Entender a engenharia de tráfego de roteamento de segmento dinâmico BGP

Contents

Introduction

Este documento descreve como entender, configurar e verificar o recurso de Engenharia de Tráfego de Roteamento de Segmento Dinâmico (SR-TE - Dynamic Segment Routing Traffic Engineering) do BGP no Cisco IOS® XR.

Prerequisites

Não há pré-requisitos para este documento.

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco IOS XR e no Cisco IOS XE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O SR-TE fornece os recursos para orientar o tráfego através de um núcleo habilitado para SR sem criação e manutenção de estado (sem estado). Uma política SR-TE é expressa como uma lista de segmentos que especifica um caminho, chamada lista de ID de segmento (SID).

Nenhuma sinalização é necessária, pois o estado está no pacote e a lista SID é processada como um conjunto de instruções pelos roteadores de trânsito.

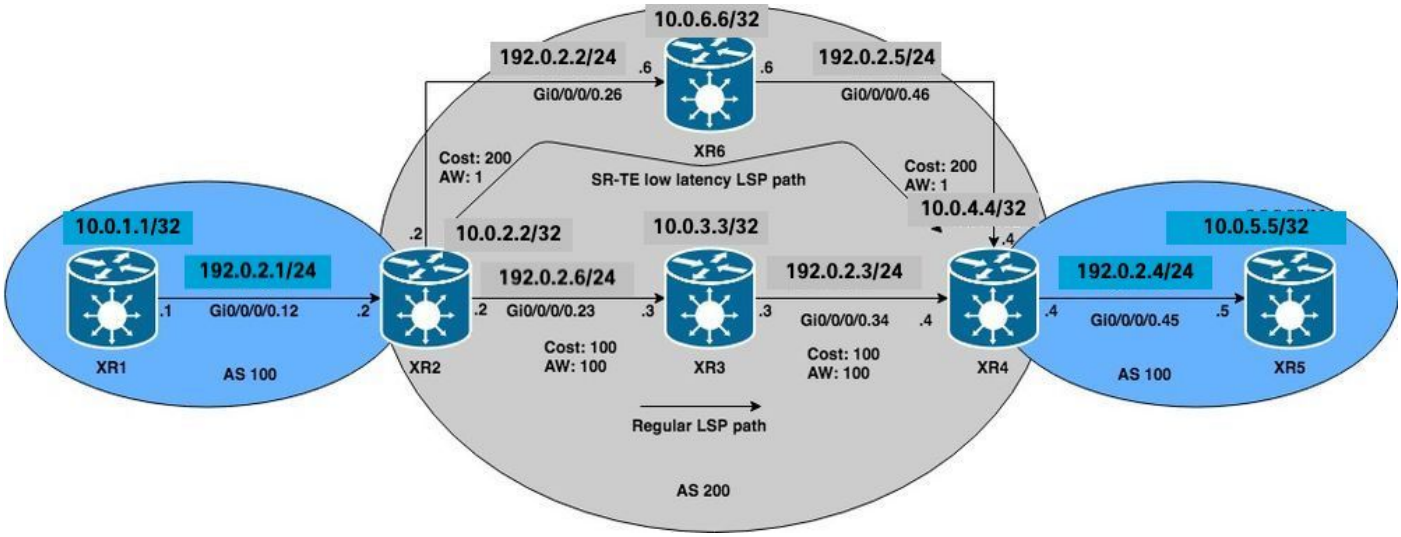
Com o protocolo de gateway de borda dinâmico (BGP - Dynamic Border Gateway Protocol) SR-TE, você pode gerar políticas SR-TE automáticas com base em critérios arbitrários, como comunidades sinalizadas por um roteador que participa de uma rede de roteamento de segmento. Para poder atender à garantia de nível de serviço (SLAs) dos aplicativos e caminhos de computação do site com base em requisitos específicos, você pode gerar políticas SR-TE automáticas para uma determinada sub-rede IP ou serviços definindo comunidades e acionando essas políticas .

> **Observação**: critérios de correspondência diferentes de comunidades também são suportados para criar políticas SR-TE dinâmicas.

Um aplicativo comum para esse recurso está em ambientes MPLS L3VPN, onde o administrador de rede pode acionar políticas de túnel SR-TE automáticas para rotear o tráfego com base em restrições específicas (atraso, largura de banda e assim por diante). Para as demonstrações neste documento, criamos um serviço L3VPN conectando XR1 e XR5 e acionamos túneis automáticos em XR2 (headend) com base em uma comunidade específica definida em XR4 (tail end) em MP-BGP.

Configurar

Diagrama de Rede



Configurações iniciais

Configurações básicas de L3VPN, roteamento de segmento e SR-TE foram habilitadas.

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 e XR4 (PEs) criaram um LSP usando o roteamento de segmento. Isso pode ser verificado usando-se o ping MPLS para o FEC de roteamento de segmento correspondente. Para esse cenário, há dois caminhos possíveis para transportar o tráfego L3VPN de XR1 para XR5:

Caminho LSP regular: XR1 > XR2 > XR3 > XR4 > XR5

Caminho LSP de baixa latência: XR1 > XR2 >XR6 > XR4 > XR5

Inicialmente, todo o tráfego entre XR1 e XR5 é roteado através de XR3 através do caminho LSP regular devido ao custo IGP mais baixo, podemos confirmar tanto LSPs quanto conectividade conforme essas verificações. O custo do IGP para acessar XR4 de XR2 via XR3 é de 201 versus 401 via XR6. Mesmo que o caminho via XR3 tenha uma métrica de caminho melhor, os serviços de baixa latência no VRF BLUE devem ser roteados pelo caminho via XR6.

```
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
```

> Observação: ao usar o aplicativo ping MPLS no roteamento de segmento, devemos usar Nil-FEC ou FEC genérico.

Se você verificar os serviços L3VPN em XR1, poderá confirmar a acessibilidade para o loopback XR5 10.0.5.5/32 e 10.0.5.55/32, respectivamente, através do caminho LSP regular. Os serviços L3VPN básicos são ativados no núcleo SR MPLS.

```
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
```

Como observado, todo o tráfego no VRF BLUE passa pelo caminho LSP regular XR1 > XR2 > XR3 > XR4 > XR5.

Configurar BGP Dynamic SR-TE

Para este exemplo, configure o XR4 (extremidade traseira) para inserir a comunidade 1:1 e enviá-la ao XR2 para sinalizar a criação de uma política SR-TE para o prefixo 10.0.5.55/32 em AZUL VRF. A seleção do caminho de política SR-TE será definida para seguir o caminho de baixa latência em vez do LSP normal. Para isso, selecione a métrica TE mais baixa (peso administrativo) via XR6. A métrica TE total (peso administrativo) via XR6 é 2, pois os pesos administrativos foram definidos como 1 nas interfaces de saída em direção a XR4 (extremidade traseira) via XR6, conforme visto no diagrama de topologia de referência e nas configurações

iniciais.

Para criar as políticas SR-TE dinâmicas, precisamos configurar qual loopback será usado como origem e qual é o intervalo de túnel dinâmico que o headend usará para gerar os túneis. Essa configuração é necessária no headend da política SR-TE XR2. defina o intervalo de túnel para um mínimo de 500 e um máximo de 500, criando efetivamente um único túnel SR-TE e o loopback de origem para loopback 0 no headend para o túnel.

```
XR2
ipv4 unnumbered mpls traffic-eng Loopback0
mpls traffic-eng
 auto-tunnel p2p
  tunnel-id min 500 max 500
 !
!
end
```

Em XR4, defina a comunidade 1:1 e aplique-a no prefixo AZUL VRF 10.0.5.55/32, isso permitirá que ela insira a comunidade na atualização BGP.

```
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
```

Verificando XR2 (headend) podemos ver que ele tem a comunidade 1:1 definida nas atualizações de VPNv4 recebidas de XR4.

```
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
```

Em XR2 (headend), crie uma política de rota RPL que corresponda à comunidade 1:1 e defina o atributo correspondente definido para engenharia de tráfego MPLS. Depois que a política é definida, podemos ir para a estrofe de configuração MPLS-TE e definir o conjunto de atributos

correspondente para a política SR-TE e indicar quais são os critérios de seleção de caminho, que são o roteamento de segmento e a métrica TE nesse caso, já que queremos escolher o caminho por meio do menor peso administrativo via XR6.

```
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
```

Verificar

Uma vez concluída, você pode observar que a interface túnel-te 500 foi criada dinamicamente para o intervalo especificado.

```
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
```

O BGP RIB indica que a política "DYN_SR-TE_POLICIES" está anexada ao prefixo, o que significa que o tráfego deve ser roteado de acordo com a política.

```
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
```

Se verificarmos o BGP RIB para o prefixo 10.0.5.55/32 em detalhes, podemos ver as informações do plano de controle que serão referenciadas para gerar o túnel SR-TE.

```
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
```

Podemos ver que a política de túnel está no estado **ativo** e **registrada**. O SID de vinculação atribuído é 24000; esse SID de vinculação pode ser usado para verificar qual túnel é usado para esse prefixo específico. Como observado anteriormente, o tunnel-te500 foi criado e instalado no LFIB.

```
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
```

> **Observação**: o SID de vinculação tem muitos casos de uso, para este documento específico, limita seu uso para verificação local, mas sua aplicação é muito mais ampla.

Como alternativa, você pode usar o **if-handle 0x00000130** da saída RIB BGP para verificar a política SR-TE atribuída ao prefixo 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
```

A política SR-TE em XR2 (headend) terá essas propriedades de uma perspectiva do plano de controle e do plano de dados para encaminhar o tráfego. As informações de estado do túnel SR-TE também podem ser vistas como por saída, que deve corresponder às verificações anteriores.

```
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
```

Verifique o prefixo diretamente no RIB AZUL VRF, podemos confirmar que o 24000 SID de

vinculação foi atribuído ao prefixo.

```
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 para VRF BLUE indica que o encaminhamento para esse prefixo é feito através do túnel-te 500 de acordo com nossa política SR-TE dinâmica de BGP.

```
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
```

Em XR1, podemos verificar a conectividade e confirmar se o tráfego está passando pelo túnel-te 500 através de caminho de baixa latência via XR6.

```
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
```

Os contadores XR2 aumentam para o túnel-te500, que corresponde à nossa política SR-TE.

```
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
```

O caminho para o prefixo 10.0.5.5/32 ainda está passando pelo caminho LSP regular através de XR3, como visto abaixo.

```
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
```

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Summary

O BGP Dynamic SR-TE oferece granularidade e aplicação automática de políticas de roteamento com a finalidade de engenharia de tráfego no núcleo habilitado para SR. A criação automática de túneis pode ser acionada com base em critérios arbitrários, o que pode permitir que os administradores de rede criem facilmente padrões de tráfego que atendam aos requisitos de aplicativos do local.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.