BGPダイナミックセグメントルーティングトラフィックエンジニアリングについて

内容

概要

このドキュメントでは、Cisco IOS® XRのBGPダイナミックセグメントルーティングトラフィックエンジニアリング(SR-TE)機能を理解、設定、および確認する方法について説明します。

前提条件

このドキュメントには前提条件はありません。

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS XR および Cisco IOS XE に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

SR-TE には、ステートを作成および維持せずに（ステートレス）、SR 対応のコアを介してトラフィックをステアリングする機能があります。SR-TE ポリシーは、セグメント ID（SID）リストと呼ばれるパスを指定するセグメントリストとして表されます。ステートはパケット内にあり、

SID リストは中継ルータによって一連の命令として処理されるため、シグナリングは必要ありません。

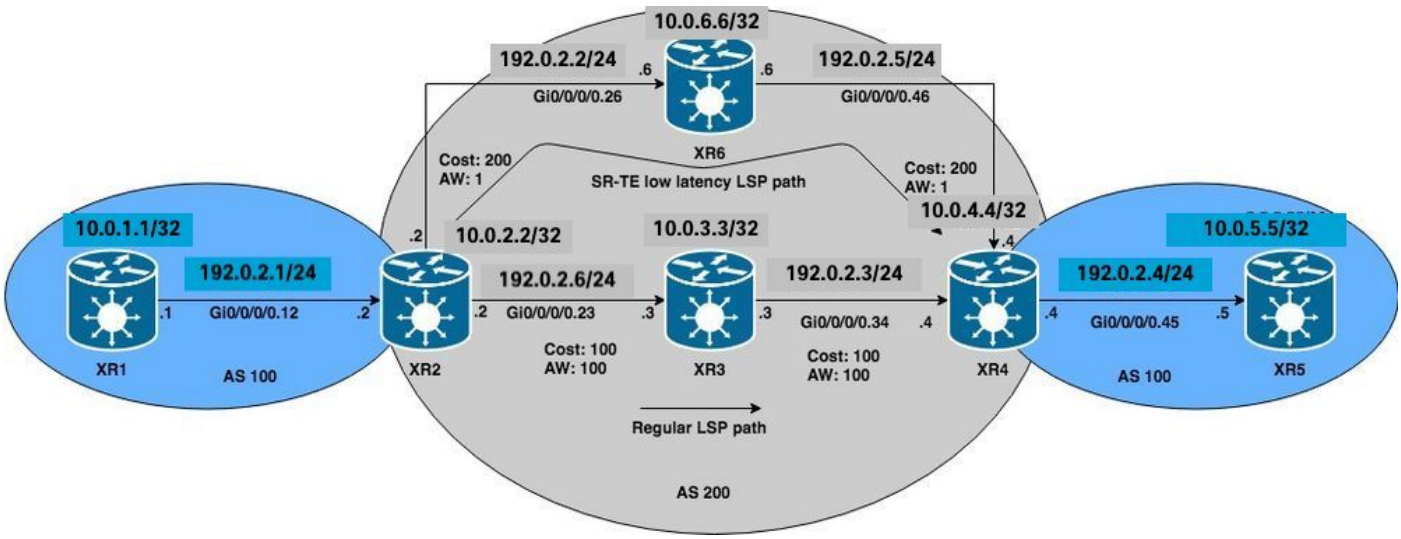
Dynamic Border Gateway Protocol（BGP；ダイナミックボーダーゲートウェイプロトコル）SR-TEを使用すると、セグメントルーティングネットワークに参加しているルータによってシグナリングされたコミュニティなど、任意の基準に基づいて自動SR-TEポリシーを生成できます。特定の要件に基づいてサイトのアプリケーションとコンピューティングパスのサービスレベル保証(SLA)を満たすことができるように、コミュニティを設定し、ポリシーをトリガーすることによって、特定のIPサブネットまたはサービスに対して自動SR-TEポリシーを生成できます。

> **注**：動的なSR-TEポリシーを作成するために、コミュニティ以外の一致基準もサポートされています。

この機能がよく適用されるのは、 MPLS L3VPN 環境です。MPLS L3VPN 環境では、ネットワーク管理者が自動 SR-TE トンネルポリシーをトリガーして、特定の制約（遅延、帯域幅など）に基づきトラフィックをルーティングできます。このドキュメントのデモでは、XR1とXR5を接続するL3VPNサービスを作成し、MP-BGPのXR4（テールエンド）に設定された特定のコミュニティに基づいて、XR2（ヘッドエンド）で自動トンネルをトリガーします。

設定

ネットワーク図



初期設定

L3VPN、セグメントルーティング、および SR-TE の基本設定が有効になっています。

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 および XR4 (PE) は、セグメントルーティングを使用して LSP を構築しています。これは、対応するセグメントルーティング FEC に対して MPLS ping を使用することで確認できます。このシナリオには、XR1 から XR5 に L3VPN トラフィックを転送できるパスが次のように 2 つあります。

通常のLSPパス：XR1 > XR2 > XR3 > XR4 > XR5

低遅延LSPパス：XR1 > XR2 >XR6 > XR4 > XR5

最初は、IGPコストが低いため、XR1とXR5の間のすべてのトラフィックは通常のLSPパスを介してXR3を経由します。次の各設定に従って、LSPと接続の両方を確認できます。XR2からXR3経由でXR4に到達するためのIGPコストは、XR6経由の401に対して201です。XR3経由のパスのパスメトリックは優れていますが、VRF BLUE上の低遅延サービスはXR6経由のパスを介してルーティングする必要があります。

```
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
```

> **注**：セグメントルーティングでping MPLSアプリケーションを使用する場合は、Nil-FECまたは汎用FECを使用する必要があります。

XR1でL3VPNサービスを確認すると、通常のLSPパスを介して、XR5ループバック10.0.5.5/32および10.0.5.55/32への到達可能性をそれぞれ確認できます。基本的な L3VPN サービスが SR MPLS コアで有効です。

```
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
```

以上のように、VRF BLUE 上のすべてのトラフィックは、通常の LSP パスである XR1 > XR2 > XR3 > XR4 > XR5 を経由します。

BGP ダイナミック SR-TE の設定

この例では、コミュニティ1:1を挿入するようにXR4（テールエンド）を設定し、それをXR2に送信して、VRF BLUE上のプレフィクス10.0.5.55/32に対するSR-TEポリシーの作成を通知します。SR-TEポリシーパスの選択は、通常のLSPではなく低遅延パスを使用するように設定されます。これを行うには、XR6経由で最小のTEメトリック(Admin Weight)を選択します。参照トポロジ図と初期設定に示されているように、XR6経由のXR4（テールエンド）に向かう発信インターフェイスでadmin weightsが1に設定されているため、XR6経由の合計TEメトリック(admin weight)は2です。

ダイナミックSR-TEポリシーを作成するには、どのループバックを送信元として使用し、ヘッドエンドがトンネルを生成するために使用するダイナミックトンネル範囲を設定する必要があります。この設定は、SR-TEポリシーXR2のヘッドエンドで必要です。トンネル範囲を500以上500以下に設定すると、1つのSR-TEトンネルと、トンネルのヘッドエンドでループバック0が作成できます。

XR2

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

XR4で、コミュニティを1:1に設定し、VRF BLUEプレフィクス10.0.5.55/32に適用します。これにより、BGPアップデートにコミュニティを挿入できます。

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（ヘッドエンド）を確認すると、XR4 から受信した VPNv4 アップデートでコミュニティが 1:1 に設定されていることがわかります。

```
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（ヘッドエンド）で、コミュニティ1:1に一致するRPLルートポリシーを作成し、MPLSトラフィックエンジニアリング用の対応するアトリビュートセットを設定します。ポリシーを設定したら、MPLS-TE 設定スタンザに移動し、SR-TE ポリシーの該当の属性セットを設定し、パスの選択基準にセグメントルーティングと TE メトリックを指定します。XR6 を介した、管理上の重みが最小のパスを選択したいためです。

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
```

確認

完了したら、tunnel-te 500 インターフェイスが指定された範囲で動的に作成されたことを確認できます。

```
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 の RIB は、「DYN_SR-TE_POLICIES」ポリシーがプレフィックスにアタッチされていることを示しています。つまり、トラフィックはポリシーに従ってルーティングされる必要があります。

```
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
```

プレフィックス 10.0.5.55/32 の BGP RIB を詳しく確認すると、SR-TE トンネルを生成するために参照されるコントロールプレーン情報を確認できます。

```
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
```

トンネルポリシーが**アップ**状態で、**登録済み**であることがわかります。割り当てられたバインド SID は 24000 です。このバインド SID を使用して、この特定のプレフィックスに使用されているトンネルを確認できます。前述のとおり、tunnel-te500 は LFIB に作成され、インストールされています。

```
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
```

> **注**：バインディングSIDには多くのユースケースがあります。この特定のドキュメントでは、ローカル検証での使用を制限しますが、そのアプリケーションの方がはるかに広範です。

または、BGP RIBの出力から与えられた**if-handle 0x00000130** を使用して、プレフィクス 10.0.5.55/32に割り当てられたSR-TEポリシーを確認できます。

```
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（ヘッドエンド）のSR-TEポリシーには、トラフィックを転送するためのコントロールプレーンとデータプレーンの観点からのこれらのプロパティがあります。また、SR-TEトンネルの状態情報は出力ごとに表示され、以前の検証と一致している必要があります。

```
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
```

VRF BLUE RIBでプレフィックスを直接確認すると、バインディングSID 24000がプレフィックスに割り当てられていることを確認できます。

```
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 BLUEのFIBは、このプレフィクスの転送がBGPダイナミックSR-TEポリシーに従って tunnel-te 500経由で行われることを示しています。

```
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
```

XR1 では、接続を確認し、トラフィックが XR6 を介した低遅延パス経由の tunnel-te 500 を通過していることを確認できます。

```
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 ポリシーに対応する tunnel-te500 の XR2 カウンタが増加しています。

```
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
```

プレフィックス10.0.5.5/32のパスは、次に示すように、XR3経由の通常のLSPパスを経由します。

```
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
```

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

要約

BGP ダイナミック SR-TE では、SR 対応のコアでのトラフィック エンジニアリングのために、ルーティングポリシーの粒度と自動適用が提供されます。トンネルの自動作成は任意の条件に基づいてトリガーできます。これにより、ネットワーク管理者はサイトのアプリケーション要件を満たすトラフィックパターンを簡単に作成できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。