Fonctionnalité MPLS, caractéristiques, et exemple unifiés de configuration

Contenu

Introduction

Ce document décrit le Commutation multiprotocole par étiquette (MPLS) unifié, qui est tout au sujet de l'évolution. Il fournit un cadre des solutions technologiques pour apporter le trafic de bout en bout simple et/ou des services à travers une infrastructure traditionnellement segmentée. Il se sert des avantages d'une infrastructure hiérarchique pendant qu'il améliore l'évolutivité et la simplicité de la conception de réseaux.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Évolution de réseau

Quand vous regardez l'historique des services paquet paquet de réseau, alors on peut observer une variation des valeurs commerciales de réseau. Ceci va des améliorations discrètes de Connectivité afin de faire des demandes aussi fluidees comme possible, aux Technologies de Collaboration afin de prendre en charge la Collaboration mobile. En conclusion, les services en nuage sur demande sont présentés avec les services d'application afin d'optimiser les outils utilisés avec une organisation et améliorer la stabilité et le coût de possession.

Figure 1

Cette amélioration continue de valeur et de fonctionnalité du réseau a comme conséquence un besoin beaucoup plus dominant de simplicité, de gestionnabilité, d'intégration, et de stabilité de réseau où des réseaux ont été segmentés en raison des îles opérationnelles disjointes et d'aucun vrai contrôle de chemin d'accès de bout en bout. Il y a maintenant un besoin de l'apporter que tout ainsi qu'une architecture simple il est facile gérer que, fournit l'évolutivité à 100,000's des Noeuds, et utilise les Technologies en cours de Haute disponibilité et de convergence rapide. Est ce ce que le MPLS unifié apporte à la table, qui est le réseau segmenté dans une visibilité d'avion et de chemin d'accès de bout en bout de contrôle simple.

Spécifications du réseau modernes

- Augmentez la demande de bande passante (le vidéo)
- Augmentez la complexité d'application (nuage et virtualisation)
- Augmentez le besoin de convergence (la mobilité)

Comment pouvez-vous simplifier des exécutions MPLS dans de plus en plus des réseaux plus vastes avec des conditions requises d'application plus complexes ?

Défis traditionnels MPLS avec différentes technologies d'accès

- La complexité afin de réaliser la convergence de 50 millisecondes avec l'ingénierie de trafic rapide reroutent (TE FRR)
- Ayez besoin pour des protocoles de routage et l'interaction sophistiqués avec des protocoles de la couche 2
- Grands réseaux fendus dans des domaines tandis que les services sont de bout en bout livré
- Mécanismes de bout en bout communs de convergence et de résilience
- Dépannez et provision de bout en bout à travers des plusieurs domaines

L'attraction unifiée MPLS est récapitulée dans cette liste :

- Nombre réduit de points opérationnels. Transportez en général les Plateformes, un service doit être configuré sur chaque élément de réseau par l'intermédiaire des points opérationnels. Le système de gestion doit connaître la topologie.Dans le MPLS unifié, avec l'intégration de toutes les îles MPLS, le nombre minimal de points opérationnels est réalisé.
- Possibilité pour provision facilement des services : Posez 3 (L3) VPN, agence de presse privée virtuelle (VPWS), service privé virtuel de RÉSEAU LOCAL (VPLS), sans pseudowire-piquer (Picowatt-piquer) ou mécanismes d'InterAS. Avec l'introduction du MPLS dans l'agrégation, on évite une certaine configuration statique qui crée des îles MPLS.
- Fournissez le transport de bout en bout MPLS.
- Maintenez les régions de Protocole IGP (Interior Gateway Protocol) les tables de routage séparées et petites.
- Convergence rapide.
- Facile à configurer et dépanner.
- Capacité d'intégrer avec toute technologie d'accès.
- Préparation d'IPv6.

Cisco Unified MPLS

Le MPLS unifié est défini par l'ajout des fonctions supplémentaires avec MPLS classique/traditionnel et il donne plus d'évolutivité, de Sécurité, de simplicité et de gestionnabilité. Afin de fournir les services MPLS de bout en bout, le chemin étiqueté de bout en bout de Commutateurs (LSP) est nécessaire. Le but est de garder les services MPLS (L2VPN MPLS VPN, MPLS) car ils sont, mais d'introduire la meilleure évolutivité. Afin de faire ceci, entrez certains des préfixes d'IGP dans le Protocole BGP (Border Gateway Protocol) (les préfixes de bouclage des Routeurs de Provider Edge (PE)), qui distribuent alors les préfixes de bout en bout.

Figure 2

Avant que l'architecture de Cisco Unified MPLS soit discutée, il est important de comprendre les fonctionnalités principales utilisées afin de faire à ceci une réalité.

Caractéristiques et composants

Diffusez les informations d'étiquette dans BGP-4 (RFC 3107)

C'est une condition préalable pour avoir une méthode extensible afin de permuter des préfixes entre les segments de réseau. Vous pourriez simplement fusionner les IGP (Protocole OSPF (Open Shortest Path First), Protocole IS-IS (Intermediate System-to-Intermediate System), ou Protocole EIGPR (Enhanced Interior Gateway Routing Protocol)) dans un domaine simple. Cependant un IGP n'est pas conçu pour porter 100,000s des préfixes. Le protocole du choix dans ce but est BGP. C'est un protocole bien-prouvé le quel prend en charge l'Internet avec 100,000's des artères et des environnements MPLS-VPN avec des millions d'entrées. Cisco Unified MPLS utilise BGP-4 avec l'échange d'informations d'étiquette (RFC3107). Quand le BGP distribue une artère, il peut également distribuer des mpls label qui sont tracés à cette artère. Les informations de mappage de mpls label pour l'artère sont diffusées dedans le message de mise à jour BGP qui contient les informations sur l'artère. Si le prochain saut n'est pas changé, l'étiquette est préservée et les modifications d'étiquette si le prochain saut change. Dans le MPLS unifié, le prochain saut change aux Routeurs de cadre de zone (abr).

Quand vous activez RFC 3107 sur les deux routeurs BGP, les Routeurs annoncent entre eux qu'ils peuvent alors envoyer des mpls label avec les artères. Si les Routeurs négocient avec succès leur capacité d'envoyer des mpls label, les Routeurs ajoutent des mpls label à toutes les mises à jour BGP sortantes.

L'échange d'étiquette est nécessaire afin de garder les informations de chemin d'accès de bout en bout entre les segments. En conséquence, chaque segment devient assez petit pour être géré par des opérateurs et en même temps il y a les informations de circuit distribuées pour la connaissance de chemin entre deux haut-parleurs différents IP.

Comment fonctionne-t-cela ?

Figure 3

Dans la figure 3 vous pouvez voir qu'il y a trois segments avec le chemin de Commutateurs étiqueté par Discovery Protocol d'étiquette (LDP LSP) et le réseau d'accès n'a pas le LDP activé. L'objectif est de les joindre ensemble de sorte qu'il y ait un chemin simple MPLS (BGP interne (iBGP) LSP hiérarchique) entre les Noeuds de Pré-agrégation (Pre-Agg). Car le réseau est un système autonome (AS) simple BGP, toutes les sessions sont des sessions d'iBGP. Chaque segment exécute ses propres chemins de l'IGP (OSPF, IS-IS, ou EIGRP) et LDP LSP dans le domaine d'IGP. Dans Cisco Unified MPLS, les Routeurs (abr) qui se joignent les segments doivent être les artère-réflecteurs intégrés BGP avec le next-hop-self et le RFC 3107 afin de porter un ipv4 + l'étiquette configurés sur les sessions. Ces speakers BGP sont dans l'architecture de Cisco Unified MPLS référencée à comme les abr.

Pourquoi les abr sont-ils des artère-réflecteurs d'en ligne ?

Un des buts du MPLS unifié est d'avoir une infrastructure de bout en bout fortement extensible. Ainsi, chaque segment devrait être maintenu simple afin de fonctionner. Tous les peerings sont des peerings d'iBGP, donc il y a un besoin de maillage global des peerings entre tous les haut-parleurs d'iBGP dans le réseau complet. Cela a comme conséquence un environnement de réseau très irréaliste s'il y a des milliers de speakers BGP. Si les abr sont faits à des artère-réflecteurs, le nombre de scruter d'iBGP est réduit au nombre du par-segment des speakers BGP » au lieu de entre « tous les » speakers BGP du complet AS.

Pourquoi next-hop-self ?

Le BGP traite la base des consultations récursives de routage. Ceci est fait afin de faciliter

l'évolutivité dans l'IGP sous-jacent qui est utilisé. Pour la recherche récursive, le BGP utilise le Prochain-saut relié à chaque entrée de route BGP. Ainsi, par exemple, si un Source-noeud désire envoyer un paquet à un Destination-noeud et si le paquet frappe le routeur BGP, puis le routeur BGP fait une consultation de routage dans sa table de routage BGP. Il trouve une artère vers le Destination-noeud et trouve le Prochain-saut comme étape suivante. Ce Prochain-saut doit être connu par l'IGP sous-jacent. En tant que la dernière étape, routeur BGP en avant le paquet en avant basé sur les informations IP et de mpls label reliées à ce Prochain-saut.

Afin de s'assurer que dans chaque segment seulement les Prochain-sauts sont nécessaires pour être connus par l'IGP, il est nécessaire que le Prochain-saut relié à l'entrée BGP soit dans le segment de réseau et pas dans un voisin ou plus loin un segment. Si vous réécrivez le bgp next-hop avec la configuration de next-hop-self, assurez-vous que le Prochain-saut est dans le segment local.

Remontez-le tout

Figure 4

La figure 4 fournit un exemple de la façon dont le préfixe « A » L3 VPN et l'échange d'étiquette fonctionne et de la façon dont la pile de mpls label est créée pour avoir les informations de chemin d'accès de bout en bout pour la circulation entre les les deux siège potentiel d'explosion.

Le réseau est divisé en tant que trois domaines indépendants IGP/LDP. La taille réduite des tables de routage et d'expédition sur les Routeurs est d'activer une meilleure stabilité et une convergence plus rapide. Le LDP est utilisé pour établir l'intradomain LSP dans des domaines. Des étiquettes BGP IPv4+ RFC 3107 sont utilisées comme protocole de distribution d'étiquette d'interdomain afin d'établir BGP hiérarchique LSP à travers des domaines. BGP3107 insère une étiquette supplémentaire dans la pile d'étiquette de transmission en architecture unifiée MPLS.

Intradomain - LDP LSP

Interdomain - BGP LSP hiérarchique

Figure 5

Le VPN préfixent « A » est annoncé par PE31 à PE11 avec l'étiquette 30 de service L3VPN et le prochain saut comme bouclage PE31 par l'intermédiaire de BGP hiérarchique LSP d'interdomain de bout en bout. Maintenant, regardez le chemin de transfert pour le préfixe VPN « A » de PE11 à PE31.

- Sur PE11, préfixez A est connu par l'intermédiaire de la session BGP avec PE31 car le prochain-saut PE31 et PE31 est périodiquement accessible par l'intermédiaire de P1 avec l'étiquette 100 BGP. PE11 a reçu les informations d'ipv4 + d'étiquette de P1 comme mises à jour BGP parce qu'il est activé avec la configuration RFC 3107 afin d'envoyer les informations d'ipv4 + d'étiquette.
- P1 est accessible de PE11 par l'intermédiaire de l'intradomain LDP LSP et il ajoute une autre étiquette LDP sur l'étiquette BGP. En conclusion, le paquet sort du noeud PE11 avec trois étiquettes. Par exemple, l'étiquette de service 30 L3VPN, l'étiquette BGP 100, et l'étiquette d'IGP de 200 LDP.
- L'étiquette de dessus LDP continue à permuter dedans l'intradomain LDP LSP et le paquet

atteint P1 avec deux étiquettes après sauter pénultième de saut (PHP).
- P1 est configuré en tant que réflecteur intégré d'artère (rr) avec l'individu de prochain-saut et il joint deux domaines ou LDP LSP d'IGP.
- Sur P1, le prochain saut pour PE31 est changé à P2 et la mise à jour est reçue par l'intermédiaire du BGP avec l'ipv4 + l'étiquette (RFC3107). L'étiquette BGP est permutée avec la nouvelle étiquette parce que le prochain-saut est changé et l'étiquette d'IGP est poussée sur le dessus.
- Le paquet sort du noeud P1 avec trois étiquettes et l'étiquette 30 de service est intacte. C'est-à-dire, de service 30 L3VPN étiquette BGP l'étiquette, les 101, et étiquette de 201 LDP.
- L'étiquette de dessus LDP permute dedans l'intradomain LDP LSP et le paquet atteint P2 avec deux étiquettes après PHP.
- Sur P2, le prochain saut pour PE31 est changé de nouveau et il est accessible par l'intermédiaire de l'IGP. L'étiquette BGP est retirée pendant qu'une étiquette BGP d'implicite-null est reçue de PE31 pour le PHP.
- Les feuilles de paquet avec deux étiquettes. Par exemple, l'étiquette de service 30 L3VPN et l'étiquette de 110 LDP.
- Sur PE31, le paquet arrive avec une étiquette après le PHP de l'étiquette LDP et basé sur l'étiquette 30 de service. Le paquet non étiqueté est expédié à la destination CE31 sous le Virtual Routing and Forwarding (VRF).

Quand vous regardez la pile de mpls label, on observe la commutation du paquet entre un périphérique source et de destination basé sur le préfixe précédent et l'échange d'étiquette dans l'environnement de commutation MPLS.

Figure 6

Convergence de Préfixe-indépendant BGP (PIC BGP)

C'est une technologie Cisco qui est utilisée dans des scénarios de panne BGP. Le réseau converge sans perte des secondes traditionnelles dans la reconvergence BGP. Quand la PIC BGP est utilisée, la plupart des scénarios de panne peuvent être réduits à un temps de reconvergence en-dessous de 100 millisecondes.

Comment est-ce que ceci est allé ?

Traditionnellement quand le BGP détecte une panne, il recalcule pour chaque entrée BGP pour le meilleur chemin. Quand il y a une table de routage avec des milliers d'entrées de route, ceci peut prendre un temps considérable. En outre, ce routeur BGP doit distribuer tous ces nouveaux meilleurs chemins à chacun de ses voisins afin de les informer de la topologie du réseau changée et des meilleur-chemins changés. Comme dernière étape, chacun des besoins réceptifs de speakers BGP d'effectuer un meilleur calcul de chemin afin de trouver les nouveaux meilleurs chemins.

Chaque fois que le premier speaker BGP détecte quelque chose mal, il commence le meilleur calcul de chemin jusqu'à ce que tous ses speakers BGP voisins aient fait leur recalcul, la circulation pourrait être lâché.

Figure 7

La PIC BGP pour la caractéristique IP et MPLS VPN améliore la convergence BGP après une panne de réseau. Cette convergence s'applique aux pannes de noyau et de périphérie et peut être utilisée dans l'IP et les réseaux MPLS. La PIC BGP pour l'IP et la caractéristique MPLS VPN crée et enregistre voie de déroutement de sauvegarde/dans la base d'informations de routage (NERVURE), le Forwarding Information Base (FIB), et le Technologie Cisco Express Forwarding (CEF) de sorte que quand une panne est détectée, voie de déroutement de sauvegarde/puisse immédiatement succéder, ainsi elle active le Basculement rapide.

Avec une réécriture simple des informations de prochain-saut la circulation est restaurée. Supplémentaire la convergence BGP de réseau se produit à l'arrière-plan, mais la circulation n'est plus affectée. Cette réécriture se produit dans un délai de 50 millisecondes. Si vous utilisez cette technologie, la convergence de réseau est réduite à des secondes à 50 millisecondes plus la convergence d'IGP.

Ajouter-chemin BGP

L'Ajouter-chemin BGP est une amélioration sur la façon dont des entrées BGP sont communiquées entre les speakers BGP. Si sur un certain speaker BGP il y a plus qu'une seule entrée vers une certaine destination, alors que le speaker BGP envoie seulement l'entrée qui est son meilleur chemin pour cette destination à ses voisins. Le résultat est qu'aucune disposition n'est prise afin de permettre la publicité des plusieurs chemins pour la même destination.

L'Ajouter-chemin BGP est une caractéristique BGP pour laisser plus comme seulement meilleur chemin, et permet des plusieurs chemins pour la même destination sans nouveaux chemins remplaçant implicitement les précédents. Cette extension au BGP est particulièrement importante afin de faciliter avec la PIC BGP, quand des artère-réflecteurs BGP sont utilisés, de sorte que les différents speakers BGP dans COMME ont accès à plus de chemins BGP comme juste « meilleur chemin BGP » selon le route-reflector.

Remplaçants sans boucles et rLFA pour la convergence rapide d'IGP

Exécutions pour réaliser la restauration de 50 millisecondes après qu'un lien ou une panne de noeud puisse être simplifié excessivement avec l'introduction d'une nouvelle technologie appelée les remplaçants sans boucles (LFAs). Le LFA améliorent les protocoles de routage d'état de lien (IS-IS et OSPF) afin de trouver des chemins de détournement d'une manière sans boucles. Le LFA permet à chaque routeur pour définir et utiliser un chemin de sauvegarde prédéterminé si une contiguïté (noeud ou lien de réseau) échoue. Afin de fournir un temps de restauration 50 millisecondes en cas de pannes de lien ou de noeud, MPLS TE FRR peut être déployé. Cependant, ceci exige l'ajout d'un autre protocole (RSVP Protocol, ou d'un RSVP) pour l'installation et la Gestion des tunnels TE. Tandis que ceci pourrait être nécessaire pour la gestion de la bande passante, l'exécution de protection et de restauration n'exige pas la gestion de la bande passante. Par conséquent, le temps système associé en plus du RSVP TE est considéré élevé pour la protection simple des liens et des Noeuds.

Le LFA peut fournir une technique simple et facile sans déploiement du RSVP TE dans de tels scénarios. En raison de ces techniques, les Routeurs interconnectés d'aujourd'hui dans les réseaux à grande échelle peuvent fournir la restauration 50 millisecondes pour des pannes de lien et de noeud sans configuration requise pour l'opérateur.

Figure 8

Le LFA-FRR est un mécanisme qui assure la protection locale pour le trafic unicast dans l'IP, le MPLS, le Fonction Ethernet over MPLS (EoMPLS), le Multiplexage inversé pour ATM (IMA) au-dessus du MPLS, le service d'émulation de circuits au-dessus du réseau de commutation de paquets (CESoPSN) au-dessus du MPLS, et le multiplexage temporel Structure-agnostique au-dessus du paquet (SAToP) au-dessus des réseaux MPLS. Cependant, quelques topologies (telles que la topologie d'anneau) exigent la protection qui n'est pas eue les moyens par seul LFA-FRR. La caractéristique du distant LFA-FRR est utile dans de telles situations.

Le distant LFA-FRR étend le comportement de base de LFA-FRR à n'importe quelle topologie. Il en avant le trafic autour d'un noeud défectueux à un distant LFA qui est plus d'un saut loin. Dans la figure 9, si le lien entre C1 et C2 n'atteint pas A1 puis le C2 envoie le paquet au-dessus d'une session dirigée LDP à C5 qui a l'accessibilité à A1.

Figure 9

Dans le distant LFA-FRR, un noeud calcule dynamiquement son noeud LFA. Après que le noeud alternatif soit déterminé (qui n'est pas directement connecté), le noeud établit automatiquement une session dirigée du protocole de distribution d'étiquette (LDP) au noeud alternatif. La session dirigée LDP permute des étiquettes pour la correction d'erreurs de transfert particulière (FEC).

Quand le lien échoue, les utilisations de noeud étiquettent l'empilement afin de percer un tunnel le trafic au noeud LFA de distant, afin d'expédier le trafic à la destination. Tous les échanges et Tunnellisation d'étiquette au noeud LFA de distant sont dynamiques en nature et preprovisioning n'est pas exigé. Le mécanisme d'échange et de Tunnellisation d'étiquette de totalité est dynamique et n'implique pas n'importe quel ravitaillement manuel.

Pour l'intradomain LSP, le distant LFA FRR est utilisé pour le trafic de l'unicast MPLS dans des topologies de sonnerie. Precalculates LFA FRR de distant un chemin de sauvegarde pour chaque préfixe dans la table de routage d'IGP, qui permet au noeud pour commuter rapidement au chemin de sauvegarde quand une panne est produite. Ceci fournit des temps de rétablissement sur l'ordre de 50 millisecondes.

Exemple d'architecture de Cisco Unified MPLS

Quand tous les outils et caractéristiques précédents sont remontés dans un environnement de réseau, il crée l'environnement de réseau MPLS de Cisco Unified. C'est l'exemple d'architecture pour de grands fournisseurs de services.

Figure 10

- Le noyau et l'agrégation sont organisés en tant que domaines distincts IGP/LDP.
- Interdomain LSP hiérarchiques basé sur RFC 3107, BGP IPv4+ étiquette qui sont étendus au Pre-agg.
- Intradomain LSP basé sur le LDP.
- Le noyau d'interdomain/agrégation LSP sont étendus dans les réseaux d'Access par la distribution de l'Interior Gateway Protocol par radio de réseaux d'Access (A EXÉCUTÉ L'IGP) dans l'iBGP d'interdomain et distribuent les préfixes étiquetés nécessaires d'iBGP passerelle

(MPC (noyau mobile de paquet)) dans A EXÉCUTÉ L'IGP (par l'intermédiaire des communautés BGP).

Exemple unifié de configuration MPLS

Ici ia un exemple simplifié de MPLS unifié.

Routeur de cadre de principale zone - Cisco IOS? XR

Routeurs de passerelle de site de Pré-agrégation et de cellules - Cisco IOS

Figure 11

200:200 La Communauté MPC
300:300 La Communauté d'agrégation

Principal domaine d'IGP	Niveau 2 d'ISIS
Domaine d'IGP d'agrégation	Niveau 1 d'ISIS
Domaine d'IGP d'Access	OSPF 0 zones

Configuration de routeur de cadre de principale zone

Figure 12

```
! IGP Configuration
router isis core-agg
net 49.0100.1010.0001.0001.00
address-family ipv4 unicast
metric-style wide
propagate level 1 into level 2 route-policy drop-all ! Disable L1 to L2 redistribution
!
interface Loopback0
ipv4 address 10.10.10.1 255.255.255.255
passive
!
interface TenGigE0/0/0/0
!
interface TenGigE0/0/0/1
circuit-type level-2-only                    ! Core facing ISIS L2 Link

!
interface TenGigE0/0/0/2
circuit-type level-1                        ! Aggregation facingis ISIS L1 Link

  !
route-policy drop-all
drop
end-policy

! BGP Configuration

router bgp 100
```

```
bgp router-id 10.10.10.1
address-family ipv4 unicast
allocate-label all                              ! Send labels with BGP routes
!
session-group infra
remote-as 100
cluster-id 1001
update-source Loopback0
!
neighbor-group agg
use session-group infra
address-family ipv4 labeled-unicast
  route-reflector-client

   route-policy BGP_Egress_Filter out         ! BGP Community based Egress filtering

   next-hop-self
!
neighbor-group mpc
use session-group infra
address-family ipv4 labeled-unicast
  route-reflector-client
   next-hop-self
!
neighbor-group core
use session-group infra
address-family ipv4 labeled-unicast
  next-hop-self

community-set Allowed-Comm
200:200,
300:300,
!
route-policy BGP_Egress_Filter
if community matches-any Allowed-Comm then
  pass
```

Configuration de Pré-agrégation

Figure 13

```
interface Loopback0
ipv4 address 10.10.9.9 255.255.255.255
!
interface Loopback1
ipv4 address 10.10.99.9 255.255.255.255

! Pre-Agg IGP Configuration

router isis core-agg
net 49.0100.1010.0001.9007.00
is-type level-1                                    !  ISIS L1 router
metric-style wide
passive-interface Loopback0                        !  Core-agg IGP loopback0

!RAN Access IGP Configuration

router ospf 1
router-id 10.10.99.9
redistribute bgp 100 subnets route-map BGP_to_RAN     !  iBGP to RAN IGP redistribution
network 10.9.9.2 0.0.0.1 area 0
```

```
network 10.9.9.4 0.0.0.1 area 0
network 10.10.99.9 0.0.0.0 area 0
distribute-list route-map Redist_from_BGP in          !  Inbound filtering to prefer
     labeled BGP learnt prefixes

ip community-list standard MPC_Comm permit 200:200
!
route-map BGP_to_RAN permit 10                       ! Only redistribute prefixes
     marked with MPC community
 match community MPC_Comm
set tag 1000
route-map Redist_from_BGP deny 10
match tag 1000
!
route-map Redist_from_BGP permit 20


! BGP Configuration
router bgp 100
bgp router-id 10.10.9.10
bgp cluster-id 909
neighbor csr peer-group
neighbor csr remote-as 100
neighbor csr update-source Loopback100               ! Cell Site - Routers RAN IGP
     loopback100 as source
neighbor abr peer-group
neighbor abr remote-as 100
neighbor abr update-source Loopback0                 ! Core POP ABRs - core-agg IGP
     loopback0 as source
neighbor 10.10.10.1 peer-group abr
neighbor 10.10.10.2 peer-group abr
neighbor 10.10.13.1 peer-group csr
!
address-family ipv4
bgp redistribute-internal
network 10.10.9.10 mask 255.255.255.255 route-map AGG_Comm   ! Advertise with
     Aggregation Community (100:100)
redistribute ospf 1                                  !  Redistribute RAN IGP prefixes
neighbor abr send-community
neighbor abr next-hop-self

 neighbor abr send-label                             !  Send labels with BGP routes
neighbor 10.10.10.1 activate
neighbor 10.10.10.2 activate
exit-address-family
!
route-map AGG_Comm permit 10
set community 300:300
```

Configuration de la passerelle de site de cellules (CSG)

Figure 14

```
interface Loopback0
ip address 10.10.13.2 255.255.255.255

! IGP Configuration
router ospf 1
router-id 10.10.13.2
network 10.9.10.0 0.0.0.1 area 0
network 10.13.0.0 0.0.255.255 area 0
```

```
network 10.10.13.3 0.0.0.0 area 0
```

Configuration MTG

Figure 15

```
Interface lookback0
ip address 10.10.11.1 255.255.255.255

! IGP Configuration
router isis core-agg
is-type level-2-only                          !  ISIS L2 router
net 49.0100.1010.0001.1001.00
address-family ipv4 unicast
metric-style wide

! BGP Configuration
router bgp 100
bgp router-id 10.10.11.1
address-family ipv4 unicast
network 10.10.11.1/32 route-policy MPC_Comm   ! Advertise Loopback-0 with MPC Community
allocate-label all                            ! Send labels with BGP routes
!
session-group infra

remote-as 100
update-source Loopback0
!
neighbor-group abr
use session-group infra
address-family ipv4 labeled-unicast
  next-hop-self
!
neighbor 10.10.6.1
use neighbor-group abr
!
neighbor 10.10.12.1
use neighbor-group abr

community-set MPC_Comm
200:200
end-set
!
route-policy MPC_Comm
set community MPC_Comm
end-policy
```

Vérifiez

Le préfixe de bouclage de la passerelle mobile de paquet (MPG) est 10.10.11.1 /32, de sorte que le préfixe soit d'intérêt. Maintenant, le regardez comment des paquets sont expédiés de CSG à MPG.

Le préfixe 10.10.11.1 MPC est connu au routeur CSG de Pre-agg avec la balise 1000 d'artère et elle peut être expédiée comme paquet étiqueté avec l'étiquette sortante 31 LDP (intra domaine LDP LSP). La communauté MPC 200:200 a été tracée avec la balise 1000 d'artère dans le noeud de Pre-agg tandis que la redistribution est dans l'OSPF.

Sortie de noeud CSG

```
CSG#sh mpls forwarding-table 10.10.11.1 detail
Local     Outgoing   Prefix          Bytes Label  Outgoing   Next Hop
Label     Label      or Tunnel Id     Switched     interface
34         31         10.10.11.1/32   0            Vl40       10.13.1.0
      MAC/Encaps=14/18, MRU=1500, Label Stack{31}
```

Sorties de noeud de Pre-Agg

Dans le noeud de Pre-agg, le préfixe MPC est redistribué du BGP à A EXÉCUTÉ le processus OSPF d'accès avec le filtrage à caractère communautaire et le processus OSPF est redistribué dans le BGP. Cette redistribution commandée est nécessaire afin de rendre l'IP de bout en bout reachabilty, en même temps chaque segment a les artères exigées par minimum.

Le préfixe 10.10.11.1/32 est connu par l'intermédiaire de BGP hierarichal 100 avec la communauté MPC 200:200 reliée. 16020 l'étiquette BGP 3107 reçue du routeur de cadre de principale zone (ABR) et l'étiquette 22 LDP est ajoutée sur le dessus pour l'expédition d'intradomain après la prochaine recherche récursive de saut.

```
Pre-AGG1#sh ip route 10.10.11.1
Routing entry for 10.10.11.1/32
Known via "bgp 100", distance 200, metric 0, type internal
Redistributing via ospf 1
Advertised by ospf 1 subnets tag 1000 route-map BGP_TO_RAN
Routing Descriptor Blocks:
* 10.10.10.2, from 10.10.10.2, 1d17h ago
    Route metric is 0, traffic share count is 1
    AS Hops 0
    MPLS label: 16020

Pre-AGG1#sh bgp ipv4 unicast 10.10.11.1
BGP routing table entry for 10.10.11.1/32, version 116586
Paths: (2 available, best #2, table default)
Not advertised to any peer
Local
  <SNIP>
Local
  10.10.10.2 (metric 30) from 10.10.10.2 (10.10.10.2)
    Origin IGP, metric 0, localpref 100, valid, internal, best
    Community: 200:200
    Originator: 10.10.11.1, Cluster list: 0.0.3.233, 0.0.2.89
    mpls labels in/out nolabel/16020

Pre-AGG1#sh bgp ipv4 unicast labels
  Network          Next Hop     In label/Out label
  10.10.11.1/32 10.10.10.1   nolabel/16021
                 10.10.10.2   nolabel/16020

Pre-AGG1#sh mpls forwarding-table 10.10.10.2 detail
Local     Outgoing  Prefix          Bytes Label   Outgoing   Next Hop
Label     Label     or Tunnel Id     Switched     interface
79         22         10.10.10.2/32 76109369     Vl10       10.9.9.1
      MAC/Encaps=14/18, MRU=1500, Label Stack{22}

Pre-AGG#sh mpls forwarding-table 10.10.11.1 detail
Local     Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label     Label      or Tunnel Id     Switched     interface
530       16020      10.10.11.1/32 20924900800   Vl10       10.9.9.1
```

```
      MAC/Encaps=14/22, MRU=1496, Label Stack{22 16020}
```

Principales sorties de noeud d'ABR

Le préfixe **10.10.11.1 est connu par l'intermédiaire de l'IGP d'intradomain (ISIS-L2)** et selon la table d'expédition MPLS. Il est accessible par LDP LSP.

```
ABR-Core2#sh ip route 10.10.11.1
Routing entry for 10.10.11.1/32
Known via "isis core-agg", distance 115, metric 20, type level-2
Installed Sep 12 21:13:03.673 for 2w3d
Routing Descriptor Blocks
  10.10.1.0, from 10.10.11.1, via TenGigE0/0/0/0, Backup
    Route metric is 0
  10.10.2.3, from 10.10.11.1, via TenGigE0/0/0/3, Protected
    Route metric is 20
No advertising protos.
```

Pour la distribution des préfixes entre les zones segmentées, le BGP avec l'étiquette (RFC 3107) est utilisé. Quels besoins de résider toujours dans les régions segmentées de l'IGP sont les bouclages du siège potentiel d'explosion et des adresses liés à l'infrastructure centrale.

Les routeurs BGP qui connectent différentes zones ensemble sont les abr qui agissent en tant que route-reflector BGP. Ces périphériques emploient la caractéristique de next-hop-self, afin d'éviter la nécessité d'avoir tous les Prochain-sauts de l'Autonomous System complet dans l'IGP, au lieu seulement des adresses IP du siège potentiel d'explosion et de l'infrastructure centrale. La détection de boucle est terminée a basé sur les bgp cluster-id.

Pour la résilience du réseau, la PIC BGP avec le BGP ajoutent la caractéristique de chemin devrait être utilisée avec le BGP et le LFA avec l'IGP. Ces caractéristiques ne sont pas utilisées dans l'exemple précédent.

Dépannez

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

Informations connexes

- Architecture sans couture MPLS
- Livre Blanc de Cisco Unified MPLS
- Système Cisco Carrier Packet Transport (CPT)
- Support et documentation techniques - Cisco Systems