Beispiel für Unified MPLS-Funktionalität, -Funktionen und -Konfiguration

Inhalt

Einführung

Dieses Dokument beschreibt Unified Multiprotocol Label Switching (MPLS), bei dem es um Skalierung geht. Es bietet ein Framework von Technologielösungen, die einfachen End-to-End-Datenverkehr und/oder -Services in einer traditionell segmentierten Infrastruktur bereitstellen. Sie nutzt sowohl die Vorteile einer hierarchischen Infrastruktur, da sie die Skalierbarkeit verbessert, als auch die Einfachheit des Netzwerkdesigns.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkentwicklung

Wenn Sie sich den Verlauf der paketbasierten Netzwerkservices anschauen, kann eine Veränderung der geschäftlichen Werte im Netzwerk beobachtet werden. Dies reicht von eigenständigen Anbindungsverbesserungen, um Anwendungen so flüssig wie möglich zu machen, bis hin zu Collaboration-Technologien zur Unterstützung mobiler Zusammenarbeit. Schließlich werden die On-Demand-Cloud-Services mit den Anwendungsdiensten eingeführt, um die in einem Unternehmen eingesetzten Tools zu optimieren und die Stabilität und die Gesamtbetriebskosten zu verbessern.

Abbildung 1

Diese kontinuierliche Wertsteigerung und Funktionserweiterung des Netzwerks führt zu einem weitaus umfassenderen Bedarf an Einfachheit, Verwaltbarkeit, Integration und Stabilität des Netzwerks, wenn Netzwerke aufgrund unzusammenhängender Betriebsinseln segmentiert wurden und keine echte End-to-End-Pfadkontrolle möglich ist. Jetzt gilt es, alle Komponenten in einer einzigen Architektur zusammenzufassen, die einfach zu verwalten ist, eine Skalierbarkeit auf mehrere 100.000 Knoten bietet und die aktuellen Hochverfügbarkeits- und Fast Convergence-Technologien verwendet. Dies bringt Unified MPLS in die Tabelle, d. h. das segmentierte Netzwerk in eine einzige Kontrollebene und End-to-End-Pfadtransparenz.

Moderne Netzwerkanforderungen

- Erhöhte Bandbreitennachfrage (Video)
- Erhöhung der Anwendungskomplexität (Cloud und Virtualisierung)
- Erhöhter Bedarf an Konvergenz (Mobilität)

Wie können Sie MPLS-Prozesse in immer größeren Netzwerken mit komplexeren Anwendungsanforderungen vereinfachen?

Herkömmliche MPLS-Herausforderungen mit unterschiedlichen Zugriffstechnologien

- Komplexität zur Erzielung einer Konvergenz von 50 Millisekunden mit Traffic Engineering Fast Reroute (TE FRR)
- Bedarf an hoch entwickelten Routing-Protokollen und Interaktion mit Layer-2-Protokollen
- Aufteilung großer Netzwerke in Domänen, Bereitstellung von Diensten im End-to-End-Bereich
- Gemeinsame End-to-End-Konvergenz und Ausfallsicherheit
- Fehlerbehebung und End-to-End-Bereitstellung über mehrere Domänen hinweg

Die Unified MPLS-Attraktivität wird in dieser Liste zusammengefasst:

- Weniger Betriebspunkte In der Regel muss ein Service über Operational Points auf jedem Netzwerkelement konfiguriert werden. Das Managementsystem muss die Topologie kennen.Bei Unified MPLS wird durch die Integration aller MPLS-Inseln die Mindestanzahl an Betriebspunkten erreicht.
- Möglichkeit zur einfachen Bereitstellung von Services: Layer-3-VPN (L3), Virtual Private Wire Service (VPWS), Virtual Private LAN Service (VPLS), ohne Mechanismen zum Pseudowire-Heften (PW-Heften) oder InterAS. Mit der Einführung von MPLS in der Aggregation wird eine statische Konfiguration vermieden, die MPLS-Inseln erstellt.
- End-to-End-MPLS-Transport
- Trennung von IGP-Bereichen (Interior Gateway Protocol) und kleinen Routing-Tabellen.
- Schnelle Konvergenz.
- Einfache Konfiguration und Fehlerbehebung
- Integration in beliebige Zugriffstechnologien
- IPv6-fähig.

Cisco Unified MPLS

Unified MPLS wird durch zusätzliche Funktionen mit klassischem/traditionellem MPLS definiert und bietet mehr Skalierbarkeit, Sicherheit, Einfachheit und Verwaltbarkeit. Um die durchgängigen MPLS-Services bereitstellen zu können, ist ein durchgängiger LSP (Label Switches Path) erforderlich. Das Ziel besteht darin, die MPLS-Services (MPLS VPN, MPLS L2VPN) unverändert beizubehalten, jedoch eine höhere Skalierbarkeit zu gewährleisten. Hierzu verschieben Sie einige IGP-Präfixe in das Border Gateway Protocol (BGP) (die Loopback-Präfixe der Provider Edge (PE)-Router), das die Präfixe dann durchgängig verteilt.

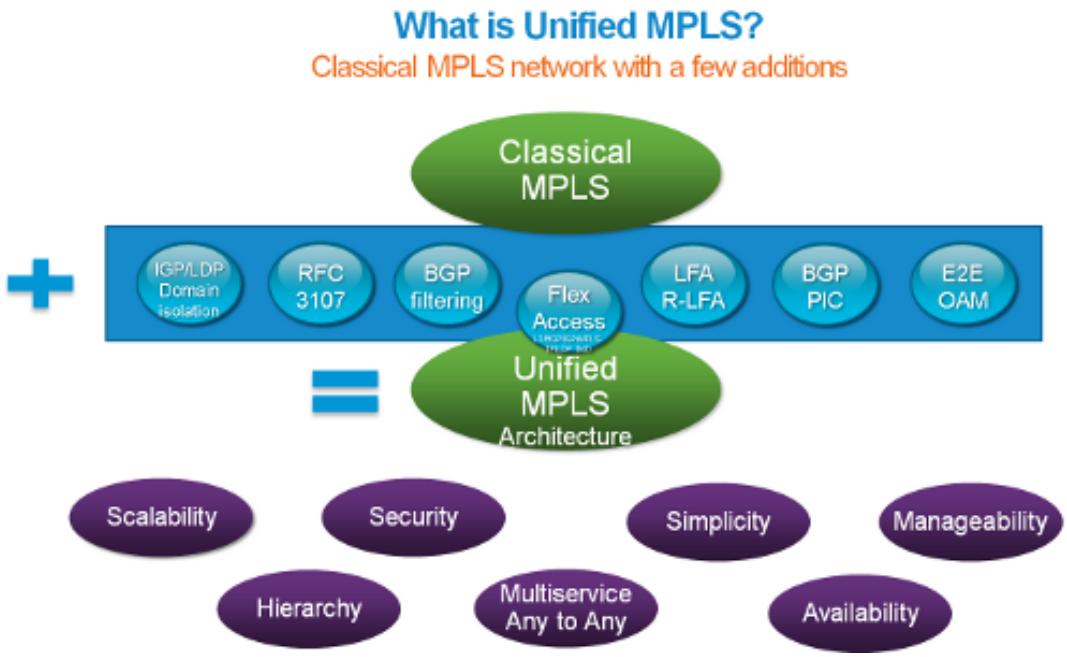

Abbildung 2

Bevor die Cisco Unified MPLS-Architektur diskutiert wird, ist es wichtig, die wichtigsten Funktionen zu verstehen, die zur Realisierung dieses Ziels verwendet werden.

Funktionen und Komponenten

Carry Label Information in BGP-4 (RFC 3107)

Voraussetzung für den Austausch von Präfixen zwischen Netzwerksegmenten ist eine skalierbare Methode. Sie können die IGPs (Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS) oder Enhanced Interior Gateway Routing Protocol (EIGRP)) einfach in einer einzigen Domäne zusammenführen. Ein IGP ist jedoch nicht für die Übertragung von 100.000 Präfixen ausgelegt. Zu diesem Zweck wird BGP als Protokoll gewählt. Es ist ein bewährtes Protokoll, das das Internet mit hunderttausend Routen und MPLS-VPN-Umgebungen mit Millionen von Einträgen unterstützt. Cisco Unified MPLS verwendet BGP-4 mit Label Information Exchange (RFC3107). Wenn das BGP eine Route verteilt, kann es auch ein diesem Route zugeordnetes MPLS-Label verteilen. Die MPLS-Labelzuordnungsinformationen für die Route werden in der BGP-Update-Nachricht mit Informationen über die Route übertragen. Wenn der nächste Hop nicht geändert wird, wird das Label beibehalten, und das Label ändert sich, wenn sich der nächste Hop ändert. In Unified MPLS wechselt der nächste Hop bei Area Border Routers (ABRs).

Wenn Sie RFC 3107 auf beiden BGP-Routern aktivieren, geben die Router einander an, dass sie anschließend MPLS-Labels mit den Routen senden können. Wenn die Router erfolgreich verhandeln, dass sie MPLS-Labels senden können, fügen die Router allen ausgehenden BGP-Updates MPLS-Labels hinzu.

Der Label-Austausch ist erforderlich, um die End-to-End-Pfadinformationen zwischen Segmenten zu erhalten. Dadurch wird jedes Segment klein genug, um von Operatoren verwaltet zu werden. Gleichzeitig werden Schaltungsinformationen für die Pfaderkennung auf zwei verschiedenen IP-Lautsprechern verteilt.

Wie funktioniert es?

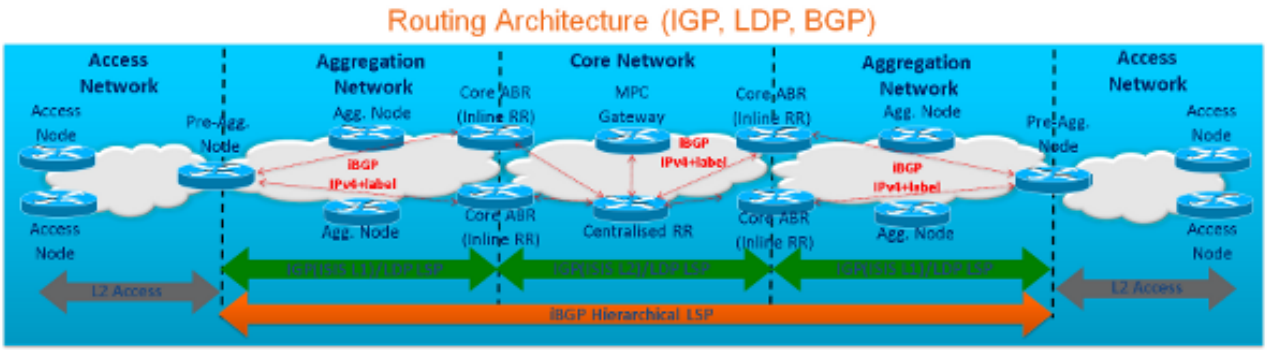

Abbildung 3

Abbildung 3 zeigt, dass es drei Segmente mit LDP LSP (Label Discovery Protocol Label Switches Path) gibt, für die LDP nicht aktiviert ist. Ziel ist es, diese Knoten zusammenzuführen, sodass ein einzelner MPLS-Pfad (interner BGP (iBGP) hierarchischer LSP) zwischen Pre-Aggregation (Pre-Aggregation)-Knoten vorhanden ist. Da das Netzwerk ein einzelnes BGP Autonomous System (AS) ist, sind alle Sitzungen iBGP-Sitzungen. Jedes Segment führt innerhalb der IGP-Domäne eigene IGP- (OSPF, IS-IS oder EIGRP) und LDP-LSP-Pfade aus. Innerhalb von Cisco Unified MPLS müssen die zu den Segmenten gehörenden Router (ABRs) BGP Inline-Routen-Reflektoren mit Next-Hop-Self und RFC 3107 sein, damit ein für die Sitzungen konfiguriertes IPv4 + Label übertragen werden kann. Diese BGP-Lautsprecher befinden sich in der Cisco Unified MPLS-Architektur, die als ABRs bezeichnet wird.

Warum sind die ABRs Inline-Routen-Reflektoren?

Eines der Ziele von Unified MPLS ist eine hochgradig skalierbare End-to-End-Infrastruktur. Daher sollte jedes Segment einfach gehalten werden, um zu funktionieren. Alle Peerings sind iBGP-Peers. Daher ist ein Full-Mesh von Peerings zwischen allen iBGP-Routern im gesamten Netzwerk erforderlich. Dies führt zu einer sehr unpraktischen Netzwerkumgebung, wenn es Tausende von BGP-Routern gibt. Wenn die ABRs Routen-Reflektoren bilden, wird die Anzahl der iBGP-Peering auf die Anzahl der BGP-Peers "pro Segment" reduziert, anstatt auf die Anzahl der BGP-Peers zwischen "allen" BGP-Routern des vollständigen AS.

Warum Next-Hop-Self?

BGP wird auf Basis rekursiver Routing-Suchvorgänge ausgeführt. Dies geschieht, um die Skalierbarkeit innerhalb des zugrunde liegenden IGP zu ermöglichen, das verwendet wird. Für die rekursive Suche verwendet BGP Next-Hop, der an jeden BGP-Routeneintrag angeschlossen ist. Wenn beispielsweise ein Quellknoten ein Paket an einen Zielknoten senden möchte und das Paket auf den BGP-Router trifft, führt der BGP-Router eine Routing-Suche in seiner BGP-Routing-Tabelle durch. Er findet eine Route in Richtung Zielknoten und den Next-Hop als nächsten Schritt. Dieser Next-Hop muss vom zugrunde liegenden IGP bekannt sein. Im letzten Schritt leitet der BGP-Router das Paket basierend auf den mit diesem Next-Hop verknüpften IP- und MPLS-Label-Informationen weiter.

Um sicherzustellen, dass innerhalb jedes Segments nur die Next-Hops vom IGP bekannt sein müssen, muss der Next-Hop, der mit dem BGP-Eintrag verbunden ist, innerhalb des Netzwerksegments und nicht innerhalb eines Nachbars oder weiter entfernten Segments sein. Wenn Sie den BGP Next-Hop mit der Next-Hop-Self-Funktion umschreiben, stellen Sie sicher, dass sich der Next-Hop im lokalen Segment befindet.

Alles miteinander verbinden

Example - 'L3VPN Services'

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

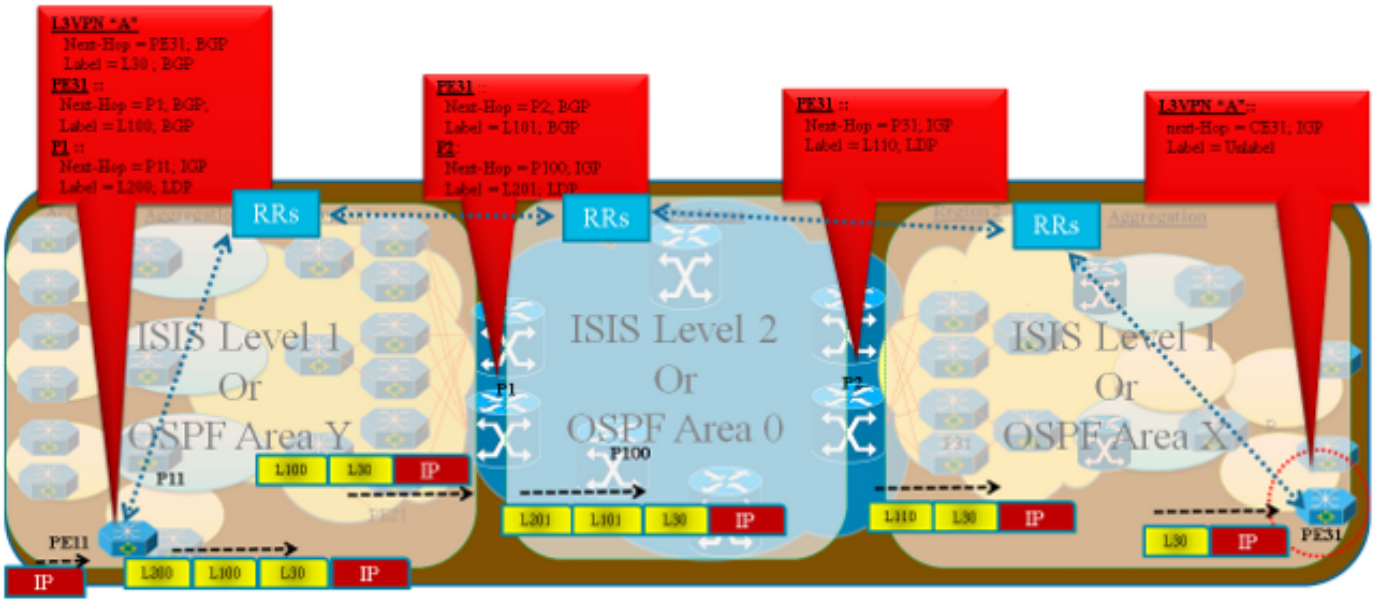

Abbildung 4

Abbildung 4 zeigt ein Beispiel für die Funktionsweise des L3-VPN-Präfix "A" und des Label-Austauschs sowie die Erstellung des MPLS-Label-Stacks, um die End-to-End-Pfadinformationen für den Datenverkehrsfluss zwischen beiden PEs zu erhalten.

Das Netzwerk wird als drei unabhängige IGP/LDP-Domänen partitioniert. Die geringere Größe der Routing- und Weiterleitungstabellen der Router ermöglicht eine höhere Stabilität und schnellere Konvergenz. LDP wird zum Aufbau domäneninterner LSPs innerhalb von Domänen verwendet. RFC 3107 BGP IPv4+-Labels werden als Domänenübergreifende Label-Verteilungsprotokolle verwendet, um hierarchische BGP LSPs über Domänen hinweg zu erstellen. BGP3107 fügt ein zusätzliches Label in den Weiterleitungs-Label-Stack der Unified MPLS-Architektur ein.

Intradomain: LDP LSP

Interdomain - Hierarchischer BGP-LSP

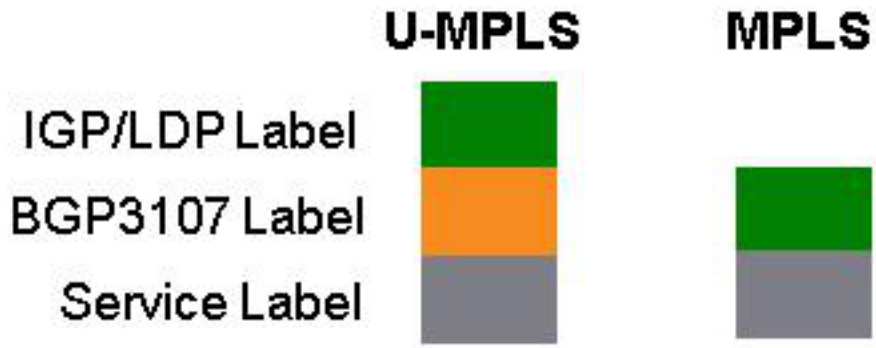

Abbildung 5

Das VPN-Präfix "A" wird PE31 mit dem L3VPN-Service-Label 30 und dem Next Hop als Loopback des PE31 über den hierarchischen End-to-End-BGP-LSP für die Domänen angekündigt. Betrachten Sie nun den Weiterleitungspfad für das VPN-Präfix "A" von PE11 zu PE31.

- Auf PE11 ist das Präfix A über die BGP-Sitzung mit PE31 als Next-Hop-PE31 bekannt, und PE31 ist rekursiv über P1 mit dem BGP-Label 100 erreichbar. PE11 erhielt IPv4 + Label-Informationen von P1 als BGP-Updates, da diese mit der RFC 3107-Funktion aktiviert wurden, um die IPv4 + Label-Informationen zu senden.
- P1 ist vom PE11 über einen domäneninternen LDP-LSP erreichbar und fügt dem BGP-Label ein weiteres LDP-Label hinzu. Schließlich wird das Paket aus dem PE11-Knoten mit drei Labels entfernt. Beispielsweise das 30-L3VPN-Service-Label, das 100-BGP-Label und das 200-LDP-IGP-Label.
- Das LDP-oberste Label tauscht weiterhin innerhalb des Domain-LDP-LSP aus, und das Paket erreicht P1 mit zwei Labels nach Penultimate Hop Popping (PHP).
- P1 wird als Inline Route Reflector (RR) mit Next-Hop Self konfiguriert und verbindet zwei IGP-Domänen oder LDP LSP.
- Auf P1 wird der nächste Hop für PE31 in P2 geändert, und das Update wird über BGP mit IPv4 + Label (RFC3107) empfangen. Das BGP-Label wird durch ein neues Label ersetzt, da Next-Hop geändert und das IGP-Label oben angedrückt wird.
- Das Paket wird aus dem P1-Knoten mit drei Labels und das Service-Label 30 ist unberührt. Das heißt, das 30-L3VPN-Service-Label, das 101-BGP-Label und das 201-LDP-Label.
- Das LDP-Top-Label tauscht innerhalb des Domain LDP LSP aus und das Paket erreicht P2 mit zwei Labels nach PHP.
- Auf P2 wird der nächste Hop für PE31 erneut geändert und ist über IGP erreichbar. Das BGP-Label wird entfernt, da ein implizites Null-BGP-Label von PE31 für PHP empfangen wird.
- Das Paket erhält zwei Labels. Beispielsweise das 30-L3VPN-Service-Label und das 110-LDP-Label.
- Auf PE31 kommt das Paket mit einem Label nach PHP des LDP-Labels und basierend auf dem Service-Label 30. Das nicht gekennzeichnete Paket wird unter Virtual Routing and Forwarding (VRF) an das CE31-Ziel weitergeleitet.

Beim Betrachten des MPLS-Label-Stacks wird in der MPLS-Switching-Umgebung das Switching des Pakets zwischen einem Quell- und Zielgerät auf der Grundlage des vorherigen Präfix- und Labelaustauschs beobachtet.

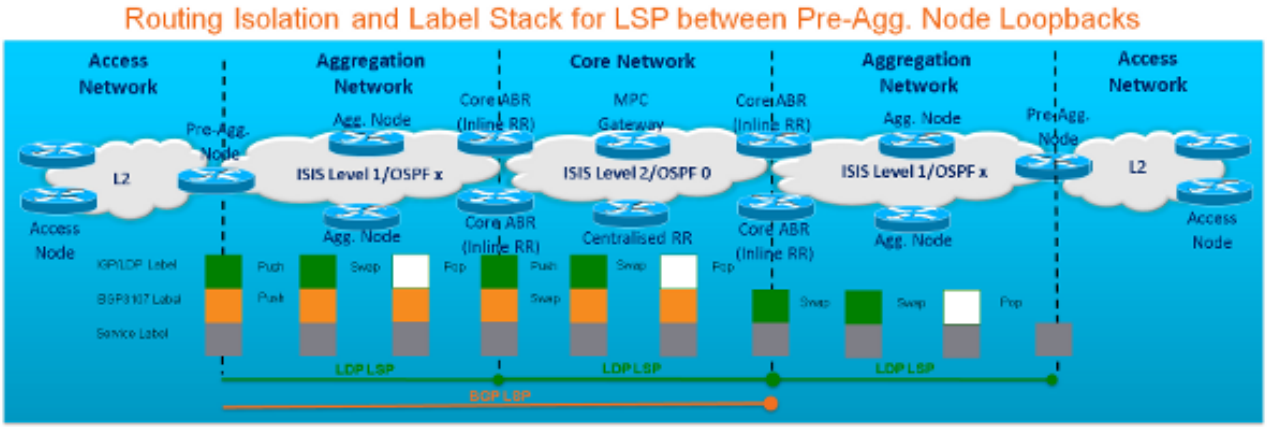

Abbildung 6

BGP-Prefix-Independent Convergence (BGP PIC)

Dies ist eine Cisco Technologie, die in BGP-Fehlerszenarien verwendet wird. Das Netzwerk konvergiert ohne Verlust der herkömmlichen Sekunden bei der BGP-Rekonvergenz. Wenn BGP PIC verwendet wird, können die meisten Fehlerszenarien auf eine Rekonvergenzzeit unter 100 ms

reduziert werden.

Wie wird das gemacht?

Wenn BGP einen Fehler erkennt, wird er für jeden BGP-Eintrag für den besten Pfad neu berechnet. Wenn eine Routing-Tabelle mit Tausenden von Routeneinträgen vorhanden ist, kann dies eine beträchtliche Zeit in Anspruch nehmen. Darüber hinaus muss dieser BGP-Router alle diese neuen besten Pfade an die einzelnen Nachbarn verteilen, um sie über die geänderte Netzwerktopologie und die geänderten besten Pfade zu informieren. Im letzten Schritt muss jeder BGP-Empfänger-Sprecher eine Berechnung des besten Pfads durchführen, um die neuen besten Pfade zu finden.

Jedes Mal, wenn der erste BGP-Sprecher einen Fehler feststellt, startet er die Berechnung des besten Pfads, bis alle benachbarten BGP-Lautsprecher eine Neuberechnung vorgenommen haben, wird der Datenverkehrsfluss möglicherweise verworfen.

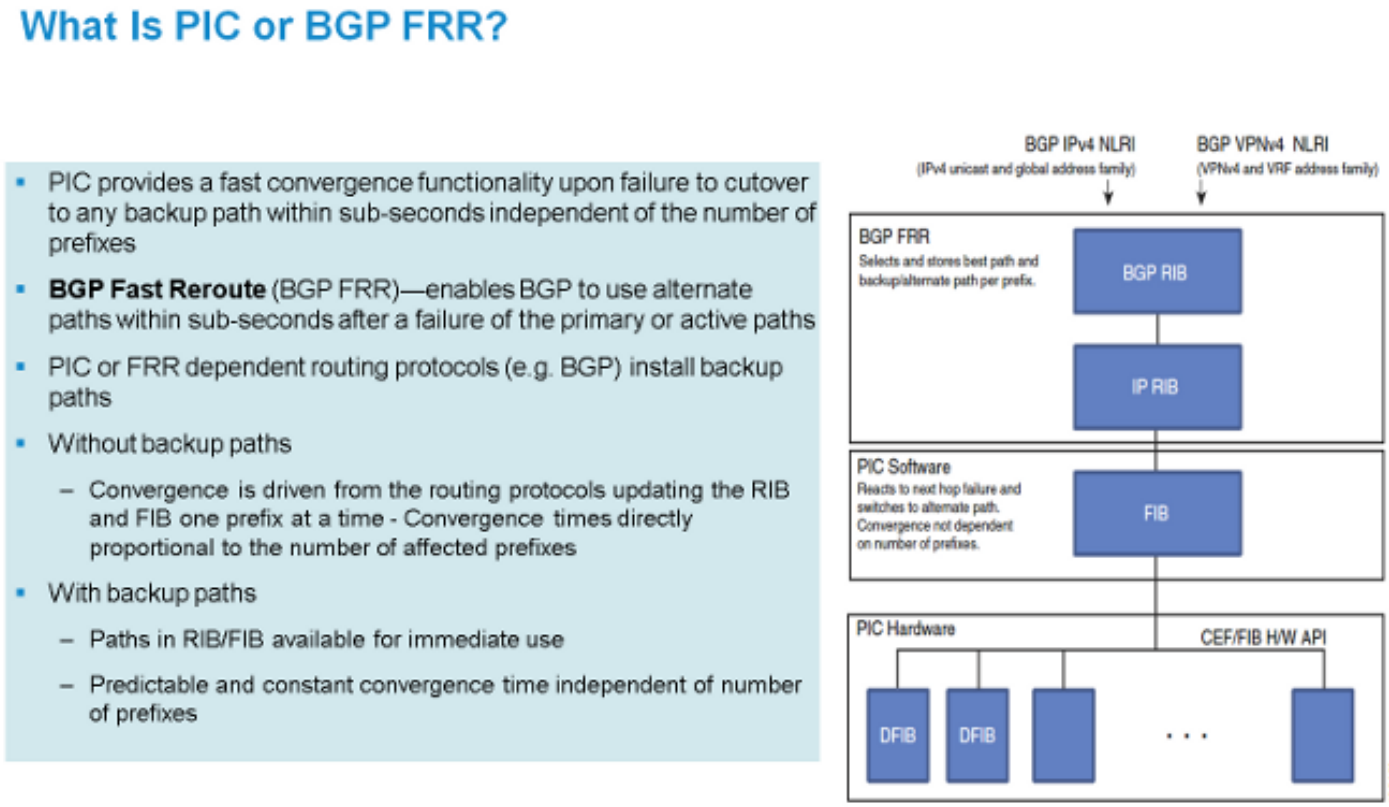

Abbildung 7

Die Funktion BGP PIC für IP und MPLS VPN verbessert die BGP-Konvergenz nach einem Netzwerkausfall. Diese Konvergenz ist sowohl für Core- als auch Edge-Ausfälle anwendbar und kann sowohl in IP- als auch in MPLS-Netzwerken verwendet werden. Der BGP PIC für IP und die MPLS VPN-Funktion erstellen und speichern einen Backup-/Alternativpfad in der Routing Information Base (RIB), der Forwarding Information Base (FIB) und Cisco Express Forwarding (CEF), sodass bei einem Ausfall der Backup-/Alternativpfad sofort übernommen werden kann, wodurch ein schnelles Failover ermöglicht wird.

Bei einer einzigen Umschreibung der Next-Hop-Informationen wird der Datenverkehrsfluss wiederhergestellt. Darüber hinaus erfolgt die BGP-Konvergenz des Netzwerks im Hintergrund, aber die Datenverkehrsflüsse sind nicht mehr betroffen. Diese Umschreibung erfolgt innerhalb von 50 ms. Wenn Sie diese Technologie verwenden, wird die Netzwerkkonvergenz von Sekunden auf 50 ms und die IGP-Konvergenz reduziert.

BGP-Add-Path

BGP Add-Path bietet eine Verbesserung der Kommunikation zwischen BGP-Routern und BGP-Routern. Wenn auf einem bestimmten BGP-Sprecher mehr als ein einziger Eintrag zu einem bestimmten Ziel vorhanden ist, sendet dieser BGP-Sprecher nur den Eintrag, der der beste Pfad für dieses Ziel ist, an seine Nachbarn. Das Ergebnis ist, dass keine Bestimmungen getroffen werden, um die Anzeige mehrerer Pfade für dasselbe Ziel zu ermöglichen.

BGP Add-Path ist eine BGP-Funktion, die mehr als nur den besten Pfad ermöglicht und mehrere Pfade für dasselbe Ziel ermöglicht, ohne dass die neuen Pfade vorherige Pfade implizit ersetzen. Diese Erweiterung auf das BGP ist besonders wichtig, um BGP PIC bei Verwendung von BGP-Routen-Reflektoren zu unterstützen, sodass die verschiedenen BGP-Lautsprecher innerhalb eines AS Zugriff auf mehr BGP-Pfade haben, als nur der "beste BGP-Pfad" entsprechend dem Routen-Reflektor.

Schleifenfreie Alternate und rLFA für schnelle IGP-Konvergenz

Durch die Einführung einer neuen Technologie, der so genannten "Loop-Free Alternates" (LFAs), können Betriebsabläufe, die nach einem Link- oder Knotenausfall eine Wiederherstellung von 50 Millisekunden ermöglichen, erheblich vereinfacht werden. LFA erweitert die Link-State-Routing-Protokolle (IS-IS und OSPF), um schleifenfreie alternative Routing-Pfade zu finden. LFA ermöglicht es jedem Router, einen vordefinierten Backup-Pfad zu definieren und zu verwenden, wenn eine Adjacency (Netzwerkknoten oder Verbindung) ausfällt. Um bei Verbindungs- oder Knotenausfällen eine Wiederherstellungszeit von 50 ms bereitzustellen, kann MPLS TE FRR bereitgestellt werden. Dies erfordert jedoch das Hinzufügen eines weiteren Protokolls (Resource Reservation Protocol, RSVP) für die Einrichtung und Verwaltung von TE-Tunneln. Dies mag für das Bandbreitenmanagement erforderlich sein, für den Schutz- und Wiederherstellungsvorgang ist jedoch kein Bandbreitenmanagement erforderlich. Daher wird der mit der Hinzufügung von RSVP TE verbundene Overhead für einen einfachen Schutz von Links und Knoten als hoch angesehen.

LFA kann eine einfache und einfache Technik bereitstellen, ohne dass in solchen Szenarien RSVP TE implementiert werden muss. Dank dieser Verfahren können die heute in großen Netzwerken verbundenen Router bei Verbindungs- und Knotenausfällen eine Wiederherstellung von 50 ms ohne Konfigurationsanforderung des Betreibers ermöglichen.

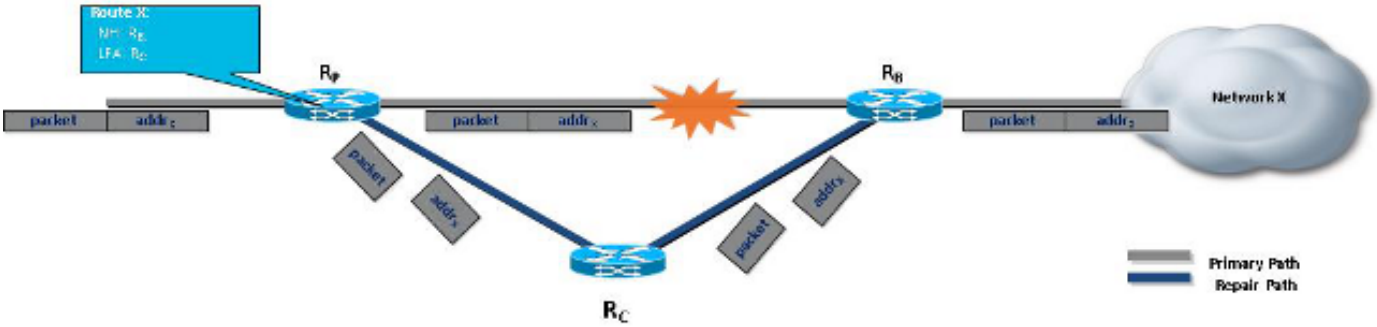

Abbildung 8

LFA-FRR ist ein Mechanismus, der lokalen Schutz für Unicast-Datenverkehr in IP, MPLS, Ethernet Over MPLS (EoMPLS), Inverse Multiplexing over ATM (IMA) über MPLS, Circuit Emulation Service over Packet Switched Network (CESoPSN) über MPLS und Structure-Agnostic Time Division Multiplexing over Packet (SAToP) über MPLS bietet Netzwerke. Einige Topologien (z. B. die Ringtopologie) benötigen jedoch Schutz, der nicht nur durch LFA-FRR gewährleistet wird. Die Remote-LFA-FRR-Funktion ist in solchen Situationen nützlich.

Das Remote-LFA-FRR erweitert das grundlegende Verhalten von LFA-FRR auf jede Topologie. Der Datenverkehr um einen ausgefallenen Knoten wird an eine Remote-LFA weitergeleitet, die mehr als einen Hop entfernt ist. Wenn die Verbindung zwischen C1 und C2 A1 nicht erreicht, sendet C2 in Abbildung 9 das Paket über eine gezielte LDP-Sitzung an C5, die an A1 erreichbar ist.

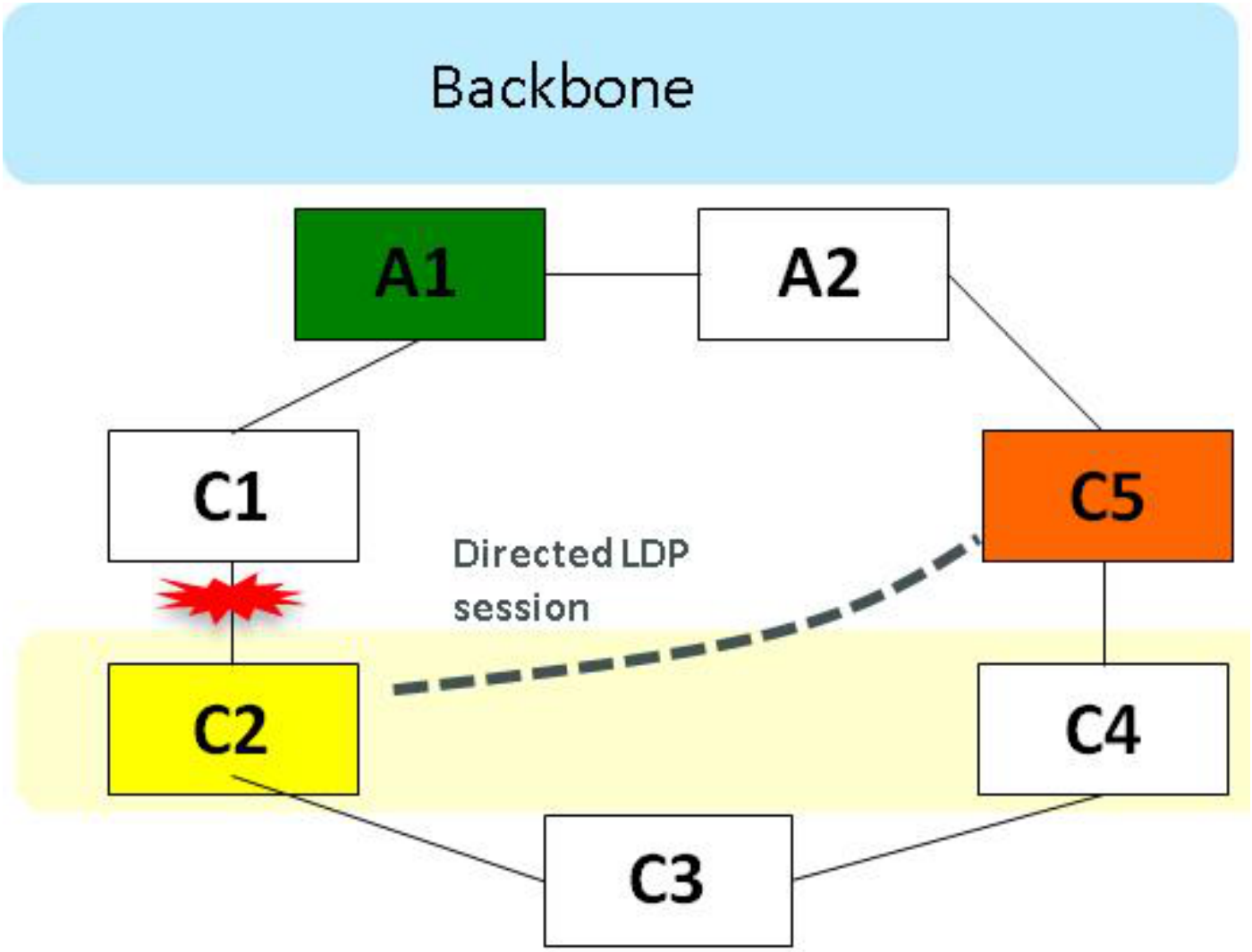

Abbildung 9

In Remote LFA-FRR berechnet ein Knoten dynamisch seinen LFA-Knoten. Nachdem der alternative Knoten bestimmt wurde (der nicht direkt verbunden ist), erstellt der Knoten automatisch eine LDP-Sitzung (Directed Label Distribution Protocol) zum alternativen Knoten. Die gezielte LDP-Sitzung tauscht Labels für die jeweilige Vorwärtsfehlerkorrektur (FEC) aus.

Wenn die Verbindung ausfällt, verwendet der Knoten Label-Stacking, um den Datenverkehr an den Remote-LFA-Knoten weiterzuleiten. Alle Label-Austauschvorgänge und das Tunneling zum Remote-LFA-Knoten sind dynamisch, und eine Vorabbereitstellung ist nicht erforderlich. Der gesamte Label-Austausch- und -Tunneling-Mechanismus ist dynamisch und erfordert keine manuelle Bereitstellung.

Für domäneninterne LSPs wird Remote-LFA FRR für Unicast-MPLS-Datenverkehr in Ring-Topologien verwendet. Mit Remote LFA FRR wird ein Backup-Pfad für jedes Präfix in der IGP-Routing-Tabelle vorberechnet, sodass der Knoten bei einem Ausfall schnell auf den Backup-Pfad umschalten kann. Dadurch werden Wiederherstellungszeiten von ca. 50 ms bereitgestellt.

Beispiel zur Cisco Unified MPLS-Architektur

Wenn alle vorherigen Tools und Funktionen in einer Netzwerkumgebung zusammengefasst sind, wird die Cisco Unified MPLS-Netzwerkumgebung erstellt. Dies ist das Architekturbeispiel für große Service Provider.

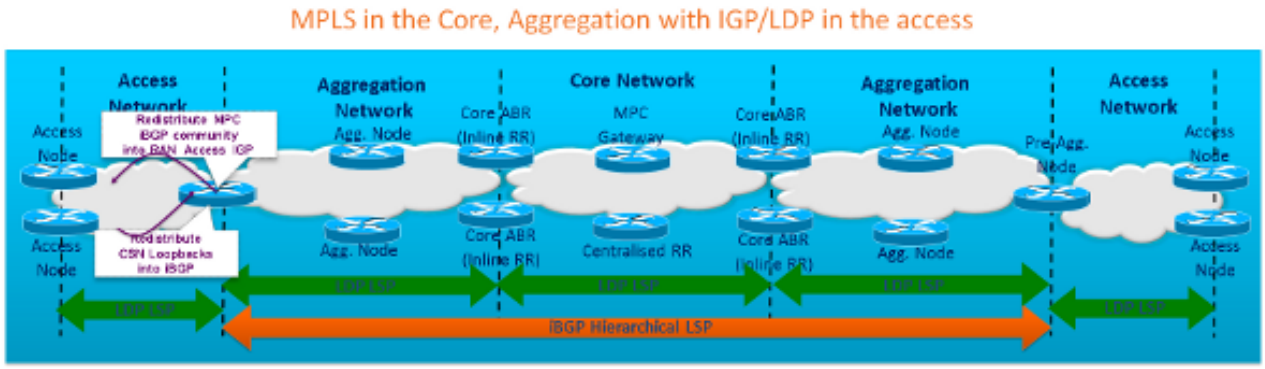

Abbildung 10

- Core und Aggregation sind als separate IGP/LDP-Domänen organisiert.
- Hierarchisch interdomain-LSPs basierend auf RFC 3107, BGP IPv4+ Labels, die auf die Pre-Agg-Klasse ausgeweitet werden.
- Intradomain-LSPs basierend auf LDP.
- Die domänenübergreifenden Core/Aggregation-LSPs werden in den Zugangsnetzwerken durch die Verteilung des Radio Access Networks Interior Gateway Protocol (RAN IGP) auf das domänenübergreifende iBGP erweitert und verteilen die erforderlichen gekennzeichneten iBGP-Präfixe (MPC (Mobile Packet Core)-Gateway) über RAN IGP (über BGP-Communitys).

Unified MPLS-Konfigurationsbeispiel

Ein vereinfachtes Beispiel für Unified MPLS.

Core Area Border Router - Cisco IOS® XR

Gateway-Router vor Aggregation und Cell Site - Cisco IOS

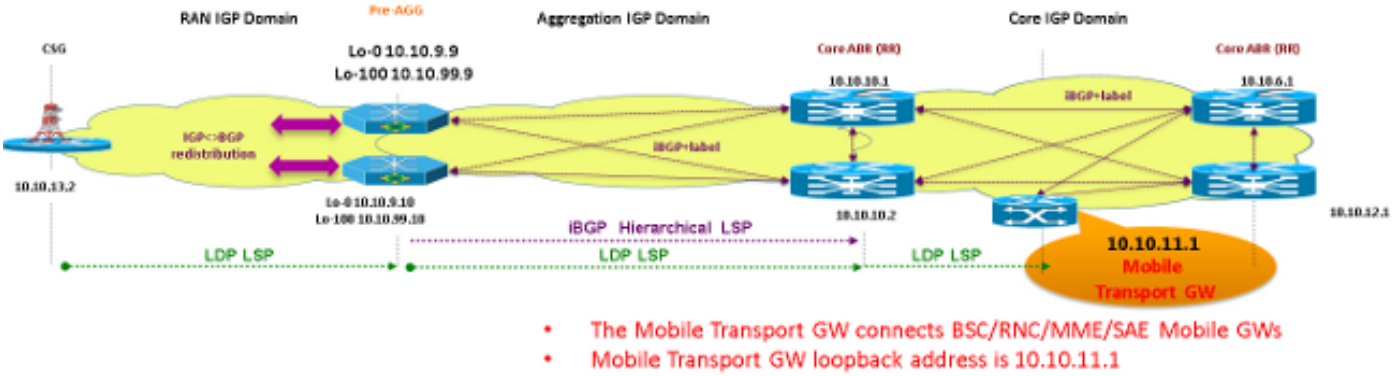

Abbildung 11

200:200 MPC-Community
300:300 Aggregation Community
Core-IGP-Domäne ISIS Stufe 2

Aggregations-IGP-Domäne ISIS Stufe 1
Zugriff auf IGP-Domäne OSPF 0-Bereiche

Konfiguration des Core Area Border Routers

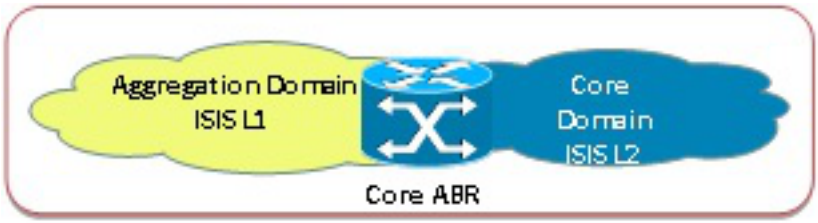

Abbildung 12

```
! 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
```

Konfiguration vor der Aggregation

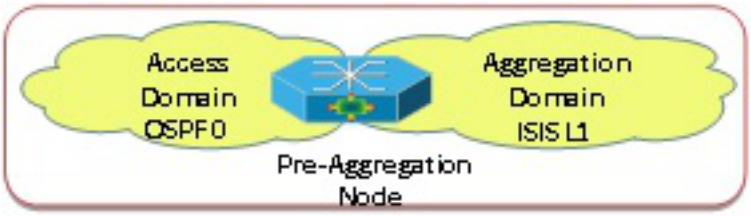

Abbildung 13

```
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-Konfiguration (Cell Site Gateway)

Abbildung 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-Konfiguration

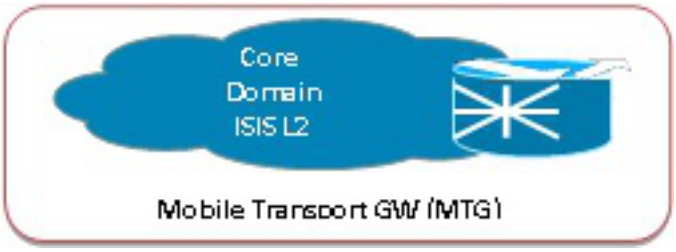

Abbildung 15

```
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
```

Überprüfen

Das Loopback-Präfix des Mobile Packet Gateway (MPG) lautet 10.10.11.1/32, sodass das Präfix von Interesse ist. Sehen Sie sich nun an, wie Pakete von CSG an MPG weitergeleitet werden.

Das MPC-Präfix 10.10.11.1 ist dem CSG-Router aus der Pre-Agg-Phase mit dem Routing-Tag 1000 bekannt und kann als Paket mit Label und ausgehendem LDP-Label 31 (Intra-Domain LDP LSP) weitergeleitet werden. Die MPC-Community 200:200 wurde im Voragg-Knoten dem Route-

Tag 1000 zugeordnet, während die Neuverteilung in OSPF erfolgt.

CSG-Knotenausgabe

```
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}
```

Ausgabe vor Agg-Knoten

Im Knoten vor der Aggregation wird das MPC-Präfix vom BGP an den OSPF-Prozess für den RAN-Zugriff mit Community-basierter Filterung umverteilt, und der OSPF-Prozess wird in BGP neu verteilt. Diese kontrollierte Umverteilung ist erforderlich, um eine End-to-End-IP-Erreichbarkeit zu ermöglichen, wobei jedes Segment über die erforderlichen Mindestrouten verfügt.

Das Präfix 10.10.11.1/32 ist über das hierarchische BGP 100 mit angeschlossener MPC 200:200-Community bekannt. Das vom Core Area Border Router (ABR) empfangene 16020-BGP 3107-Label und das LDP-Label 22 werden nach der nächsten Hop-rekursiven Suche zur domäneninternen Weiterleitung hinzugefügt.

```
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-Knotenausgänge

Das Präfix **10.10.11.1 ist über Intra-Domain IGP (ISIS-L2)** und gemäß der MPLS-Weiterleitungstabelle **bekannt**. Er ist über LDP LSP erreichbar.

```
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.
```

Für die Verteilung der Präfixe zwischen den segmentierten Bereichen wird BGP mit dem Label (RFC 3107) verwendet. Die Loopbacks der PEs und Adressen im Zusammenhang mit der zentralen Infrastruktur müssen sich weiterhin in den segmentierten Bereichen des IGP befinden.

Die BGP-Router, die verschiedene Bereiche miteinander verbinden, sind die ABRs, die als BGP-Routen-Reflektor fungieren. Diese Geräte verwenden die Next-Hop-Self-Funktion, um zu verhindern, dass alle Next-Hops des vollständigen autonomen Systems im IGP gespeichert werden müssen, anstatt nur die IP-Adressen der PEs und der zentralen Infrastruktur. Die Loop-Erkennung wird basierend auf den BGP-Cluster-IDs abgeschlossen.

Für die Ausfallsicherheit des Netzwerks sollte BGP PIC mit der BGP Add Path-Funktion mit BGP und LFA mit IGP verwendet werden. Diese Features werden im vorherigen Beispiel nicht verwendet.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Nahtlose MPLS-Architektur
- Cisco Unified MPLS-Whitepaper
- Cisco Carrier Packet Transport (CPT)-System
- Technischer Support und Dokumentation - Cisco Systems