Unified MPLS-functies, functies en Configuratievoorbeeld

Inhoud

Inleiding

In dit document wordt Unified Multiprotocol Label Switching (MPLS) beschreven, en dit gaat allemaal over schalen. Het biedt een kader van technologische oplossingen om eenvoudig end-to-end verkeer en/of diensten over een traditioneel gesegmenteerde infrastructuur te brengen. Het maakt gebruik van zowel de voordelen van een hiërarchische infrastructuur aangezien het de schaalbaarheid verbetert als de eenvoud van netwerkontwerp.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Netwerkevolutie

Wanneer u de geschiedenis van de op netwerkpakketten gebaseerde services bekijkt, kan een verandering in de bedrijfswaarden van het netwerk worden waargenomen. Dit gaat van discrete aansluitingsverbeteringen om toepassingen zo vloeiend mogelijk te maken, naar samenwerkingstechnologieën om mobiele samenwerking te ondersteunen. Tenslotte worden de on-demand-cloudservices geïntroduceerd met de toepassingsservices om de instrumenten die bij een organisatie worden gebruikt te optimaliseren en de stabiliteit en de kosten van eigendom te verbeteren.

Figuur 1

Deze voortdurende waarde- en functionaliteit-verbetering van het netwerk resulteert in een veel verdergaande behoefte aan netwerkeenvoud, beheersbaarheid, integratie en stabiliteit waar netwerken zijn gesegmenteerd als gevolg van onaangepaste operationele eilanden en geen echte end-to-end-snelheidscontrole. Nu is er een behoefte om het allemaal samen te brengen met één enkele architectuur die gemakkelijk te beheren is, die schaalbaarheid biedt aan 100.000 knooppunten, en de huidige Hoge beschikbaarheid en de Fast Convergence technologie gebruikt. Dit is wat Unified MPLS naar de tabel brengt: het gesegmenteerde netwerk in één besturingsplane en end-to-end padzicht.

Moderne netwerkvereisten

- Verhoogde bandbreedte-vraag (video)
- Hogere toepassingscomplexiteit (cloud en virtualisatie)
- Toename van de behoefte aan convergentie (mobiliteit)

Hoe kunt u MPLS-bewerkingen in steeds grotere netwerken vereenvoudigen met ingewikkelder toepassingsvereisten?

Traditionele MPLS-uitdagingen met verschillende toegangstechnologieën

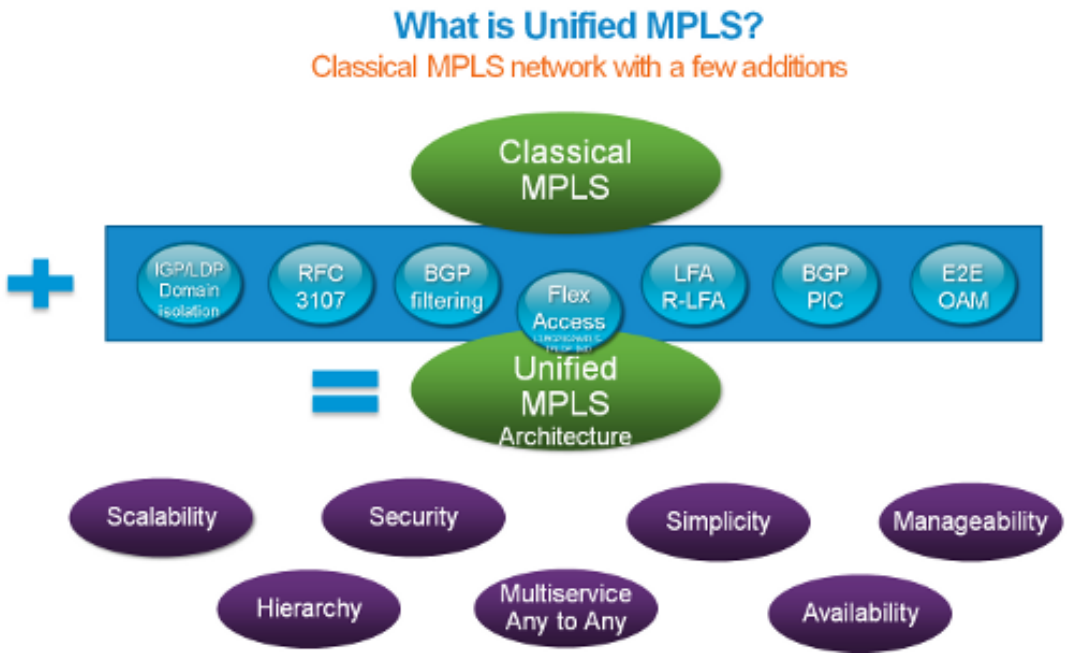
- Complexiteit om 50 milliseconde convergentie met Traffic Engineering Fast Reroute (TE FRR) te bereiken
- Noodzaak van geavanceerde routingprotocollen en interactie met Layer 2-protocollen
- Verdeel grote netwerken in domeinen terwijl de diensten van eind tot eind worden geleverd
- Gemeenschappelijke end-to-end convergentie- en veerkrachtigheidsmechanismen
- Probleemoplossing en end-to-end provisie voor meerdere domeinen

De Unified MPLS-verbinding wordt in deze lijst samengevat:

- Verminderd aantal operationele punten. In het algemeen moeten transportplatforms op elk netwerkelement een dienst worden ingesteld via operationele punten. Het beheersysteem moet de topologie kennen.In Unified MPLS wordt met de integratie van alle MPLS-eilanden het minimumaantal operationele punten bereikt.
- Mogelijke dienstverlening: Layer 3 (L3) VPN, Virtual Private Wire Service (VPWS), Virtual Private LAN Service (VPLS), zonder Pseudodraadverbinden (PW-stitching) of InterAS-mechanismen. Door de introductie van MPLS in de aggregatie wordt enige statische configuratie vermeden die tot MPLS-eilanden leidt.
- End-to-end MPLS-transport bieden
- Bewaar interior Gateway Protocol (IGP)-gebieden die van elkaar zijn gescheiden en kleine routingtabellen.
- Snelle convergentie.
- Eenvoudig te configureren en problemen op te lossen.
- Mogelijkheid om te integreren met elke toegangstechnologie.
- IPv6-bereidheid.

Cisco Unified MPLS

Unified MPLS wordt gedefinieerd door de toevoeging van extra functies aan klassieke/traditionele MPLS en biedt meer schaalbaarheid, beveiliging, eenvoud en beheerbaarheid. Om de MPLS services end-to-end te leveren is end-to-end Label Switches Path (LSP) nodig. Het doel is om de MPLS-services (MPLS VPN, MPLS L2VPN) ongewijzigd te laten, maar toch een grotere schaalbaarheid te introduceren. Om dit te doen, verplaats sommige van de IGP prefixes in Border Gateway Protocol (BGP) (de loopback prefixes van de PE (Provider Edge) routers), die dan de prefixes end-to-end distribueert.



Figuur 2

Voordat de Cisco Unified MPLS-architectuur wordt besproken, is het belangrijk om de belangrijkste functies te begrijpen die zijn gebruikt om dit werkelijkheid te maken.

Functies en componenten

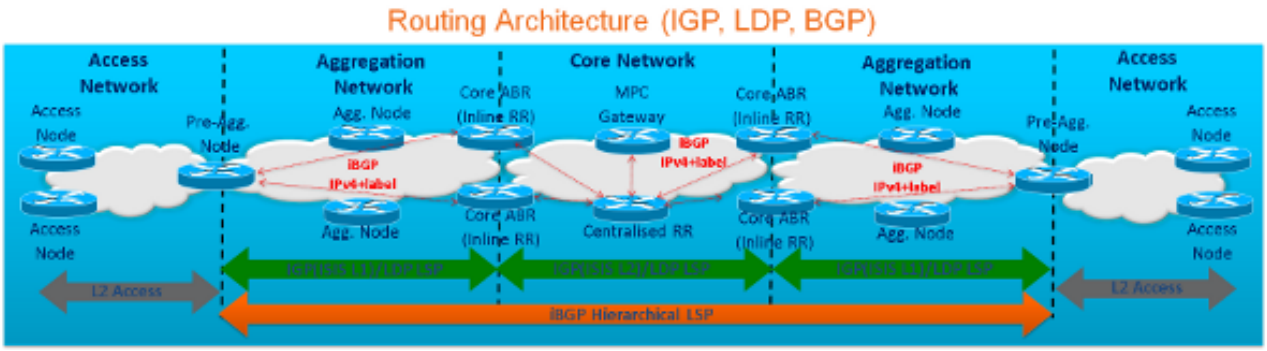
Etikelinformatie in BGP-4 (RFC 3107)

Het is een eerste vereiste om een schaalbare methode te hebben om prefixes tussen netwerksegmenten uit te wisselen. U kunt IGPs (Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS) of Enhanced Interior Gateway Routing Protocol (DHCP) eenvoudigweg samenvoegen naar één domein. Een IGP is echter niet ontworpen om 100.000 prefixes te dragen. Het hiertoe te kiezen protocol is BGP. Het is een goed bewezen protocol dat het internet ondersteunt met 100.000 s routes en MPLS-VPN omgevingen met miljoenen ingangen. Cisco Unified MPLS maakt gebruik van BGP-4 met informatie-uitwisseling (RFC3107). Wanneer BGP een route distribueert, kan het ook een MPLS-label distribueren dat aan die route in kaart is gebracht. De MPLS-informatie voor het in kaart brengen van de route wordt in het BGP-update bericht vervoerd dat de informatie over de route bevat. Als de volgende hop niet wordt gewijzigd, wordt het etiket bewaard en verandert het etiket als de volgende hop verandert. In Unified MPLS verandert de volgende hop in Area Border Routers (ABR's).

Wanneer u RFC 3107 op beide BGP routers toelaat, adverteren de routers met elkaar dat ze vervolgens MPLS-labels met de routes kunnen verzenden. Als de routers met succes onderhandelen over hun mogelijkheid om MPLS-labels te verzenden, voegen de routers MPLS-labels toe aan alle uitgaande BGP-updates.

De labeluitwisseling is nodig om de end-to-end pad informatie tussen segmenten te bewaren. Als resultaat hiervan wordt elk segment klein genoeg om door exploitanten te worden beheerd en tegelijkertijd is er circuitinformatie verdeeld om het pad tussen twee verschillende IP-sprekers te bewustzijn.

Hoe werkt het?



Figuur 3

In afbeelding 3 kunt u zien dat er drie segmenten zijn met een label detectieprotocol (LDP LSP) en dat het toegangsnetwerk niet is ingeschakeld voor LDP. Het doel is om ze samen te voegen zodat er één MPLS-pad (Interne BGP (iBGP) hiërarchische LSP) tussen pre-Aggregation (Pre-Aggregation) knooppunten is. Aangezien het netwerk één enkel BGP Autonoom Systeem (AS) is, zijn alle sessies iBGP sessies. Elk segment runt zijn eigen IGP (OSPF, IS-IS, of DHCP) en LDP LSP paden binnen het IGP domein. Binnen Cisco Unified MPLS moeten de routers (ABR's) die zich bij de segmenten aansluiten BGP-inline routereflectors zijn met de Next-hop-Self en RFC 3107 om een IPv4 + Label te kunnen dragen die op de sessies is geconfigureerd. Deze BGP-sprekers zijn binnen de Cisco Unified MPLS Architecture die aan de ABR's worden gekoppeld.

Waarom zijn de ABR's inline routereflectoren?

Een van de doelen van Unified MPLS is om een zeer schaalbare end-to-end infrastructuur te hebben. Elk segment moet dus eenvoudig worden gehouden om te kunnen functioneren. Alle peerings zijn iBGP-peerings, daarom is er een volledige vermaasd netwerk van peeringen tussen alle iBGP-sprekers binnen het volledige netwerk nodig. Dat levert een zeer onpraktische netwerkomgeving op als er duizenden BGP-sprekers zijn. Als de ABR's routereflectoren worden gemaakt, wordt het aantal iBGP-peering verminderd tot het aantal BGP-sprekers 'per-segment' in plaats van tussen alle BGP-sprekers van de complete AS.

Waarom zichzelf?

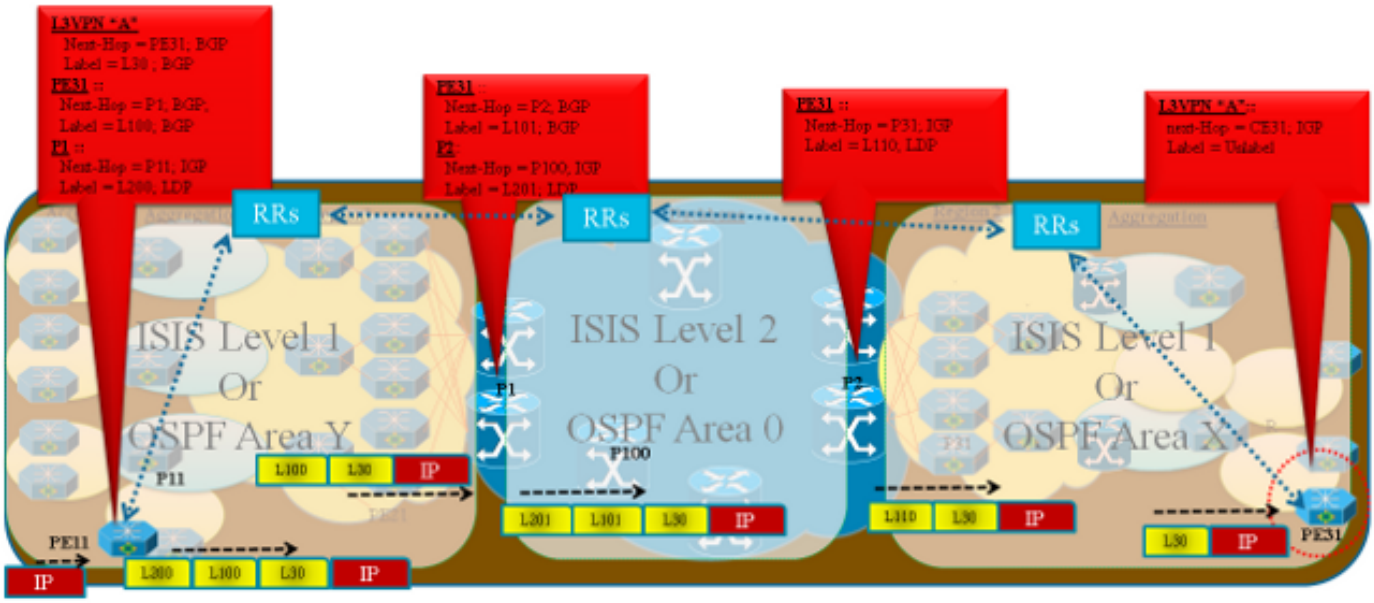
BGP opereert op de basis van recursieve routing lookups. Dit gebeurt om schaalbaarheid binnen het onderliggende IGP die wordt gebruikt, op te vangen. Voor de recursieve raadpleging, gebruikt BGP Next-Hop verbonden aan elke BGP route ingang. Als een Source-Node bijvoorbeeld een pakket naar een knooppunt van de bestemming en een pakket naar de BGP-router wil sturen, doet de BGP-router een routingraadpleging in zijn BGP-routingtabel. Het vindt een route naar Destination-Node en vindt de Next-Hop als een volgende stap. Deze volgende hop moet bekend zijn door de onderliggende IGP. Als laatste stap voorwaarts gaat de BGP-router het pakket verder op basis van de IP- en MPLS-labelinformatie die bij die Next-Port is gevoegd.

Om ervoor te zorgen dat in elk segment alleen de Next-Hops door de IGP bekend moeten worden, is het nodig dat de Next-Hop die aan de BGP-ingang is gekoppeld, zich binnen het netwerksegment bevindt en niet binnen een buursegment of verder weg segment. Als u de BGP Next-Hop herschrijft met de Next-Hop-Self functie, zorg er dan voor dat de Next-Hop binnen het lokale segment valt.

Alles samenvoegen

Example - 'L3VPN Services'

- PE11 sends L3VPN traffic for an L3VPN prefix "A" to PE31



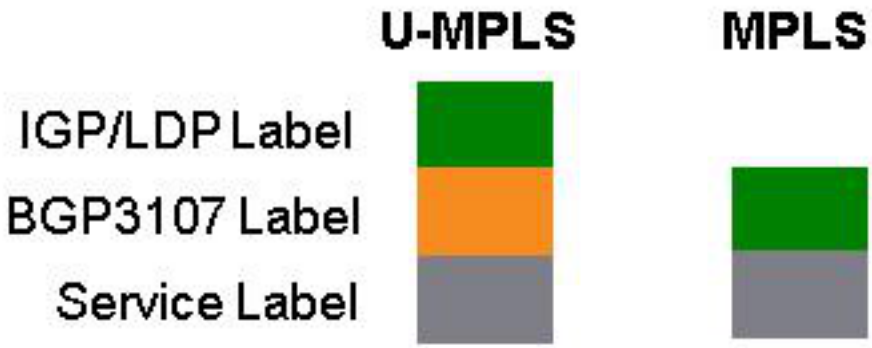
Figuur 4

Afbeelding 4 geeft een voorbeeld van hoe het voorvoegsel "A" en de labeluitwisseling van L3 VPN werken en hoe de MPLS-labelstack is gemaakt om de end-to-end padinformatie te hebben voor de verkeersstroom tussen beide PE's.

Het netwerk is verdeeld in drie onafhankelijke IGP/LDP-domeinen. De verminderde omvang van het verzenden en het verzenden van tabellen op de routers is om betere stabiliteit en snellere convergentie mogelijk te maken. LDP wordt gebruikt om LSP's binnen het domein te bouwen binnen domeinen. RFC 3107 BGP IPv4+-etiketten worden gebruikt als verdelingsprotocol voor meerdere domeinen om hiërarchische BGP LSP's in meerdere domeinen te bouwen. BGP3107 voegt één extra etiket in de het door:sturen label stapel in de Unified MPLS architectuur in.

Intradomein - LDP LSP

Interdomein - BGP hiërarchisch LSP

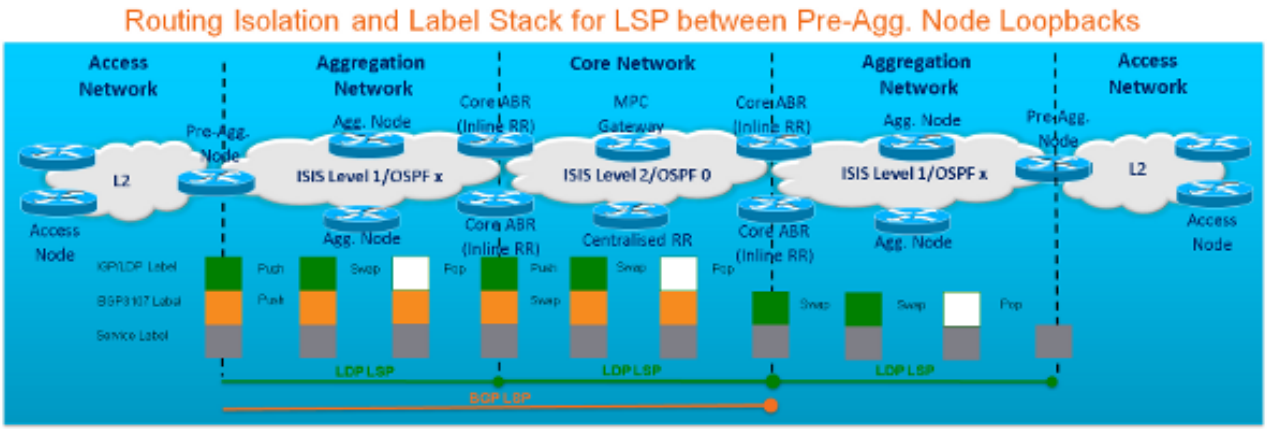


Afbeelding 5

VPN Prefixe 'A' wordt door PE31 naar PE11 geadverteerd met L3VPN service label 30 en volgende hop als PE31's loopback via end-to-end interdomein hiërarchische BGP LSP. Kijk nu naar het verzendpad voor VPN prefix 'A' van PE11 tot PE31.

- Op PE11 is Prefixa via BGP-sessie met PE31 bekend als next-hop PE31 en PE31 is recursief bereikbaar via P1 met BGP-label 100. PE11 heeft IPv4 + labelinformatie van P1 ontvangen als BGP-updates, omdat het is ingeschakeld met de functie RFC 3107 om de informatie te verzenden IPv4 + labelinformatie.
- P1 is bereikbaar via PE11 via LDP LSP binnen het domein en voegt een ander LDP-label toe boven op het BGP-label. Tenslotte gaat het pakje uit het PE11 knooppunt met drie labels. Bijvoorbeeld, het 30 L3VPN servicelabel, het 100 BGP etiket, en het 200 LDP IGP etiket.
- Het LDP-toplabel blijft in het LDP-label ruilen en het PHP-pakket bereikt P1 met twee labels na PHP Popping.
- P1 wordt ingesteld als inline Route Reflector (RR) met de volgende hop en het sluit zich aan bij twee IGP domeinen of LDP LSP.
- Op P1 wordt de volgende hop voor PE31 veranderd in P2 en de update wordt ontvangen via BGP met IPv4 + Label (RFC3107). Het BGP-label wordt vervangen door een nieuw label omdat de volgende hop is gewijzigd en het IGP-label bovenaan is gedrukt.
- Het pakje gaat uit het P1-knooppunt met drie labels en servicelabels 30 is niet aangeraakt. Dat wil zeggen, het 30 L3VPN service label, 101 BGP label en 201 LDP-label.
- De LDP top label swaps in intradomain LDP LSP en het pakje bereikt P2 met twee labels na PHP.
- Op P2 wordt de volgende hop voor PE31 opnieuw gewijzigd en via IGP bereikbaar. Het BGP label is verwijderd als een impliciet-nul BGP label is ontvangen van PE31 voor PHP.
- Het pakje verlaat met twee labels. Bijvoorbeeld, het 30 L3VPN serviceteken en het 110 LDP etiket.
- Op PE31 wordt het pakket geleverd met één label na PHP van het LDP-label en gebaseerd op het servicelabel 30. Het niet-gemerkte pakket wordt doorgestuurd naar de CE31-bestemming onder Virtual Routing and Forwarding (VRF).

Wanneer u de MPLS-labelstack bekijkt, wordt de switching van het pakket tussen een bron- en doelapparaat op basis van het vorige prefix en label exchange waargenomen binnen de MPLS-switching omgeving.



Figuur 6

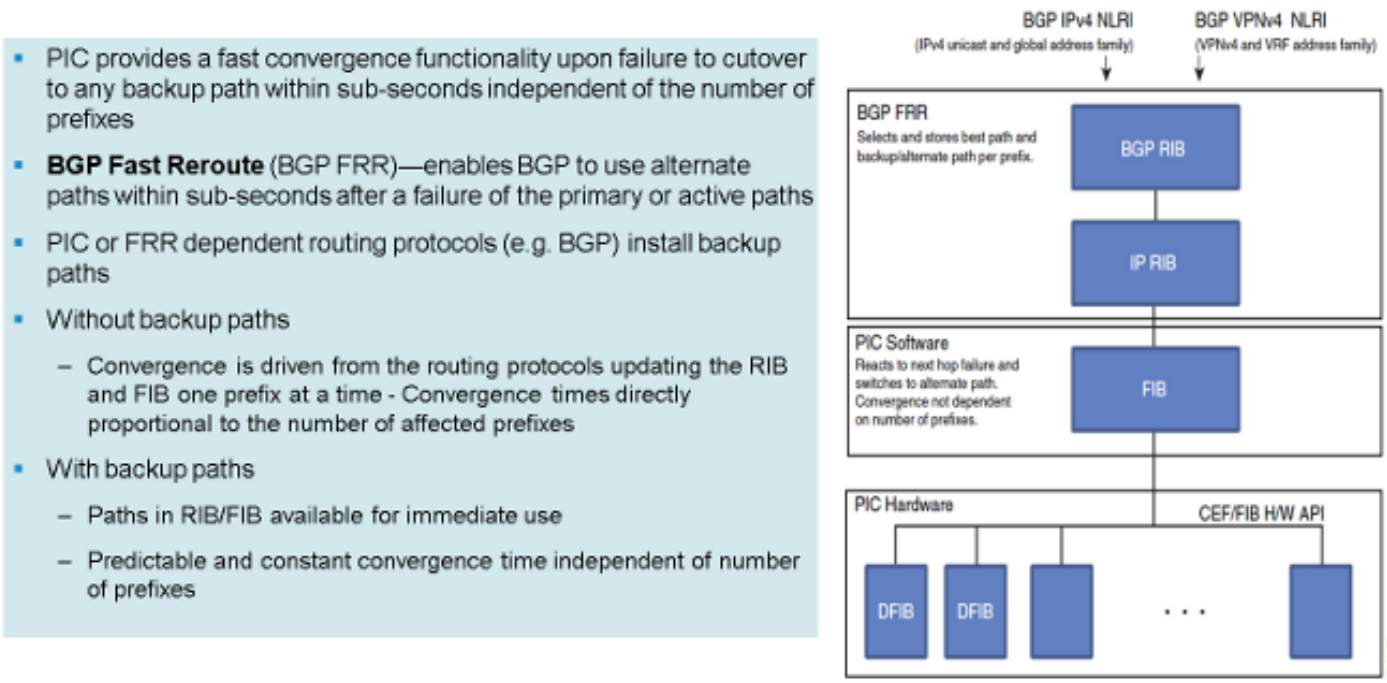
BGP-prefixonafhankelijke conversie (BGP PIC)

Dit is een Cisco-technologie die in BGP-mislukkingsscenario's wordt gebruikt. Het netwerk convergeert zonder verlies van de traditionele seconden in de BGP reconversie. Wanneer BGP PIC wordt gebruikt, kunnen de meeste mislukkingsscenario's worden gereduceerd tot een reconversietijd onder 100 msec.

Hoe gaat dat?

Traditioneel wanneer BGP een mislukking ontdekt, herberekent het voor elke BGP ingang voor het beste pad. Wanneer er een routingtabel is met duizenden route-items, kan dit een aanzienlijke hoeveelheid tijd in beslag nemen. Bovendien moet deze BGP-router al die nieuwe beste paden naar elk van zijn buren distribueren om ze te informeren over de veranderde netwerktopologie en de veranderde best-paden. Als laatste stap moet elke begunstigde BGP-spreker een beste padberekening maken om de nieuwe best paden te vinden.

Iedere keer als de eerste spreker van de BGP iets verkeerds detecteert, start hij de beste berekening totdat alle BGP-sprekers van de buur hun herberekening hebben uitgevoerd, kan de verkeersstroom vallen.



Figuur 7

De BGP PIC voor IP en MPLS VPN optie verbetert BGP convergentie na een netwerkstoring. Deze convergentie is van toepassing op zowel kern- als randstoringen en kan zowel in IP- als MPLS-netwerken worden gebruikt. De BGP PIC voor IP en de optie MPLS VPN maken en slaan een back-up/alternatieve route op in de Routing Information Base (RIB), door:sturen van informatiebasis (FIB) en Cisco Express Forwarding (CEF), zodat wanneer een fout wordt gedetecteerd, de back-up/alternatieve route onmiddellijk kan worden overgenomen, zodat deze snelle failover mogelijk maakt.

Met één herschrijven van de volgende-hopinformatie wordt de verkeersstroom hersteld. Daarnaast is de BGP-convergentie op de achtergrond aanwezig, maar zijn de verkeersstromen niet meer van invloed. Dit herschrijven gebeurt binnen 50 msec. Als u deze technologie gebruikt, is de netwerkconvergentie beperkt tot van seconden tot 50 msec plus de IGP convergentie.

BGP add-pad

BGP Add-Path is een verbetering in de manier waarop BGP-items worden gecommuniceerd

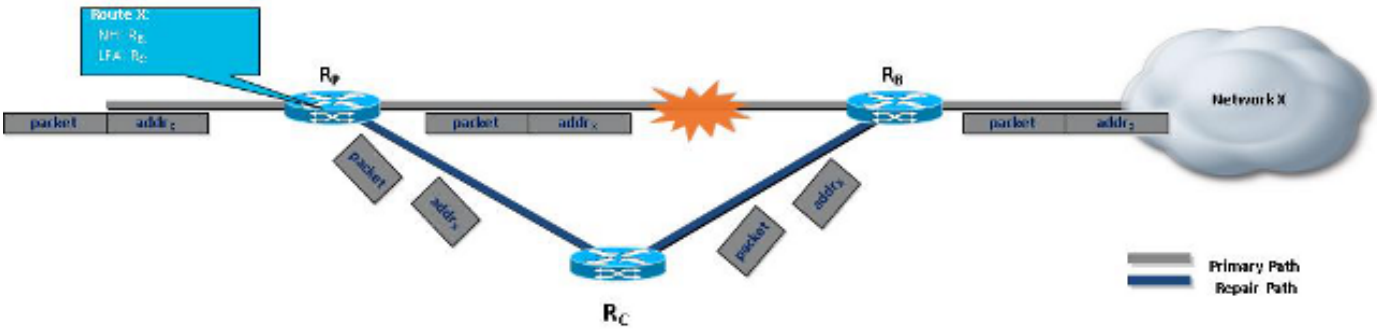
tussen BGP-sprekers. Als er op een bepaalde spreker van de BGP meer dan één enkele vermelding naar een bepaalde bestemming is, dan stuurt die spreker van de BGP alleen de vermelding die voor die bestemming de beste weg is naar zijn buren. Het gevolg is dat er geen bepalingen worden vastgesteld om reclame voor meerdere paden voor dezelfde bestemming mogelijk te maken.

BGP Add-Path is een BGP-optie om meer als alleen het beste pad toe te staan en biedt meerdere paden voor dezelfde bestemming zonder de nieuwe paden impliciet ter vervanging van eerdere paden. Deze uitbreiding naar BGP is met name belangrijk om te helpen met BGP PIC, wanneer BGP-routereflectoren worden gebruikt, zodat de verschillende BGP-luidsprekers binnen een AS toegang hebben tot meer BGP-paden als enkel het "best BGP-pad" in overeenstemming met de routereflector.

Loop-Free Alternates en RFA voor IGP Fast-Convergence

Activiteiten om 50 milliseconden herstel te bereiken na een storing van de verbinding of de knoop kunnen drastisch worden vereenvoudigd door de introductie van een nieuwe technologie die "loop-free alternates" (LFA's) wordt genoemd. LFA verbetert de link-staat routingprotocollen (IS-IS en OSPF) om alternatieve routingpaden op een loop-vrije manier te vinden. LFA staat elke router toe om een voorbepaald reservepad te definiëren en te gebruiken als een nabijheid (netwerkknooppunt of link) mislukt. Om een hersteltijd van 50 msec te leveren in het geval van een koppeling of een knooppunt, kan MPLS TE FRR worden ingezet. Dit vereist echter de toevoeging van een ander protocol (Resource Reservation Protocol, of RSVP) voor installatie en beheer van TE-tunnels. Terwijl dit voor bandbreedtebeheer noodzakelijk kan zijn, vereist de bescherming en de restauratie verrichting geen bandbreedtebeheer. Daarom wordt de overheadkosten verbonden aan de toevoeging van RSVP TE hoog geacht voor eenvoudige bescherming van koppelingen en knooppunten.

LFA kan een eenvoudige en gemakkelijke techniek bieden zonder de inzet van RSVP TE in dergelijke scenario's. Als resultaat van deze technieken kunnen de onderling verbonden routers van vandaag in grootschalige netwerken een herstel van 50 msec leveren voor link- en knooppunten zonder dat de operator zich hoeft te configureren.

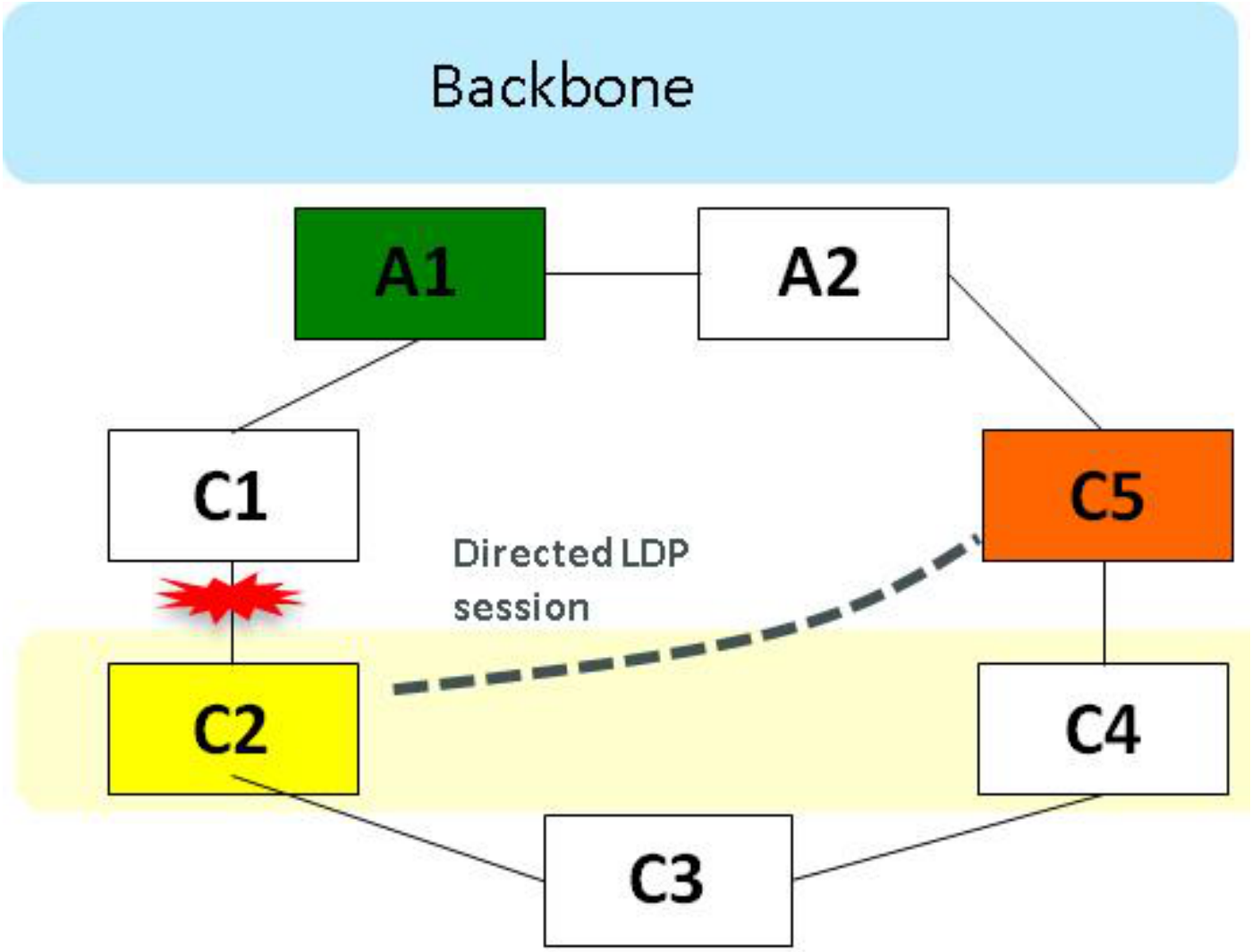


Figuur 8

LFA-FRR is een mechanisme dat lokale bescherming biedt voor eenastverkeer in IP, MPLS, Ethernet over MPLS (EoMPLS), Inverse Multiplexing over ATM (IMA) via MPLS, Circuit Emulation Service over Packet Switched Network (CESoPSN) via MPLS en Structure-Astic Time Division Multiplexing over Packet (SATo) P) via MPLS-netwerken. Sommige topologieën (zoals de ringtopologie) vereisen echter bescherming die niet alleen door LFA-FRR wordt geboden. De functie Remote LFA-FRR is in dergelijke situaties handig.

De Remote LFA-FRR breidt het basisgedrag van LFA-FRR uit tot elke topologie. Het geeft het

verkeer rond een mislukt knooppunt door naar een afgelegen LFA die meer dan één hop verwijderd is. In afbeelding 9, als de koppeling tussen C1 en C2 geen A1 bereikt, verstuurt C2 het pakket over een geregisseerde LDP-sessie naar C5 dat bereikbaarheid voor A1 heeft.



Afbeelding 9

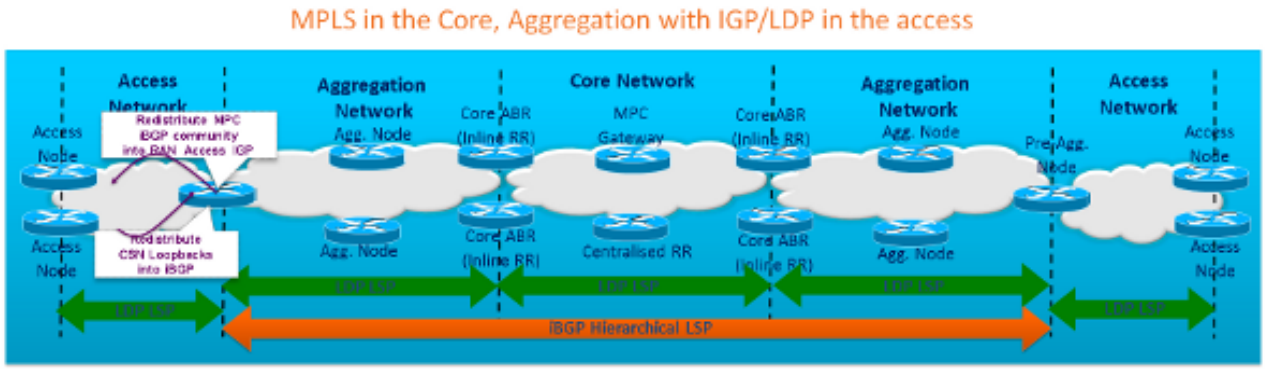
In Remote LFA-FRR compileert een knooppunt dynamisch het LFA-knooppunt. Nadat het alternatieve knooppunt is ingesteld (dat niet rechtstreeks is aangesloten), stelt het knooppunt automatisch een LDP-sessie (Label Distribution Protocol) in voor het alternatieve knooppunt. De gerichte LDP-sessielabels voor de specifieke forward error Correction (FEC).

Wanneer de koppeling faalt, gebruikt het knooppunt het label stapelend om het verkeer naar het externe LFA-knooppunt te tunnen, om het verkeer naar de bestemming door te sturen. Alle labeluitwisselingen en het afstemmen op het afgelegen LFA-knooppunt zijn dynamisch van aard en prebevoorrading is niet vereist. Het hele systeem voor het uitwisselen en tunnelen van etiketten is dynamisch en omvat geen handmatige voorzieningen.

Voor LSP's met een intradomein wordt LFA FRR op afstand gebruikt voor MPLS-verkeer in ringtopologieën. Remote LFA FRR berekent een back-uppad voor elk prefix in de IGP-routingtabel, zodat de knooppunt snel op het reservepad kan overschakelen wanneer er een storing optreedt. Dit levert een hersteltijd van ongeveer 50 msec.

Cisco Unified MPLS-architectuurvoorbeeld

Wanneer alle vorige gereedschappen en functies binnen een netwerkomgeving zijn geïnstalleerd, maakt het de Cisco Unified MPLS-netwerkomgeving aan. Dit is het architectuurvoorbeeld voor grote dienstverleners.



Afbeelding 10

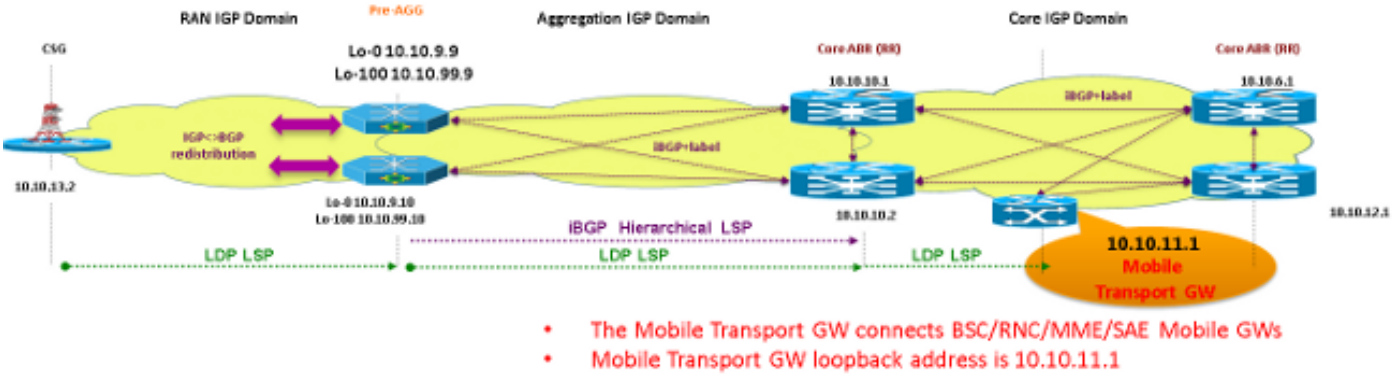
- De Core en Aggregatie worden georganiseerd als afzonderlijke IGP/LDP-domeinen.
- Binnen-domein hiërarchische LSP's gebaseerd op RFC 3107, BGP IPv4+ labels die uitgebreid worden naar de voorpagina.
- Op LDP gebaseerde LSP's met een intradomein.
- De Core/Aggregatie LSP's tussen domeinen worden in de Access Networks uitgebreid door de distributie van het Radio Access Networks Interior Gateway Protocol (RAN IGP) naar het interdomein iBGP en distribueren de benodigde geëtiketteerde iBGP-prefixes (MPC (Mobile Packet Core) gateway) naar RAN IGP (via BGP-gemeenschappen).

Unified MPLS-configuratievoorbeeld

Hier een vereenvoudigd voorbeeld van Unified MPLS.

Core Area Border Router - Cisco IOS® XR

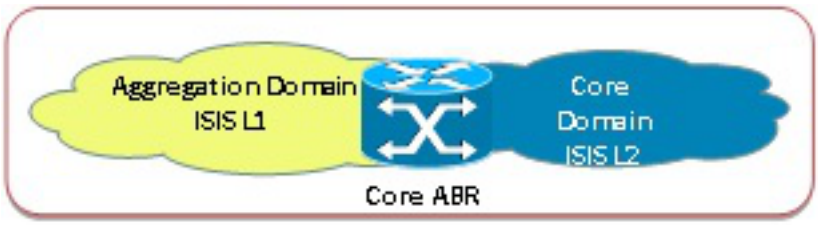
Pre-Aggregatie en Cell Site Gateway routers - Cisco IOS



Afbeelding 11

200:200 MPC-community	
300:300 Aggregatie-community	
Core IGP-domein	ISIS-niveau 2
IGP-domein voor aggregatie	ISIS-niveau 1
Access IGP-domein	OSPF 0-gebieden

Configuratie van kerngebieden

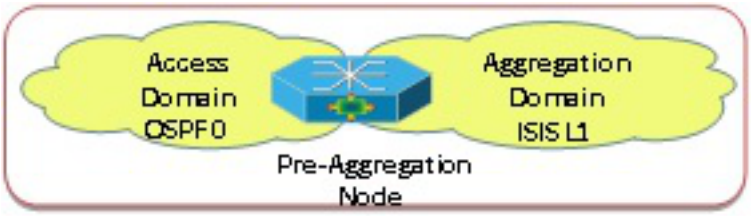


Afbeelding 12

```
! 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
ibgp policy out enforce-modifications
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
```

Configuratie vóór aggregatie



Afbeelding 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
```

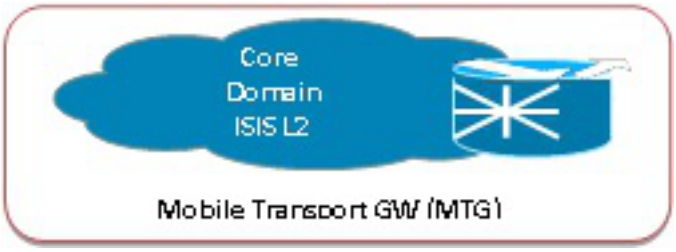
```
! BGP Configuration
router bgp 100
ibgp policy out enforce-modifications
bgp router-id 10.10.9.10
bgp cluster-id 909
neighbor csr peer-group
neighbor csr remote-as 100
neighbor csr update-source Loopback100                ! Cell Site - Routers RAN IGP
     loopback100 as source
neighbor abr peer-group
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 (300:300)
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
```

CSG-configuratie (Cell Site Gateway)

Afbeelding 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
```

MTG-configuratie



Afbeelding 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
ibgp policy out enforce-modifications
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
```

Verifiëren

Het voorvoegsel van het mobiele Packet Gateway *(*MPG) is 10.10.11.1/32, dus dat voorvoegsel is van belang. Bekijk nu hoe pakketten van CSG naar MPG worden verzonden.

Het MPC-voorvoegsel 10.10.11.1 is bekend bij de CSG-router vanaf Pre-agg met routetag 1000 en kan worden doorgestuurd als een geëtiketteerd pakket met het uitgaande LDP-label 31 (intra-domein LDP LSP). De MPC community 200:200 werd in kaart gebracht met routetag 1000 in pre-

agg knooppunt terwijl de herdistributie in OSPF is.

CSG-knooppunt

```
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}
```

Uitvoer van voorAGG-knooppunt

In preagg-knooppunt wordt het MPC-voorvoegsel opnieuw verdeeld van BGP naar RAN-toegangsproces OSPF met gemeenschapsgebaseerde filtering en het OSPF-proces wordt herverdeeld in BGP. Deze gecontroleerde herverdeling is noodzakelijk om eind-aan-eind IP bereikbaarheid te maken, tezelfdertijd heeft elk segment minimaal vereiste routes.

Het voorvoegsel van 10.10.11.1/32 staat bekend via hierarichal BGP 100 met de MPC 200:200 community in de bijlage. Het label 16020 BGP 3107 dat van de kern Area Border Router (ABR) wordt ontvangen en het LDP-label 22 wordt bovenop toegevoegd voor intradomeinverzending na de volgende terugkerende raadpleging van hop.

```
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}
```

Core ABR-knooppunten

Het voorvoegsel **10.10.11.1 is bekend via IGP (ISIS-L2)** en volgens de MPLS-verzendtabel. Het is bereikbaar via 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.
```

Voor de verdeling van de prefixes tussen de gesegmenteerde gebieden wordt BGP met het label (RFC 3107) gebruikt. Wat nog in de gesegmenteerde gebieden van het IGP moet liggen, zijn de achterdeurtjes van de PE's en de adressen die verband houden met de centrale infrastructuur.

De BGP-routers die verschillende gebieden onderling verbinden, zijn de ABR's die fungeren als een BGP-routereflector. Deze apparaten maken gebruik van de functie Next-Hop-Self om te voorkomen dat alle Next-Hops van het volledige Autonome Systeem binnen het IGP moeten worden geïnstalleerd, in plaats van alleen de IP-adressen van de PE's en de centrale infrastructuur. De detectie van de lijn wordt voltooid op basis van de BGP Cluster-ID's.

Voor netwerkveerkracht moet BGP PIC met de BGP Add Path optie met BGP en LFA met IGP worden gebruikt. Deze functies worden niet in het vorige voorbeeld gebruikt.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Naadloze MPLS-architectuur
- Cisco Unified MPLS-witboek
- Cisco CPT-systeem (Carrier Packet Transport)
- Technische ondersteuning en documentatie – Cisco Systems