對具有重複NAT端點的SD-WAN集線器隧道進行故障排除

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

- 控制平面NAT學習
- 資料平面NAT學習和VCONTROL
- 埠保留、埠重疊和埠隨機化

拓撲示例

為什麼會發生衝突

- 不同的vBonds可以觀察到相同的公共終結點
- 同一廣告到達一個網路中心
- 重複的分支機構地址發生私有 — 公有(AS-Public)衝突
- NAT端點重新分配

症狀和影響

診斷問題

- 步驟1.記錄軟體和分支傳輸狀態
- 步驟2.在OMP中查詢重複的終結點
- 步驟3.比較邏輯TLOC與中心會話所有權
- 步驟4.檢驗NAT網關的實際工作情況
- 步驟5.檢查Wireshark中的VCONTROL
- 步驟6.確認受影響的路徑並保留證據

變通辦法和限制

- 使用具有唯一分配的穩定獨立於端點的對映
- 禁用不同分支之間的埠重疊
- 對小型受控組使用埠偏移
- 禁用源埠保留或啟用隨機分配
- 單獨的公有地址或保留埠塊
- 保留備用傳輸並協調恢復

相關軟體缺陷

附錄:解碼IPv4 VCONTROL報尾

相關資訊

簡介

本文描述當分支共用一個公共網路地址轉換(NAT)端點時，如何識別並緩解中心隧道故障。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Catalyst軟體定義的廣域網(SD-WAN)架構和控制連線
- 重疊管理通訊協定(OMP)、傳輸定位器(TLOC)、雙向轉送偵測(BFD)和IP安全(IPsec)
- 多重協定標籤交換(MPLS)傳輸網路
- NAT對映和過濾器行為
- 使用Wireshark進行基本資料包分析

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS® XE Catalyst SD-WAN路由器
- Cisco Catalyst SD-WAN控制器(vSmart)
- Cisco Catalyst SD-WAN驗證器(vBond)

中心會話所有權故障在Cisco IOS XE 17.18.2上重現，且成對金鑰可運行。命令可用性和輸出欄位因平台和版本而異。

示例使用私有地址或RFC 5737保留的文檔地址，以及通用裝置名稱。CLI摘錄被縮短，並使用規範化的識別符號。介面名稱和某些輸出欄位因平台和版本而異。

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。

⚠ 注意：配置更改和連線重置可能會中斷流量。使用批准的維護計畫。初始診斷命令是只讀的。

背景資訊

從正確識別對稱NAT的場景開始。分支A向vBond 1註冊，分支B向vBond 2註冊。如RFC 7857所允

許，當這些連線的目的地不同時，NAT網關可以將相同的轉換源IP地址和埠分配給這些連線。因此，兩個分支可以為其公共網際網路TLOC通告相同的公共端點，即使兩個分支都報告NAT型別A。

示例拓撲使用公共Internet顏色。同一場景可能涉及其他公共顏色，例如商業網際網路。將診斷濾鏡應用於實際受影響的傳輸顏色；字面公用internet顏色不是必需條件。

注意:Cisco Catalyst SD-WAN不支援來自不同站點的TLOC，這些站點向公共接收邊緣通告相同的公共IP地址和UDP埠。在此衝突條件下的接收器行為是不可預測的。即使對稱NAT正確識別，也可能發生這種情況。僅對NAT進行正確分類並不能保證通告的端點是唯一的。

控制平面NAT學習

在vBond註冊期間，邊緣會傳送其專用傳輸地址和埠。vBond將觀察該連線上的源地址和埠，並將觀察的端點返回到邊緣。Edge可以通過OMP將此資訊通告為TLOC的公共地址和埠屬性，包括具有公共顏色（如公共網際網路或商業網際網路）的TLOC。

該觀察描述了與該vBond的連線。使用與目的地相關的NAT，通向集線器的對映可以不同。路由器會比較NAT觀察結果，以便對對映行為進行分類。在show sdwan control local-properties中，A表示與地址及埠相關的對映，E表示與終端無關的對映。顯示的分類描述了路由器的決策；nat轉換表或資料包捕獲驗證NAT網關的實際行為。

例如，運行show sdwan control local-properties並找到傳輸的NAT TYPE列。此縮短的輸出保留了NAT型別的圖例和選定的介面列，並具有規範化的地址：

<#root>

Spoke-A# show sdwan control local-properties

```
...
 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                          PUBLIC         PUBLIC PRIVATE         PRIVATE                          NAT
INTERFACE                 IPv4           PORT   IPv4            PORT    COLOR          STATE     TYPE
GigabitEthernet2          192.168.9.11    12346  192.168.9.11    12346   mpls           up         E
GigabitEthernet3          203.0.113.10    23012  192.168.11.11   12346   biz-internet   up         A
```

商務Internet傳輸報告A並通告203.0.113.10:23012作為其公共端點。MPLS傳輸報告E並且具有相同的私有和公共端點。從NAT TYPE中讀取分類;僅地址或埠相等並不能識別NAT型別。N表示路由器尚未獲知分類。

資料平面NAT學習和VCONTROL

在集線器可以處理加密的BFD封包之前，它必須找到對應對等體和通道的傳入IPsec安全關聯(SA)。SA標識加密金鑰以及驗證和解密資料包所需的其他狀態。接收器使用端點資訊和封裝安全負載(ESP)安全引數索引(SPI)來定位該狀態。SPI本身不是全域性唯一的分支識別符號。

對稱NAT後的分支通常向可到達的集線器發起流量。這將為該特定目標建立一個對映。集線器看到的源地址或埠可能與之前通過vBond獲知並在OMP中通告的公共端點不同。因此，收到的外部報頭並不總是與已安裝隧道狀態的端點匹配。集線器需要一種方法，將此新的有線上終端與已知的遠端TLOC及其IPsec狀態相關聯，才能解密BFD。

對於此處討論的IPv4 BFD-over-IPsec格式，SD-WAN將終端資訊放在UDP負載末尾的可見VCONTROL報尾中，而不是加密的BFD負載。集線器可以在解密前讀取此資訊。VCONTROL攜帶終端資訊，而不是加密金鑰，並且不自行建立對等體標識。

例如，在初始隧道建立期間，資料平面學習完成之前：

```
Spoke B advertised through OMP:       203.0.113.10:12346
Spoke B observed at the hub:          203.0.113.10:45678
VCONTROL carried source endpoint:    203.0.113.10:12346
```

接收方首先嘗試其正常端點/SPI查詢。如果查詢沒有找到SA，則VCONTROL源端點會提供回退。在本示例中，集線器可以使用傳送的203.0.113.10:12346及其本地目標上下文和SPI，以定位與已知遠端TLOC關聯的入站SA，即使資料包從203.0.113.10:45678到達。

所選SA提供接收金鑰上下文。SPI會在該上下文中選擇適用的金鑰生成。然後，集線器執行IPsec驗證和解密；只有通過所需檢查的資料包才可用於BFD處理。僅可讀尾部或成功查詢並不能證明身份驗證、解密或BFD接收成功。

因此，觀察到的源埠和承載的源埠之間的差異可以使用對稱NAT正常。要使對等關係起作用，集線器必須將資料包與正確的隧道和金鑰狀態相關聯，並瞭解實際返回端點。在本例中，成功學習使網路中心可以將返回流量傳送到203.0.113.10:45678。這不同於通過vBond進行控制平面學習。

VCONTROL不強制接收器覆蓋現有端點/SPI匹配。如果重複的端點狀態將資料包與錯誤的對等體或金鑰生成相關聯，則幀尾不保證恢復。它提供查詢提示；它無法區分兩個攜帶相同端點的對等體而沒有正確的周圍隧道和加密狀態。

當報告NAT型別E時，適用的BFD資料包上也存在VCONTROL。它的存在不是對稱NAT標誌，並且不包括在每個普通IPsec資料包中。對於此處介紹的IPv4 BFD格式，在兩個專用顏色之間省略public-TLOC資訊。

通過資料平面獲知的對等特定端點並不意味著分支必須為每個目標使用新端點替換其OMP通告。不同的已學習對映是對稱NAT遍歷的預期部分。

通道啟動後，獲知該通道自己的已轉換端點的傳送者可攜帶該端點作為其來源資訊。這是傳送方的每個隧道公共終結點，而不是遠端終結點或新的全域性OMP通告。請始終比較來自同一觀察期的資料包、OMP通告和會話狀態。

埠保留、埠重疊和埠隨機化

以下是不同的行為：

行為	含義
源埠保留	NAT網關嘗試將分支的原始UDP源埠(例如12346)保留為轉換後的源埠。
目標之間的埠重疊	NAT網關重複使用一個轉換的IP:用於與不同外部目標通訊的不同內部端點的埠。
埠隨機化	NAT網關使用隨機分配方法選擇轉換埠。
獨立於端點的對映	存在對映時，一個內部終結點在外部目標之間保留相同的轉換終結點。

RFC 7857第3節允許當目標不同時，不同內部端點的外部埠重疊。NAT使用流的五元組來區分流。這不允許兩個同時的、無法區分的UDP流到達同一目的地。隨機分配和儲存是獨立的分配選擇；二者均不建立端點獨立性。

拓撲示例

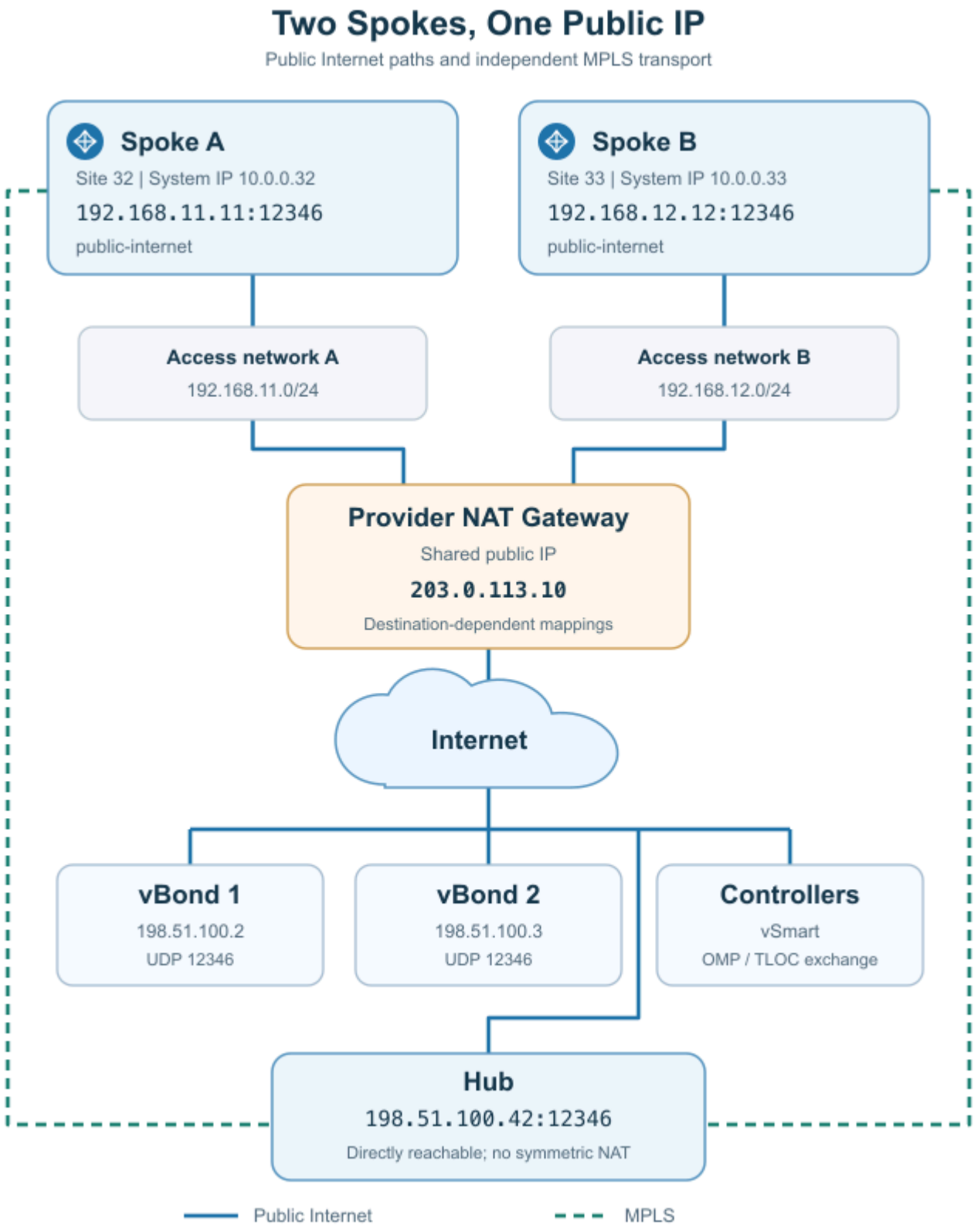

圖1.共用NAT網關、獨立的分支接入網路和獨立的MPLS傳輸。

分支A使用192.168.11.11:12346，分支B使用192.168.12.12:12346。兩者通過NAT網關共用公共地址203.0.113.10。集線器有一個直接可到達的地址，不在對稱NAT的後面。兩個分支可以通告相同的公共IP：埠，即使它們的專用端點不同。

為什麼會發生衝突

不同的vBonds可以觀察到相同的公共終結點

請考慮以下同時UDP對映：

對等	專用源	轉換後的源	目的地
A	192.168.11.11:12346	203.0.113.10:12346	vBond 1, 198.51.100.2:12346
B	192.168.12.12:12346	203.0.113.10:12346	vBond 2, 198.51.100.3:12346

由於NAT也會檢查遠端端點，因此回覆會正確返回。vBond 1的回覆屬於A的對映；來自vBond 2的回覆屬於B的對映。

兩台路由器還可以聯絡其他vBond並正確檢測與目標相關的對映。例如，保持每個分支的私有源元組不變，並考慮以下觀察順序：

對等	首次接受的虛擬連線觀察	與Other vBond的比較	結果
A	vBond 1返回 203.0.113.10:12346	vBond 2返回 203.0.113.10:40001	NAT A;保留的公共元組 203.0.113.10:12346
B	vBond 2返回 203.0.113.10:12346	vBond 1返回 203.0.113.10:40002	NAT A;保留的公共元組 203.0.113.10:12346

每台路由器的vBond觀測結果各不相同，因此檢測NAT A是正確的。儘管如此，所保留的第一個觀察結果在兩台路由器上仍然相符。分類A不會在所有輻條之間分配唯一公共埠，並且訪問兩個vBonds也不能保證唯一性。

每個分支都接收註冊應答中vBond觀察到的公有地址和埠，並使用保留的觀察結果填充其本地傳輸屬性。分支在其通過OMP通告給SD-WAN控制器的TLOC屬性中包括公共端點及其專用端點。然後，控制器根據適用的控制策略將TLOC分配到其他Edge;vBond本身並不發起OMP通告。

如果兩個分支保留相同的觀察公共端點，則OMP可以包含：

```
TLOC system IP   Color            Public endpoint        Private endpoint
10.0.0.32        public-internet   203.0.113.10:12346     192.168.11.11:12346
10.0.0.33        public-internet   203.0.113.10:12346     192.168.12.12:12346
```

由於系統IP不同，這些路由保持不同的邏輯TLOC。

同一廣告到達一個網路中心

NAT網關必須區分兩個輻條何時與同一個集線器連線。一個可能的分配是：

對等	源到集線器的轉換	目的地
A	203.0.113.10:12346	198.51.100.42:12346
B	203.0.113.10:45678	198.51.100.42:12346

集線器有兩個通告相同目標端點的邏輯對等點，而資料包可以從不同的實際端點到達。在常規對稱NAT操作下，資料平面學習有助於建立返回對映。

當不同對等體共用此傳輸金鑰選擇的會話狀態時，會出現集線器會話所有許可權制：

```
Hub-local IP + hub-local port + remote IP + remote port + protocol
```

如果兩個通告選擇相同的金鑰，則來自後續對等體的更新可以替換共用狀態的所有權資訊。一個對等體的後續退出、刪除或重新建立會話可能會干擾另一個對等體的IPsec/BFD狀態。當該狀態已經與錯誤的對等體或流生成相關聯時，資料平面學習無法保證恢復。

可見尾部不是獨立的對等識別符號：兩個分支可以具有相同的源端點。如果集線器選擇屬於錯誤對等體或金鑰生成的現有IPsec狀態，則即使資料包到達集線器，身份驗證和學習也會失敗。為了建立特定封包順序，思科技術協助中心(TAC)必須將所選SA與其對等路由器及層代相關聯。僅封包尾部無法證明。

僅相同的公共IP不會建立衝突。不同的遠端埠通常會產生不同的傳輸金鑰。同時檢查所選集線器本地地址、本地埠和協定。如果第三對等體通告相同的端點，則它還可以競爭該金鑰；故障模式取決於事件順序。

重複的分支機構地址發生私有 — 公有(AS-Public)衝突

思科錯誤ID CSCwx12986可能導致邊緣在NAT比較期間發生自動來源連線埠躍點後，在其公用TLOC屬性中通告私有RFC 1918元組。如果不同的分支機構重複使用相同的私有地址和埠，則這些不正確的公共屬性可能會跨對等體匹配並暴露中心會話所有權問題。

例如，兩個分支都可以在單獨的分支防火牆後面使用192.168.11.11。每個防火牆都將其分支網路分隔開，並轉換源地址。如果上游提供程式NAT網關再次轉換它，則路徑具有兩個NAT階段，或雙重NAT。獨立的虛擬路由和轉發(VRF)環境是隔離重疊分支地址的另一種方式。

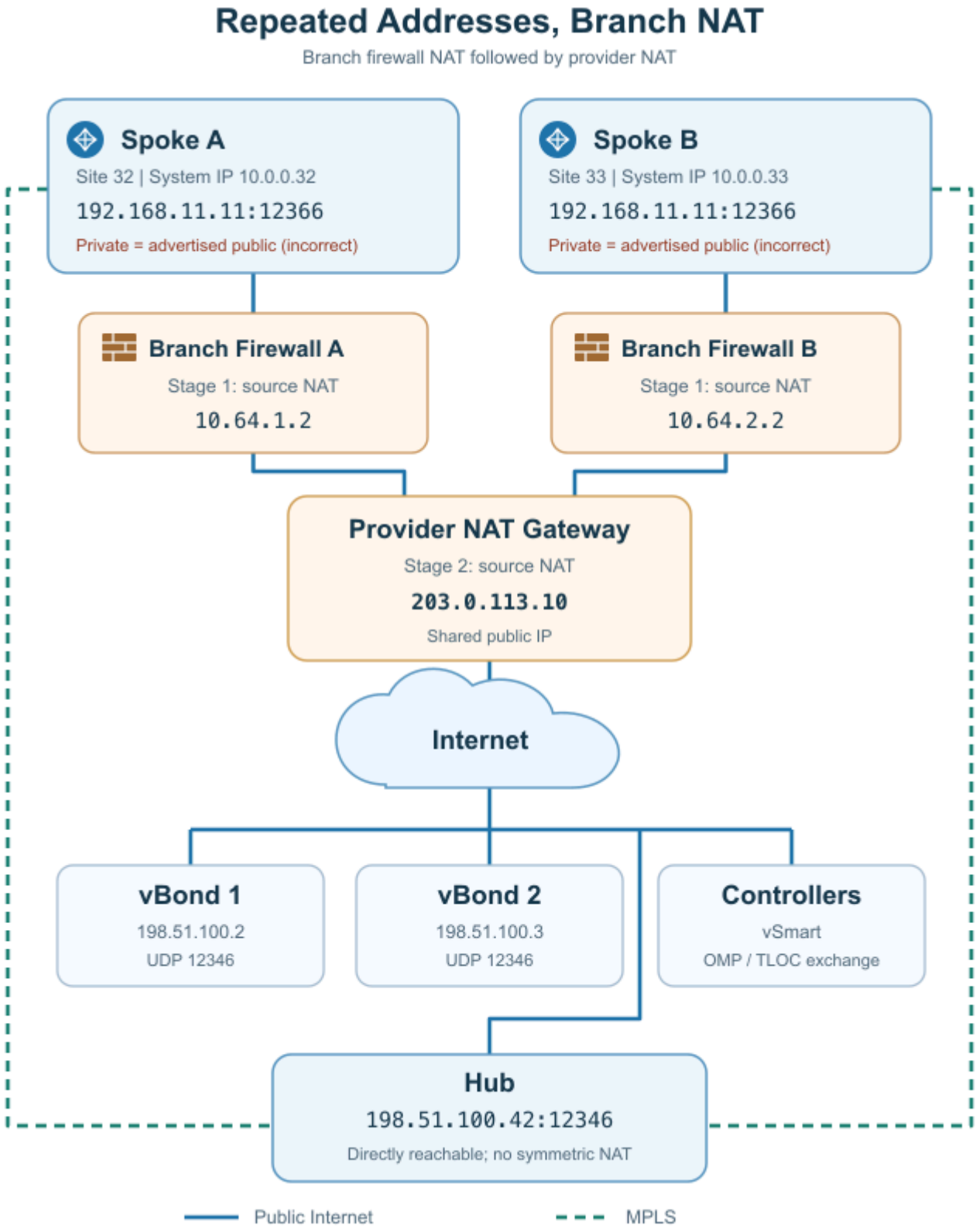

圖2.分支機構防火牆和提供商NAT轉換。錯誤的公共TLOC屬性保留原始專用端點，而資料包使用轉換後的源地址。

如果兩個分支在其公共網際網路TLOC上遇到缺陷，並使用相同的跳後源埠，則集線器可以接收以下通告：

對等	連線埠躍點之後的私人端點	公共TLOC終結點不正確
A	192.168.11.11:12366	192.168.11.11:12366
B	192.168.11.11:12366	192.168.11.11:12366

附註：重複的私有地址和雙NAT不是思科錯誤ID CSCwx12986本身的先決條件。額外的跨對等體衝突需要匹配通告的IP：埠值和相同的集線器本地地址、埠和協定。具有不同通告埠的相同私有IP不會建立此衝突。

在沒有NAT的傳輸中，公有和私有地址相等是正常現象。公共欄位中的RFC 1918地址只有在與預期路徑和觀察的轉換相抵觸時才可疑。唯一的分支私有地址可避免本示例中的重複 — 私有元組重疊；它們不會阻止前面介紹的單獨的translated-public port-reuse場景。

NAT端點重新分配

在NAT對映到期後，當中心節點仍然保留舊對等體狀態時，也可以將端點重新分配給另一個分支。將對映歷史記錄與中心會話生命週期進行比較，以確定新舊所有者之間的重疊。

症狀和影響

典型指標包括：

- 當受影響的BFD路徑關閉或無法恢復時，控制連線將保持Up。
- 兩個不同的系統IP通告相同的公共IP：埠。
- 集線器保留兩個邏輯TLOC，但篩選的平台會話檢視缺少一個對等體或顯示不一致的系統IP、遠端顏色、鑑別器、隧道或SA資訊。
- 一個對等體的傳輸撤銷或重建會干擾具有相同端點的另一個對等體。
- 受影響路徑上的IPsec輸入丟棄可能會增加。

該故障可能導致受影響的傳輸路徑不可用。如果這是分支的唯一可用傳輸路徑，則該分支與重疊隔離。在大型網路中心，共用一個NAT地址的輪輻會增加需要關聯的數量，但必須測量受影響路徑的數量；無法從該地址後面的站點數量推斷出該地址。

診斷問題

步驟1.記錄軟體和分支傳輸狀態

在每個受影響的Cisco IOS XE Edge上，將<affected-color>替換為實際傳輸顏色，例如biz-internet或public-internet:

<#root>

show clock detail

show version | include Cisco IOS XE Software

show sdwan control local-properties

show sdwan control connections | include

show sdwan omp peers

記錄私有/公有地址以及埠、介面、顏色、NAT型別、站點ID和控制狀態。在第一個完整的本地屬性示例之後，使用此緊湊過濾器來保留介面標題和選定的傳輸行。用受影響的介面替換TenGigabitEthernet0/1/0.10:

<#root>

show sdwan control local-properties "wan-interface-list" | include INTERFACE|PUBLIC|TenGigabitEthernet0/

對於主要方案，兩個分支上的相關欄位均可讀取。這是欄位摘要，而不是本地列佈局：

```
Field                         Spoke A                Spoke B
System IP                     10.0.0.32              10.0.0.33
Color                         public-internet        public-internet
Private endpoint              192.168.11.11:12346     192.168.12.12:12346
Public endpoint               203.0.113.10:12346      203.0.113.10:12346
NAT type                      A                      A
vSmart controls on transport  Up                     Up
```

Up控制連線驗證控制器關係。它不會驗證分支到中心的BFD路徑或公共端點的唯一性。

步驟2.在OMP中查詢重複的終結點

在Cisco IOS XE集線器上：

<#root>

show clock detail

show sdwan omp tlocs table | include 203.0.113.10

在SD-WAN控制器(vSmart)上：

<#root>

show clock

show omp tlocs | tab | include 203.0.113.10

此控制器輸出使用規範化的識別符號。省略IPv6和區域列：

<#root>

vSmart# show omp tlocs | tab | include 203.0.113.10

```
TLOC IP     COLOR            ENCAP FROM PEER  STATUS KEY PUBLIC IP     PORT  PRIVATE IP     PORT
10.0.0.32   public-internet ipsec 10.0.0.5   C,R    1   203.0.113.10 12346 192.168.11.11 12346
                               10.0.0.32  C,I,R  1   203.0.113.10 12346 192.168.11.11 12346
10.0.0.33   public-internet ipsec 10.0.0.5   C,R    1   203.0.113.10 12346 192.168.12.12 12346
                               10.0.0.33  C,I,R  1   203.0.113.10 12346 192.168.12.12 12346
```

比較TLOC系統IP、顏色、封裝、公共IP和公共埠。從不同控制器到同一邏輯TLOC的多個路徑是正常的。候選衝突是具有相同有效端點的兩個不同的對等身份。

在30-60秒後重複篩選的命令，並保留兩個時間戳。持續的重疊是有用的證據；完全同時的命令不是必需的。對於短暫的瞬變，請使用TAC收集OMP事件和相應的會話生命週期記錄。

對於兩個可疑對等體，保留其各自的TLOC表條目：

<#root>

```
show sdwan omp tlocs table | include 10.0.0.32
```

```
show sdwan omp tlocs table | include 10.0.0.33
```

如需透過Cisco IOS XE上的IPv4 TLOC詳細資訊的精簡檢視，請使用以下過濾器。使用正在調查的對等裝置替換系統IP，並在ip <system-IP>選擇器周圍保留引號：

<#root>

```
show sdwan omp tlocs "ip 10.0.0.32" | exclude not set| 0|None|efault|::
```

```
show sdwan omp tlocs "ip 10.0.0.33" | exclude not set| 0|None|efault|::
```

比較兩個對等體的公有和私有地址/埠屬性。此過濾器忽略此檢視中的匹配未設定、零值、預設和IPv6行。

步驟3.比較邏輯TLOC與中心會話所有權

檢查傳送到FTM的TLOC狀態。比較兩個對等體的系統IP、顏色、公共IP地址和公共UDP埠。

<#root>

```
show platform software sdwan ttmd tlocs
```

運行以下命令以比較轉發表管理器(FTM)、BFD和平台會話記錄：

<#root>

```
show sdwan ftm bfd tloc | include 10.0.0.32
```

```
show sdwan ftm bfd tloc | include 10.0.0.33
```

```
show sdwan bfd sessions | include 10.0.0.32

show sdwan bfd sessions | include 10.0.0.33

show platform software sdwan session dstip 203.0.113.10

show platform software sdwan session remote-sysip 10.0.0.32 detail

show platform software sdwan session remote-sysip 10.0.0.33 detail
```

此示例顯示具有規範化識別符號的模式。為了清楚起見，列標籤被新增到過濾的FTM行；它們不是過濾命令輸出的一部分：

<#root>

```
Hub# show sdwan ftm bfd tloc | include 10.0.0.32

System IP  Remote color     Encap  TLOC index  State
10.0.0.32  public-internet  IPSEC  32827       DOWN

Hub# show sdwan ftm bfd tloc | include 10.0.0.33

System IP  Remote color     Encap  TLOC index  State
10.0.0.33  public-internet  IPSEC  32828       DOWN

Hub# show platform software sdwan session dstip 203.0.113.10

RemoteSysIP Color        Proto SrcIp         SPort DstIp        DPort DPubIp       PPort BFD-LD TUN-ID
10.0.0.32   mpls         IPSEC 192.168.9.42  12346 203.0.113.10 12346 203.0.113.10 12346 20184  798
10.0.0.32   biz-internet IPSEC 192.168.10.42 12346 203.0.113.10 12346 203.0.113.10 12346 20183  799
```

OMP和FTM保留兩個邏輯對等體標識，而此會話查詢僅顯示共用目標的分支A。輻條A也具有下行FTM狀態；平台會話表中的狀態並不表示健康的路徑。FTM TLOC索引與作業階段表中的BFD本機鑑別器(BFD-LD)不同。此模式是調查各層所有權的原因之一。僅缺少CLI行無法建立資料包丟失。

在此表中，Color代表本地傳輸；在詳細檢視中使用Remote color以標識遠端TLOC。比較DstIp和DPubIp:獲知的實際目標可能與與會話關聯的公共終結點不同。如果僅目標過濾器不再匹配獲知的地址，則使用對等體特定檢視。

Invalid next hop、SA識別符號0或In HW:FALSE提供其他證據，而不是唯一簽名。這些欄位也可能

會在普通安裝或襯底故障期間出現。

步驟4.檢驗NAT網關的實際工作情況

請向NAT或服務提供商操作員詢問包含以下欄位的併發UDP轉換記錄：

Spoke	Inside source	Translated source	External destination
A	192.168.11.11:12346	203.0.113.10:12346	198.51.100.2:12346
B	192.168.12.12:12346	203.0.113.10:12346	198.51.100.3:12346
A	192.168.11.11:12346	203.0.113.10:12346	198.51.100.42:12346
B	192.168.12.12:12346	203.0.113.10:45678	198.51.100.42:12346

這是一個示例性的轉換表。對您的NAT平台使用等效的診斷命令。在Cisco IOS XE NAT網關上，從：

<#root>

show ip nat translations | include 203.0.113.10

保留內部源列和目標列。僅包含已轉換的源的清單無法顯示為何對不同的vBonds或哪個分支擁有中心對映重複使用有效。

捕獲vBonds和集線器的NAT之前和之後受影響的UDP流。保留完整的資料包長度，以便不會截斷VCONTROL尾部。使用與TAC同意的受限交換連線埠分析器(SPAN)或嵌入式封包擷取(EPC)收集。比較捕獲點之間的相同流；不要從非同步捕獲時鐘推斷延遲。

步驟5.檢查Wireshark中的VCONTROL

對於此處介紹的IPv4 BFD/VCONTROL格式，請使用附錄中的Lua解碼器。將代碼另存為sdwan_vctrl.lua，與您的捕獲儲存在同一個資料夾中。此診斷解碼器顯示可見欄位；它不會解密ESP或驗證身份驗證。其作用域是完整的、具有預期的BFD/VCONTROL標誌和尾部結構的非巢狀IPv4/UDP資料包。

從包含解碼器和捕獲的資料夾運行Wireshark命令：

<#root>

**wireshark -n **

```
  -X lua_script:sdwan_vctrl.lua \

  -d udp.port==12346,sdwan_vctrl \

  -d udp.port==45678,sdwan_vctrl \

  -r hub.pcap
```

將示例埠替換為捕獲中的埠。在Windows或macOS上，如果Wireshark執行檔不在PATH中，請使用它的完整路徑。

或者，在Wireshark啟動時加載Lua指令碼，選擇相關的UDP數據包，然後導航到分析>解碼為可。將適用的源和目標UDP埠條目分配到SDWAN_VCTRL/SD-WAN VCTRL(IPv4)。 另一個連線埠上的顯式UDPENCAP專案可以優先於此解碼器。將更改應用到此分析會話。

應用此顯示篩選器：

```
sdwan_vctrl && ip.addr == 203.0.113.10
```

展開SD-WAN VCTRL > Visible VCONTROL尾部並進行比較：

```
Outer IPv4 source:       203.0.113.10
Outer UDP source port:   45678
Carried source IPv4:     203.0.113.10
Carried source UDP port: 12346
Carried destination:     198.51.100.42:12346
```

這些示例值描述資料平面學習完成之前的初始隧道建立。它們將B的實際中心對映與其承載端點一起顯示。NAT會修改外部標頭；它不會重寫此尾部中的終端資訊。僅此不相符本身並不說明錯誤。

運行TShark命令進行精簡匯出：

<#root>

```
tshark -n -X lua_script:sdwan_vctrl.lua \

  -d udp.port==12346,sdwan_vctrl \
```

```
  -d udp.port==45678,sdwan_vctrl \

  -r hub.pcap -Y sdwan_vctrl -T fields \

  -e frame.number -e ip.src -e udp.srcport -e ip.dst -e udp.dstport \

  -e sdwan_vctrl.spi \

  -e sdwan_vctrl.src_ip -e sdwan_vctrl.src_port \

  -e sdwan_vctrl.dst_ip -e sdwan_vctrl.dst_port
```

若沒有自訂解碼器，此處所述的IPv4格式會在UDP負載的結尾處使用這個17位元組型別長度值(TLV)標尾。鏈路層填充在UDP負載之外：

```
81 00 0f cb 00 71 0a 30 3a c6 33 64 2a 30 3a 00 11
|  |     |           |     |           |     |
|  |     |           |     |           |     +-- Complete trailer length: 17
|  |     |           |     |           +-------- Destination port: 12346
|  |     |           |     +-------------------- Destination: 198.51.100.42
|  |     |           +-------------------------- Source port: 12346
|  |     +-------------------------------------- Source: 203.0.113.10
|  +-------------------------------------------- TLV length: 15
+----------------------------------------------- Type: 0x81
```

不要將此固定佈局應用於IPv6、其他控制格式、截斷的資料包或任意加密的資料。空的解碼器過濾器可能表示資料包超出其支援的格式。可讀的源端點也不是經過身份驗證的系統IP標籤。

附註：Wireshark中的通用ESP序列警告不是路由器反重播診斷。在得出驗證或所有權結論之前，請將資料包與路由器計數器和日誌關聯起來。

步驟6.確認受影響的路徑並保留證據

在集線器上，圍繞觀察到的故障取兩個QuantumFlow處理器(QFP)計數器樣本：

<#root>

show clock detail

```
show platform hardware qfp active statistics drop | include Ipsec

show sdwan bfd sessions | include 10.0.0.32

show sdwan bfd sessions | include 10.0.0.33
```

使用計數器差異而不是絕對合計。聚合IPsec丟棄可能有其他原因。確認資料包到達受影響的傳輸，並將其與對等體、端點、BFD鑑別器、隧道、SA和事件時間關聯。

為兩個OMP快照、分支本地屬性和控制元件、兩個對等體的中心會話詳細資訊、BFD狀態、轉換記錄、限定捕獲和軟體版本提供TAC。如果可用，請包含相關管理技術和連線/撤銷歷史記錄。避免在一個大型中心位置重複收集整個表。

單獨測試服務可達性，並記錄實際選擇的傳輸。零秒BFD啟動指示不是持續恢復。

變通辦法和限制

與Cisco TAC和NAT操作員一起評估這些緩解選項。限制涉及到達公共集線器的重複通告端點；這並不意味著對稱NAT、共用公共地址或重複私有編址通常不受支援。恢復程式和降低效率取決於部署。

使用具有唯一分配的穩定獨立於端點的對映

圖示序列的一個NAT端預防選項是為每個不同的分支傳輸端點提供跨vBond、控制器和集線器目標的穩定、唯一的轉換UDP端點。請求跨分支的端點獨立性和唯一性。在NAT網關故障切換或狀態重建之後，驗證轉換記錄和捕獲的結果。

例如，A可以始終使用203.0.113.10:4001，而B始終使用203.0.113.10:4002。靜態轉換或合適的分配策略可以提供此行為，具體取決於NAT平台和訪問設計。

與端點無關的對映不需要無限制的入站訪問。保留所需的防火牆控制。NAT策略糾正不會自動刪除以前通告或程式設計的會話狀態；與TAC協調新的發現週期和恢復。

禁用不同分支之間的埠重疊

如果支援，請在相關SD-WAN分支中唯一保留轉換後的UDP終端。不要僅僅因為目的地不同而重複使用它們。這將直接刪除前面顯示的同時重複vBond對映，即使NAT網關保留一些與目標相關的行

為也是如此。

該設定可能會佔用更多埠或需要額外的公有地址。它本身不會使每個分支的對映獨立於端點，並且它不會在後續端點重新分配後解析過時的接收器狀態。

對於多個NAT階段或冗餘NAT網關，檢查最終網際網路邊界的可見分配。一個NAT例項內的唯一性不會在共用同一公有地址的其他例項間建立唯一性。

對小型受控組使用埠偏移

port-offset命令提供值0到19。例如，分支A可以保留偏移0，分支B可以使用偏移1。在分支B上運行以下配置命令：

<#root>

```
Spoke-B# config-transaction

Spoke-B(config)# system

Spoke-B(config-system)# port-offset 1

Spoke-B(config-system)# commit

Spoke-B(config-system)# end

Spoke-B# show sdwan control local-properties
```

更改後檢驗活動源埠和轉換埠。對此系統設定的更改可以重建跨傳輸的控制和資料連線。這不是無中斷的診斷步驟。

這20個偏移提供了20個不同的基本埠組，偏移為0是一個選擇。它們不是一個公共IP後面的20台SD-WAN路由器的通用限制。此特定的解決方法僅提供20個唯一的偏移選項，並要求NAT網關保留這些選項並區分它們。當重複使用偏移時，它作為唯一性方案失敗。埠跳躍不會新增更多偏移標識。

例如，124台路由器不能都在一個共用地址後接收唯一偏移。每個公共地址組最多包含20台路由器的僅偏移方案至少需要七個組。此演算法不是容量建議或替代對NAT行為的驗證。重寫或重疊轉換埠的NAT網關即使使用更少的路由器，也會使方案失敗。

禁用源埠保留或啟用隨機分配

沒有保留偏好的策略可以減少許多輻條接收到：12346的傾向於不同的vBonds。隨機分配可以在更大的埠池上分發這些對映。

然而，僅改變並不能保證避免衝突。隨機分配器仍可以跨目標重複使用埠，更改到集線器的對映，或在保留舊集線器狀態時重新分配已過期的端點。驗證在使用者和目標之間分配是否唯一。僅隨機埠不能建立唯一性。

與其操作員一起檢查NAT網關上的源埠保留和分配設定。適用的配置取決於NAT平台；使用轉換記錄和資料包捕獲驗證到vBonds和集線器的結果對映。

轉換後的埠可能不在原始SD-WAN基本埠範圍之內。檢查防火牆規則，使其不會僅僅因為源埠更改而拒絕合法轉換的流量。

單獨的公有地址或保留埠塊

專用轉換地址或每個分支保留的非重疊埠塊可以為不同的活動分支提供不同的通告端點。策略必須在發現和集線器路徑以及冗餘NAT節點間一致應用。可能需要其他地址空間和提供商支援。對映停用後的動態重複使用仍需要正確的中心會話生命週期管理。

保留備用傳輸並協調恢復

在調查受影響的Internet路徑時，經過驗證的MPLS或其他合格路徑可以保留服務。阻止共用NAT地址的底層訪問控制清單(ACL)僅提供包含功能：它可以刪除該地址後面每個分支的Internet冗餘，並且不會自動撤銷其OMP通告。

控制清除、介面重置、NAT狀態清除或集線器重新載入可以臨時重新建立狀態。沒有保證防止再次發生。請勿將寬清除作為第一個診斷步驟。保留證據，儘可能更正分配條件，並與TAC商定最小恢復操作。驗證恢復路徑上持續的BFD Up和雙向流量。

相關軟體缺陷

思科錯誤 ID	與本條相關的範圍
CSCww45867	不同對等體通告同一公共TLOC端點時的中心會話所有許可權制的文檔。此記錄跟蹤文檔更新，而不是軟體更正。

思科錯誤 ID	與本條相關的範圍
CSCwx12986	自動埠跳躍/NAT學習序列可以在公共TLOC欄位中保留私有元組。如果分支機構重複使用相同的專用IP：埠，則不正確的公共終端可以在對等體之間匹配。糾正此製造者缺陷不會阻止有效的轉換公共埠重複使用。
CSCwx48929	當發現返回到同一個vBond時，NAT分類可能會錯誤地變成E。正確的分類不會阻止有效的different-vBond port-reuse場景。

思科錯誤ID CSCwx12986和思科錯誤ID CSCwx48929的更正不能保證唯一通告的公共端點，且自身也不能消除此衝突情況。關閉Cisco錯誤ID CSCww45867文檔記錄不會改變軟體行為。通過Cisco TAC確認適用的限制和緩解。

附錄:解碼IPv4 VCONTROL報尾

將此代碼另存為sdwan_vctrl.lua。診斷解碼器不對資料包進行身份驗證或解密其負載。它使用sdwan_vctrl顯示過濾器，並註冊一個顯式Decode As選項。資料包捕獲保持不變。

```
-- Cisco SD-WAN IPv4 VCONTROL trailer decoder.
-- Explicit UDP "Decode As" only; does not decrypt ESP.
-- Scope: complete ordinary IPv4/UDP packets, one IP/UDP layer.

local p = Proto("sdwan_vctrl", "SD-WAN VCTRL (IPv4)")

local f = {
    spi       = ProtoField.uint32("sdwan_vctrl.spi",
                    "Wire SPI including control flags", base.HEX),
    sequence  = ProtoField.uint32("sdwan_vctrl.sequence",
                    "ESP sequence number", base.DEC),
    type      = ProtoField.uint8("sdwan_vctrl.type",
                    "Trailer type", base.HEX),
    tlv_len   = ProtoField.uint16("sdwan_vctrl.tlv_len",
                    "TLV length", base.DEC),
    src_ip    = ProtoField.ipv4("sdwan_vctrl.src_ip",
                    "Carried source IPv4"),
    src_port  = ProtoField.uint16("sdwan_vctrl.src_port",
                    "Carried source UDP port", base.DEC),
    dst_ip    = ProtoField.ipv4("sdwan_vctrl.dst_ip",
                    "Carried destination IPv4"),
    dst_port  = ProtoField.uint16("sdwan_vctrl.dst_port",
                    "Carried destination UDP port", base.DEC),
    total_len = ProtoField.uint16("sdwan_vctrl.total_len",
                    "Complete trailer length", base.DEC)
}
p.fields = f

-- Field extractors must be created outside the dissector.
local get_udp_length = Field.new("udp.length")
local get_ip_version = Field.new("ip.version")
local get_ip_proto   = Field.new("ip.proto")
```

```
function p.dissector(tvb, pinfo, tree)
    local lengths = { get_udp_length() }
    local versions = { get_ip_version() }
    local protocols = { get_ip_proto() }

    -- Deliberately skip nested/tunnelled protocol stacks.
    if #lengths ~= 1 or #versions ~= 1 or #protocols ~= 1 then
        return 0
    end
    if tonumber(versions[1].value) ~= 4 or
       tonumber(protocols[1].value) ~= 17 then
        return 0
    end

    -- UDP length includes its 8-byte header.
    local n = tonumber(lengths[1].value) - 8

    -- Require the full declared payload, not a truncated fragment.
    if n < 25 or tvb:reported_len() ~= n or tvb:len() ~= n then
        return 0
    end

    -- Exact BFD + VCTRL control-bit combination.
    local spi = tvb(0, 4):uint()
    if math.floor(spi / 0x10000000) ~= 0xA then
        return 0
    end

    -- Trailer is at the end of UDP payload, not Ethernet frame.
    local o = n - 17

    if tvb(o, 1):uint() ~= 0x81 or
       tvb(o + 1, 2):uint() ~= 15 or
       tvb(o + 15, 2):uint() ~= 17 then
        return 0
    end

    local root = tree:add(p, tvb())
    root:add(f.spi,      tvb(0, 4))
    root:add(f.sequence, tvb(4, 4))

    local trailer = root:add(tvb(o, 17),
                             "Visible VCONTROL trailer")
    trailer:add(f.type,      tvb(o,      1))
    trailer:add(f.tlv_len,   tvb(o + 1,  2))
    trailer:add(f.src_ip,    tvb(o + 3,  4))
    trailer:add(f.src_port,  tvb(o + 7,  2))
    trailer:add(f.dst_ip,    tvb(o + 9,  4))
    trailer:add(f.dst_port,  tvb(o + 13, 2))
    trailer:add(f.total_len, tvb(o + 15, 2))

    pinfo.cols.protocol = "SDWAN-VCTRL"
    return n
end

DissectorTable.get("udp.port"):add_for_decode_as(p)
```

相關資訊

- RFC 7857，第3節：埠重疊行為
- RFC 4787:單播UDP的NAT行為要求
- RFC 5737:為文檔保留的IPv4地址塊
- Cisco Catalyst SD-WAN設計手冊
- Cisco IOS XE Catalyst SD-WAN系統命令：port-offset
- Cisco SD-WAN埠偏移配置
- Wireshark命令列參考
- TShark命令列參考
- 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）。