

Kenntnis der Datenverkehrsplanung für dynamische BGP-Segment-Routing

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Startkonfigurationen](#)

[Konfigurieren von dynamischem BGP-SR-TE](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zusammenfassung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die BGP Dynamic Segment Routing Traffic Engineering (SR-TE)-Funktion in Cisco IOS® XR verstehen, konfigurieren und überprüfen können.

Voraussetzungen

Für dieses Dokument bestehen keine Voraussetzungen.

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco IOS XR und Cisco IOS XE.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

SR-TE bietet die Möglichkeit, den Datenverkehr über einen SR-fähigen Kern ohne Staterstellung und -verwaltung (stateless) zu steuern. Eine SR-TE-Richtlinie wird als eine Liste von Segmenten ausgedrückt, die einen Pfad angibt, der als Segment ID (SID)-Liste bezeichnet

wird. Es ist keine Signalisierung erforderlich, da sich der Status im Paket befindet und die SID-Liste von den Transit-Routern als Befehlssatz verarbeitet wird.

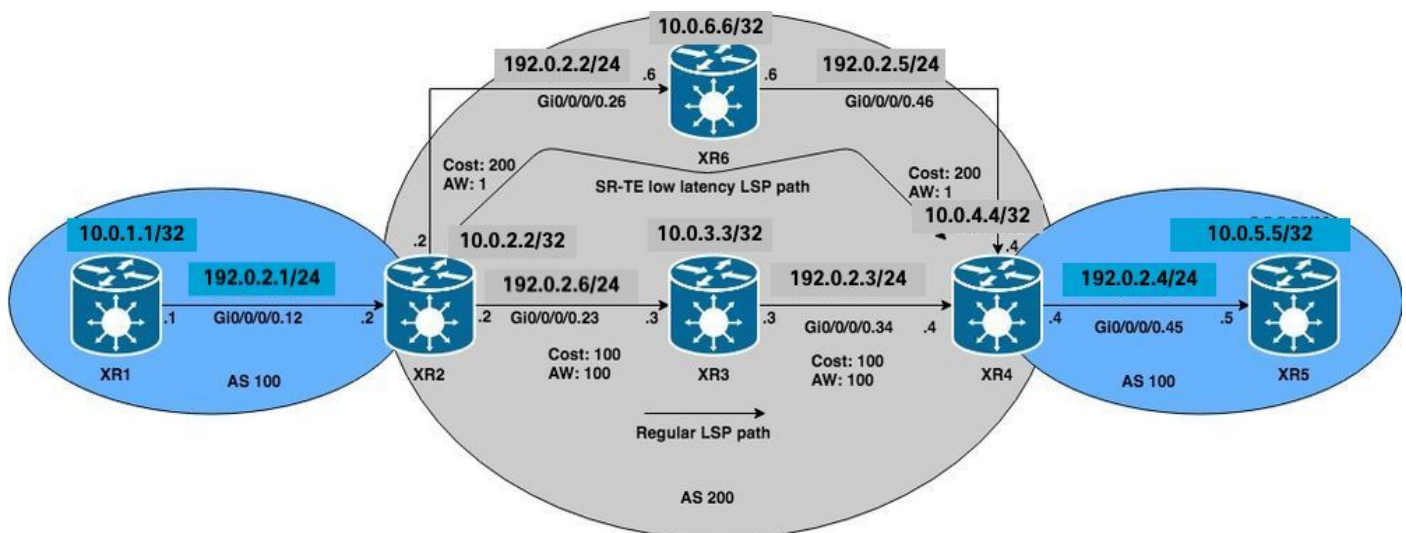
Mit dem Dynamic Border Gateway Protocol (BGP) SR-TE können Sie automatische SR-TE-Richtlinien erstellen, die auf beliebigen Kriterien basieren, z. B. Communities, die von einem Router signalisiert werden, der an einem Segment Routing-Netzwerk teilnimmt. Um die Service Level Assurance (SLAs) für die Anwendungen und Computing-Pfade des Standorts auf der Grundlage spezifischer Anforderungen erfüllen zu können, können Sie automatische SR-TE-Richtlinien für ein bestimmtes IP-Subnetz oder bestimmte IP-Services erstellen, indem Sie Communities einrichten und diese Richtlinien auslösen.

Hinweis: Zur Erstellung dynamischer SR-TE-Richtlinien werden auch andere Anpassungskriterien als Communities unterstützt.

Eine häufige Anwendung dieser Funktion ist in MPLS-L3VPN-Umgebungen, in denen der Netzwerkadministrator automatische SR-TE-Tunnelrichtlinien auslösen kann, um den Datenverkehr auf der Grundlage bestimmter Einschränkungen (Verzögerung, Bandbreite usw.) weiterzuleiten. Für die Demonstrationen in diesem Dokument erstellen wir einen L3VPN-Service, der XR1 und XR5 verbindet und Auto-Tunnel auf XR2 (Headend) basierend auf einer bestimmten Community auf XR4 (Tail-End) auf MP-BGP auslöst.

Konfigurieren

Netzwerkdiagramm



Startkonfigurationen

L3VPN, Segment Routing und SR-TE wurden als Basiskonfigurationen aktiviert.

```
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 und XR4 (PEs) haben einen LSP mit Segment Routing erstellt. Dies kann mithilfe von MPLS Ping für den entsprechenden Segment Routing FEC überprüft werden. Für dieses Szenario gibt es zwei mögliche Pfade, um den L3VPN-Verkehr von XR1 nach XR5 zu transportieren:

Regulärer LSP-Pfad: XR1 > XR2 > **XR3** > XR4 > XR5

LSP-Pfad mit niedriger Latenz: XR1 > XR2 > **XR6** > XR4 > XR5

Anfänglich wird der gesamte Datenverkehr zwischen XR1 und XR5 aufgrund der niedrigeren IGP-Kosten über den regulären LSP-Pfad durch XR3 geroutet. Wir können sowohl LSPs als auch die Konnektivität gemäß diesen Anforderungen bestätigen. Die IGP-Kosten für die Verbindung mit XR4 vom XR2 über XR3 betragen 201 gegenüber 401 über XR6. Obwohl der Pfad über XR3 eine bessere Pfadmetrik aufweist, müssen Dienste mit niedriger Latenz in VRF BLAU über XR6 über den Pfad geleitet werden.

```
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

Hinweis: Wenn Sie die MPLS-Anwendung für das Segment-Routing mit Ping verwenden, müssen Sie Nil-FEC oder generische FEC verwenden.

Wenn Sie die L3VPN-Dienste auf dem XR1 überprüfen, können Sie die Erreichbarkeit des XR5-Loopbacks 10.0.5.5/32 bzw. 10.0.5.55/32 über den regulären LSP-Pfad bestätigen. Grundlegende L3VPN-Dienste sind im SR MPLS-Core aktiviert.

```
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
```

Wie festgestellt, durchläuft der gesamte Datenverkehr auf VRF BLAU den regulären LSP-Pfad XR1 > XR2 > XR3 > XR4 > XR5.

Konfigurieren von dynamischem BGP-SR-TE

Konfigurieren Sie in diesem Beispiel XR4 (Tail-End) so, dass die Community 1:1 eingefügt und an XR2 gesendet wird, um die Erstellung einer SR-TE-Richtlinie für das Präfix 10.0.5.55/32 auf VRF BLAU zu signalisieren. Die SR-TE-Richtlinienpfadauswahl wird so festgelegt, dass sie den Pfad mit niedriger Latenz anstelle des regulären LSP verwendet. Wählen Sie dazu die niedrigste TE-Metrik (Admin Weight) über XR6 aus. Die gesamte TE-Metrik (Admin-Gewichtung) über XR6 beträgt 2, da Admin-Gewichtungen für ausgehende Schnittstellen zu XR4 (Tail-End) über XR6 auf

1 festgelegt wurden (siehe Referenztopologie-Diagramm und Erstkonfigurationen).

Um die dynamischen SR-TE-Richtlinien zu erstellen, müssen wir konfigurieren, welches Loopback als Quelle verwendet wird und welchen dynamischen Tunnelbereich das Headend zum Generieren der Tunnel verwendet. Diese Konfiguration ist am Headend der SR-TE-Richtlinie XR2 erforderlich. Setzen Sie den Tunnelbereich auf mindestens 500 und maximal 500, und erstellen Sie effektiv einen einzelnen SR-TE-Tunnel und den Quell-Loopback zu Loopback. opback 0 am Headend für den Tunnel.

XR2

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

Legen Sie auf XR4 für die Community 1:1 fest, und wenden Sie sie auf das VRF BLAU-Präfix 10.0.5.55/32 an, damit die Community in das BGP-Update eingefügt werden kann.

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
  !
!
```

Beim Überprüfen von XR2 (Headend) wird auf die von XR4 empfangenen VPNv4-Updates Community 1:1 festgelegt.

```
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
```

Erstellen Sie auf dem XR2 (Headend) eine RPL-Routenrichtlinie, die der Community 1:1 entspricht, und legen Sie den entsprechenden Attributsatz für das MPLS-Traffic-Engineering fest.

Nachdem die Richtlinie festgelegt wurde, können wir den MPLS-TE-Konfigurationsstanza aufrufen und den entsprechenden Attributsatz für die SR-TE-Richtlinie festlegen und die Pfadauswahlkriterien angeben. In diesem Fall sind dies Segment-Routing und TE-Metrik, da wir den Pfad über die niedrigste administrative Gewichtung per XR6 auswählen möchten.

```

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

```

Überprüfung

Nach Abschluss des Vorgangs können Sie beobachten, dass die Schnittstelle tunnel-te 500 für den angegebenen Bereich dynamisch erstellt wurde.

```
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 RIB gibt an, dass die Richtlinie "DYN_SR-TE_POLICIES" mit dem Präfix verknüpft ist, was bedeutet, dass der Datenverkehr entsprechend der Richtlinie geroutet werden muss.

```
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

```

Wenn wir die BGP-RIB für das Präfix 10.0.5.55/32 im Detail überprüfen, werden die Informationen der Kontrollebene angezeigt, auf die verwiesen wird, um den SR-TE-Tunnel zu generieren.

```
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
```

Die Tunnelrichtlinie ist **aktiv** und **registriert**. Die zugewiesene Bindungs-SID ist 24000. Mithilfe dieser Bindungs-SID kann überprüft werden, welcher Tunnel für dieses Präfix verwendet wird. Wie bereits erwähnt, wurde tunnel-te500 erstellt und im LFIB installiert.

```
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
```

Hinweis: Binding SID kann in vielen Fällen verwendet werden. In diesem Dokument ist die Verwendung für die lokale Überprüfung eingeschränkt, die Anwendung ist jedoch viel breiter.

Alternativ können Sie die angegebene **if-handle 0x00000130** aus der BGP RIB-Ausgabe verwenden, um die SR-TE-Richtlinie zu überprüfen, die dem Präfix 10.0.5.55/32 zugewiesen ist.

```
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

Die SR-TE-Richtlinie auf dem XR2 (Headend) verfügt über diese Eigenschaften für die Weiterleitung von Datenverkehr aus Sicht einer Kontroll- und Datenebene. Die Statusinformationen des SR-TE-Tunnels können ebenfalls als Ausgabe betrachtet werden, die mit vorherigen Überprüfungen übereinstimmen muss.

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

Überprüfen Sie das Präfix direkt auf der VRF BLUE RIB. Wir können bestätigen, dass die bindende SID 24000 dem Präfix zugewiesen wurde.

```
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 für VRF BLAU gibt an, dass die Weiterleitung für dieses Präfix über tunnel-te 500 gemäß unserer dynamischen BGP-SR-TE-Richtlinie erfolgt.

```
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

Auf dem XR1 können wir die Konnektivität prüfen und bestätigen, dass der Datenverkehr über den Tunnel-te 500 über den XR6-Pfad mit niedriger Latenz geleitet wird.

```
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

```

Die XR2-Zähler erhöhen sich für den tunnel-te500, was unserer SR-TE-Richtlinie entspricht.

```
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

Der Pfad für das Präfix 10.0.5.5/32 durchläuft weiterhin den regulären LSP-Pfad über XR3 (siehe unten).

```
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

```

Fehlerbehebung

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

Zusammenfassung

BGP Dynamic SR-TE bietet eine präzise Steuerung und automatische Durchsetzung von Routing-Richtlinien für Traffic Engineering im SR-fähigen Core. Die automatische Tunnelerstellung kann anhand beliebiger Kriterien ausgelöst werden, sodass Netzwerkadministratoren problemlos Datenverkehrsmuster erstellen können, die die Anwendungsanforderungen des Standorts erfüllen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.