Why set tloc-action in a Centralized Control Policy Does Not Work?

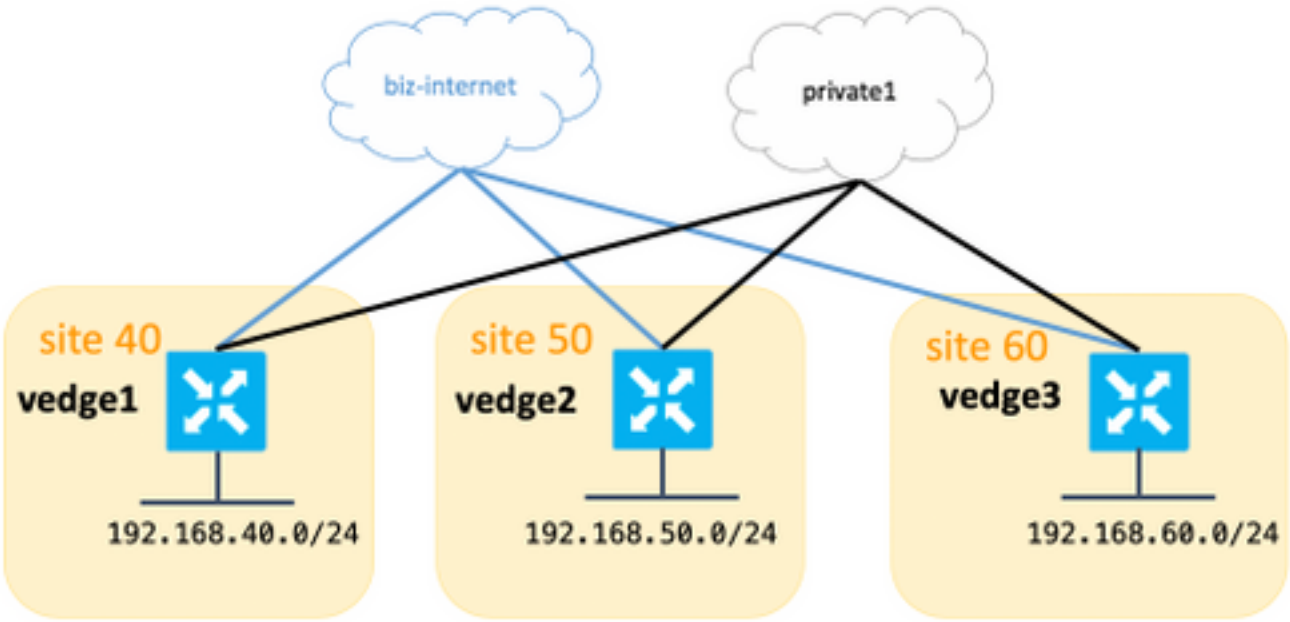
Contents

Introduction

This document describes the problem that occurs with Overlay Management Protocol (OMP) routes if the **set tloc-action** command in centralized control policy is used and explains the reason why it happens and how to solve it.

Topology

In order to understand the problem better, refer to this simple topology diagram that depicts the setup:



Configuration

For the purpose of this article, vEdge and the Controllers Software version 18.3.5 was used.

All sites have connection to **biz-internet** and **private** colors, this table summarizes the

configuration.

hostname	site-id	system-ip	ip-address on biz-internet link	ip-address on private1 link
vEdge1	40	192.168.30.104	192.168.109.181	192.168.110.181
vEdge2	50	192.168.30.105	192.168.109.182	192.168.110.182
vEdge3	60	192.168.30.106	192.168.109.183	192.168.110.183
vSmart	1	192.168.30.103		

There are no special configurations on vEdges. Configuration with two default routes is pretty simple and omitted here for brevity.

On vSmart, this configuration was applied:

```
 lists
  vpn-list VPN_40
   vpn 40
  !
  site-list sites_40_60
   site-id 40
   site-id 60
  !
  prefix-list SITE_40
   ip-prefix 192.168.40.0/24
  !
  prefix-list SITE_60
   ip-prefix 192.168.60.0/24
  !
 !
control-policy REDIRECT_VIA_VEDGE2
  sequence 10
   match route
    prefix-list SITE_40
   !
   action accept
    set
     tloc-action primary
```

```
     tloc 192.168.30.105 color biz-internet encap ipsec
    !
   !
  !
  sequence 20
   match route
    prefix-list SITE_60
   !
   action accept
    set
     tloc-action primary
     tloc 192.168.30.105 color biz-internet encap ipsec
    !
   !
  !
  default-action accept
 !
apply-policy
 site-list sites_40_60
  control-policy REDIRECT_VIA_VEDGE2 out
 !
!
```

The main goal of this policy is to redirect traffic from site 40 to site 60 via intermediate destination site 50 and use **biz-internet** preferably.

Problem

From the **show omp routes** output, you see that routes via **biz-internet** can not be installed on vEdge1, vEdge3 and status is set to Invalid and unresolved (**Inv,U**):

```
vedge1# show omp routes | b PATH
                                          PATH                      ATTRIBUTE
VPN    PREFIX              FROM PEER      ID     LABEL    STATUS    TYPE       TLOC IP
COLOR            ENCAP  PREFERENCE
-----------------------------------------------------------------------------------------------
--------------------------------------
40     192.168.40.0/24     0.0.0.0        68     1002     C,Red,R   installed  192.168.30.104
biz-internet     ipsec  -
                           0.0.0.0        81     1002     C,Red,R   installed  192.168.30.104
private1         ipsec  -
40     192.168.50.0/24     192.168.30.103 4      1002     C,I,R     installed  192.168.30.105
biz-internet     ipsec  -
                           192.168.30.103 10     1002     C,I,R     installed  192.168.30.105
private1         ipsec  -
40 192.168.60.0/24 192.168.30.103 8 1002 Inv,U installed 192.168.30.105 biz-internet ipsec -
192.168.30.103 9 1002 C,I,R installed 192.168.30.106 biz-internet ipsec -

vedge3# show omp routes | b PATH
                                          PATH                      ATTRIBUTE
VPN    PREFIX              FROM PEER      ID     LABEL    STATUS    TYPE       TLOC IP
COLOR            ENCAP  PREFERENCE
-----------------------------------------------------------------------------------------------
--------------------------------------
40 192.168.40.0/24 192.168.30.103 19 1002 Inv,U installed 192.168.30.105 biz-internet ipsec -
192.168.30.103 20 1002 C,I,R installed 192.168.30.104 biz-internet ipsec - 40 192.168.50.0/24
192.168.30.103 16 1002 C,I,R installed 192.168.30.105 biz-internet ipsec - 192.168.30.103 21
1002 C,I,R installed 192.168.30.105 private1 ipsec - 40 192.168.60.0/24 0.0.0.0 68 1002 C,Red,R
installed 192.168.30.106 biz-internet ipsec - 0.0.0.0 81 1002 C,Red,R installed 192.168.30.106
```

```
private1 ipsec -
```

At the same time, you see data plane tunnels on **biz-internet** up and running between vEdge1 and vEdge3:

```
vedge1# show bfd sessions
                                       SOURCE TLOC      REMOTE TLOC
DST PUBLIC                        DST PUBLIC         DETECT      TX
SYSTEM IP        SITE ID  STATE       COLOR            COLOR            SOURCE IP
IP                                PORT        ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME
TRANSITIONS
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
-------------
192.168.30.105   50       up          biz-internet     biz-internet     192.168.109.181
192.168.109.182                   12366       ipsec  7           1000           0:02:52:22      0
192.168.30.105   50       up          private1         private1         192.168.110.181
192.168.110.182                   12366       ipsec  7           1000           0:00:00:12      1
192.168.30.106   60       up          biz-internet     biz-internet     192.168.109.181
192.168.109.183                   12366       ipsec  7           1000           0:02:52:22      0
192.168.30.106   60       up          private1         private1         192.168.110.181
192.168.110.183                   12366       ipsec  7           1000           0:00:56:28      0


vedge3# show bfd sessions
                                       SOURCE TLOC      REMOTE TLOC
DST PUBLIC                        DST PUBLIC         DETECT      TX
SYSTEM IP        SITE ID  STATE       COLOR            COLOR            SOURCE IP
IP                                PORT        ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME
TRANSITIONS
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
-------------
192.168.30.104   40       up          biz-internet     biz-internet     192.168.109.183
192.168.109.181                   12366       ipsec  7           1000           0:02:54:25      0
192.168.30.104   40       up          private1         private1         192.168.110.183
192.168.110.181                   12366       ipsec  7           1000           0:00:58:30      0
192.168.30.105   50       up          biz-internet     biz-internet     192.168.109.183
192.168.109.182                   12366       ipsec  7           1000           0:02:54:25      0
192.168.30.105   50       up          private1         private1         192.168.110.183
192.168.110.182                   12366       ipsec  7           1000           0:00:57:26      0
```

In the **show omp route** detailed output, you see the **tloc** set properly and also the **untimate-tloc** is set, but status is **Inv,U** and loss reason is **invalid**:

```
vedge3# show omp routes 192.168.40.0/24 detail

-------------------------------------------------
omp route entries for vpn 40 route 192.168.40.0/24
-------------------------------------------------
            RECEIVED FROM:
peer            192.168.30.103
path-id         19
label 1002 status Inv,U loss-reason invalid lost-to-peer 192.168.30.103 lost-to-path-id 20
Attributes: originator 192.168.30.104 type installed tloc 192.168.30.105, biz-internet, ipsec
ultimate-tloc 192.168.30.104, biz-internet, ipsec -- primary domain-id not set overlay-id 1
site-id 40 preference not set tag not set origin-proto connected origin-metric 0 as-path not set
unknown-attr-len not set RECEIVED FROM: peer 192.168.30.103 path-id 20 label 1002 status C,I,R
loss-reason not set lost-to-peer not set lost-to-path-id not set Attributes: originator
192.168.30.104 type installed tloc 192.168.30.104, biz-internet, ipsec ultimate-tloc not set
```

```
domain-id not set overlay-id 1 site-id 40 preference not set tag not set origin-proto connected
origin-metric 0 as-path not set unknown-attr-len not set
```

> **Note**: An ultimate-tloc is the TLOC to which the intermediate hop builds data plane tunnel (IPsec or Generic Routing Encapsulation (GRE)) in order to get to the final destination.

> **Note: tloc-action** is only supported end-to-end if the transport color is the same from a site to the intermediate hop and from the intermediate hop to the final destination. If the transport used to get to the intermediate hop from a site is a different color than the transport used from the intermediate hop to get to the final destination, then this will cause an issue with tloc-action.

You can see that the main goal is not achieved and the traffic follows direct path as can be seen on the host from 192.168.40.0/24 subnet:

```
traceroute -n 192.168.60.20
traceroute to 192.168.60.20 (192.168.60.20), 30 hops max, 60 byte packets
 1  192.168.40.104  0.288 ms  0.314 ms  0.266 ms
 2  192.168.60.106  0.911 ms  1.045 ms  1.140 ms
 3  192.168.60.20  1.213 ms !X  1.289 ms !X  1.224 ms !X
```

Solution

As a root cause, initially it was suspected that software defect CSCvm64622 was hit, but after additional investigation, it was found that it was misconfiguration due to the fact that product documentation was not clear about **tloc-action** requirements. So, documentation section with regards to the TLOC action is updated with this:

> **Note**: If the action is **accept set tloc-action**, configure the **service TE** on the intermediate destination.

Hence, in currect scenario **service TE** configuration is required on vEdge2 in order to make centralized control policy work because you use Traffic Engineering (TE) essentially by steering via an arbitrary path:

```
vedge2(config)# vpn 40
vedge2(config-vpn-40)# service ?
Possible completions:
  FW  IDP  IDS  TE  netsvc1  netsvc2  netsvc3  netsvc4
vedge2(config-vpn-40)# service TE
vedge2(config-vpn-40)# commit
Commit complete.
```

It resolves the problem with control policy since vEdge2 starts to advertise the TE service:

```
vsmart1# show omp services | b PATH
                                                PATH
VPN     SERVICE  ORIGINATOR      FROM PEER       ID     LABEL    STATUS
-------------------------------------------------------------------------
40      VPN      192.168.30.104  192.168.30.104  68     1002     C,I,R
                                 192.168.30.104  81     1002     C,I,R
40      VPN      192.168.30.105  192.168.30.105  68     1002     C,I,R
```

```
                                192.168.30.105   81     1002     C,I,R
40     VPN      192.168.30.106  192.168.30.106   68     1002     C,I,R
                                192.168.30.106   81     1002     C,I,R
40     TE 192.168.30.105 192.168.30.105 68 1007 C,I,R 192.168.30.105 81 1007 C,I,R
```

vEdge1 and vEdge3 install the routes successfully now, note that the status is set to **C,I,R**:

```
vedge3# show omp routes 192.168.40.0/24 detail

---------------------------------------------------
omp route entries for vpn 40 route 192.168.40.0/24
---------------------------------------------------
            RECEIVED FROM:
peer            192.168.30.103
path-id      19 label 1002 status C,I,R loss-reason not set lost-to-peer not set lost-to-path-id
not set Attributes: originator 192.168.30.104 type installed tloc 192.168.30.105, biz-internet,
ipsec ultimate-tloc 192.168.30.104, biz-internet, ipsec -- primary domain-id not set overlay-id
1 site-id 40 preference not set tag not set origin-proto connected origin-metric 0 as-path not
set unknown-attr-len not set RECEIVED FROM: peer 192.168.30.103 path-id 20 label 1002 status R
loss-reason tloc-action lost-to-peer 192.168.30.103 lost-to-path-id 19 Attributes: originator
192.168.30.104 type installed tloc 192.168.30.104, biz-internet, ipsec ultimate-tloc not set
domain-id not set overlay-id 1 site-id 40 preference not set tag not set origin-proto connected
origin-metric 0 as-path not set unknown-attr-len not set vedge3# show ip routes 192.168.40.0/24
| b PROTOCOL PROTOCOL NEXTHOP NEXTHOP NEXTHOP VPN PREFIX PROTOCOL SUB TYPE IF NAME ADDR VPN TLOC
IP COLOR ENCAP STATUS ----------------------------------------------------------------------------
------------------------------------------------------------------ 40 192.168.40.0/24 omp - - -
- 192.168.30.105 biz-internet ipsec F,S
```