BGP dynamische segmentrouting van verkeer begrijpen

Inhoud

Inleiding

Dit document beschrijft hoe de BGP Dynamic Segment Routing Traffic Engineering (SR-TE)-functie in Cisco IOS® XR moet worden begrepen, geconfigureerd en geverifieerd.

Voorwaarden

Er zijn geen voorwaarden voor dit document.

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS XR en Cisco IOS XE.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

SR-TE biedt de mogelijkheden om verkeer door een SR-enabled kern te sturen zonder staatsvorming en onderhoud (stateless). Een SR-TE beleid wordt uitgedrukt als een lijst met segmenten die een pad aangeeft, de zogenaamde SID-lijst (Segment ID). Geen signalering is

vereist omdat de staat in het pakket staat en de SID-lijst wordt verwerkt als een verzameling instructies door de transitrouters.

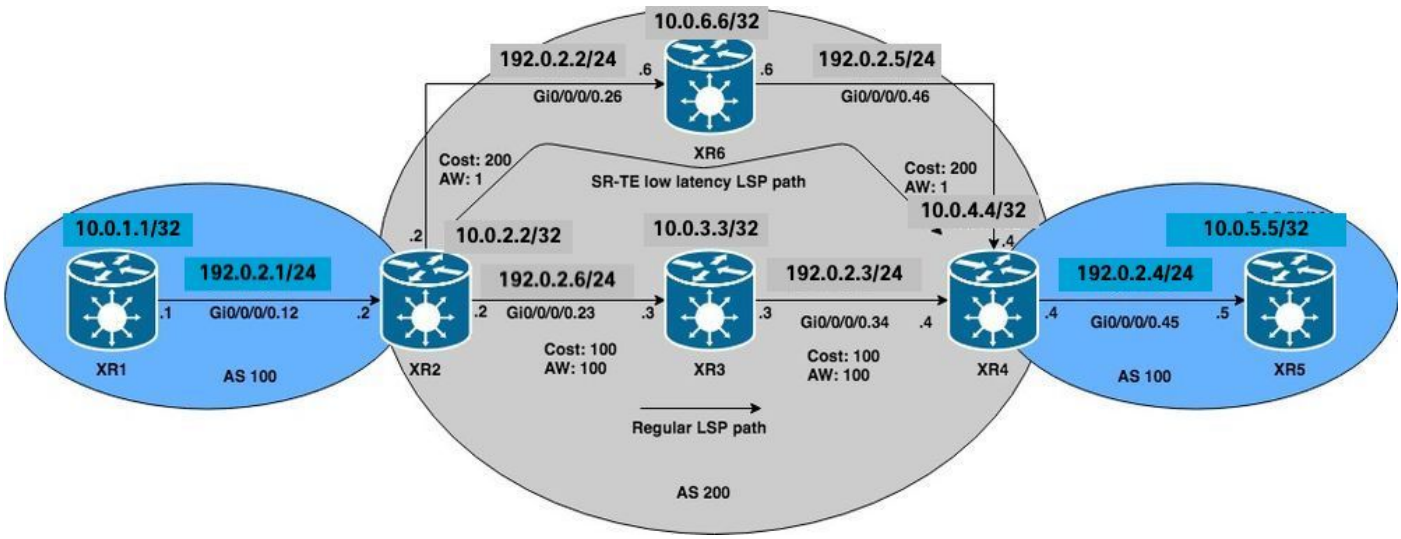
Met Dynamic Border Gateway Protocol (BGP) SR-TE kunt u automatisch SR-TE-beleid genereren op basis van willekeurige criteria zoals gemeenschappen die zijn gesignaleerd door een router die deelneemt aan een netwerk voor segmentrouting. Om te kunnen voldoen aan de Service Level Assurance (SLA's) van de toepassingen van de site en om paden te berekenen op basis van specifieke vereisten, kunt u automatisch SR-TE-beleid genereren voor een bepaalde IP-subnetverbinding of -services door gemeenschappen in te stellen en dit beleid te activeren.

> **Opmerking**: matching van andere criteria dan gemeenschappen wordt ook ondersteund om dynamisch SR-TE-beleid te maken.

Een veel gebruikte toepassing voor deze functie is in MPLS L3VPN-omgevingen, waar de netwerkbeheerder automatisch SR-TE-tunnelbeleid kan activeren om verkeer te routeren op basis van specifieke beperkingen (vertraging, bandbreedte, enzovoort). Voor de demonstraties in dit document maken we een L3VPN-service voor het verbinden van XR1 en XR5 en starten we automatisch tunnels op XR2 (head-end) gebaseerd op een bepaalde community ingesteld op XR4 (tail end) op MP-BGP.

Configureren

Netwerkdiagram



Eerste configuraties

L3VPN, Segment Routing en SR-TE basisconfiguraties zijn ingeschakeld.

XR1

```
hostname XR1
logging console debugging
interface Loopback0
 ipv4 address 10.0.1.1 255.255.255.255
!
interface GigabitEthernet0/0/0/0.12
 ipv4 address 192.0.2.1 255.255.255.0
```

```
 encapsulation dot1q 12
!
route-policy PASS
  pass
end-policy
!
router bgp 100
 bgp router-id 10.0.1.1
 address-family ipv4 unicast
  network 10.0.1.1/32
 !
 neighbor 192.0.2.7
  remote-as 200
  address-family ipv4 unicast
   route-policy PASS in
   route-policy PASS out
  !
 !
!
end
```

XR2

```
hostname XR2 logging console debugging vrf BLUE address-family ipv4 unicast import route-target
1:1 ! export route-target 1:1 ! ! ! interface Loopback0 ipv4 address 10.0.2.2 255.255.255.255 !
interface GigabitEthernet0/0/0/0.12 vrf BLUE ipv4 address 192.0.2.7 255.255.255.0 encapsulation
dot1q 12 ! interface GigabitEthernet0/0/0/0.23 ipv4 address 192.0.2.8 255.255.255.0
encapsulation dot1q 23 ! interface GigabitEthernet0/0/0/0.26 ipv4 address 192.0.2.9
255.255.255.0 encapsulation dot1q 26 ! route-policy PASS pass end-policy ! ! router ospf 1
segment-routing mpls segment-routing forwarding mpls segment-routing sr-prefer address-family
ipv4 area 0 mpls traffic-eng interface Loopback0 prefix-sid index 2 ! interface
GigabitEthernet0/0/0/0.23 cost 100 network point-to-point ! interface GigabitEthernet0/0/0/0.26
cost 200 network point-to-point ! ! mpls traffic-eng router-id Loopback0 ! router bgp 100 bgp
router-id 10.0.2.2 address-family vpnv4 unicast ! neighbor 10.0.4.4 remote-as 200 update-source
Loopback0 address-family vpnv4 unicast ! ! vrf BLUE rd 1:1 address-family ipv4 unicast !
neighbor 192.0.2.10 remote-as 200 address-family ipv4 unicast route-policy PASS in route-policy
PASS out as-override ! ! ! ! mpls oam ! mpls traffic-eng interface GigabitEthernet0/0/0/0.23
admin-weight 100 ! interface GigabitEthernet0/0/0/0.26 admin-weight 1 ! ! end
```

XR3

```
hostname XR3 logging console debugging interface Loopback0 ipv4 address 10.0.3.3 255.255.255.255
! ! interface GigabitEthernet0/0/0/0.23 ipv4 address 192.0.2.11 255.255.255.0 encapsulation
dot1q 23 ! interface GigabitEthernet0/0/0/0.34 ipv4 address 192.0.2.12 255.255.255.0
encapsulation dot1q 34 ! router ospf 1 segment-routing mpls segment-routing forwarding mpls
segment-routing sr-prefer address-family ipv4 area 0 mpls traffic-eng interface Loopback0
prefix-sid index 3 ! interface GigabitEthernet0/0/0/0.23 cost 100 network point-to-point !
interface GigabitEthernet0/0/0/0.34 cost 100 network point-to-point ! ! mpls traffic-eng router-
id Loopback0 ! mpls oam ! mpls traffic-eng interface GigabitEthernet0/0/0/0.23 admin-weight 100
! interface GigabitEthernet0/0/0/0.34 admin-weight 100 ! ! end
```

XR4

```
hostname XR4 logging console debugging vrf BLUE address-family ipv4 unicast import route-target
1:1 ! export route-target 1:1 ! ! ! interface Loopback0 ipv4 address 10.0.4.4 255.255.255.255 !
interface GigabitEthernet0/0/0/0.34 ipv4 address 192.0.2.13 255.255.255.0 encapsulation dot1q 34
! interface GigabitEthernet0/0/0/0.45 vrf BLUE ipv4 address 192.0.2.14 255.255.255.0
encapsulation dot1q 45 ! interface GigabitEthernet0/0/0/0.46 ipv4 address 192.0.2.15
255.255.255.0 encapsulation dot1q 46 ! route-policy PASS pass end-policy ! ! router ospf 1
segment-routing mpls segment-routing forwarding mpls segment-routing sr-prefer address-family
ipv4 area 0 mpls traffic-eng interface Loopback0 prefix-sid index 4 ! interface
GigabitEthernet0/0/0/0.34 cost 100 network point-to-point ! interface GigabitEthernet0/0/0/0.46
cost 200 network point-to-point ! ! mpls traffic-eng router-id Loopback0 ! router bgp 100 bgp
router-id 10.0.4.4 address-family vpnv4 unicast ! neighbor 10.0.2.2 remote-as 200 update-source
Loopback0 address-family vpnv4 unicast ! ! vrf BLUE rd 1:1 bgp unsafe-ebgp-policy address-family
ipv4 unicast ! neighbor 192.0.2.16 remote-as 200 address-family ipv4 unicast route-policy PASS
```

```
in route-policy PASS out as-override ! ! ! ! mpls oam ! mpls traffic-eng interface
GigabitEthernet0/0/0/0.34 admin-weight 100 ! interface GigabitEthernet0/0/0/0.46 admin-weight 1
! ! end
```

XR5

```
hostname XR5
logging console debugging
interface Loopback0
description REGULAR LSP PATH ipv4 address 10.0.5.5 255.255.255.255 ! interface Loopback1
description DELAY SENSITIVE - LOW LATENCY PATH (1:1) ipv4 address 10.0.5.55 255.255.255.255 !
interface GigabitEthernet0/0/0/0.45 ipv4 address 192.0.2.16 255.255.255.0 encapsulation dot1q 45
! route-policy PASS pass end-policy ! router bgp 100 bgp router-id 10.0.5.5 bgp unsafe-ebgp-
policy address-family ipv4 unicast network 10.0.5.5/32 network 10.0.5.55/32 ! neighbor
192.0.2.14 remote-as 200 address-family ipv4 unicast route-policy PASS in route-policy PASS out
! ! ! mpls oam ! end
```

XR6

```
hostname XR6 logging console debugging interface Loopback0 ipv4 address 10.0.6.6 255.255.255.255
! interface GigabitEthernet0/0/0/0.26 ipv4 address 192.0.2.17 255.255.255.0 encapsulation dot1q
26 ! interface GigabitEthernet0/0/0/0.46 ipv4 address 192.0.2.18 255.255.255.0 encapsulation
dot1q 46 ! router ospf 1 segment-routing mpls segment-routing forwarding mpls segment-routing
sr-prefer address-family ipv4 area 0 mpls traffic-eng interface Loopback0 prefix-sid index 6 !
interface GigabitEthernet0/0/0/0.26 cost 200 network point-to-point ! interface
GigabitEthernet0/0/0/0.46 cost 200 network point-to-point ! ! mpls traffic-eng router-id
Loopback0 ! mpls oam ! mpls traffic-eng interface GigabitEthernet0/0/0/0.26 admin-weight 1 !
interface GigabitEthernet0/0/0/0.46 admin-weight 1 ! ! end
```

XR2 en XR4 (PEs) hebben een LSP gebouwd met behulp van Segment Routing, dit kan worden geverifieerd met behulp van MPLS ping voor het corresponderende Segment Routing FEC. Voor dit scenario zijn er twee mogelijke paden om het L3VPN verkeer te transporteren van XR1 naar XR5:

Normaal LSP-pad: XR1 > XR2 > XR3 > XR4 > XR5

LSP-pad met lage latentie: XR1 > XR2 >XR6 > XR4 > XR5

Aanvankelijk wordt al het verkeer tussen XR1 en XR5 via XR3 via het reguliere LSP-pad gerouteerd vanwege lagere IGP-kosten, kunnen we zowel LSP's als connectiviteit bevestigen volgens deze versies. De kosten van IGP om XR4 van XR2 via XR3 te bereiken zijn 201 versus 401 via XR6. Hoewel het pad via XR3 een betere padmetriek heeft, moeten diensten met een lage latentie op VRF BLUE via XR6 door het pad worden geleid.

```
RP/0/0/CPU0:XR2#ping mpls ipv4 10.0.4.4/32 fec-type generic verbose

Sending 5, 100-byte MPLS Echos to 10.0.4.4/32,
      timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!      size 100, reply addr 192.0.2.13, return code 3
!      size 100, reply addr 192.0.2.13, return code 3
!      size 100, reply addr 192.0.2.13, return code 3
```

```
!      size 100, reply addr 192.0.2.13, return code 3
!      size 100, reply addr 192.0.2.13, return code 3

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
```

> Opmerking: bij het gebruik van de toepassing ping MPLS in Segment Routing moeten we Nil-FEC of generieke FEC gebruiken.

Als u de L3VPN-services op XR1 verifieert, kunt u de bereikbaarheid voor XR5 loopback 10.0.5.5/32 en 10.0.5.55/32 respectievelijk via het reguliere LSP-pad bevestigen. Basis L3VPN-services zijn ingeschakeld in de SR MPLS-kern.

```
RP/0/0/CPU0:XR1#ping 10.0.5.5 source 10.0.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.5.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/9 ms

RP/0/0/CPU0:XR1#ping 10.0.5.55 source 10.0.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.5.55, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/9 ms


RP/0/0/CPU0:XR1#traceroute 10.0.5.5 source 10.0.1.1

Type escape sequence to abort.
Tracing the route to 10.0.5.5

 1  192.0.2.7 9 msec  0 msec  0 msec
 2  192.0.2.11 [MPLS: Labels 16004/24002 Exp 0] 0 msec  0 msec  0 msec
 3  192.0.2.13 [MPLS: Label 24002 Exp 0] 0 msec  0 msec  0 msec
 4  192.0.2.16 0 msec  *  0 msec

RP/0/0/CPU0:XR1#traceroute 10.0.5.55 source 10.0.1.1

Type escape sequence to abort.
Tracing the route to 10.0.5.55

 1  192.0.2.7 9 msec  0 msec  0 msec
 2  192.0.2.11 [MPLS: Labels 16004/24005 Exp 0] 0 msec  0 msec  0 msec
 3  192.0.2.13 [MPLS: Label 24005 Exp 0] 0 msec  0 msec  0 msec
 4  192.0.2.16 0 msec  *  0 msec
```

Zoals opgemerkt, gaat al verkeer op VRF BLAUW door de reguliere LSP weg XR1 > XR2 > XR3 > XR4 > XR5.

BGP dynamische SR-TE configureren

Stel bij dit voorbeeld XR4 (staartuiteinde) in om gemeenschap 1:1 in te voegen en naar XR2 te sturen om een SR-TE-beleid voor prefix 10.0.5.55/32 op VRF BLUE aan te geven. SR-TE beleidspadselectie wordt ingesteld om de pad met lage latentie te nemen in plaats van de reguliere LSP; dit doet u door de laagste TE metriek (Admin-gewicht) te selecteren via XR6. De totale TE-metriek (admin-gewicht) via XR6 is 2, omdat de admin-gewichten zijn ingesteld op 1 bij uitgaande interfaces naar XR4 (staartuiteinde) via XR6, zoals te zien is in het referentietopologiediagram en de initiële configuraties.

Om het dynamische SR-TE beleid te creëren, moeten we configureren welke loopback zal worden gebruikt als bron en wat de dynamische tunnelbereik is dat de head-end zal gebruiken om de tunnels te genereren. Deze configuratie is vereist aan de head-end van het SR-TE beleid XR2. Stel het tunnelbereik in op een minimum van 500 en een maximum van 500, effectief het creëren van één SR-TE tunnel en de bron loopback naar loopback 0 aan de head-end voor de tunnel.

XR2

```
ipv4 unnumbered mpls traffic-eng Loopback0
mpls traffic-eng
 auto-tunnel p2p
  tunnel-id min 500 max 500
 !
!
end
```

Op XR4, plaats de gemeenschap 1:1 en pas het op het VRF BLAUWE prefix 10.0.5.55/32 toe, zal dit het toestaan om de gemeenschap in de BGP update op te nemen.

XR4

```
route-policy COMMUNITY_1:1
  # 1:1 Community
  if destination in (10.0.5.55/32) then
    set community (1:1)
  endif
  pass
end-policy
!
router bgp 100
 vrf BLUE
 !
  neighbor 192.0.2.16
  address-family ipv4 unicast
    route-policy COMMUNITY_1:1 in
 !
!
end
```

Bij het verifiëren van XR2 (head-end) kunnen we zien dat de community 1:1 is ingesteld op de VPNv4 updates die van XR4 zijn ontvangen.

```
RP/0/0/CPU0:XR2#show bgp vrf BLUE 10.0.5.55/32 detail
BGP routing table entry for 10.0.5.55/32, Route Distinguisher: 1:1 Versions: Process bRIB/RIB
SendTblVer Speaker 36 36 Flags: 0x00043001+0x00000200; Last Modified: Nov 23 17:50:59.798 for
00:02:53 Paths: (1 available, best #1) Advertised to CE peers (in unique update groups):
192.0.2.10 Path #1: Received by speaker 0 Flags: 0x4000000085060005, import: 0x9f Advertised to
CE peers (in unique update groups): 192.0.2.10 200 10.0.4.4 (metric 201) from 10.0.4.4
(10.0.4.4) Received Label 24005 Origin IGP, metric 0, localpref 100, valid, internal, best,
group-best, import-candidate, imported Received Path ID 0, Local Path ID 0, version 36
Community: 1:1
      Extended community: RT:1:1
      Source AFI: VPNv4 Unicast, Source VRF: BLUE, Source Route Distinguisher: 1:1
```

Op XR2 (head-end) moet u een RPL-routebeleid maken dat overeenkomt met de gemeenschap 1:1 en de bijbehorende attribuutset instellen voor MPLS traffic engineering. Nadat het beleid is ingesteld, kunnen we naar de configuratie MPLS-TE gaan en de bijbehorende attribuut-set voor het SR-TE beleid instellen en aangeven wat de padselectiecriteria zijn, die in dit geval Segment Routing en TE metriek zijn omdat we via XR6 het pad willen kiezen via het laagste administratieve

gewicht.

```
XR2
route-policy DYN_BGP_SR-TE
  # Matches community 1:1
  if community matches-every (1:1) then
    set mpls traffic-eng attributeset DYN_SR-TE_POLICIES
  endif
  pass
end-policy
!
router bgp 100
!
 neighbor 10.0.4.4
 address-family vpnv4 unicast
   route-policy DYN_BGP_SR-TE in
  !
mpls traffic-eng
 attribute-set p2p-te DYN_SR-TE_POLICIES
  path-selection
   metric te
   segment-routing adjacency unprotected
  !
end
```

Verifiëren

Zodra voltooid, kunt u opmerken dat tunnel-te 500 interface dynamisch is gemaakt voor het gespecificeerde bereik.

```
RP/0/0/CPU0:XR2#show mpls traffic-eng tunnels segment-routing tabular

           Tunnel   LSP     Destination          Source    Tun    FRR  LSP  Path
             Name    ID         Address         Address  State  State Role  Prot
----------------- ----- --------------- --------------- ------ ------ ---- -----
    ^tunnel-te500     2         10.0.4.4         10.0.2.2     up  Inact Head Inact
^ = automatically created P2P/P2MP tunnel
```

BGP RIB geeft aan dat het beleid "DYN_SR-TE_POLICY" aan het prefix is gekoppeld, wat betekent dat het verkeer volgens het beleid moet worden gerouteerd.

```
RP/0/0/CPU0:XR2#show bgp vrf BLUE

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf BLUE)
*> 10.0.1.1/32         192.0.2.10                0             0 200 i
*>i10.0.5.5/32         10.0.4.4                  0    100      0 200 i
*>i10.0.5.55/32        10.0.4.4 T:DYN_SR-TE_POLICIES
                                                 0    100      0 200 i
```

Als we de BGP RIB voor het prefix 10.0.5.55/32 in detail verifiëren kunnen we de informatie van het besturingsplane zien waarnaar zal worden verwezen om de SR-TE tunnel te genereren.

```
RP/0/0/CPU0:XR2#show bgp vrf BLUE 10.0.5.55/32 detail

BGP routing table entry for 10.0.5.55/32, Route Distinguisher: 1:1
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                39          39
    Flags: 0x00041001+0x00000200;
Last Modified: Nov 23 17:55:22.798 for 00:04:43
Paths: (1 available, best #1)
  Advertised to CE peers (in unique update groups):
    192.0.2.10
  Path #1: Received by speaker 0
  Flags: 0x4000000085060005, import: 0x9f
  Advertised to CE peers (in unique update groups):
    192.0.2.10
  200
    10.0.4.4 T:DYN_SR-TE_POLICIES (metric 201) from 10.0.4.4 (10.0.4.4)
      Received Label 24005
      Origin IGP, metric 0, localpref 100, valid, internal, best, group-best, import-candidate,
imported
      Received Path ID 0, Local Path ID 0, version 39
      Community: 1:1
      Extended community: RT:1:1
      TE tunnel attribute-set DYN_SR-TE_POLICIES, up, registered, binding-label 24000, if-handle
0x00000130

      Source AFI: VPNv4 Unicast, Source VRF: BLUE, Source Route Distinguisher: 1:1
```

We zien dat het tunnelbeleid staat en geregistreerd is. De toegewezen bindende SID is 24000, deze bindende SID kan worden gebruikt om te verifiëren welke tunnel voor dit bepaalde prefix wordt gebruikt. Zoals eerder opgemerkt, werd tunnel-te500 in het LFIB gecreëerd en geïnstalleerd.

```
RP/0/0/CPU0:XR2#show mpls forwarding labels 24000 detail
Local Outgoing Prefix Outgoing Next Hop Bytes Label Label or ID Interface Switched ------ ------
----- ----------------- ------------ --------------- ------------ 24000  Pop         No ID
tt500        point2point     0
     Updated: Nov 23 17:55:23.267
     Label Stack (Top -> Bottom): { }
     MAC/Encaps: 0/0, MTU: 0
     Packets Switched: 0
```

> Opmerking: Binding SID heeft veel gebruikscases, voor dit specifieke document beperkt het gebruik ervan voor lokale verificatie, maar de toepassing is veel breder.

U kunt ook de gegeven if-handle 0x00000130 van de BGP RIB-uitvoer gebruiken om het SR-TE-beleid te controleren dat is toegewezen aan prefix 10.0.5.55/32.

```
RP/0/0/CPU0:XR2#show mpls forwarding tunnels ifh 0x00000130 detail
Tunnel Outgoing Outgoing Next Hop Bytes Name Label Interface Switched ------------- -----------
------------ -------------- ------------ tt500        (SR) 24003       Gi0/0/0/0.26 192.0.2.17
0
     Updated: Nov 23 17:55:23.267
     Version: 138, Priority: 2
     Label Stack (Top -> Bottom): { 24003 }
     NHID: 0x0, Encap-ID: N/A, Path idx: 0, Backup path idx: 0, Weight: 0
     MAC/Encaps: 18/22, MTU: 1500
     Packets Switched: 0
```

```
  Interface Name: tunnel-te500, Interface Handle: 0x00000130, Local Label: 24001
  Forwarding Class: 0, Weight: 0
  Packets/Bytes Switched: 0/0
```

SR-TE beleid op XR2 (head-end) zal deze eigenschappen hebben vanuit een besturingsplane en dataplane perspectief om voorwaarts verkeer te sturen. Ook staat informatie van de SR-TE tunnel kan worden gezien als per uitvoer, die moet overeenkomen met eerdere verificaties.

```
RP/0/0/CPU0:XR2#show mpls traffic-eng tunnels segment-routing p2p 500

Name: tunnel-te500  Destination: 10.0.4.4  Ifhandle:0x130 (auto-tunnel for BGP default)
  Signalled-Name: auto_XR2_t500
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10, (Segment-Routing) type dynamic  (Basis for Setup, path weight 2)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Fri Nov 23 17:55:23 2018 (00:09:01 ago)
  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0x0
    Metric Type: TE (interface)
    Path Selection:
      Tiebreaker: Min-fill (default)
      Protection: Unprotected Adjacency
    Hop-limit: disabled
    Cost-limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forward class: 0 (default)
    Forwarding-Adjacency: disabled
    Autoroute Destinations: 0
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Path Protection: Not Enabled
    Attribute-set: DYN_SR-TE_POLICIES (type p2p-te)
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    SRLG discovery: Disabled
  History:
    Tunnel has been up for: 00:09:01 (since Fri Nov 23 17:55:23 UTC 2018)
    Current LSP:
      Uptime: 00:09:01 (since Fri Nov 23 17:55:23 UTC 2018)
    Reopt. LSP:
      Last Failure:
        LSP not signalled, identical to the [CURRENT] LSP
        Date/Time: Fri Nov 23 17:56:53 UTC 2018 [00:07:31 ago]

  Segment-Routing Path Info (OSPF 1 area 0)
    Segment0[Link]: 192.0.2.9 - 192.0.2.17, Label: 24005
    Segment1[Link]: 192.0.2.18 - 192.0.2.15, Label: 24003
Displayed 1 (of 1) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

Controleer het prefix direct op VRF BLUE RIB, we kunnen bevestigen dat de binding SID 24000 is toegewezen aan het prefix.

```
RP/0/0/CPU0:XR2#show route vrf BLUE 10.0.5.55/32 detail
```

```
Routing entry for 10.0.5.55/32
  Known via "bgp 100", distance 200, metric 0
  Tag 200, type internal
  Installed Nov 23 17:55:23.267 for 00:10:38
  Routing Descriptor Blocks
    10.0.4.4, from 10.0.4.4
      Nexthop in Vrf: "default", Table: "default", IPv4 Unicast, Table Id: 0xe0000000
      Route metric is 0
      Label: 0x5dc5 (24005)
      Tunnel ID: None
      Binding Label: 0x5dc0 (24000)
      Extended communities count: 0
      Source RD attributes: 0x0000:1:1
      NHID:0x0(Ref:0)
  Route version is 0x5 (5)
  No local label
  IP Precedence: Not Set
  QoS Group ID: Not Set
  Flow-tag: Not Set
  Fwd-class: Not Set
  Route Priority: RIB_PRIORITY_RECURSIVE (12) SVD Type RIB_SVD_TYPE_REMOTE
  Download Priority 3, Download Version 27
  No advertising protos.
```

FIB voor VRF BLUE geeft aan dat doorsturen voor dit prefix gebeurt via tunnel-te 500 volgens ons BGP dynamisch SR-TE beleid.

```
RP/0/0/CPU0:XR2#show cef vrf BLUE 10.0.5.55/32 detail
10.0.5.55/32, version 27, internal 0x1000001 0x0 (ptr 0xa142a574) [1], 0x0 (0x0), 0x208
(0xa159d208) Updated Nov 23 17:55:23.287 Prefix Len 32, traffic index 0, precedence n/a,
priority 3 gateway array (0xa129f23c) reference count 1, flags 0x4038, source rib (7), 0 backups
[1 type 1 flags 0x48441 (0xa15b780c) ext 0x0 (0x0)] LW-LDI[type=0, refc=0, ptr=0x0, sh-ldi=0x0]
gateway array update type-time 1 Nov 23 17:55:23.287 LDI Update time Nov 23 17:55:23.287 via
local-label 24000, 3 dependencies, recursive [flags 0x6000]     path-idx 0 NHID 0x0 [0xa1605bf4
0x0]
    recursion-via-label
    next hop VRF - 'default', table - 0xe0000000
    next hop via 24000/0/21
     next hop tt500        labels imposed {ImplNull 24005}


    Load distribution: 0 (refcount 1)

    Hash  OK  Interface                 Address
    0     Y   Unknown                   24000/0
```

Op XR1 kunnen we de connectiviteit verifiëren en bevestigen dat het verkeer door tunnel-te 500 via lage latency pad via XR6 gaat.

```
RP/0/0/CPU0:XR1#traceroute 10.0.5.55 source 10.0.1.1

Type escape sequence to abort.
Tracing the route to 10.0.5.55

 1  192.0.2.7 0 msec  0 msec  0 msec
 2  192.0.2.17 [MPLS: Labels 24003/24005 Exp 0] 0 msec  0 msec  0 msec
 3  192.0.2.15 [MPLS: Label 24005 Exp 0] 0 msec  0 msec  0 msec
 4  192.0.2.16 0 msec  *  9 msec
```

XR2 tellers verhogen voor de tunnel-te500 die overeenkomt met ons SR-TE beleid.

```
RP/0/0/CPU0:XR2#show mpls forwarding tunnels

Tunnel        Outgoing    Outgoing     Next Hop        Bytes
Name          Label       Interface                    Switched
------------- ----------- ------------ --------------- ------------
tt500        (SR) 24003       Gi0/0/0/0.26 192.0.2.17        2250
```

Het pad voor prefix 10.0.5.5/32 gaat nog steeds door het reguliere LSP-pad via XR3 zoals hieronder te zien is.

```
RP/0/0/CPU0:XR1#traceroute 10.0.5.5 source 10.0.1.1

Type escape sequence to abort.
Tracing the route to 10.0.5.5

 1  192.0.2.7 0 msec  0 msec  0 msec
 2  192.0.2.11 [MPLS: Labels 16004/24002 Exp 0] 0 msec  0 msec  0 msec
 3  192.0.2.13 [MPLS: Label 24002 Exp 0] 0 msec  0 msec  0 msec
 4  192.0.2.16 0 msec  *  0 msec
```

Problemen oplossen

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

Samenvatting

BGP Dynamic SR-TE biedt granulariteit en het automatisch afdwingen van routeringsbeleid voor de doeleinden van traffic engineering in de SR-enabled core. Automatische tunnelcreatie kan worden geactiveerd op basis van willekeurige criteria, die netwerkbeheerders in staat kunnen stellen om eenvoudig verkeerspatronen te creëren die voldoen aan de toepassingsvereisten van de site.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.