Esempio di funzionalità, funzionalità e configurazione di MPLS unificato

Sommario

Introduzione

Questo documento descrive MPLS (Unified Multiprotocol Label Switching), che riguarda tutto il ridimensionamento. Fornisce una struttura di soluzioni tecnologiche per portare traffico e/o servizi end-to-end in un'infrastruttura tradizionalmente segmentata. Sfrutta i vantaggi di un'infrastruttura gerarchica migliorando la scalabilità e la semplicità di progettazione della rete.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Evoluzione della rete

Se si controlla la cronologia dei servizi basati sui pacchetti di rete, è possibile osservare un cambiamento nei valori aziendali della rete. Questo va dai miglioramenti della connettività discreta per rendere le applicazioni il più fluide possibile alle tecnologie di collaborazione per supportare la collaborazione mobile. Infine, i servizi cloud on demand vengono introdotti con i servizi delle applicazioni per ottimizzare gli strumenti utilizzati con un'organizzazione e migliorare la stabilità e il costo di proprietà.

Figura 1

Questo miglioramento continuo del valore e delle funzionalità della rete determina un'esigenza molto più diffusa di semplicità, gestibilità, integrazione e stabilità della rete, dove le reti sono state segmentate a causa di isole operative disgiunte e senza un reale controllo completo dei percorsi. Ora è necessario riunire tutte queste funzionalità in un'unica architettura, facile da gestire, che offre scalabilità fino a 100.000 nodi e utilizza le attuali tecnologie di elevata disponibilità e rapida convergenza. Questo è quanto porta MPLS unificato alla tabella, ovvero la rete segmentata in un singolo control plane e la visibilità del percorso end-to-end.

Requisiti di rete moderni

- Aumento della richiesta di larghezza di banda (Video)

- Aumento della complessità delle applicazioni (cloud e virtualizzazione)
- Maggiore necessità di convergenza (mobilità)

Come è possibile semplificare le operazioni MPLS in reti sempre più grandi con requisiti applicativi più complessi?

Sfide MPLS tradizionali con diverse tecnologie di accesso

- Complessità necessaria per ottenere una convergenza di 50 millisecondi con TE (Traffic Engineering Fast Reroute)
- Necessità di protocolli di routing sofisticati e interazione con i protocolli di layer 2
- Suddividere reti di grandi dimensioni in domini mentre i servizi vengono forniti end-to-end
- Meccanismi comuni di convergenza e resilienza end-to-end
- Risoluzione dei problemi e provisioning completo su più domini

L'attrazione MPLS unificata è riepilogata nel seguente elenco:

- Riduzione del numero di punti operativi. Nelle piattaforme di trasporto generiche, un servizio deve essere configurato su ogni elemento di rete tramite punti operativi. Il sistema di gestione deve conoscere la topologia.In MPLS unificato, con l'integrazione di tutte le isole MPLS, viene raggiunto il numero minimo di punti operativi.
- Possibilità di fornire facilmente servizi: VPN di livello 3 (L3), VPWS (Virtual Private Wire Service), VPLS (Virtual Private LAN Service), senza meccanismi di pseudowire-stitching (PW-stitching) o InterAS. Con l'introduzione di MPLS all'interno dell'aggregazione, viene evitata una certa configurazione statica che crea le isole MPLS.
- Fornire il trasporto MPLS end-to-end.
- Mantenere le aree IGP (Interior Gateway Protocol) separate e piccole tabelle di routing.
- Convergenza rapida.
- Facile da configurare e risolvere i problemi.
- Possibilità di integrazione con qualsiasi tecnologia di accesso.
- Predisposizione per IPv6.

Cisco Unified MPLS

Unified MPLS è definito dall'aggiunta di funzionalità aggiuntive con MPLS classico/tradizionale e offre maggiore scalabilità, sicurezza, semplicità e gestibilità. Per fornire i servizi MPLS è necessario un percorso LSP (Label Switch Path) end-to-end completo. L'obiettivo è mantenere i servizi MPLS (MPLS VPN, MPLS L2VPN) così come sono, ma introdurre una maggiore scalabilità. A tal fine, spostare alcuni dei prefissi IGP nel Border Gateway Protocol (BGP) (i prefissi di loopback dei router Provider Edge (PE)), che quindi distribuisce i prefissi end-to-end.

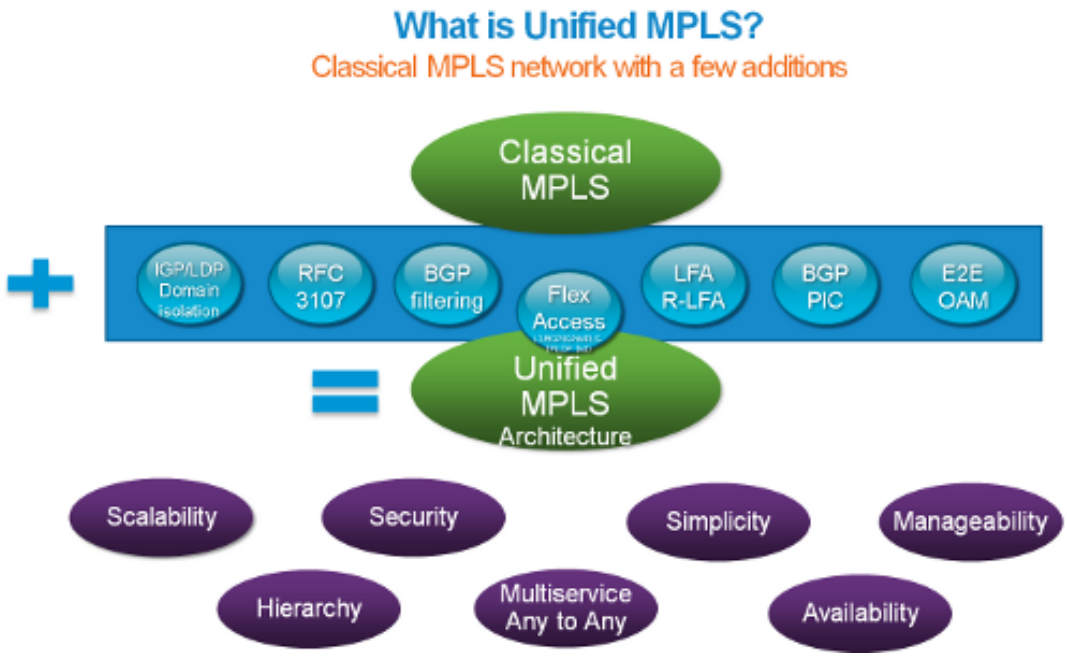

Figura 2

Prima di parlare dell'architettura Cisco Unified MPLS, è importante comprendere le funzionalità chiave utilizzate per realizzare questo obiettivo.

Caratteristiche e componenti

Informazioni sulle etichette da trasportare in BGP-4 (RFC 3107)

Èun prerequisito per disporre di un metodo scalabile per lo scambio di prefissi tra segmenti di rete. È sufficiente unire gli IGP (Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS) o Enhanced Interior Gateway Routing Protocol (EIGRP)) in un singolo dominio. Tuttavia un IGP non è progettato per trasportare 100.000 di prefissi. Il protocollo scelto a tale scopo è BGP. Si tratta di un protocollo ampiamente collaudato che supporta Internet con 100.000 di percorsi e ambienti MPLS-VPN con milioni di voci. Cisco Unified MPLS utilizza il protocollo BGP-4 con scambio di informazioni sulle etichette (RFC3107). Quando BGP distribuisce una route, può anche distribuire un'etichetta MPLS mappata a tale route. Le informazioni sul mapping dell'etichetta MPLS per la route sono contenute nel messaggio di aggiornamento BGP che contiene le informazioni sulla route. Se l'hop successivo non viene modificato, l'etichetta viene mantenuta e l'etichetta cambia se cambia l'hop successivo. In MPLS unificato, l'hop successivo cambia in corrispondenza dei router di confine area (ABR).

Quando si abilita la RFC 3107 su entrambi i router BGP, i router si annunciano a vicenda di poter inviare etichette MPLS con le route. Se i router riescono a negoziare la possibilità di inviare etichette MPLS, aggiungono le etichette MPLS a tutti gli aggiornamenti BGP in uscita.

Lo scambio di etichette è necessario per mantenere le informazioni sul percorso end-to-end tra i segmenti. Ne consegue che ciascun segmento diventa così piccolo da poter essere gestito dagli operatori e che, allo stesso tempo, le informazioni sui circuiti vengono distribuite tra due diffusori IP diversi per consentire il riconoscimento del percorso.

Come funziona?

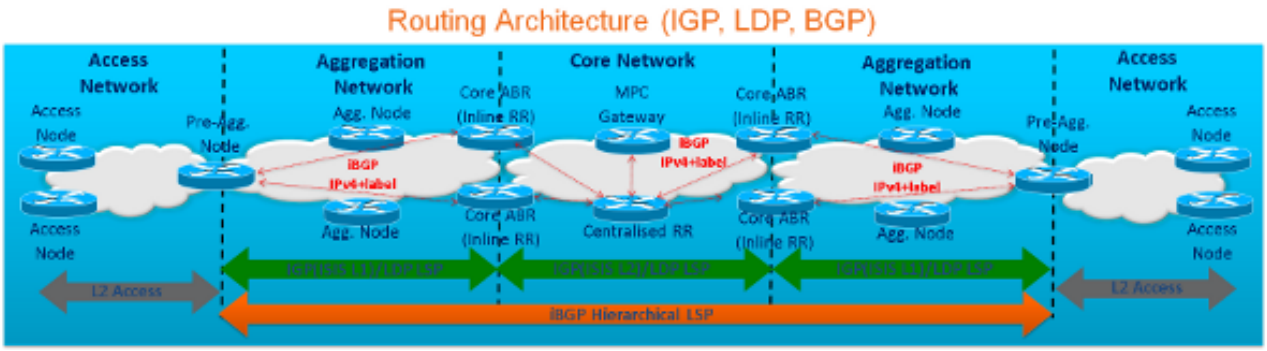

Figura 3

Nella Figura 3 è possibile vedere che esistono tre segmenti con Label Discovery Protocol Labeled Switches Path (LDP LSP) e la rete di accesso non ha LDP abilitato. L'obiettivo è unirli in modo che vi sia un unico percorso MPLS (LSP gerarchico interno BGP (iBGP)) tra i nodi pre-aggregazione (pre-aggregazione). Poiché la rete è un singolo BGP Autonomous System (AS), tutte le sessioni sono sessioni iBGP. Ogni segmento esegue i propri percorsi IGP (OSPF, IS-IS o EIGRP) e LDP LSP all'interno del dominio IGP. All'interno di Cisco Unified MPLS, i router (ABR) che si uniscono ai segmenti devono essere riflettori di route BGP in linea con Next-Hop-Self e RFC 3107 per avere un'etichetta IPv4 + configurata sulle sessioni. Questi altoparlanti BGP sono integrati nell'architettura Cisco Unified MPLS, nota come ABR.

Perché i riflettori di percorso in linea degli ABR?

Uno degli obiettivi di Unified MPLS è disporre di un'infrastruttura end-to-end altamente scalabile. Pertanto, ogni segmento dovrebbe essere tenuto semplice per poter funzionare. Tutti i peer sono iBGP, quindi è necessario un mesh completo di peer tra tutti gli altoparlanti iBGP all'interno della rete completa. Il che si traduce in un ambiente di rete molto poco pratico se ci sono migliaia di altoparlanti BGP. Se gli ABR sono fatti riflettori di rotta, il numero di peer iBGP viene ridotto al numero di diffusori BGP 'per segmento' invece che tra 'tutti' diffusori BGP dell'AS completo.

Perché il prossimo hop?

Il protocollo BGP funziona sulla base di ricerche di routing ricorsive. Questa operazione viene eseguita per adattare la scalabilità all'interno dell'IGP sottostante utilizzato. Per la ricerca ricorsiva, BGP utilizza l'hop successivo collegato a ciascuna voce della route BGP. Pertanto, ad esempio, se un nodo di origine desidera inviare un pacchetto a un nodo di destinazione e il pacchetto raggiunge il router BGP, il router BGP esegue una ricerca di routing nella relativa tabella di routing BGP. Trova una route verso il nodo di destinazione e trova l'hop successivo come passaggio successivo. Questo hop successivo deve essere noto all'IGP sottostante. Infine, il router BGP inoltra il pacchetto in base alle informazioni sull'etichetta IP e MPLS allegate all'hop successivo.

Per accertarsi che all'interno di ciascun segmento solo gli hop successivi debbano essere noti all'IGP, è necessario che l'hop successivo collegato alla voce BGP si trovi all'interno del segmento di rete e non all'interno di un segmento adiacente o più lontano. Se si riscrive il protocollo BGP Next-Hop con la funzione Next-Hop-Self, verificare che l'hop successivo si trovi nel segmento locale.

Metti Tutto Insieme

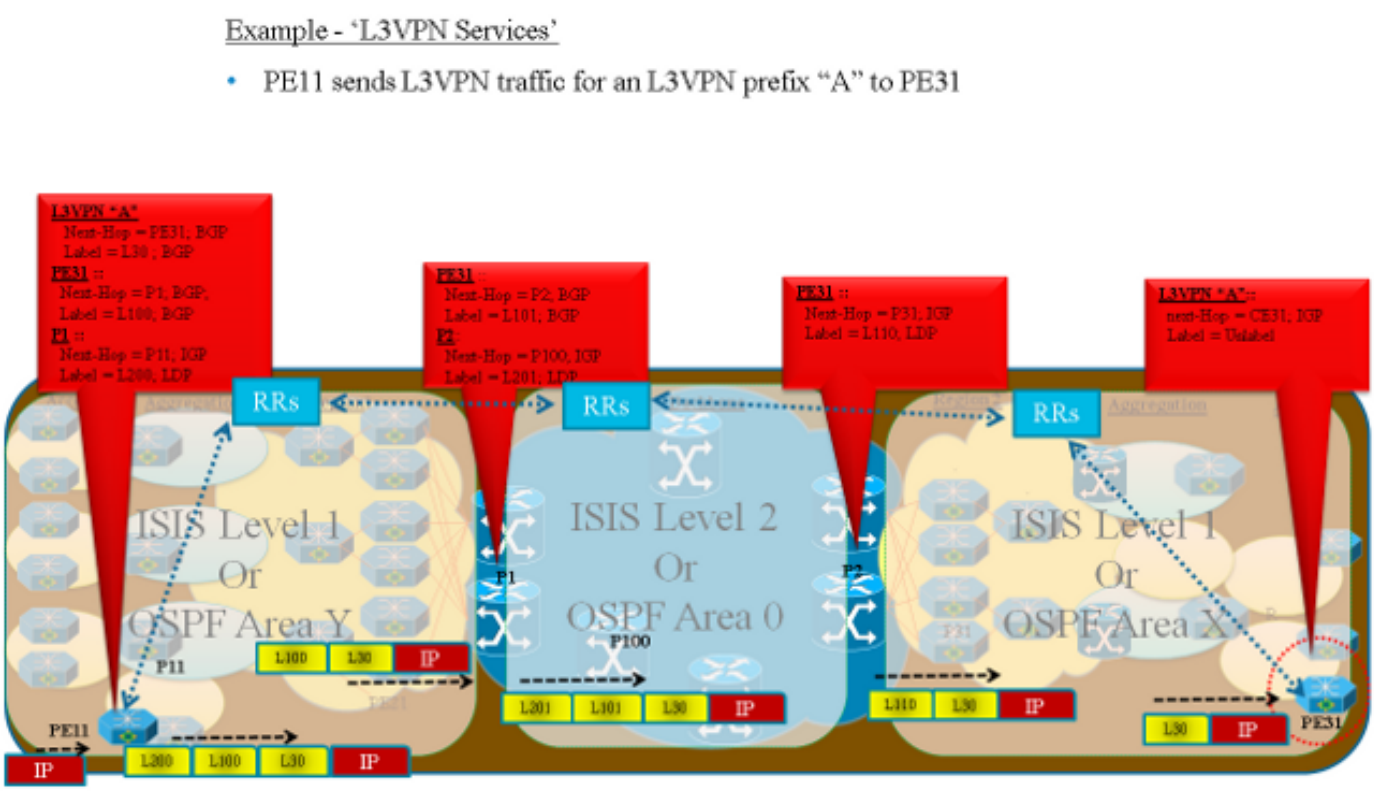

Figura 4

Nella Figura 4 viene illustrato un esempio di come funzionano il prefisso 'A' della VPN L3 e lo scambio di etichette e di come viene creato lo stack di etichette MPLS in modo che disponga delle informazioni sul percorso end-to-end per il flusso di traffico tra entrambi i PE.

La rete è suddivisa in tre domini IGP/LDP indipendenti. La riduzione delle dimensioni delle tabelle di routing e inoltro sui router consente una maggiore stabilità e una convergenza più rapida. Il protocollo LDP viene utilizzato per creare provider di servizi di traduzione all'interno del dominio. Le etichette IPv4+ BGP della RFC 3107 sono usate come protocollo di distribuzione delle etichette tra domini per compilare LSP BGP gerarchici tra domini. BGP3107 inserisce un'etichetta aggiuntiva nello stack di etichette di inoltro nell'architettura Unified MPLS.

Intradomain - LDP LSP

Interdomain - LSP gerarchico BGP

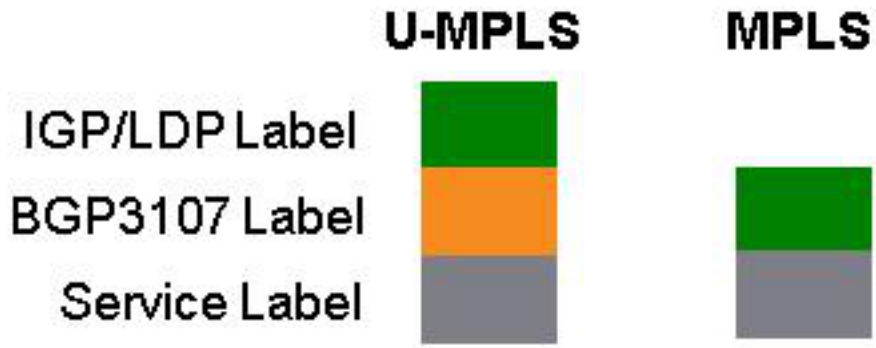

Figura 5

Il prefisso VPN 'A' viene annunciato da PE31 a PE11 con l'etichetta di servizio L3VPN 30 e l'hop successivo come loopback di PE31 tramite LSP BGP gerarchico interdominio end-to-end. Osservare ora il percorso di inoltro per il prefisso VPN 'A' da PE11 a PE31.

- In PE11, il prefisso A è noto tramite la sessione BGP con PE31 come PE31 dell'hop successivo e PE31 è raggiungibile in modo ricorsivo tramite P1 con etichetta BGP 100. PE11 ha ricevuto informazioni su IPv4 + etichetta da P1 come aggiornamenti BGP perché è abilitato con la funzione RFC 3107 per inviare le informazioni su IPv4 + etichetta.
- P1 è raggiungibile da PE11 tramite LSP LDP intradomain e aggiunge un'altra etichetta LDP sopra l'etichetta BGP. Infine, il pacchetto esce dal nodo PE11 con tre etichette. Ad esempio, l'etichetta del servizio 30 L3VPN, l'etichetta 100 BGP e l'etichetta 200 LDP IGP.
- L'etichetta superiore LDP continua a scambiarsi in LDP LDP intradomain e il pacchetto raggiunge P1 con due etichette dopo Penultimate Hop Popping (PHP).
- P1 è configurato come Inline Route Reflector (RR) con il self-hop successivo e si unisce a due domini IGP o LDP LSP.
- In P1, l'hop successivo per PE31 viene modificato in P2 e l'aggiornamento viene ricevuto tramite BGP con IPv4 + etichetta (RFC3107). L'etichetta BGP viene sostituita con una nuova etichetta perché l'hop successivo viene modificato e l'etichetta IGP viene spostata in primo piano.
- Il pacchetto esce dal nodo P1 con tre etichette e l'etichetta di servizio 30 rimane invariata. ovvero l'etichetta del servizio 30 L3VPN, l'etichetta 101 BGP e l'etichetta 201 LDP.
- L'etichetta superiore LDP si scambia in LDP LDP, un LDP intradominale, e il pacchetto raggiunge il P2 con due etichette dopo il PHP.
- In P2, l'hop successivo per PE31 viene nuovamente modificato ed è raggiungibile tramite IGP. L'etichetta BGP viene rimossa quando un'etichetta BGP implicita-null viene ricevuta da PE31 per PHP.
- Il pacchetto va via con due etichette. Ad esempio, l'etichetta del servizio 30 L3VPN e l'etichetta 110 LDP.
- In PE31, il pacchetto arriva con un'etichetta dopo PHP dell'etichetta LDP e basata sull'etichetta di servizio 30. Il pacchetto senza etichetta viene inoltrato alla destinazione CE31 in VRF (Virtual Routing and Forwarding).

Quando si controlla lo stack di etichette MPLS, nell'ambiente di commutazione MPLS si osserva la commutazione del pacchetto tra un dispositivo di origine e uno di destinazione in base al prefisso e allo scambio di etichette precedenti.

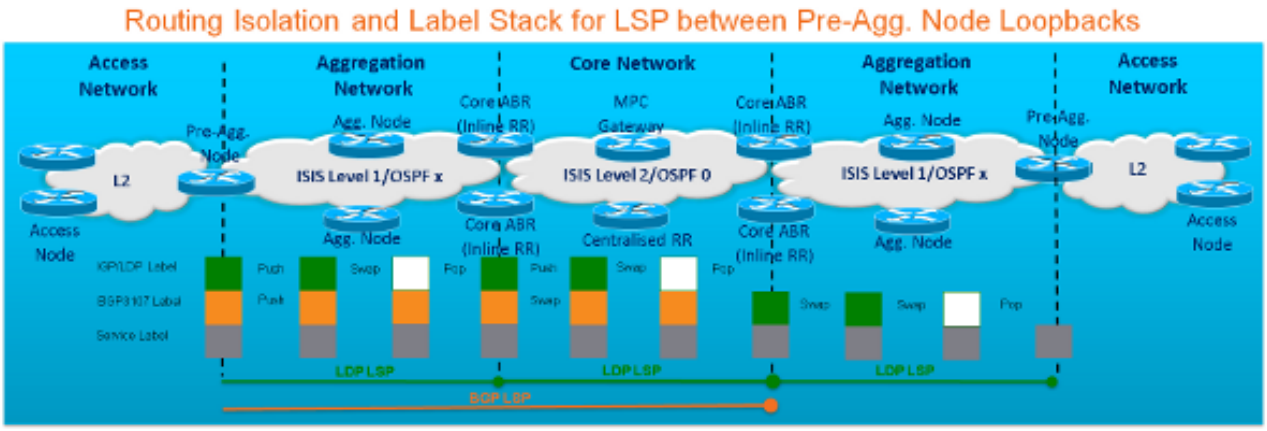

Figura 6

BGP Prefix-Independent Convergence (BGP PIC)

Questa tecnologia Cisco è utilizzata in scenari di errore BGP. La rete converge senza una perdita dei secondi tradizionali nella riconversione BGP. Quando si usa BGP PIC, la maggior parte degli

scenari di errore può essere ridotta a un tempo di riconvergenza inferiore a 100 msec.

Come si fa?

In genere, quando BGP rileva un errore, ricalcola per ogni voce BGP il percorso migliore. Se esiste una tabella di routing con migliaia di voci di route, l'operazione può richiedere molto tempo. Inoltre, il router BGP deve distribuire tutti i nuovi percorsi migliori a ciascuno dei propri vicini per informarli della topologia di rete modificata e dei percorsi migliori modificati. Infine, per individuare i nuovi percorsi migliori, ciascun altoparlante BGP ricevente deve eseguire un calcolo del percorso migliore.

Ogni volta che il primo altoparlante BGP rileva un errore, avvia il calcolo del miglior percorso finché tutti gli altoparlanti BGP adiacenti non hanno eseguito il ricalcolo, il flusso del traffico potrebbe essere interrotto.

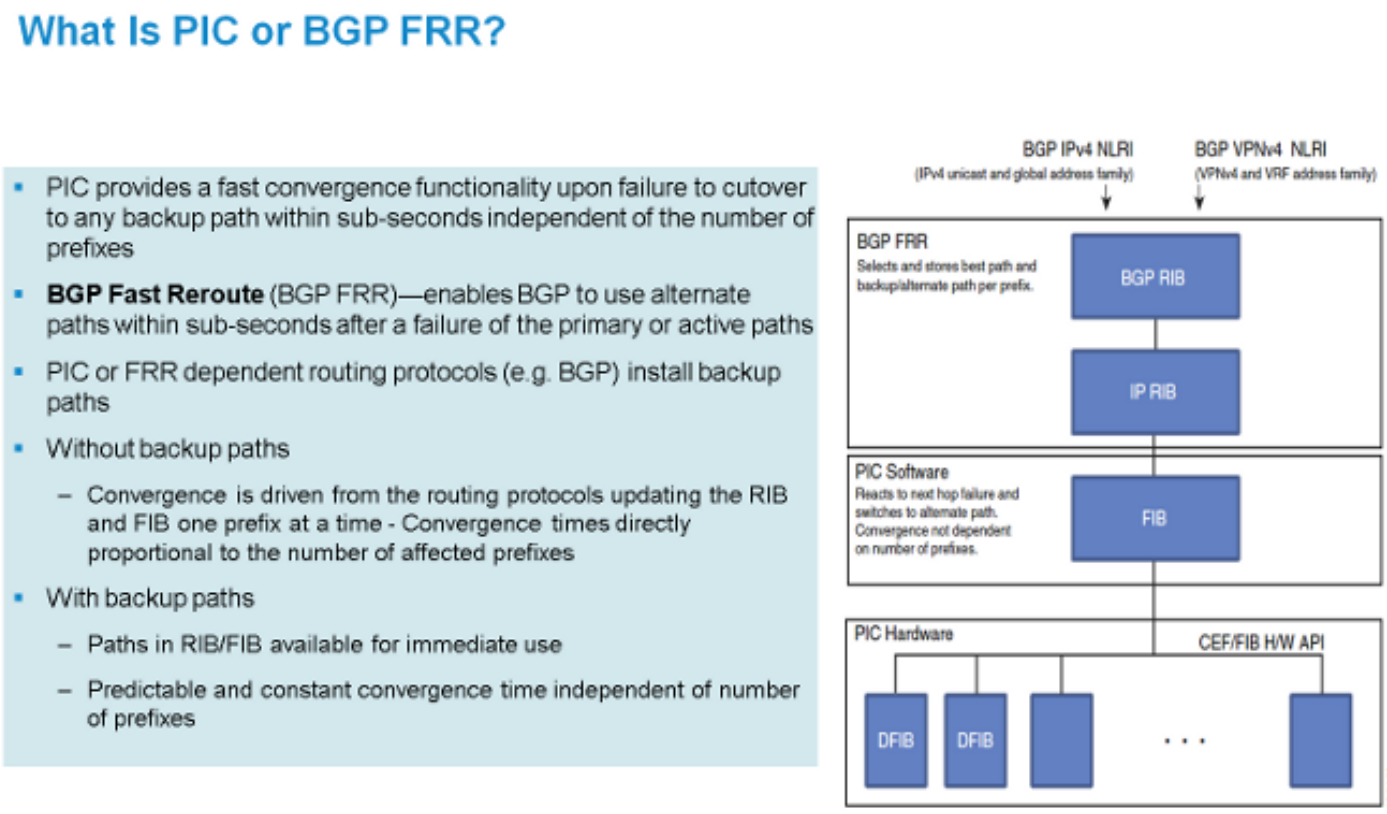

Figura 7

La funzione BGP PIC per IP e MPLS VPN migliora la convergenza BGP dopo un errore di rete. Questa convergenza è applicabile sia ai guasti del core che ai edge e può essere utilizzata sia nelle reti IP che MPLS. La funzione BGP PIC per IP e MPLS VPN crea e memorizza un percorso di backup/alternativo nel database di informazioni di routing (RIB, Routing Information Base), nel database di informazioni di inoltro (FIB, Forwarding Information Base) e in Cisco Express Forwarding (CEF, Cisco Express Forwarding) in modo che, quando viene rilevato un errore, il percorso di backup/alternativo possa subentrare immediatamente, consentendo un failover rapido.

Con una singola riscrittura delle informazioni dell'hop successivo, il flusso del traffico viene ripristinato. Inoltre, la convergenza BGP della rete avviene in background, ma i flussi di traffico non sono più influenzati. Questa riscrittura avviene entro 50 msec. Se si utilizza questa tecnologia, la convergenza di rete viene ridotta da secondi a 50 msec più la convergenza IGP.

Percorso aggiuntivo BGP

BGP Add-Path rappresenta un miglioramento nella comunicazione delle voci BGP tra altoparlanti BGP. Se su un certo diffusore BGP c'è più di una voce verso una certa destinazione, allora quel diffusore BGP invia solo la voce che è il suo miglior percorso per quella destinazione ai suoi vicini. Ne consegue che non sono previste disposizioni per consentire la pubblicità di percorsi multipli per la stessa destinazione.

Add-Path BGP è una funzione BGP che consente di impostare più percorsi come solo il miglior percorso e consente più percorsi per la stessa destinazione senza che i nuovi percorsi sostituiscano implicitamente quelli precedenti. Questa estensione a BGP è particolarmente importante quando si usano i riflettori di route BGP, in modo che i diversi diffusori BGP all'interno di un ASA abbiano accesso a più percorsi BGP come "miglior percorso BGP" in base al riflettore di route.

Alternative senza loop e rLFA per IGP Fast-Convergence

Le operazioni per ottenere un ripristino di 50 millisecondi dopo un errore di un collegamento o di un nodo possono essere notevolmente semplificate con l'introduzione di una nuova tecnologia denominata LFA (Loop-Free Alternates). LFA migliora i protocolli di routing dello stato del collegamento (IS-IS e OSPF) in modo da trovare percorsi di routing alternativi senza loop. LFA consente a ciascun router di definire e utilizzare un percorso di backup predeterminato in caso di errore di un'adiacenza (nodo o collegamento di rete). Per garantire un tempo di ripristino di 50 msec in caso di errori di collegamento o nodo, è possibile distribuire MPLS TE FRR. Tuttavia, è necessario aggiungere un altro protocollo (Resource Reservation Protocol o RSVP) per la configurazione e la gestione dei tunnel TE. Sebbene questa operazione sia necessaria per la gestione della larghezza di banda, le operazioni di protezione e ripristino non richiedono la gestione della larghezza di banda. Pertanto, il sovraccarico associato all'aggiunta di RSVP TE è considerato elevato per la semplice protezione di collegamenti e nodi.

LFA può fornire una tecnica semplice e facile senza l'installazione di RSVP TE in tali scenari. Grazie a queste tecniche, gli attuali router interconnessi in reti su larga scala possono fornire un ripristino di 50 msec in caso di errori di collegamenti e nodi senza un requisito di configurazione per l'operatore.

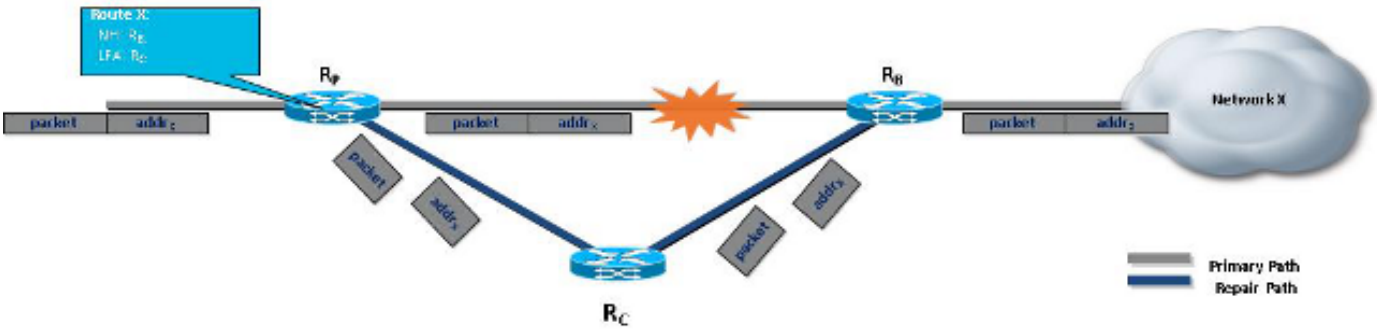

Figura 8

LFA-FRR è un meccanismo che fornisce protezione locale per il traffico unicast in IP, MPLS, Ethernet over MPLS (EoMPLS), Inverse Multiplexing over ATM (IMA) over MPLS, Circuit Emulation Service over Packet Switched Network (CESoPSN) over MPLS e Structure-Async Time Division Multiplexing over Packet (SAToP) over MPLS. Tuttavia, alcune topologie (ad esempio la topologia ad anello) richiedono una protezione che non è garantita dalla sola LFA-FRR. La funzione LFA-FRR remota è utile in queste situazioni.

La funzionalità remota LFA-FRR estende il comportamento di base di LFA-FRR a qualsiasi

topologia. Inoltra il traffico intorno a un nodo guasto a un'interfaccia LFA remota che si trova a più di un hop di distanza. Nella Figura 9, se il collegamento tra C1 e C2 non riesce a raggiungere A1, C2 invia il pacchetto tramite una sessione LDP diretta a C5, che ha raggiungibilità ad A1.

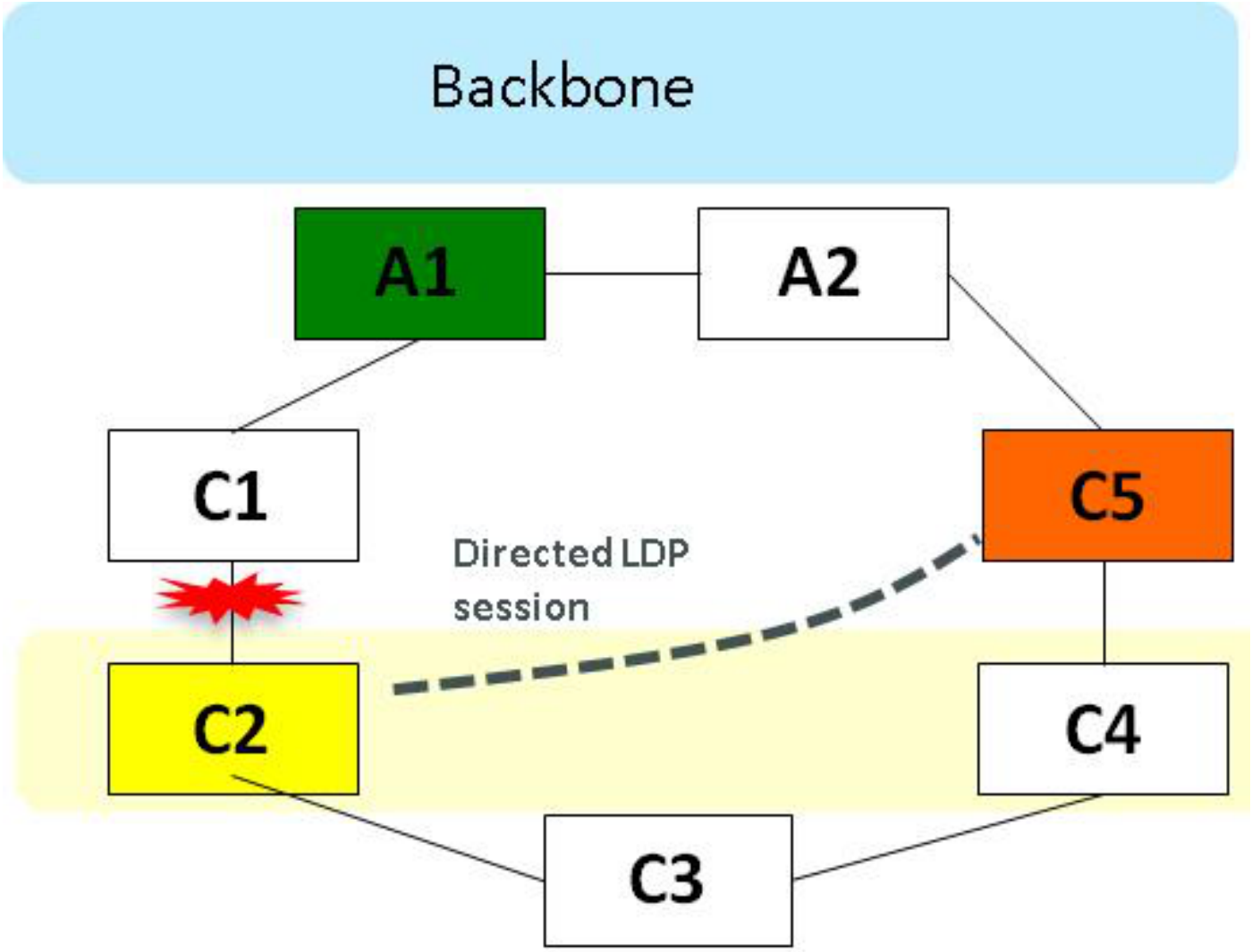

Figura 9

In Remote LFA-FRR, un nodo calcola dinamicamente il proprio nodo LFA. Dopo aver determinato il nodo alternativo (che non è connesso direttamente), il nodo stabilisce automaticamente una sessione LDP diretta al nodo alternativo. La sessione LDP diretta scambia etichette per la particolare correzione progressiva dell'errore (FEC).

Quando il collegamento ha esito negativo, il nodo utilizza lo stack di etichette per eseguire il tunnel del traffico verso il nodo LFA remoto e inoltrare il traffico alla destinazione. Tutti gli scambi di etichette e il tunneling al nodo LFA remoto sono di natura dinamica e non è necessario preprovisioning. L'intero meccanismo di scambio di etichette e tunneling è dinamico e non implica alcuna fornitura manuale.

Per i provider di servizi di traduzione intradomini, la FRR LFA remota viene utilizzata per il traffico MPLS unicast nelle topologie ring. La FRR LFA remota precalcola un percorso di backup per ogni prefisso nella tabella di routing IGP, che consente al nodo di passare rapidamente al percorso di backup quando si verifica un errore. che offre tempi di ripristino dell'ordine di 50 msec.

Esempio di architettura Cisco Unified MPLS

Quando tutti gli strumenti e le funzionalità precedenti vengono riuniti in un ambiente di rete, viene creato l'ambiente di rete Cisco Unified MPLS. Esempio di architettura per provider di servizi di grandi dimensioni.

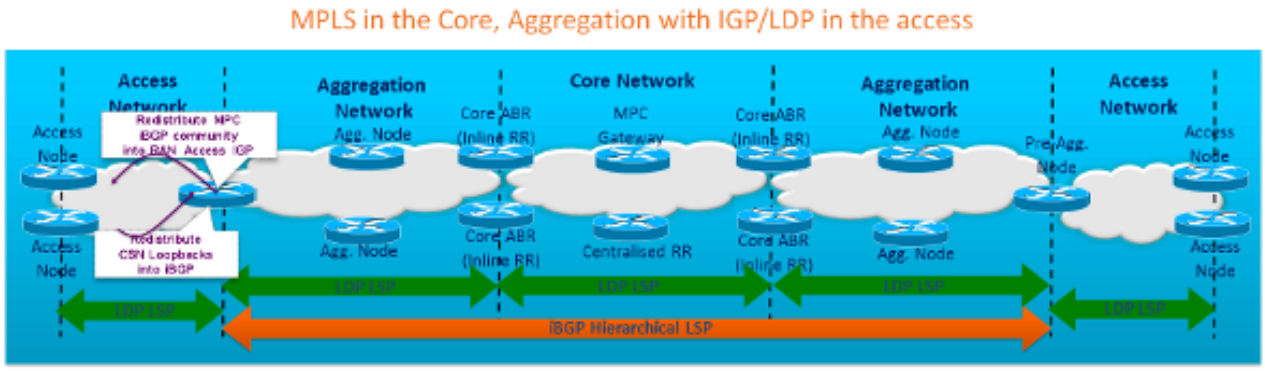

Figura 10

- Core e Aggregation sono organizzati come domini IGP/LDP distinti.
- LSP gerarchici interdominio basati su RFC 3107, etichette BGP IPv4+ estese al pre-agg.
- Provider di servizi di traduzione intradomini basati su LDP.
- I processori LSP di base/aggregazione dell'interdominio vengono estesi nelle reti di accesso tramite la distribuzione del protocollo RAN IGP (Radio Access Networks Interior Gateway Protocol) nell'interdominio iBGP e distribuiscono i prefissi iBGP (MPC (Mobile Packet Core) obbligatori nell'IGP RAN (tramite le community BGP).

Esempio di configurazione MPLS unificata

Di seguito è riportato un esempio semplificato di MPLS unificato.

Core Area Border Router - Cisco IOS® XR

Router per gateway di pre-aggregazione e siti cellulari - Cisco IOS

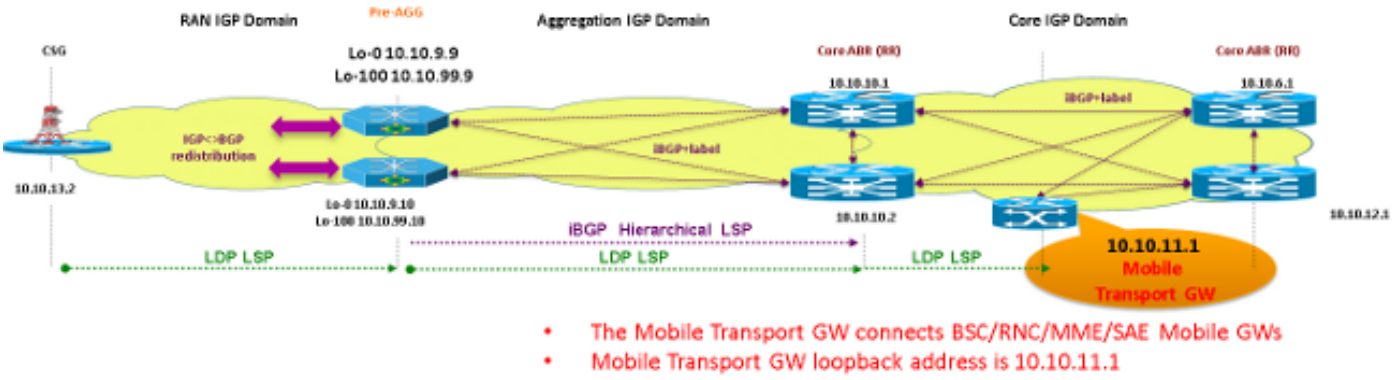

Figura 11

200:200 Community MPC	
300:300 Aggregation Community	
Dominio IGP di base	ISIS livello 2
Dominio IGP di aggregazione	ISIS livello 1
Accesso a dominio IGP	Aree OSPF 0

Configurazione Core Area Border Router

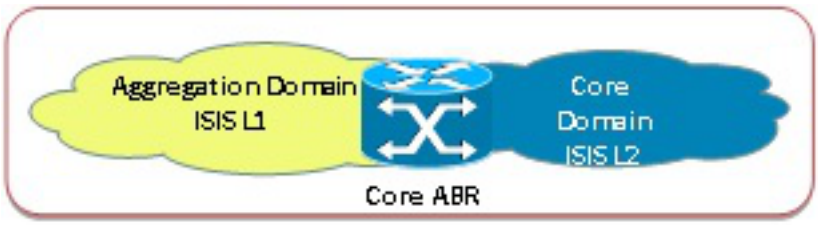

Figura 12

```
! 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
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
```

Configurazione pre-aggregazione

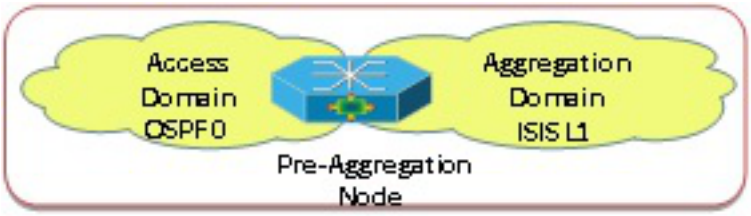

Figura 13

```
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
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
```

Configurazione di CSG (Cell Site Gateway)

Figura 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
```

Configurazione MTG

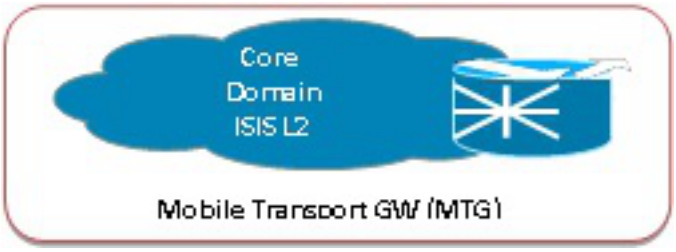

Figura 15

```
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
```

Verifica

Il prefisso di loopback di Mobile Packet Gateway (MPG) è 10.10.11.1/32, quindi il prefisso è rilevante. Ora, guardate come i pacchetti vengono inoltrati da CSG a MPG.

Il prefisso MPC 10.10.11.1 è noto al router CSG dal pre-agg con tag di route 1000 e può essere inoltrato come pacchetto con etichetta LDP in uscita 31 (LDP all'interno del dominio). La community MPC 200:200 è stata mappata con tag route 1000 nel nodo Pre-agg mentre la

ridistribuzione è in OSPF.

Output 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            Vl40       10.13.1.0
      MAC/Encaps=14/18, MRU=1500, Label Stack{31}
```

Uscite nodo pre-aggregazione

Nel nodo Pre-agg, il prefisso MPC viene ridistribuito dal processo BGP al processo OSPF di accesso RAN con filtro basato sulla community e il processo OSPF viene ridistribuito in BGP. Questa ridistribuzione controllata è necessaria per garantire la raggiungibilità IP end-to-end e allo stesso tempo per ciascun segmento sono richiesti percorsi minimi.

Il prefisso 10.10.11.1/32 è noto tramite BGP 100 gerarchico con la community MPC 200:200 collegata. L'etichetta 16020 BGP 3107 ricevuta dal core Area Border Router (ABR) e l'etichetta LDP 22 vengono aggiunte in cima per l'inoltro all'intradominio dopo la ricerca ricorsiva dell'hop successivo.

```
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}
```

Uscite core ABR Node

Il prefisso **10.10.11.1 è noto tramite IGP intradominio (ISIS-L2)** e come nella tabella di inoltro MPLS. È raggiungibile tramite 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.
```

Per la distribuzione dei prefissi tra le aree segmentate, viene utilizzato BGP con etichetta (RFC 3107). Ciò che deve ancora risiedere all'interno delle aree segmentate dell'IGP sono i loopback delle PE e gli indirizzi relativi all'infrastruttura centrale.

I router BGP che connettono diverse aree sono i router ABR che agiscono come Route-Reflector BGP. Questi dispositivi utilizzano la funzione Next-Hop-Self, per evitare la necessità di avere tutti gli hop successivi del sistema autonomo completo all'interno dell'IGP, invece che solo gli indirizzi IP dei PE e dell'infrastruttura centrale. Rilevamento loop completato in base agli ID del cluster BGP.

Per la resilienza della rete, BGP PIC con la funzione BGP Add Path deve essere utilizzato con BGP e LFA con IGP. Queste funzioni non sono utilizzate nell'esempio precedente.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Architettura MPLS perfetta
- White paper Cisco Unified MPLS
- Sistema Cisco Carrier Packet Transport (CPT)
- Documentazione e supporto tecnico – Cisco Systems