

BGP Dynamic Segment Routing 트래픽 엔지니어링 이해

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[초기 컨피그레이션](#)

[BGP 동적 SR-TE 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[요약](#)

소개

이 문서에서는 Cisco IOS[®] XR에서 BGP SR-TE(Dynamic Segment Routing Traffic Engineering) 기능을 이해, 구성 및 확인하는 방법에 대해 설명합니다.

사전 요구 사항

이 문서에 대한 필수 구성 요소가 없습니다.

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS XR 및 Cisco IOS XE를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SR-TE는 상태 생성 및 유지 관리(상태 비저장) 없이 SR 지원 코어를 통해 트래픽을 전달하는 기능을 제공합니다. SR-TE 정책은 SID(Segment ID) 목록이라는 경로를 지정하는 세그먼트 목록으로 표시됩니다. 상태가 패킷에 있고 SID 목록이 트랜짓 라우터에 의해 명령 집합으로 처리되므로 시그널링은 필요하지 않습니다.

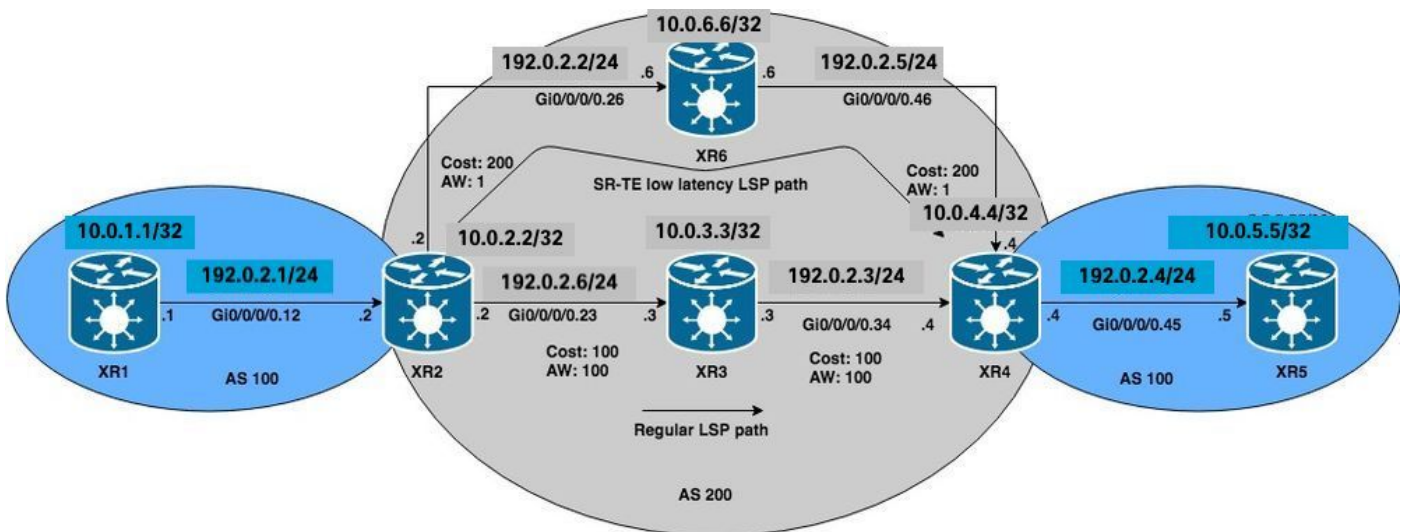
BGP(Dynamic Border Gateway Protocol) SR-TE를 사용하면 세그먼트 라우팅 네트워크에 참여하는 라우터에서 신호를 보낸 커뮤니티 등의 임의 기준을 기반으로 자동 SR-TE 정책을 생성할 수 있습니다. 특정 요구 사항에 따라 사이트 애플리케이션 및 컴퓨팅 경로의 SLA(서비스 수준 보증)를 충족하려면 커뮤니티를 설정하고 이러한 정책을 트리거하여 지정된 IP 서브넷 또는 서비스에 대한 자동 SR-TE 정책을 생성할 수 있습니다.

참고: 동적 SR-TE 정책을 생성하기 위해 커뮤니티 이외의 일치 기준도 지원됩니다.

이 기능에 대한 일반적인 애플리케이션은 MPLS L3VPN 환경에 있습니다. 네트워크 관리자는 특정 제약 조건(지연, 대역폭 등)을 기반으로 트래픽을 라우팅하도록 자동 SR-TE 터널 정책을 트리거할 수 있습니다. 이 문서의 데모에서는 MP-BGP의 XR4(tail end)에 설정된 특정 커뮤니티를 기반으로 XR1과 XR5를 연결하는 L3VPN 서비스를 생성하고 XR2(headend)에서 자동 터널을 트리거합니다.

구성

네트워크 다이어그램



초기 컨피그레이션

L3VPN, 세그먼트 라우팅 및 SR-TE 기본 구성이 활성화되었습니다.

```

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 및 XR4(PE)는 Segment Routing을 사용하여 LSP를 구축했으며, 이는 해당 Segment Routing FEC에 대해 MPLS ping을 사용하여 확인할 수 있습니다. 이 시나리오에서는 XR1에서 XR5로 L3VPN 트래픽을 전송하는 가능한 두 가지 경로가 있습니다.

일반 LSP 경로: XR1 > XR2 > XR3 > XR4 > XR5

지연 시간이 짧은 LSP 경로: XR1 > XR2 > XR6 > XR4 > XR5

처음에는 IGP 비용이 낮기 때문에 XR1과 XR5 간의 모든 트래픽이 일반 LSP 경로를 통해 XR3를 통해 라우팅되므로, LSP와 연결을 모두 확인해도 됩니다. XR3를 통해 XR2에서 XR4로 이동하는 IGP 비용은 XR6를 통해 401인 것에 비해 201입니다. XR3를 통한 경로가 더 나은 경로 메트릭을 가지고 있더라도 VRF BLUE의 짧은 대기 시간 서비스는 XR6를 통한 경로를 통해 라우팅되어야 합니다.

```
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
```

참고: 세그먼트 라우팅에서 ping MPLS 애플리케이션을 사용할 때는 Nil-FEC 또는 일반 FEC를 사용해야 합니다.

XR1에서 L3VPN 서비스를 확인하는 경우, 일반 LSP 경로를 통해 각각 XR5 루프백 10.0.5.5/32 및 10.0.5.55/32에 연결할 수 있는지 확인할 수 있습니다. 기본 L3VPN 서비스는 SR MPLS 코어에서 활성화됩니다.

```
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
```

관찰한 대로 VRF BLUE의 모든 트래픽은 일반 LSP 경로 XR1 > XR2 > XR3 > XR4 > XR5를 통과합니다.

BGP 동적 SR-TE 구성

이 예에서는 XR4(tail end)를 구성하여 community 1:1을 삽입하고 이를 XR2로 전송하여 VRF BLUE에서 접두사 10.0.5.55/32에 대한 SR-TE 정책을 생성함을 알립니다. SR-TE 정책 경로 선택은 일반 LSP가 아닌 저지연 경로를 사용하도록 설정됩니다. XR6을 통해 가장 낮은 TE 메트릭(Admin Weight)을 선택하여 이렇게 하십시오. 참조 토폴로지 다이어그램 및 초기 컨피그레이션에 표시된 대로 XR6을 통해 XR4(테일 엔드)로 향하는 발신 인터페이스에서 관리자 가중치가 1로 설정되었으므로 XR6을 통한 총 TE 메트릭(관리자 가중치)은 2입니다.

동적 SR-TE 정책을 생성하려면 소스로 사용할 루프백과 헤드엔드에서 터널을 생성하는 데 사용할 동적 터널 범위를 구성해야 합니다. 이 구성은 SR-TE 정책 XR2의 헤드엔드에서 필요합니다. 터널 범위를 최소 500에서 최대 500으로 설정하여 터널의 헤드엔드에서 단일 SR-TE 터널을 생성하고 소스 루프백에서 루프백 0을 생성합니다.

```

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

```

XR4에서 커뮤니티를 1:1로 설정하고 VRF BLUE 접두사 10.0.5.55/32에 적용하면 BGP 업데이트에 커뮤니티를 삽입할 수 있습니다.

```

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

```

XR2 확인(headend) XR4에서 수신한 VPNv4 업데이트에 커뮤니티 1:1이 설정되어 있음을 확인할 수 있습니다.

```

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

```

XR2(headend)에서 커뮤니티 1:1과 일치하는 RPL 경로 정책을 생성하고 MPLS 트래픽 엔지니어링에 대한 해당 특성 집합을 설정합니다. 정책이 설정되면 MPLS-TE 컨피그레이션 표준으로 이동하여 SR-TE 정책에 해당하는 특성 집합을 설정하고 경로 선택 기준이 무엇인지 나타낼 수 있습니다. 이 경우 XR6를 통해 가장 낮은 관리 가중치를 통해 경로를 선택하려고 하므로 세그먼트 라우팅 및 TE 메트릭입니다.

```

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

```

다음을 확인합니다.

완료되면 tunnel-te 500 인터페이스가 지정된 범위에 대해 동적으로 생성되었음을 확인할 수 있습니다.

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

Tunnel Name	LSP ID	Destination Address	Source Address	Tun State	FRR State	LSP Role	Path Prot
^tunnel-te500	2	10.0.4.4	10.0.2.2	up	Inact	Head	Inact

^ = automatically created P2P/P2MP tunnel

BGP RIB는 "DYN_SR-TE_POLICIES" 정책이 접두사에 연결되어 있음을 나타냅니다. 즉, 트래픽은 정책에 따라 라우팅되어야 합니다.

```
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

```

접두사 10.0.5.55/32에 대한 BGP RIB를 자세히 확인하면 SR-TE 터널을 생성하는 데 참조될 컨트롤 플레인 정보를 확인할 수 있습니다.

```
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

```

터널 정책이 **up** 상태이고 **등록된** 것을 확인할 수 있습니다. 할당된 바인딩 SID가 24000, 이 바인딩 SID를 사용하여 이 특정 접두사에 어떤 터널이 사용되는지 확인할 수 있습니다. 앞에서 관찰한 대로 tunnel-te500이 생성되어 LFIB에 설치되었습니다.

```

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

```

참고: 이 특정 문서의 경우 SID 바인딩에는 여러 사용 사례가 있지만, 로컬 확인에 사용되는 범위가 훨씬 넓습니다.

또는 BGP RIB 출력에서 **지정된 if-handle 0x00000130**를 사용하여 접두사 10.0.5.55/32에 대해 할당된 SR-TE 정책을 확인할 수 있습니다.

```

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

```

XR2(headend)의 SR-TE 정책에는 트래픽을 포워딩하기 위해 컨트롤 플레인 및 데이터 플레인 관점에서 이러한 속성이 포함됩니다. 또한 SR-TE 터널의 상태 정보를 출력별로 볼 수 있으며, 이는 이전 검증과 일치해야 합니다.

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)

BFDDetection: 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

VRF BLUE RIB에서 접두사를 직접 확인합니다. 바인딩 SID 번호가 24000에 할당되었는지 확인할 수 있습니다.

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.

```

VRF BLUE용 FIB는 BGP 동적 SR-TE 정책에 따라 터널 테(tunnel-te) 500을 통해 이 접두사에 대한 포워딩이 수행됨을 나타냅니다.

```

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

XR1에서는 연결을 확인하고 트래픽이 XR6를 통해 짧은 대기 시간 경로를 통해 tunnel-te 500을 통과하는지 확인할 수 있습니다.

```
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

```

SR-TE 정책에 해당하는 tunnel-te500에 대해 XR2 카운터가 증가합니다.

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

Tunnel Name	Outgoing Label	Outgoing Interface	Next Hop	Bytes Switched
-------------	----------------	--------------------	----------	----------------

tt500 (SR) 24003 Gi0/0/0/0.26 192.0.2.17 2250

접두사 10.0.5.5/32에 대한 경로는 아래 그림과 같이 XR3를 통해 일반 LSP 경로를 통해 계속 전달됩니다.

```
RP/0/0/CPU0:XR1#tracert 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
```

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

요약

BGP Dynamic SR-TE는 SR 지원 코어에서 트래픽 엔지니어링을 위해 라우팅 정책을 세분화하고 자동으로 적용합니다. 자동 터널 생성은 임의의 기준에 따라 트리거될 수 있으며, 이를 통해 네트워크 관리자는 사이트의 애플리케이션 요구 사항에 부합하는 트래픽 패턴을 쉽게 생성할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.