

排除vEdge雙向轉發檢測和資料平面連線問題

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[控制平面資訊](#)

[檢查控制本地屬性](#)

[檢查控制連線](#)

[重疊管理通訊協定](#)

[驗證是否已從vEdge通告OMP TLOC](#)

[驗證vSmart接收和通告TLOC](#)

[雙向轉發檢測](#)

[瞭解show bfd sessions命令](#)

[命令show tunnel statistics](#)

[存取清單](#)

[網路位址轉換](#)

[如何使用工具stun-client檢測NAT對映和過濾器。](#)

[CLI中使用的資料平面隧道的「傳送」支援的NAT型別](#)

[防火牆](#)

[安全性](#)

[DSCP標籤流量的ISP問題](#)

[調試BFD](#)

[相關資訊](#)

簡介

本文檔介紹控制平面連線之後的vEdge資料平面連線問題，但是站點之間沒有資料平面連線。

必要條件

需求

思科建議瞭解解決Cisco Software Defined Wide Area Network (SDWAN) 方案。

採用元件

本文件所述內容不限於特定軟體和硬體版本。本文檔重點介紹vEdge平台。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

對於Cisco Edge路由器(控制器模式中的Cisco IOS® XE路由器)，請閱讀。

控制平面資訊

檢查控制本地屬性

要檢查vEdge上的接 Wide Area Network (WAN) 口的狀態，請使用命令 `show control local-properties wan-interface-list`。

在此輸出中，您可以看到RFC 4787 Network Address Translation (NAT) Type。

當vEdge位於NAT裝置（防火牆、路由器等）後面時，會使用公共和專用IPv4地址、公共和專用源埠來構建資料平面隧 User Datagram Protocol (UDP) 道。

您還可以找到通道介面的狀態、顏色和已設定的控制連線的最大數量。

```
vEdge1# show control local-properties wan-interface-list NAT TYPE: E -- indicates End-point independent mapping A -- indicates Address-port dependent
```

透過這些資料，您可以確定有關如何建立資料通道以及設定資料通道時預期會使用哪些連線埠（從路由器的角度）。

檢查控制連線

確保不構成資料平面隧道的顏色與重疊中的控制器建立了控制連線，這一點非常重要。

否則，vEdge不會將信 Transport Locator (TLOC) 息傳送到vSmart通 Overlay Management Protocol (OMP)道。


您可以使用命令驗證它是否可 `show control connections` 操作，並查詢狀 connect 態。

```
vEdge1# show control connections PEER PEER CONTROLLER PEER PEER PEER SITE DOMAIN PEER PRIV PEER PUB GROUP TYPE PROT SY
```

如果介面（不形成資料隧道）嘗試連線，請通過使用該顏色成功啟動控制連線，以解決此問題。

或者，在tunnel interface部 `max-control-connections 0` 分下的選定介面中設定的。

```
vpn 0 interface ge0/1 ip address 10.20.67.10/24 tunnel-interface encapsulation ipsec color mpls restrict max-control-connections 0 no allow-service bgp all
```

 **注意：**有時，您可以使用命令 `no control-connections` 來實現相同的目標。但是，該命令不會建立最大數量的控制連線。此命令從15.4版已棄用，在較新的軟體上不再使用。

重疊管理通訊協定

驗證是否已從vEdge通告OMP TLOC

無法傳送OMP TLOC，因為介面嘗試通過該顏色形成控制連線，並且無法到達控制器。

檢查顏色（資料通道）是否將該特定顏色的TLOC傳送到vSmarts。

使用命 `show omp tlocs advertised` 令檢查傳送到OMP對等體的TLOC。

示例：顏色 `mpls` 和 `gold`。沒有針對彩色mpls向vSmart傳送TLOC。

```
vEdge1# show omp tlocs advertised C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext -> extranet Stg
```

示例：顏色 `mpls` 和 `gold`。對兩種顏色都傳送TLOC。

```
vEdge2# show omp tlocs advertised C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext -> extranet Stg
```

 **注意：**對於任何本地生成的控制平面資訊，「**FROM PEER**」欄位設定為0.0.0.0。當您查詢本地生成的資訊時，請確保基於此值匹配。

驗證vSmart接收和通告TLOC

TLOC現在會通告給vSmart。確認它從正確的對等體接收TLOC並將其通告給另一個vEdge。

示例：vSmart從10.1.0.2 vEdge1接收TLOC。

<#root>

```
vSmart1# show omp tlocs received
```

```
C -> chosen I -> installed
```

```
Red -> redistributed Rej -> rejected L -> looped
```

```
R -> resolved
```

```
S -> stale Ext -> extranet Stg -> staged Inv -> invalid PUBLIC PRIVATE ADDRESS PSEUDO PUBLIC PRIVATE P
```

```
10.1.0.2 mpls ipsec 10.1.0.2 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 -
```

```
10.1.0.2 blue ipsec 10.1.0.2 C,I,R 1 198.51.100.187 12406 10.19.146.2 12406 :: 0 :: 0 -
```

```
10.1.0.30 mpls ipsec 10.1.0.30 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 - 10.1.0.30 gold
```

如果您未看到TLOC或在此處看到任何其他代碼，請檢查以下內容：

<#root>

vSmart-vIPtela-MEX# show omp tlocs received

C -> chosen

I -> installed

Red -> redistributed

Rej -> rejected

L -> looped

R -> resolved

S -> stale Ext -> extranet Stg -> staged

Inv -> invalid

PUBLIC PRIVATE ADDRESS PSEUDO PUBLIC PRIVATE PUBLIC IPV6 PRIVATE IPV6 BFD FAMILY TLOC IP COLOR ENCAP F

10.1.0.2 mpls ipsec 10.1.0.2 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 -

10.1.0.2 blue ipsec 10.1.0.2 Rej,R,Inv 1 198.51.100.187 12406 10.19.146.2 12406 :: 0 :: 0 -

10.1.0.30 mpls ipsec 10.1.0.30 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 - 10.1.0.30 gold i

驗證沒有阻止TLOC的策略。

show run policy control-policy — 查詢在vSmart中拒絕您的TLOC的任**advertised** 何 **received** tloc-list。

<#root>

vSmart1(config-policy)# sh config policy lists tloc-list SITE20

tloc 10.1.0.2 color blue encap ipsec

!! control-policy SDWAN

sequence 10 match tloc tloc-list SITE20 ! action reject ---->

here we are rejecting the TLOC 10.1.0.2,blue,ipsec !! default-action accept !

apply-policy

site-list SITE20

control-policy SDWAN in ----->

the policy is applied to control traffic coming IN the vSmart, it will filter the tlocs before adding i



註：如果TLOC為或， **Rejected** 則 **Invalid**不會將其通告到其他vEdge。

確保策略在從vSmart通告時不會過濾TLOC。您可以看到在vSmart上收到了TLOC，但在另一個vEdge上看不到它。

示例1：在C、I、R中具有TLOC的vSmart。

<#root>

```
vSmart1# show omp tlocs
```

```
C -> chosen I -> installed
```

```
Red -> redistributed Rej -> rejected L -> looped
```

```
R -> resolved
```

```
S -> stale Ext -> extranet Stg -> staged Inv -> invalid PUBLIC PRIVATE ADDRESS PSEUDO PUBLIC PRIVATE P
```

```
10.1.0.2 mpls ipsec 10.1.0.2 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 - 10.1.0.2 blue ipse
```

```
10.1.0.30 mpls ipsec 10.1.0.30 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 - 10.1.0.30 gold
```

示例2:vEdge1沒有看到來自vEdge2的藍色的TLOC。它只看到MPLS TLOC。

<#root>

```
vEdge1# show omp tlocs C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext -> extranet Stg -> staged I
```

```
10.1.0.2 mpls ipsec 10.1.0.3 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 up
```

```
10.1.0.30 mpls ipsec 10.1.0.3 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 up 10.1.0.30 gold
```

檢查策略時，可以看到TLOC未出現在vEdge1上的原因。

<#root>

```
vSmart1# show running-config policy policy lists tloc-list SITE20
```

```
tloc 10.1.0.2 color blue encaps ipsec
```

```
! site-list SITE10 site-id 10 !! control-policy SDWAN sequence 10 match tloc
```

```
tloc-list SITE20
```

```
! action reject !! default-action accept !
```

```
apply-policy
```

```
site-list SITE10
```

```
control-policy SDWAN out
```

```
!
```

```
!
```

雙向轉發檢測

瞭解show bfd sessions命令

以下是在輸出中要查詢的關鍵內容：

<#root>

```
vEdge-2# show bfd sessions SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX SYSTEM IP SITE ID STATE COLOR COLOR
10.1.0.5 10 down blue gold 10.19.146.2 203.0.113.225 4501 ipsec 7 1000 NA 7
10.1.0.30 30 up blue gold 10.19.146.2 192.0.2.129 12386 ipsec 7 1000 0:00:00:22 2 10.1.0.4 40 up blue
10.1.0.4 40 up mpls mpls 10.20.67.10
```

- **SYSTEM IP**：對等體system-ip
- **SOURCE and REMOTE TLOC COLOR**：這對於瞭解預期接收和傳送的TLOC非常有用。
- **SOURCE IP**：它是源 private IP。如果您位於NAT之後，則此資訊會顯示在這裡(使用時可以看到 show control local-properties <wan-interface-list>)。
- **DST PUBLIC IP**：無論隧道是否位於NAT之 **Data Plane** 後，vEdge都將使用該目標來形成隧道。(示例：直接連線到Internet的vEdge或鏈 **Multi-Protocol Label Switching (MPLS)** 接)
- **DST PUBLIC PORT** vEdge使用的公共NAT埠，用於形成到達 **Data Plane** 程vEdge的隧道。
- **TRANSITIONS**:BFD會話狀態從更改為 (反之亦然) NA 的 UP 更改次數。

命令show tunnel statistics

可以 show tunnel statistics 顯示有關資料平面隧道的資訊。您可以確定是否為vEdge之間的特定IPSEC隧道傳送或接收資料包。

這有助於您瞭解資料包是否到達每一端，並隔離節點之間的連線問題。

在該示例中，當多次運行該命令時，可以在或中注意到一個增量或tx-pkts 無 rx-pkts增量。



提示：如果tx-pkts的計數器遞增，則向對等體傳輸資料。如果rx-pkts不增加，則表示沒有從對等方接收資料。在這種情況下，請檢查另一端並確認tx-pkts是否遞增。

<#root>

TCP vEdge2# show tunnel statistics

TUNNEL SOURCE DEST TUNNEL MSS PROTOCOL SOURCE IP DEST IP PORT PORT SYSTEM IP LOCAL COLOR REMOTE COLOR MTU tx-

```

ipsec 172.16.16.147 10.88.244.181 12386 12406 10.1.0.5 public-internet default 1441 38282 5904968 38276
ipsec 172.16.16.147 10.152.201.104 12386 63364 10.1.0.0 public-internet default 1441 33421 5158814 334

TUNNEL
PROTOCOL SOURCE IP DEST IP SOURCE PORT DEST PORT SYSTEM IP LOCAL COLOR REMOTE COLOR
-----
ipsec 172.16.16.147 10.88.244.181 12386 12406 10.1.0.5 public-internet default
ipsec 172.16.16.147 10.152.201.104 12386 63364 10.1.0.0 public-internet default 144
ipsec 172.16.16.147 10.152.204.31 12386 58851 10.1.0.7 public-internet public-internet
ipsec 172.24.90.129 10.88.244.181 12426 12406 10.1.0.5 biz-internet default
ipsec 172.24.90.129 10.152.201.104 12426 63364 10.1.0.0 biz-internet default 144
ipsec 172.24.90.129 10.152.204.31 12426 58851 10.1.0.7 biz-internet public-internet

```

另一個有用的命令 `show tunnel statistics bfd` 可用於檢查特定資料平面隧道內傳送和接收的BFD資料包的數量：

```
vEdge1# show tunnel statistics bfd BFD BFD BFD BFD BFD BFD BFD PMTU PMTU PMTU PMTU TUNNEL SOURCE DEST ECHO TX ECHO RX BFD
```

存取清單

檢視輸出後，訪問清單是一個有用的必要步驟 `show bfd sessions` 。

現在知道私有、公共IP和埠了，您可以建立以與SRC_PORT、DST_PORT、SRC_IP、DST_IP匹 Access Control List (ACL) 配。

這有助於驗證已傳送和已接收的BFD消息。

在此可找到ACL配置的示例：

```

policy access-list checkbfd-out sequence 10 match source-ip 192.168.0.92/32 destination-ip 198.51.100.187/32 source-port 12426 destination-port 12426 !
default-action accept
!
access-list checkbfd-in sequence 20 match source-ip 198.51.100.187/32 destination-ip 192.168.0.92/32 source-port 12426 destination-port 12426 ! action a
vpn 0
interface ge0/0
access-list checkbfd-in in
access-list checkbfd-out out
!
!
!

```

在範例中，此ACL使用兩個序列。序列10匹配從此vEdge傳送到對等體的BFD消息。序列20則相反。

它與來源(Private)連線埠和目的地(Public)連線埠相符。如果vEdge使用NAT，請確保檢查正確的源埠和目標埠。

要檢查每個序列計數器上的命中數，請發出 `show policy access-list counters <access-list name>`

```
vEdge1# show policy access-list-counters NAME COUNTER NAME PACKETS BYTES ----- checkbfd bfd-out-to
```


網路位址轉換

如何使用工具 `stun-client` 檢測 NAT 對映和過濾器。

如果您已完成所有步驟，而且您正在執行 NAT，則下一步是識別行 **UDP NAT Traversal (RFC 4787) Map and Filter** 為。

此工具用於在 vEdge 位於 NAT 裝置後面時發現本地 vEdge 外部 IP 地址。

此命令獲取裝置的埠對映，並選擇性地發現本地裝置和伺服器（公共伺服器：示例 `google stun` 伺服器）之間的 NAT 屬性。

 **注意：**有關更多詳細資訊，請訪問 [Docs Viptela - STUN 客戶端](#)

<#root>

```
vEdge1# tools stun-client vpn 0 options "--mode full --localaddr 192.168.12.100 12386 --verbosity 2 stur
stunclient --mode full --localaddr 192.168.12.100 stun.l.google.com in VPN 0 Binding test: success
Local address: 192.168.12.100:12386
Mapped address: 203.0.113.225:4501
Behavior test: success

Nat behavior: Address Dependent Mapping

Filtering test: success

Nat filtering: Address and Port Dependent Filtering
```


在軟體的較新版本中，語法可以稍有不同：

<#root>

```
vEdge1# tools stun-client vpn 0 options "--mode full --localaddr 192.168.12.100 --localport 12386 --verh
```

在本示例中，您使用連線到 Google STUN 伺服器的 UDP 源埠 12386 執行完整的 NAT 檢測測試。

此命令的輸出為您提供了 NAT 行為以及基於 RFC 4787 的 NAT 過濾器型別。

 註：使用時， tools stun請記得在通道介面上允許STUN服務，否則無法使用。使 allow-service stun 用以允許stun資料通過。

<#root>

```
vEdge1# show running-config vpn 0 interface ge0/0 vpn 0 interface ge0/0 ip address 10.19.145.2/30 ! tunnel-interface encapsulation ipsec color gold max-  
allow-service stun  
! no shutdown !!
```

這顯示了STUN術語 (全錐NAT) 與RFC 4787 (UDP的NAT行為) 之間的對映。

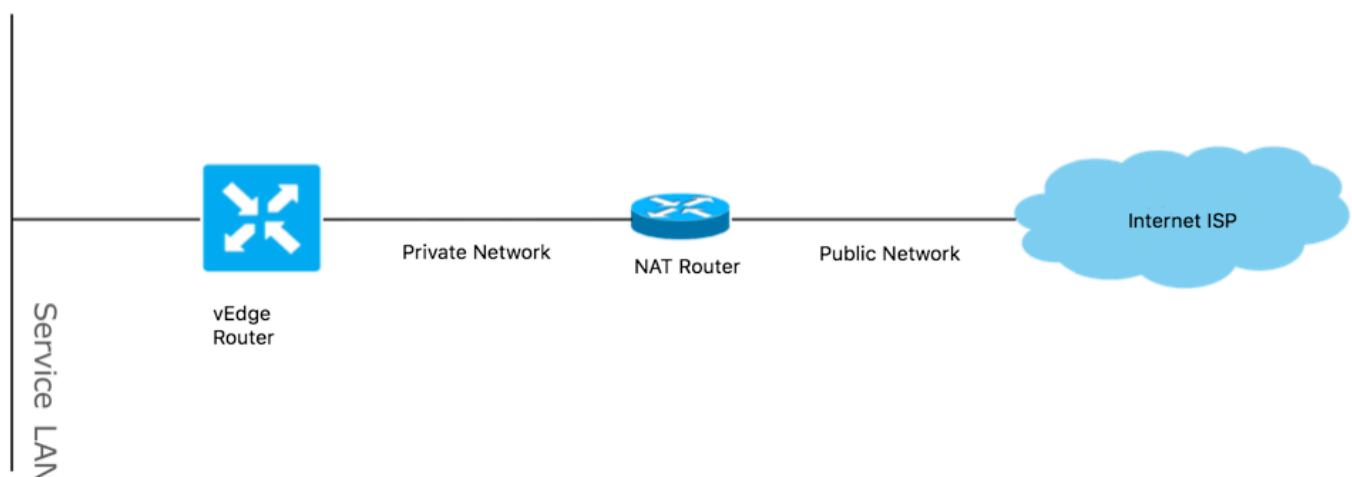
NAT Traversal Mapping Between used Viptela Terminologies		
STUN RFC 3489 Terminology	RFC 4787 Terminology	
	Mapping Behavior	Filtering Behavior
Full-cone NAT	Endpoint-Independent Mapping	Endpoint-Independent Filtering
Restricted Cone NAT	Endpoint-Independent Mapping	Address-Dependent Filtering
Port-Restricted Cone NAT	Endpoint-Independent Mapping	Address and Port-Dependent Filtering
Symmetric NAT	Address-and(or) Port-Dependent Mapping	Address-Dependent Filtering
		Address and Port-Dependent Filtering

CLI中使用的資料平面隧道的「傳送」支援的NAT型別

在大多數情況下，您的公共顏色 (如商業internet或公共internet) 可以直接連線到internet。

在其他情況下，vEdge WAN介面和實際網際網路服務提供商後面有一個NAT裝置。

通過這種方式，vEdge可以具有私有IP，而其它裝置 (路由器、防火牆等) 可以是具有面向公有IP地址的裝置。



如果您的NAT型別不正確，則可能是不允許建立資料平面隧道的最常見原因之一。以下是受支援的NAT型別。

NAT Traversal Support		
Source	Destination	Supported (YES/NO)
Full-Cone NAT	Full-cone NAT	Yes
Full-Cone NAT	Restricted Cone NAT	Yes
Full-Cone NAT	Port-Restricted Cone NAT	Yes
Full-Cone NAT	Symmetric NAT	Yes
Restricted Cone NAT	Full-cone NAT	Yes
Restricted Cone NAT	Restricted Cone NAT	Yes
Restricted Cone NAT	Port-Restricted Cone NAT	Yes
Restricted Cone NAT	Symmetric NAT	Yes
Port-Restricted Cone NAT	Full-cone NAT	Yes
Port-Restricted Cone NAT	Restricted Cone NAT	Yes
Port-Restricted Cone NAT	Port-Restricted Cone NAT	Yes
Port-Restricted Cone NAT	Symmetric NAT	No
Symmetric NAT	Full-cone NAT	Yes
Symmetric NAT	Restricted Cone NAT	yes
Symmetric NAT	Port-Restricted Cone NAT	No
Symmetric NAT	Symmetric NAT	No

防火牆

如果您已在不支援的Source和Destination型別中檢查了NAT及其非NAT，則防火牆可能會阻止用於形成隧道的端 Data Plane 口。

確保在用於資料平面連線的防火牆中開啟以下埠 vEdge to vEdge Data Plane:

UDP12346到13156

對於從vEdge到控制器的控制連線：

UDP12346到13156

TCP 23456 to 24156

確保開啟這些埠，以便成功連線資料平面隧道。

檢查用於資料平面隧道的源埠和目標埠時，可以使用 `show tunnel statistics` 或 `show bfd sessions | tab` 不可 `show bfd sessions`用。

它不會顯示任何來源連線埠，只會顯示您可以看到的目的地連線埠：

```
vEdge1# show bfd sessions SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX SYSTEM IP SITE ID STATE COLOR COLOR
```

 注意：有關使用的SD-WAN防火牆埠的詳細資訊，請參閱[此處](#)。

安全性

如果觀察到ACL計數器增加入站和出站流量，請檢查幾個迭代 **show system statistics diff** and ensure there are no drops.

<#root>

```
vEdge1# show policy access-list-counters NAME COUNTER NAME PACKETS BYTES -----
```

```
checkbfd bfd-out-to-dc1-from-br1 55 9405
```

```
bfd-in-from-dc1-to-br1 54 8478
```

在此輸出中，隨**rx_replay_integrity_drops** 著的每次迭代增加 **show system statistics diff** command.

<#root>

```
vEdge1#show system statistics diff
```

```
rx_pkts : 5741427
ip_fwd : 5952166
ip_fwd_arp : 3
ip_fwd_to_egress : 2965437
ip_fwd_null_mcast_group : 26
ip_fwd_null_nhop : 86846
ip_fwd_to_cpu : 1413393
ip_fwd_from_cpu_non_local : 15
ip_fwd_rx_ipsec : 1586149
ip_fwd_mcast_pkts : 26
rx_bcast : 23957
rx_mcast : 304
rx_mcast_link_local : 240
rx_implicit_acl_drops : 12832
rx_ipsec_decap : 21
rx_spi_ipsec_drops : 16
```

```
rx_replay_integrity_drops : 1586035
```

```
port_disabled_rx : 2
rx_invalid_qtags : 212700
rx_non_ip_drops : 1038073
pko_wred_drops : 3
bfd_tx_record_changed : 23
rx_arp_non_local_drops : 19893
rx_arp_reqs : 294
rx_arp_replies : 34330
arp_add_fail : 263
tx_pkts : 4565384
tx_mcast : 34406
port_disabled_tx : 3
tx_ipsec_pkts : 1553753
tx_ipsec_encap : 1553753
tx_pre_ipsec_pkts : 1553753
tx_pre_ipsec_encap : 1553753
tx_arp_replies : 377
```

```
tx_arp_reqs : 34337
tx_arp_req_fail : 2
bfd_tx_pkts : 1553675
bfd_rx_pkts : 21
bfd_tx_octets : 264373160
bfd_rx_octets : 3600
bfd_pmtu_tx_pkts : 78
bfd_pmtu_tx_octets : 53052
rx_icmp_echo_requests : 48
rx_icmp_network_unreach : 75465
rx_icmp_other_types : 47
tx_icmp_echo_requests : 49655
tx_icmp_echo_replies : 48
tx_icmp_network_unreach : 86849
tx_icmp_other_types : 7
vEdge1# show system statistics diff
```

```
rx_pkts : 151
ip_fwd : 157
ip_fwd_to_egress : 75
ip_fwd_null_nhop : 3
ip_fwd_to_cpu : 43
ip_fwd_rx_ipsec : 41
rx_bcast : 1
```

rx_replay_integrity_drops : 41

```
rx_invalid_qtags : 7
rx_non_ip_drops : 21
rx_arp_non_local_drops : 2
tx_pkts : 114
tx_ipsec_pkts : 40
tx_ipsec_encap : 40
tx_pre_ipsec_pkts : 40
tx_pre_ipsec_encap : 40
tx_arp_reqs : 1
bfd_tx_pkts : 40
bfd_tx_octets : 6800
tx_icmp_echo_requests : 1
```

vEdge1# show system statistics diff

```
rx_pkts : 126
ip_fwd : 125
ip_fwd_to_egress : 58
ip_fwd_null_nhop : 3
ip_fwd_to_cpu : 33
ip_fwd_rx_ipsec : 36
rx_bcast : 1
rx_implicit_acl_drops : 1
```

rx_replay_integrity_drops : 35

```
rx_invalid_qtags : 6
rx_non_ip_drops : 22
rx_arp_replies : 1
tx_pkts : 97
tx_mcast : 1
tx_ipsec_pkts : 31
tx_ipsec_encap : 31
```

```
tx_pre_ipsec_pkts : 31
tx_pre_ipsec_encap : 31
bfd_tx_pkts : 32
bfd_tx_octets : 5442
rx_icmp_network_unreach : 3
tx_icmp_echo_requests : 1
tx_icmp_network_unreach : 3
vEdge1# show system statistics diff
```

```
rx_pkts : 82
ip_fwd : 89
ip_fwd_to_egress : 45
ip_fwd_null_nhop : 3
ip_fwd_to_cpu : 24
ip_fwd_rx_ipsec : 22
rx_bcast : 1
rx_implicit_acl_drops : 1
```

```
rx_replay_integrity_drops : 24
```

```
rx_invalid_qtags : 2
rx_non_ip_drops : 14
rx_arp_replies : 1
tx_pkts : 62
tx_mcast : 1
tx_ipsec_pkts : 24
tx_ipsec_encap : 24
tx_pre_ipsec_pkts : 24
tx_pre_ipsec_encap : 24
tx_arp_reqs : 1
bfd_tx_pkts : 23
bfd_tx_octets : 3908
rx_icmp_network_unreach : 3
tx_icmp_echo_requests : 1
tx_icmp_network_unreach : 3
```

```
vEdge1# show system statistics diff
```

```
rx_pkts : 80
ip_fwd : 84
ip_fwd_to_egress : 39
ip_fwd_to_cpu : 20
ip_fwd_rx_ipsec : 24
```

```
rx_replay_integrity_drops : 22
```

```
rx_invalid_qtags : 3
rx_non_ip_drops : 12
tx_pkts : 66
tx_ipsec_pkts : 21
tx_ipsec_encap : 21
tx_pre_ipsec_pkts : 21
tx_pre_ipsec_encap : 21
bfd_tx_pkts : 21
bfd_tx_octets : 3571
```

首先，在vEdge上執行 `request security ipsec-rekey`。然後，檢視的幾個 `show system statistics diff` 迭代並檢視是否仍看 `rx_replay_integrity_drops`

到。

如果是，請檢查您的安全配置。

```
vEdge1# show running-config security security
ipsec
authentication-type sha1-hmac ah-sha1-hmac
!
```

DSCP標籤流量的ISP問題

預設情況下，從vEdge路由器到控制器的所有控制和管理流量都通過DTLS或TLS連線傳輸，並標有DSCP值CS6（十進位制48）。

對於資料位置隧道流量，vEdge路由器使用IPsec或GRE封裝來相互傳送資料流量。

為了進行資料平面故障檢測和效能測量，路由器會定期相互傳送BFD資料包。

這些BFD資料包還使用DSCP值CS6（十進位制48）進行標籤。

從ISP的角度來看，此類流量被視為具有DSCP值CS6的UDP流量，因為vEdge路由器和SD-WAN控制器會複製預設情況下標籤到外部IP報頭的DSCP。

以下是tcpdump在傳輸ISP路由器上運行時的外觀：

```
14:27:15.993766 IP (tos 0xc0, ttl 64, id 44063, offset 0, flags [DF], proto UDP (17), length 168) 192.168.109.5.12366 > 192.168.20.2.12346: [udp sum ok]
```

此處可以看到，所有資料包都標有TOS位元組0xc0（也稱為DS欄位）（等於十進位制192或110 000 00的二進位制）。

前6個高位對應於DSCP位值（以十進位制或CS6表示48）。

輸出中的前2個封包對應控制平面通道，其餘2個封包對應資料平面通道流量。

根據封包長度和TOS標籤，它可以信心十足地斷定是BFD封包（RX和TX方向）。這些資料包也使用CS6進行標籤。

有時，某些服務提供商（尤其是MPLS第3層VPN/MPLS第2層VPN服務提供商）維護不同的SLA，並可根據DSCP標籤以不同方式處理不同類別的流量。

例如，如果您有高級服務來優先處理DSCP EF和CS6語音和信令流量。

由於幾乎總是會管制優先流量，即使沒有超過上行鏈路的總頻寬，這種型別的流量可能會出現資料包丟失，因此BFD會話也可能出現抖動。

在某些情況下，如果服務提供商路由器上的專用優先順序隊列匱乏，您不會看到正常流量發生任何丟棄(例如，當您從vEdge路由器運行簡單ping時)。

這是因為此類流量標示為預設DSCP值0，如下圖所示 (TOS位元組)：

```
15:49:22.268044 IP (tos 0x0, ttl 62, id 0, offset 0, flags [DF], proto UDP (17), length 142) 192.168.110.5.12366 > 192.168.109.7.12346: [no cksum] UDP,
```

但同時，您的BFD會話會翻動：

```
show bfd history DST PUBLIC DST PUBLIC RX TX SYSTEM IP SITE ID COLOR STATE IP PORT ENCAP TIME PKTS PKTS DEL -----
```

這裡的nping可以方便進行疑難排解：

```
vedge2# tools nping vpn 0 options "--tos 0x0c --icmp --icmp-type echo --delay 200ms -c 100 -q" 192.168.109.7 Nping in VPN 0 Starting Nping 0.6.47 (ht
```

調試BFD

如果需要更深入的調查，請在vEdge路由器上運行BFD調試。

轉發流量管理器(FTM)負責vEdge路由器上的BFD操作，因此您需要 **debug ftm bfd** 它。

所有調試輸出都存 `/var/log/tmplog/vdebug` 儲在檔案中，如果您希望控制檯上出現這些消息(類似Cisco IOS行**terminal monitor** 為)，則可以使用**monitor start /var/log/tmplog/vdebug**。

要停止日誌記錄，您可以使用 **monitor stop /var/log/tmplog/vdebug**

以下是輸出查詢由於逾時而關閉的BFD作業階段的方式(IP位址為192.168.110.6的遠端TLOC無法再連線):

```
log:local7.debug: May 7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_state[1008]: BFD-session TNL 192.168.110.5:12366->192.168.110.6:123
```

要啟用的另一個有價值的調試 **Tunnel Traffic Manager (TTM)** 是事件調試 **debug ttm events**。

以下是 **BFD DOWN** 從TTM角度看事件的外觀：

```
log:local7.debug: May 7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Received TTM Msg LINK_BFD, Client: ftmd, AF: LINK log:loc
```

相關資訊

- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。