

Funciones unificadas, características, y ejemplo de configuración MPLS

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Evolución de la red](#)

[Cisco unificó el MPLS](#)

[Características y componentes](#)

[Lleve la información de la escritura de la etiqueta en BGP-4 \(el RFC 3107\)](#)

[Convergencia de la Prefijo-independiente BGP \(IMAGEN BGP\)](#)

[Agregar-trayectoria BGP](#)

[Suplentes sin loop y rLFA para la convergencia rápida IGP](#)

[Cisco unificó el ejemplo de la arquitectura MPLS](#)

[Ejemplo unificado de la configuración de MPLS](#)

[Router del borde del área de la base -¿Cisco IOS? XR](#)

[Configuración del router del borde del área de la base](#)

[Configuración de la PRE-agregación](#)

[Configuración del gateway del sitio de la célula \(CSG\)](#)

[Configuración del MTG](#)

[Verificación](#)

[Salida del nodo CSG](#)

[Salidas del nodo PRE-Agg](#)

[Salidas del nodo de la base ABR](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe el Multiprotocol Label Switching (MPLS) unificado, que está todo sobre el escalamiento. Proporciona un marco de las soluciones de la tecnología para traer el tráfico de extremo a extremo y/o los servicios simples a través de una infraestructura tradicionalmente dividida en segmentos. Hace uso de las ventajas de una infraestructura jerárquica mientras que mejora el scalability y la simplicidad del diseño de red.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Evolución de la red

Cuando usted mira el historial de los servicios del paquete basado de la red, después un cambio en los valores de negocio de la red puede ser observado. Esto va de las mejoras de conexión discretas para hacer las aplicaciones tan fluidas como sea posible, a las Tecnologías de la Colaboración para soportar la Colaboración móvil. Finalmente, presentan a los servicios a pedido de la nube con los servicios de aplicación para optimizar las herramientas usadas con una organización y mejorar la estabilidad y el costo de propiedad.

Figura 1

Esta mejora continua del valor y de las funciones de la red da lugar a una necesidad mucho más penetrante de la simplicidad, de la manejabilidad, de la integración, y de la estabilidad de la red donde las redes se han dividido en segmentos como resultado de las islas operativas desunidas y de ningún control real del trayecto de extremo a extremo. Ahora hay una necesidad de traerla que toda así como una sola arquitectura que sea fácil de manejar, proporcione el scalability a 100,000's de los Nodos, y utiliza las Tecnologías actuales de la Alta disponibilidad y de la convergencia rápida. Esto es lo que trae el MPLS unificado a la tabla, que es la red dividida en segmentos en una visibilidad del avión y del trayecto de extremo a extremo del solo control.

Requisitos de la red moderna

- Aumente la demanda del ancho de banda (el vídeo)
- Aumente la complejidad de la aplicación (nube y la virtualización)
- Aumente la necesidad de la convergencia (la movilidad)

¿Cómo puede usted simplificar las operaciones MPLS en redes cada vez más grandes con más requisitos de aplicación compleja?

Desafíos tradicionales MPLS con diversas Tecnologías del acceso

- Complejidad para alcanzar la convergencia de 50 milisegundos con el Fast ReRoute de la ingeniería de tráfico (TE FRR)
- Necesite para los Routing Protocol y la interacción sofisticados con los protocolos de la capa 2
- Parta las Redes grandes en los dominios mientras que los servicios son de punta a punta entregado
- Mecanismos de punta a punta comunes de la convergencia y de la elasticidad
- Troubleshooting y disposición de punta a punta a través de los dominios múltiples

La atracción unificada MPLS se resume en esta lista:

- Número reducido de puntas operativas. En las Plataformas generales del transporte, un servicio tiene que ser configurado en cada elemento de redes vía las puntas operativas. El sistema de administración tiene que conocer la topología. En el MPLS unificado, con la integración de todas las islas MPLS, el número mínimo de puntas operativas se alcanza.
- Posibilidad para provision fácilmente los servicios: Acode 3 (L3) VPN, agencia de noticias privada virtual (VPWS), servicio virtual del LAN privado (VPL), sin la pseudowire-costura (Picoavatio-costura) o los mecanismos de InterAS. Con la introducción de MPLS dentro de la agregación, se evita una cierta configuración estática que crea las islas MPLS.
- Proporcione el transporte de punta a punta MPLS.
- Mantenga las áreas del Interior Gateway Protocol (IGP) las tablas de ruteo separadas y pequeñas.
- Convergencia rápida.
- Fácil configurar y resolver problemas.
- Capacidad de integrar con cualquier tecnología del acceso.
- Disposición del IPv6.

Cisco unificó el MPLS

El MPLS unificado es definido por la adición de funciones extra con el MPLS clásico/tradicional y da más scalability, Seguridad, simplicidad y manejabilidad. Para entregar los servicios MPLS de punta a punta, la trayectoria etiquetada de punta a punta de los Switches (LSP) es necesaria. La meta es guardar los servicios MPLS (MPLS VPN, MPLS L2VPN) pues son, sino introducir el mayor scalability. Para hacer esto, trasládese algunos de los prefijos IGP al Border Gateway Protocol (BGP) (los prefijos del loopback de los Routers del borde del proveedor (PE)), que entonces distribuye los prefijos de punta a punta.

Figura 2

Antes de que se discuta la arquitectura unificada Cisco MPLS, es importante entender las características fundamentales usadas para hacer esto una realidad.

Características y componentes

Lleve la información de la escritura de la etiqueta en BGP-4 (el RFC 3107)

Es un requisito previo para tener un método escalable para intercambiar los prefijos entre los segmentos de red. Usted podría combinar simplemente los IGP (Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), o el Enhanced Interior Gateway Routing Protocol (EIGRP)) en un solo dominio. Sin embargo un IGP no se diseñó para llevar 100,000s de los prefijos. El protocolo de la opción para ese propósito es BGP. Es un protocolo bien-probado que soporta Internet con 100,000's de las rutas y de los entornos MPLS-VPN con millones de entradas. Cisco unificó las aplicaciones BGP-4 MPLS con el intercambio de información de la escritura de la etiqueta (RFC3107). Cuando el BGP distribuye una ruta, puede también distribuir una escritura de la etiqueta MPLS que se asocia a esa ruta. La información de mapeo de la escritura de la etiqueta MPLS para la ruta se lleva adentro el mensaje de la actualización de BGP que contiene la información sobre la ruta. Si el salto siguiente no se cambia, se preserva la escritura de la etiqueta y los cambios de la escritura de la etiqueta si el salto siguiente cambia. En el MPLS unificado, el salto siguiente cambia en los routers del borde del área (ABR).

Cuando usted habilita el RFC 3107 en ambos routers BGP, el Router hace publicidad el uno al otro que él puede entonces enviar las escrituras de la etiqueta MPLS con las rutas. Si el Router negocia con éxito su capacidad de enviar las escrituras de la etiqueta MPLS, el Router agrega las escrituras de la etiqueta MPLS a todas las actualizaciones de BGP salientes.

El intercambio de la escritura de la etiqueta es necesario para guardar la información de trayecto de extremo a extremo entre los segmentos. Como consecuencia, cada segmento llega a ser bastante pequeño para ser manejado por los operadores y al mismo tiempo hay información de circuito distribuida para la conciencia de la trayectoria entre dos diversos altavoces IP.

¿Cómo trabaja?

Figura 3

En el cuadro 3 usted puede ver que hay tres segmentos con el Discovery Protocol de la escritura de la etiqueta etiquetado la trayectoria del Switches (LDP LSP) y la red de acceso no tiene LDP habilitado. El objetivo es unirse a lo junto de modo que haya una sola trayectoria MPLS (Internal BGP (iBGP) LSP jerárquico) entre los Nodos de la PRE-agregación (PRE-Agg). Pues la red es un solo sistema BGP, todas las sesiones son sesiones del iBGP. Cada segmento funciona con sus propias trayectorias IGP (OSPF, IS-IS, o EIGRP) y LDP LSP dentro del dominio IGP. Dentro de Cisco unificó el MPLS, el Router (ABR) que se une a los segmentos debe ser reflectores de ruta en línea BGP con el Siguiendo-Salto-uno mismo y el RFC 3107 para llevar un IPv4 + la escritura de la etiqueta configurados en las sesiones. Estos BGP de conversaciones están dentro de la arquitectura unificada Cisco MPLS referida como a ABR.

¿Por qué son los ABR reflectores de ruta en línea?

Una de las metas del MPLS unificado es tener una infraestructura de punta a punta altamente escalable. Así, cada segmento se debe mantener simple para actuar. Todos los peerings son peerings del iBGP, por lo tanto hay una necesidad de un full-mesh de los peerings entre todos los interlocutores iBGP dentro de la red completa. Eso da lugar a un entorno de red muy poco práctico si hay millares de BGP de conversaciones. Si los ABR se hacen los reflectores de ruta, el número de mirada del iBGP se reduce al número del por-segmento de los BGP de conversaciones” en vez entre “de todos los” BGP de conversaciones del completo COMO.

¿Por qué Siguiendo-Salto-uno mismo?

El BGP actúa encendido la base de las operaciones de búsqueda del ruteo recursivo. Esto se hace para acomodar el scalability dentro del IGP subyacente se utiliza que. Para las operaciones de búsqueda recurrentes, el BGP utiliza el Next-Hop asociado a cada entrada de la ruta BGP. Así, por ejemplo, si un nodo de origen desea de enviar un paquete a un nodo de destino y si el paquete golpea al router BGP, después el router BGP hace las operaciones de búsqueda de la encaminamiento en su tabla de BGP Routing. Encuentra una ruta hacia el nodo de destino y encuentra el Next-Hop como siguiente paso. Este Next-Hop se debe saber por el IGP subyacente. Como el último paso, el router BGP adelanta el paquete hacia adelante basado sobre información de la escritura de la etiqueta IP y MPLS asociados a ese Next-Hop.

Para asegurarse que dentro de cada segmento solamente los saltos siguientes son necesarios ser sabidos por el IGP, es necesario que el Next-Hop asociado a la entrada BGP está dentro del segmento de red y no dentro de un vecino o más lejos de un segmento. Si usted reescribe el Next-Hop BGP con la característica del Siguiete-Salto-uno mismo, asegúrese de que el Next-Hop esté dentro del segmento local.

Júntelo todo

‘Figura 4’

El cuadro 4 proporciona un ejemplo de cómo el prefijo “A” L3 VPN y el intercambio de la escritura de la etiqueta actúa y de cómo la pila de etiquetas MPLS se crea para tener la información de trayecto de extremo a extremo para el flujo de tráfico entre ambos PE.

La red se divide como tres dominios independientes IGP/LDP. El tamaño reducido de la encaminamiento y de las tablas de reenvío en el Routers es habilitar una mejor estabilidad y una convergencia más rápida. El LDP se utiliza para construir el intradomain LSP dentro de los dominios. Las escrituras de la etiqueta del RFC 3107 BGP IPv4+ se utilizan como Label Distribution Protocol del interdomain para construir BGP jerárquico LSP a través de los dominios. BGP3107 inserta una escritura de la etiqueta adicional en la pila de etiquetas de envío en la arquitectura unificada MPLS.

Intradomain - LDP LSP

Interdomain - BGP LSP jerárquico

Figura 5

El VPN prefija “A” es hecho publicidad por PE31 a PE11 con la escritura de la etiqueta 30 del servicio L3VPN y el salto siguiente como loopback PE31 vía el interdomain de punta a punta BGP jerárquico LSP. Ahora, mirada en el trayecto de reenvío para el prefijo “A” VPN de PE11 a PE31.

- En PE11, prefije A se sabe vía la sesión de BGP con PE31 pues el Next-Hop PE31 y PE31 es recurrentemente accesible vía el P1 con la escritura de la etiqueta 100 BGP. PE11 recibió la información del IPv4 + de la escritura de la etiqueta del P1 como actualizaciones de BGP porque se habilita con la característica del RFC 3107 para enviar la información del IPv4 + de la escritura de la etiqueta.
- El P1 es accesible de PE11 vía el intradomain LDP LSP y agrega otra escritura de la etiqueta LDP encima de la escritura de la etiqueta BGP. Finalmente, el paquete sale del nodo PE11 con tres escrituras de la etiqueta. Por ejemplo, la escritura de la etiqueta del servicio 30

- L3VPN, la escritura de la etiqueta de 100 BGP, y la escritura de la etiqueta de 200 LDP IGP.
- La escritura de la etiqueta del top LDP continúa intercambiando adentro el intradomain LDP LSP y el paquete alcanza el P1 con dos escrituras de la etiqueta después del Penultimate Hop Popping (PHP).
- Se configura el P1 mientras que el reflector de ruta en línea (RR) con el uno mismo y él del Next-Hop se une a dos dominios IGP o LDP LSP.
- En el P1, el salto siguiente para PE31 se cambia al P2 y la actualización se recibe vía el BGP con el IPv4 + la escritura de la etiqueta (RFC3107). La escritura de la etiqueta BGP se intercambia con la nueva escritura de la etiqueta porque se cambia el Next-Hop y la escritura de la etiqueta IGP se avanza en el top.
- El paquete sale del nodo P1 con tres escrituras de la etiqueta y la escritura de la etiqueta 30 del servicio está sin tocar. Es decir, la escritura de la etiqueta del servicio 30 L3VPN, escritura de la etiqueta de 101 BGP, y escritura de la etiqueta de 201 LDP.
- La escritura de la etiqueta del top LDP intercambia adentro el intradomain LDP LSP y el paquete alcanza el P2 con dos escrituras de la etiqueta después del PHP.
- En el P2, el salto siguiente para PE31 se cambia otra vez y es accesible vía el IGP. Se quita la escritura de la etiqueta BGP mientras que una escritura de la etiqueta implícito-nula BGP se recibe de PE31 para el PHP.
- Las hojas del paquete con dos escrituras de la etiqueta. Por ejemplo, la escritura de la etiqueta del servicio 30 L3VPN y la escritura de la etiqueta de 110 LDP.
- En PE31, el paquete llega con una escritura de la etiqueta después del PHP de la escritura de la etiqueta LDP y basado en la escritura de la etiqueta 30 del servicio. El paquete sin etiqueta se remite al destino CE31 bajo el ruteo virtual y expedición (VRF).

Cuando usted mira la pila de etiquetas MPLS, la transferencia del paquete entre un dispositivo de origen y de destino basado sobre el prefijo anterior y el intercambio de la escritura de la etiqueta se observa dentro del Switching Environment MPLS.

'Figura 6'

Convergencia de la Prefijo-independiente BGP (IMAGEN BGP)

Ésta es una tecnología de Cisco que se utiliza en los escenarios de falla BGP. La red converge sin una pérdida de los segundos tradicionales en el reconvergence BGP. Cuando se utiliza la IMAGEN BGP, la mayoría de los escenarios de falla se pueden reducir a un rato del reconvergence debajo de 100 milisegundos.

¿Cómo se hace esto?

Tradicionalmente cuando el BGP detecta un error, recalcula para cada entrada BGP para el mejor trayecto. Cuando hay una tabla de ruteo con los millares de entradas de la ruta, éste puede tomar una cantidad de tiempo considerable. Además, este router BGP necesita distribuir todos esos nuevos mejores trayectos a cada uno de sus vecinos para informarles la topología de red cambiada y los mejores trayectos cambiados. Como el último paso, cada uno de las necesidades receptoras de los BGP de conversaciones de hacer un cálculo del mejor trayecto para encontrar los nuevos mejores trayectos.

Cada vez que el primer BGP de conversación detecta algo mal, comienza el cálculo del mejor trayecto hasta que los todos sus vecinos BGP de conversaciones hayan hecho su cálculo, el flujo

de tráfico puede ser que sea caído.

Figura 7

La IMAGEN BGP para la característica IP y del MPLS VPN mejora la convergencia BGP después de un desperfecto de la red. Esta convergencia es aplicable a los errores de la base y del borde y se puede utilizar en el IP y las redes MPLS. La IMAGEN BGP para el IP y la característica del MPLS VPN crea y salva un respaldo/un trayecto alternativo en el Routing Information Base (RIB), la Base de información de reenvío (FIB), y el Cisco Express Forwarding (CEF) de modo que cuando detectan a un error, el respaldo/el trayecto alternativo pueda asumir el control inmediatamente, así habilita la Conmutación por falla rápida.

Con una sola reescritura de la información del Next-Hop se restablece el flujo de tráfico. La convergencia BGP de la red sucede además en el fondo, pero los flujos de tráfico no se afectan más. Esta reescritura sucede en el plazo de 50 milisegundos. Si usted utiliza esta tecnología, la convergencia de red se reduce a partir de los segundos a 50 milisegundos más la convergencia IGP.

Agregar-trayectoria BGP

La Agregar-trayectoria BGP es una mejora en cómo las entradas BGP se comunican entre los BGP de conversaciones. Si en cierto BGP de conversación hay más que una sola entrada hacia cierto destino, después que el BGP de conversación envía solamente la entrada que es su mejor trayecto para ese destino a sus vecinos. El resultado es que no se adopta ningunas disposiciones para permitir el anuncio de los trayectos múltiples para el mismo destino.

La Agregar-trayectoria BGP es una característica BGP para permitir más como solamente el mejor trayecto, y permite los trayectos múltiples para el mismo destino sin las nuevas trayectorias que substituyen implícito los anteriores. Esta extensión al BGP es determinado importante para ayudar con la IMAGEN BGP, cuando se utilizan los reflectores de ruta BGP, de modo que los diversos BGP de conversaciones dentro del COMO tienen acceso a más trayectos BGP como apenas el “mejor trayecto BGP” de acuerdo con el reflector de ruta.

Suplentes sin loop y rLFA para la convergencia rápida IGP

Operaciones para alcanzar la restauración de 50 milisegundos después de que un link o una falla de nodo se pueda simplificar dramáticamente con la introducción de una tecnología nueva llamada los suplentes sin loop (LFAs). El LFA aumenta los protocolos Link-State Routing (IS-IS y OSPF) para encontrar las trayectorias del ruteo alternativo de una manera sin loop. El LFA permite que cada router defina y utilice un trayecto de backup predeterminado si una adyacencia (nodo de red o link) falla. Para entregar un rato de 50 restauraciones msec en caso del link o de las fallas de nodo, el MPLS TE FRR puede ser desplegado. Sin embargo, esto requiere la adición de otro protocolo (Resource Reservation Protocol, o de RSVP) para la configuración y la Administración de los túneles TE. Mientras que esto pudo ser necesario para la administración del ancho de banda, la operación de la protección y de la restauración no requiere la administración del ancho de banda. Por lo tanto, el asociado de arriba con la adición de RSVP TE se considera alto para la protección simple de los links y de los Nodos.

El LFA puede proporcionar una técnica simple y fácil sin el despliegue de RSVP TE en tales

escenarios. Como resultado de estas técnicas, el Router interconectado de hoy en las redes a gran escala puede entregar la restauración en 50 ms para el link y las fallas de nodo sin los requisitos para la configuración para el operador.

Figura 8

El LFA-FRR es un mecanismo que proporciona la protección local para el tráfico de unidifusión en el IP, el MPLS, el Ethernet por MPLS (EoMPLS), el Inverse Multiplexing over ATM (IMA) sobre el MPLS, el Circuit Emulation Service sobre el Packet Switched Network (CESoPSN) sobre el MPLS, y la división de tiempo Estructura-agnóstica multiplexando sobre el paquete (SAToP) sobre las redes MPLS. Sin embargo, algunas topologías (tales como la topología en anillo) requieren la protección que no es permitida por LFA-FRR solamente. La característica del telecontrol LFA-FRR es útil en tales situaciones.

El telecontrol LFA-FRR amplía el comportamiento básico de LFA-FRR a cualquier topología. Él adelanta el tráfico alrededor de un nodo fallado a un telecontrol LFA que es más de un salto lejos. En el cuadro 9, si el link entre el C1 y el C2 no puede alcanzar el A1 entonces el C2 envía el paquete sobre una sesión LDP dirigida a C5 que tenga accesibilidad al A1.

Figura 9

En el telecontrol LFA-FRR, un nodo computa dinámicamente su nodo LFA. Después de que se determine el nodo alternativo (que no está conectado directamente), el nodo establece automáticamente una sesión dirigida del Protocolo de distribución de etiquetas (LDP) al nodo alternativo. La sesión LDP dirigida intercambia las escrituras de la etiqueta para la corrección de errores de reenvío determinada (FEC).

Cuando el link falla, las aplicaciones del nodo etiquetan empilar para hacer un túnel el tráfico al nodo LFA del telecontrol, para remitir el tráfico al destino. Todos los intercambios y Tunelización de la escritura de la etiqueta al nodo LFA del telecontrol son dinámicos en la naturaleza y el preprovisioning no se requiere. El intercambio y el mecanismo de tunelización de la escritura de la etiqueta del conjunto es dinámicos y no implica ningún aprovisionamiento manual.

Para el intradomain LSP, el telecontrol LFA FRR se utiliza para el tráfico del unicast MPLS en topologías en anillo. Precalculates LFA FRR del telecontrol un trayecto de backup para cada prefijo en la tabla de ruteo IGP, que permite que el nodo conmute rápidamente al trayecto de backup cuando encuentran a un error. Esto proporciona los tiempos de recuperación por orden de 50 milisegundos.

Cisco unificó el ejemplo de la arquitectura MPLS

Cuando todas las herramientas y características anteriores se ponen juntas dentro de un entorno de red, crea el entorno de red MPLS unificado Cisco. Éste es el ejemplo de la arquitectura para los proveedores de servicio grandes.

Figura 10

- La base y la agregación se ordenan como dominios distintos IGP/LDP.

- Interdomain los LSP jerárquicos basado en el RFC 3107, BGP IPv4+ etiqueta que se amplían hacia fuera al PRE-agg.
- Intradomain LSP basado en el LDP.
- La base del interdomain/la agregación LSP es ampliada en las redes de acceso por la distribución del protocolo Interior Gateway Protocols de radio de las redes de acceso (RAN IGP) en el iBGP del interdomain y distribuye los prefijos etiquetados necesarios del iBGP gateway (de MPC (base móvil del paquete)) en RAN IGP (vía las comunidades BGP).

Ejemplo unificado de la configuración de MPLS

Aquí ia un ejemplo simplificado del MPLS unificado.

Router del borde del área de la base -¿Cisco IOS? XR

Routers de gateway del sitio de la PRE-agregación y de la célula - Cisco IOS

Figura 11

200:200 Comunidad de MPC
300:300 Comunidad de la agregación

Dominio IGP de la base Nivel 2 ISIS
Dominio IGP de la agregación Nivel 1 ISIS
Dominio IGP del acceso OSPF 0 áreas

Configuración del router del borde del área de la base

Figura 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

```

Configuración de la PRE-agregación

Figura 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

```

Configuración del gateway del sitio de la célula (CSG)

```
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
```

Configuración del MTG

Figura 15

```
Interface loopback0
ip address 10.10.11.1 255.255.255.255
```

! IGP Configuration

```
router isis core-agg
is-type level-2-only
net 49.0100.1010.0001.1001.00
address-family ipv4 unicast
metric-style wide
```

! ISIS L2 router

! 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
allocate-label all
!
session-group infra
```

**! Advertise Loopback-0 with MPC Community
! Send labels with BGP routes**

```
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
```

Verificación

El prefijo del loopback del gateway móvil del paquete (MPG) es 10.10.11.1 /32, de modo que el prefijo esté de interés. Ahora, mirada en cómo los paquetes se remiten de CSG a MPG.

El prefijo 10.10.11.1 de MPC se sabe al router CSG del PRE-agg con la etiqueta 1000 de la ruta y puede ser remitida como paquete etiquetado con la escritura de la etiqueta saliente 31 LDP (el intra dominio LDP LSP). Asociaron a la comunidad de MPC 200:200 con la etiqueta 1000 de la ruta en el nodo PRE-agg mientras que la redistribución está en el OSPF.

Salida del nodo 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            V140      10.13.1.0
          MAC/Encaps=14/18, MRU=1500, Label Stack{31}
```

Salidas del nodo PRE-Agg

En el nodo PRE-agg, el prefijo de MPC se redistribuye del BGP al proceso OSPF del acceso RAN con la filtración basada en la Comunidad y el proceso OSPF se redistribuye en el BGP. Esta redistribución controlada es necesaria para hacer el IP de punta a punta reachability, al mismo tiempo cada segmento tiene rutas requeridas mínimo.

El prefijo 10.10.11.1/32 se sabe vía BGP hierarichal 100 con la comunidad de MPC 200:200 asociada. 16020 la escritura de la etiqueta BGP 3107 recibida del router del borde del área de la base (ABR) y la escritura de la etiqueta 22 LDP se agrega en el top para la expedición del intradomain después de las operaciones de búsqueda recurrentes del salto siguiente.

```
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	V110		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	V110		10.9.9.1

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

Salidas del nodo de la base ABR

El prefijo 10.10.11.1 se sabe vía el intradomain IGP (ISIS-L2) y según la tabla de reenvío MPLS. Es accesible con 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.
```

Para la distribución de los prefijos entre las áreas divididas en segmentos, el BGP con la escritura de la etiqueta (RFC 3107) se utiliza. Qué necesidades todavía de residir dentro de las áreas divididas en segmentos del IGP son los loopback de los PE y de los direccionamientos relacionados con la infraestructura central.

Los routers BGP que conectan diversas áreas juntas son los ABR que actúan como reflector de ruta BGP. Estos dispositivos utilizan la característica del Siguiendo-Salto-uno mismo, para evitar la necesidad de comer todos los saltos siguientes del sistema autónomo completo dentro del IGP, en vez solamente de los IP Addresses de los PE y de la infraestructura central. Se completa la detección del loop basó sobre el BGP Cluster-ID.

Para la resistencia de la red, la IMAGEN BGP con el BGP agrega la característica de la trayectoria se debe utilizar con el BGP y el LFA con el IGP. Estas características no se utilizan en el ejemplo anterior.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Arquitectura inconsútil MPLS](#)

- [Cisco unificó el White Paper MPLS](#)
- [Sistema del transporte del paquete del portador de Cisco \(CPT\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)