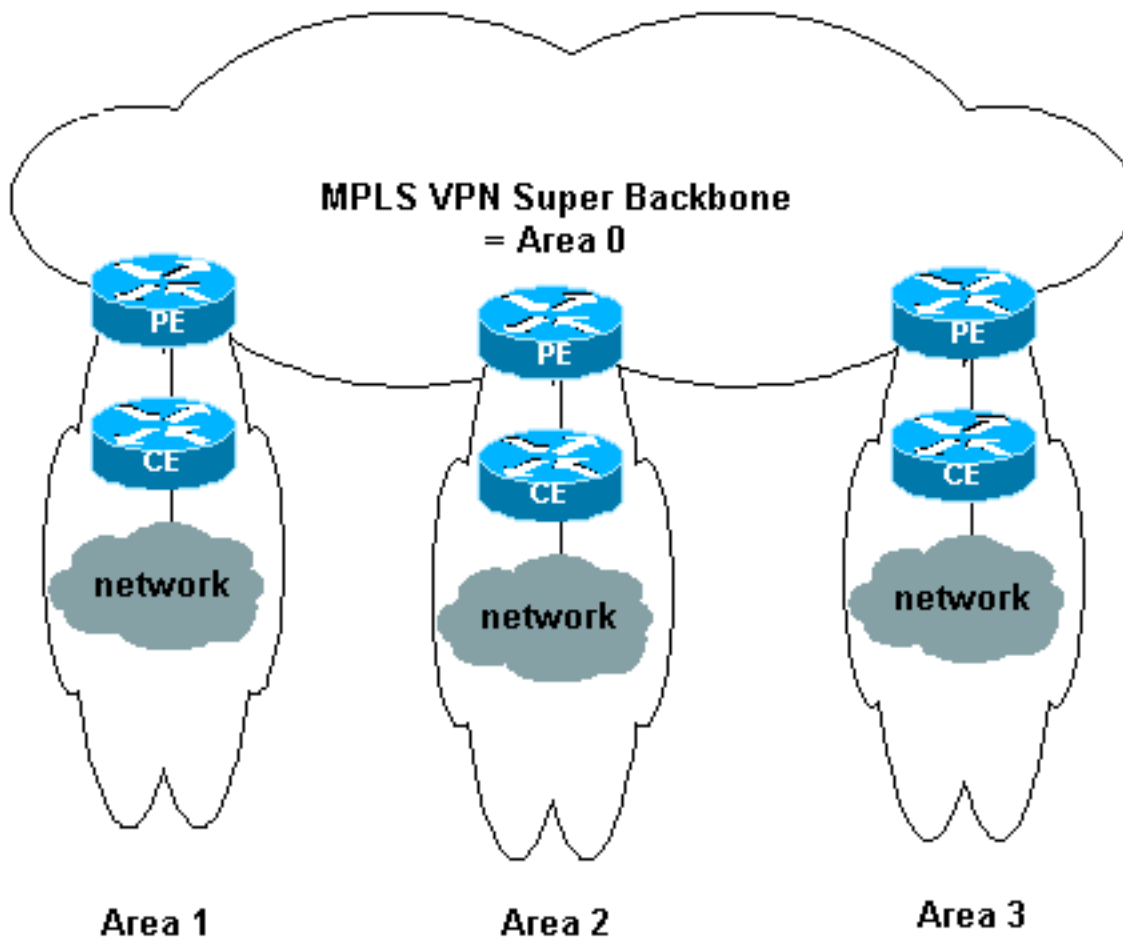
- [Les communautés cibles de la route VPN](#)
- [Distribution par BGP d'informations de routage de VPN](#)
- [Transmission MPLS](#)

[Utilisant l'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).

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

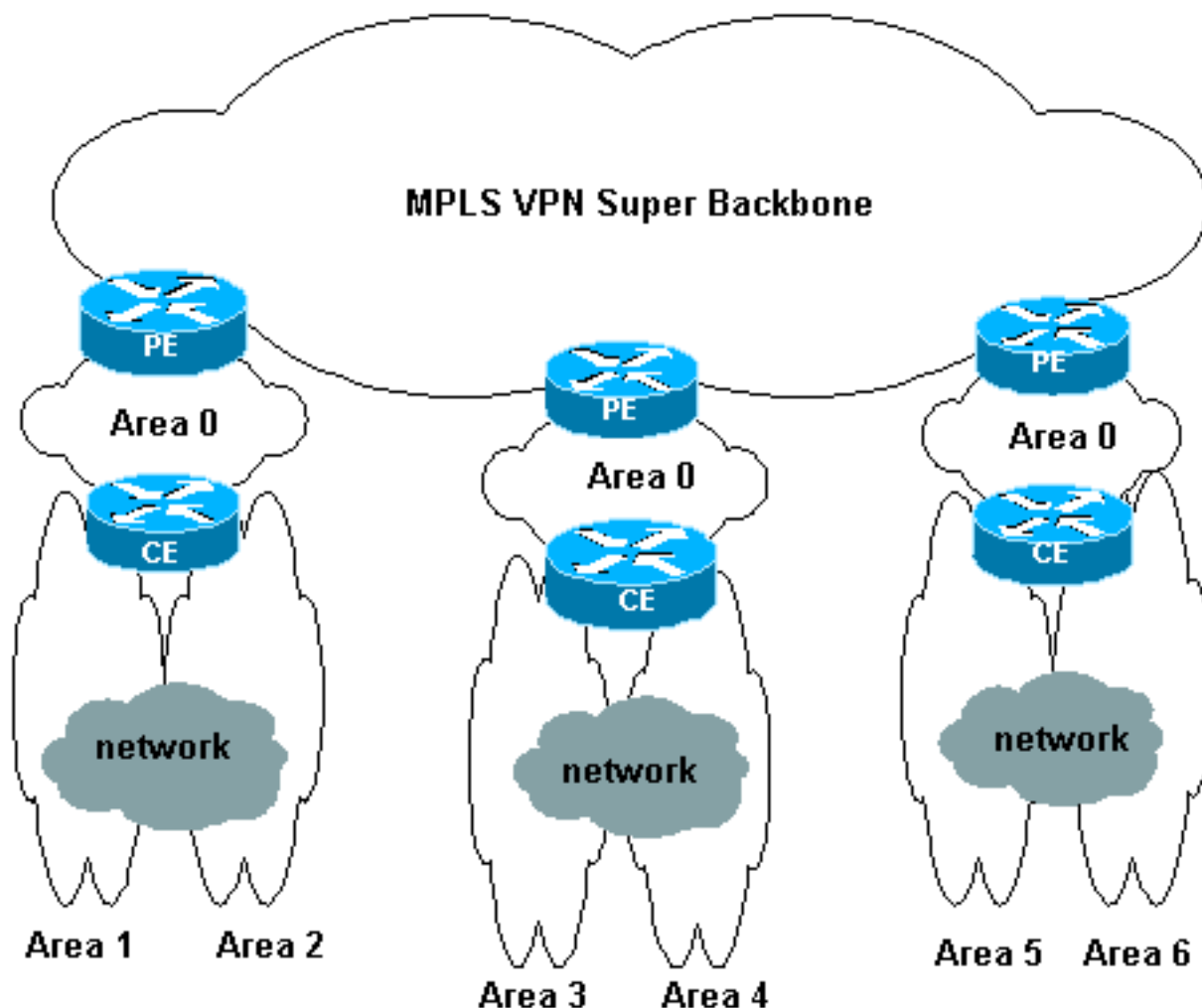
Dans des cas simples, le circuit principal superbe MPLS VPN est combiné avec le circuit principal traditionnel de la zone 0. Ceci signifie qu'il n'y a aucun circuit principal de la zone 0 sur le réseau client, puisque le circuit principal superbe MPLS VPN joue le même rôle que le circuit principal de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



Dans ce diagramme :

- Les Routeurs de PE sont les Routeurs de borne d'ABR et d'Autonomous System (ASBR).
- Les Routeurs de la CE sont les Routeurs simples OSPF.
- Les informations VPN sont transportées utilisant 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 comme circuit principal divisé de la zone 0. Ceci est affiché dans le diagramme ci-dessous :



Dans ce cas :

- Les Routeurs de PE sont des Routeurs d'ABR et ASBR.
- Les Routeurs de la CE sont des Routeurs d'ABR.
- Les LSAs contenant les informations VPN sont transportés utilisant 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 deuxième installation affichée ci-dessus. Vous pouvez trouver une configuration d'échantillon qui utilise la première installation dans [MPLS VPN au-dessus d'atmosphère : avec l'OSPF du côté client \(sans zone 0\)](#).

Les informations OSPF sont transportées avec des attributs de la communauté BGP étendue (les y compris qui identifient le réseau OSPF). Chaque VPN doit avoir son propre processus OSPF. Pour spécifier ceci, émettez la commande suivante :

ID de <process de router ospf > routage ou forwarding instance name du vrf <VPN >

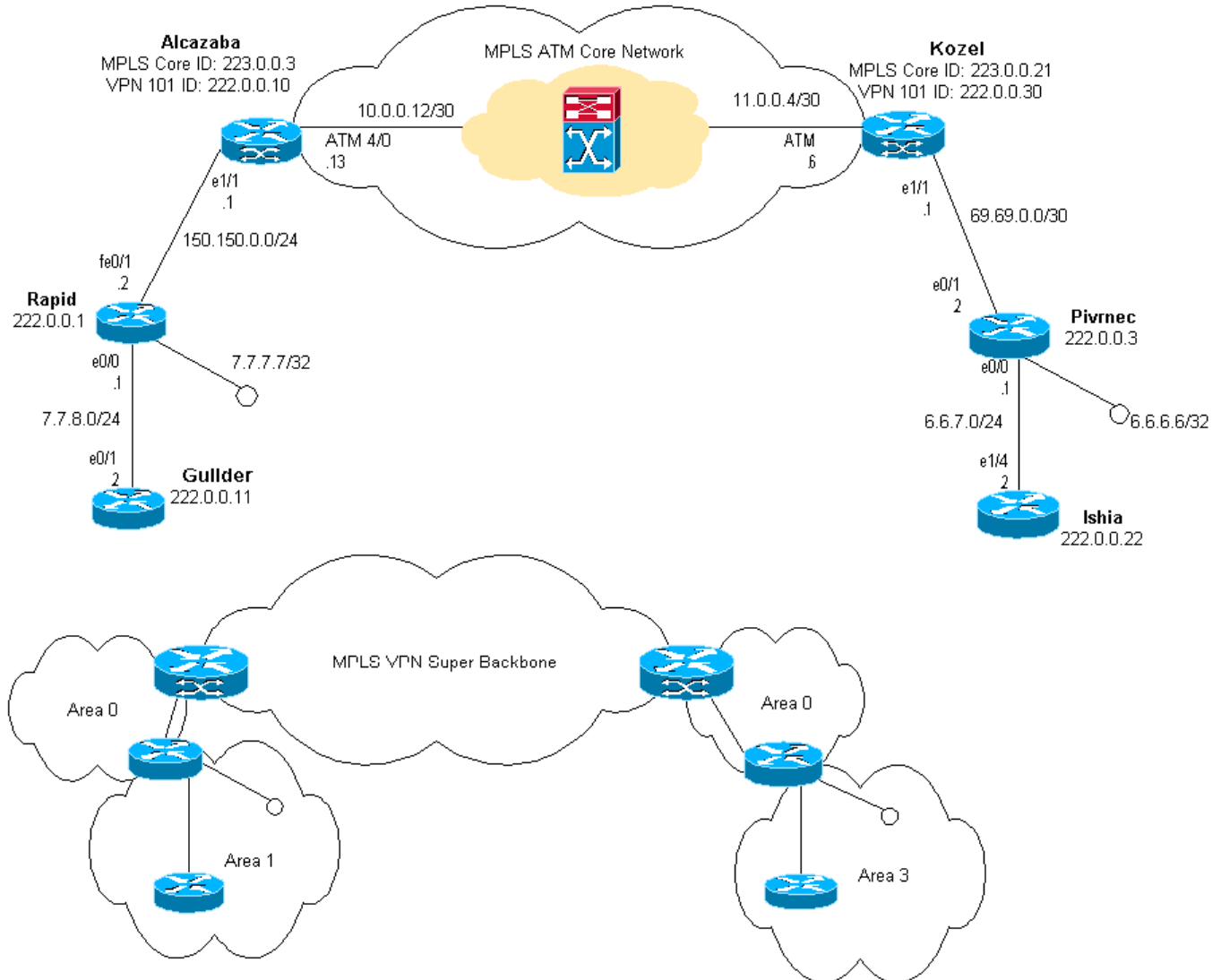
Configurez

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

Note: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'[Outil de recherche de commande](#) (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Procédure de configuration

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

Partie I

Assurez-vous que l'**ip cef** est activé. Si vous utilisez un routeur de Cisco 7500, assurez-vous que l'**ip cef distribué** est activé. Sur le siège potentiel d'explosion, une fois que le MPLS est installé :

1. Créez un VRF pour chaque VPN connecté à l'aide de la commande **ip vrf <VPN routing/forwarding instance name>** . Lorsque vous effectuez cela :Émettez la commande ci-dessous de spécifier 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 à quel VPN il

appartient. *moteur de distinction de route du rd <VPN >* Installez les propriétés d'importation et d'exportation pour les communautés BGP étendues. Celles-ci sont utilisées pour filtrer le processus d'importation et d'exportation. *route-target [exportation/importation/chacun des deux] la communauté étendue du <target VPN >*

2. Configurez les détails de transfert pour les interfaces respectives en émettant cette commande : *nom <table d'ip vrf forwarding >* Souvenez-vous pour installer l'adresse IP après avoir fait ceci.
3. Selon le protocole de routage PE-CE que vous utilisez, vous devriez maintenant faire un ou plusieurs de ce qui suit : Configurez les artères statiques comme suit : *masque de préfixe de vrf-name d'ip route vrf [adresse du prochain saut] [interface {interface-nombre}]* Configurez le Protocole RIP (Routing Information Protocol) en émettant la commande : *routage/forwarding instance name du vrf <VPN d'ipv4 d'address-family >* Une fois que ceci est fait, sélectionnez les commandes normales de configuration RIP. Notez cela : Ceci est seulement appliqué aux interfaces de transfert pour le VRF en cours. Il est nécessaire de redistribuer le BGP correct dans le RIP. En faire ceci, souvenez-vous pour spécifier également la mesure utilisée. Déclarez les informations sur les voisins BGP. Configurez l'OSPF en émettant la nouvelle commande Cisco IOS : *ID de <process de router ospf > routage/forwarding instance name du vrf <VPN >*. Notez cela : Ceci est seulement appliqué aux interfaces de transfert pour le VRF en cours. Il est nécessaire de redistribuer le BGP correct dans l'OSPF. En faire ceci, souvenez-vous pour spécifier également la mesure utilisée. Une fois que le processus OSPF est attribué 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

Configurez le BGP entre les Routeurs de PE. Il y a plusieurs façons de configurer BGP, comme utiliser les méthodes de réflecteur de route ou de confédération. La méthode utilisée ici – configuration de voisinage directe – est la plus simple et moins l'extensible.

1. Déclarez les différents voisins.
2. Écrivez le *routage/forwarding instance name du vrf <VPN d'ipv4 d'address-family >* pour chaque VPN actuel à ce routeur PE. Effectuez une ou plusieurs des étapes suivantes, selon les besoins : Redistribuez les informations de routage statiques. Redistribuez les informations de routage de RIP. Redistribuez les informations de routage OSPF. Activez le voisinage BGP avec les routeurs de la CE.
3. Entrez le mode d'**address-family vpnv4**, et : Activez les voisins. Spécifiez que la communauté étendue doit être utilisée. Ceci est obligatoire.

Configurations

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

Alcazaba
<pre>ip cef ! ip vrf vpn1 rd 1:101 route-target export 1:101</pre>

```

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
 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 0
 network 222.0.0.0 0.0.0.255 area 0
!
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
!
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 0
 network 222.0.0.0 0.0.0.255 area 0
!
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 FastEthernet0/0
 ip address 7.7.8.1 255.255.255.0
 duplex auto
 speed auto
!
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 0
 network 222.0.0.1 0.0.0.0 area 1
!
```

Pivrtec

```
!
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 FastEthernet0/0
 ip address 6.6.7.1 255.255.255.0
 duplex auto
 speed auto
!
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 0
 network 222.0.0.3 0.0.0.0 area 3
!
```

Guilder

```
!
interface Loopback0
 ip address 222.0.0.11 255.255.255.255
!
interface Ethernet0/1
 ip address 7.7.8.2 255.255.255.0
!
router ospf 2
 network 7.7.8.0 0.0.0.255 area 1
 network 222.0.0.0 0.0.0.255 area 1
!
```

Ischions

```
!  
interface Loopback0  
  ip address 222.0.0.22 255.255.255.255  
!  
interface Ethernet1/4  
  ip address 6.6.7.2 255.255.255.0  
!  
router ospf 1  
  log-adjacency-changes  
  network 6.6.7.0 0.0.0.255 area 3  
  network 222.0.0.0 0.0.0.255 area 3  
!
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) (clients [enregistrés](#) uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

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

Émettez les deux premières commandes ci-dessus d'afficher le VRF pour un VPN particulier au routeur PE.

Commandes d'OSPF-particularité

Commandes pour un routeur PE

Les informations suivantes de show ospf de commandes pour le VRF correspondant. Les la plupart des parties importantes de la sortie ci-dessous sont affichées en **texte en gras**.

Note: Vous ne devez pas spécifier le VRF en émettant ces commandes.

```
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 Superbackbone  
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 BACKBONE(0)

Number of interfaces in this area is 2
Area has no authentication
SPF algorithm executed 4 times
Area ranges are
Number of LSA 13. Checksum Sum 0x715C5
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 database

OSPF Router with ID (222.0.0.10) (Process ID 2)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
222.0.0.1	222.0.0.1	272	0x80000009	0xCA39	1
222.0.0.10	222.0.0.10	197	0x80000003	0xFCFF	2

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
150.150.0.1	222.0.0.10	197	0x80000002	0xEA6E

Summary Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
6.6.6.6	222.0.0.10	197	0x80000002	0x4768
6.6.7.0	222.0.0.10	750	0x80000001	0xD4D7
7.7.7.7	222.0.0.1	272	0x80000002	0x72CC
7.7.8.0	222.0.0.1	1003	0x80000003	0x635
69.69.0.0	222.0.0.10	197	0x80000002	0x2228
222.0.0.1	222.0.0.1	272	0x80000002	0x5A21
222.0.0.3	222.0.0.10	197	0x80000004	0xE8FA
222.0.0.11	222.0.0.1	1010	0x80000001	0x5C0C
222.0.0.22	222.0.0.10	752	0x80000001	0x9435
222.0.0.30	222.0.0.10	199	0x80000002	0x795B

Alcazaba#show ip ospf 2 interface

Loopback1 is up, line protocol is up

Internet Address 222.0.0.10/32, Area 0

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 0

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 00:00:08

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 6, maximum is 6

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)

Commandes pour un routeur CE

Dans ce cas, le routeur CE est un ABR parce qu'il est également connecté à une autre zone. Si ce routeur devait avoir seulement des interfaces dans la zone 0, ce serait un routeur ordinaire, pas un ABR ou un ASBR.

```
rapid#show ip ospf
```

```
Routing Process "ospf 1" with ID 222.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
It is an area border router
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 2. 2 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 14 times
    Area ranges are
    Number of LSA 13. Checksum Sum 0x715C5
    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
  Area 1
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 48 times
    Area ranges are
    Number of LSA 16. Checksum Sum 0x8CCBE
    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
```

```
rapid#show ip ospf database
```

```
OSPF Router with ID (222.0.0.1) (Process ID 1)
```

```
Router Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	Checksum	Link count
222.0.0.1	222.0.0.1	331	0x80000009	0xCA39	1
222.0.0.10	222.0.0.10	259	0x80000003	0xFCFF	2

```
Net Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	Checksum
150.150.0.1	222.0.0.10	259	0x80000002	0xEA6E

Summary Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
6.6.6.6	222.0.0.10	259	0x80000002	0x4768
6.6.7.0	222.0.0.10	812	0x80000001	0xD4D7
7.7.7.7	222.0.0.1	331	0x80000002	0x72CC
7.7.8.0	222.0.0.1	1062	0x80000003	0x635
69.69.0.0	222.0.0.10	259	0x80000002	0x2228
222.0.0.1	222.0.0.1	331	0x80000002	0x5A21
222.0.0.3	222.0.0.10	260	0x80000004	0xE8FA
222.0.0.11	222.0.0.1	1069	0x80000001	0x5C0C
222.0.0.22	222.0.0.10	813	0x80000001	0x9435
222.0.0.30	222.0.0.10	260	0x80000002	0x795B

Router Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
222.0.0.1	222.0.0.1	1078	0x80000029	0x658E	3
222.0.0.10	222.0.0.10	2962	0x80000003	0xFCFF	2
222.0.0.11	222.0.0.11	1080	0x80000003	0xA97F	2

Net Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum
7.7.8.2	222.0.0.11	1081	0x80000001	0x93DA
150.150.0.1	222.0.0.10	2962	0x80000002	0xEA6E

Summary Net Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum
6.6.6.6	222.0.0.1	332	0x80000002	0x69C5
6.6.6.6	222.0.0.10	2720	0x80000002	0x4768
6.6.7.0	222.0.0.1	820	0x80000001	0xF635
69.69.0.0	222.0.0.1	341	0x80000002	0x4485
150.150.0.0	222.0.0.1	341	0x80000004	0x57CB
222.0.0.3	222.0.0.1	341	0x80000002	0xF56
222.0.0.3	222.0.0.10	2727	0x80000002	0xECF8
222.0.0.10	222.0.0.1	341	0x80000002	0x6404
222.0.0.22	222.0.0.1	820	0x80000001	0xB692
222.0.0.30	222.0.0.1	341	0x80000002	0x9BB8

Summary ASB Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum
222.0.0.10	222.0.0.1	341	0x80000002	0x4C1C

Commandes pour le routeur courant alternatif

Émettez la commande suivante d'afficher la table de Routage IP :

```
Guilden#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 [110/21] via 7.7.8.1, 00:06:33, Ethernet0/1
222.0.0.0/32 is subnetted, 6 subnets
O IA    222.0.0.30 [110/21] via 7.7.8.1, 00:06:33, Ethernet0/1
O IA    222.0.0.22 [110/41] via 7.7.8.1, 00:06:33, Ethernet0/1
O IA    222.0.0.10 [110/21] via 7.7.8.1, 00:06:33, Ethernet0/1
C       222.0.0.11 is directly connected, Loopback0
O IA    222.0.0.3 [110/31] via 7.7.8.1, 00:06:33, Ethernet0/1
O       222.0.0.1 [110/11] via 7.7.8.1, 00:06:33, Ethernet0/1
6.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O IA    6.6.6.6/32 [110/31] via 7.7.8.1, 00:06:34, Ethernet0/1
O IA    6.6.7.0/24 [110/40] via 7.7.8.1, 00:06:34, Ethernet0/1
7.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       7.7.7.7/32 [110/11] via 7.7.8.1, 00:06:35, Ethernet0/1
C       7.7.8.0/24 is directly connected, Ethernet0/1
10.0.0.0/22 is subnetted, 1 subnets
C       10.200.8.0 is directly connected, Ethernet0/0
150.150.0.0/24 is subnetted, 1 subnets
O IA    150.150.0.0 [110/20] via 7.7.8.1, 00:06:35, Ethernet0/1

```

Mpls label

Confirmez qu'il y a deux étiquettes sur la pile d'étiquette sur le routeur de commutateur d'étiquette d'entrée (LSR) comme suit :

```

Alcazaba#show tag-switching forwarding-table vrf vpn1 6.6.7.2 detail
Local  Outgoing  Prefix          Bytes tag  Outgoing  Next Hop
tag    tag or VC   or Tunnel Id    switched   interface
None   2/41        6.6.7.0/24      0          AT4/0.1   point2point
      MAC/Encaps=4/12, MTU=4466, Tag Stack{2/41(vcd=10) 29}
      000A8847 0000A0000001D000

```

Maintenant, confirmez qu'ils apparaissent sur la sortie LSR :

```

Kozel#show tag-switching forwarding-table vrf vpn1 6.6.7.2 detail
Local  Outgoing  Prefix          Bytes tag  Outgoing  Next Hop
tag    tag or VC   or Tunnel Id    switched   interface
29     Untagged   6.6.7.0/24[V]   1466      Et1/1     69.69.0.2
      MAC/Encaps=0/0, MTU=1500, Tag Stack{}
      VPN route: vpn1
      Per-packet load-sharing

```

Commandes de test

Vous pouvez maintenant émettre la **commande ping** de tester que tout est bien :

```

Ischia#ping 222.0.0.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 222.0.0.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
Ischia#trac

```

```
Ischia#traceroute 222.0.0.11
```

```
Type escape sequence to abort.
```

```
Tracing the route to 222.0.0.11
```

```
 1 6.6.7.1 0 msec 0 msec 0 msec  
 2 69.69.0.1 0 msec 0 msec 0 msec  
 3 150.150.0.1 4 msec 4 msec 0 msec  
 4 150.150.0.2 4 msec 0 msec 0 msec  
 5 7.7.8.2 4 msec * 0 msec
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Plus de MPLS au-dessus des informations sur ATM](#)
- [Support technique - Cisco Systems](#)