排除網路地址轉換故障，常見問題

目錄

簡介

本檔案介紹網路位址轉譯(NAT)路由器程式的工作方式，並提供一些常見問題的答案。

通用NAT

問：什麼是NAT?

A.網路位址轉譯(NAT)是專為IP位址保留而設計的。它允許使用未註冊IP地址的專用IP網路連線到Internet。NAT在路由器上運行，通常是在您將兩個網路連線到一起時，它將內部網路中的私有（非全域性唯一）地址轉換為合法地址，然後將資料包轉發到另一個網路。

作為此功能的一部分，可以配置NAT以僅向外部世界通告整個網路的一個地址。這有效地隱藏了該地址後面的整個內部網路，從而提供了額外的安全性。NAT提供安全和地址保護的雙重功能，通常在遠端訪問環境中實施。

問： NAT如何工作？

答：基本上，NAT允許單個裝置（如路由器）作為網際網路（或公共網路）和本地網路（或專用網路）之間的代理，這意味著只需要一個唯一的IP地址代表整個電腦組到其網路之外的任何裝置。

問：如何配置NAT?

答：要配置傳統NAT，您需要在路由器上至少建立一個介面（NAT外部）和路由器上的另一個介面（NAT內部），並且需要為資料包報頭中的IP地址(以及負載（如果需要）建立一組轉換規則，並且需要配置它們。要配置Nat虛擬介面(NVI)，您需要至少一個介面配置了NAT啟用以及上述相同的一組規則。

有關詳細資訊，請參閱Cisco IOS IP編址服務配置指南或其有關配置NAT虛擬介面的部分。

問：Cisco IOS®軟體和Cisco自適應安全裝置(ASA)實施NAT的主要區別是什麼？

A.基於Cisco IOS軟體的NAT與Cisco ASA中的NAT功能沒有根本區別。主要區別包括實施和設計要求中支援的不同流量型別。有關在Cisco ASA裝置上配置NAT的詳細資訊（包括支援的流量型別），請參閱NAT配置示例。

問：Cisco IOS NAT可用在哪個Cisco路由硬體上？如何訂購硬體？

A.Cisco Feature Navigator工具允許客戶識別功能(NAT)，並找到該Cisco IOS軟體功能的可用版本和硬體版本。請參閱思科功能導航以使用此工具。

問：NAT是在路由之前還是之後發生的？

A. NAT處理事務的順序取決於資料包是從內部網路傳輸到外部網路還是從外部網路傳輸到內部網路。路由後發生內部到外部轉換，路由前發生外部到內部轉換。有關詳細資訊，請參閱NAT操作順序。

問：NAT能否在公共無線LAN環境中部署？

是的。NAT — 靜態IP支援功能為具有靜態IP地址的使用者提供支援，並使這些使用者能夠在公共無線LAN環境中建立IP會話。

問：NAT是否對內部網路上的伺服器執行TCP負載均衡？

答：是。使用NAT，可以在內部網路上建立虛擬主機，以協調實際主機之間的負載平衡。

問：是否可以限制NAT轉換的數量？

是的。速率限制NAT轉換功能可以限制路由器上最大併發NAT運算元。這樣，使用者就可以更好地控制NAT地址的使用方式，速率限制NAT轉換功能可用於限制病毒、蠕蟲和拒絕服務攻擊的影響。

問：如何為NAT使用的IP子網或地址獲取或傳播路由？

A.如果出現以下情況，則會獲知NAT建立的IP地址的路由：

- 內部全域性地址池源自下一跳路由器的子網。
- 靜態路由條目在下一跳路由器中配置，並在路由網路中重新分配。

當內部全域性地址與本地介面匹配時，NAT會安裝IP別名和ARP條目，在這種情況下，路由器canproxy-arp會為這些地址新增地址。如果不需要此行為，請使用no-alias關鍵字。

配置NAT池時，可以使用add-route選項進行自動路由注入。

問：Cisco IOS NAT支援多少個併發NAT會話？

A.NAT會話限制由路由器中的可用DRAM數量限定。每個NAT轉換在DRAM中消耗大約312個位元組。因此，10,000次轉換（比一般情況下在單個路由器上處理的要多）會消耗大約3 MB。因此，典型的路由硬體擁有足夠的記憶體來支援數千個NAT轉換。但是，也建議驗證平台規格。

問：使用Cisco IOS NAT可以預期哪種路由效能？

答：Cisco IOS NAT支援Cisco Express Forwarding(CEF)交換、快速交換和進程交換。對於12.4T版本及更高版本，不再支援快速交換路徑。對於Cat6k平台，交換順序為Netflow（硬體交換路徑）、CEF、進程路徑。

效能取決於以下幾個因素：

- 應用型別及其流量型別

- 是否嵌入IP地址
- 交換和檢查多個報文
- 需要來源連線埠
- 轉換數
- 當時運行的其他應用程式
- 硬體和處理器的型別

問：Cisco IOS NAT能否應用於子介面？

是的。源和/或目標NAT轉換可應用於具有IP地址的任何介面或子介面（包括撥號器介面）。無法使用無線虛擬介面配置NAT。無線虛擬介面在寫入NVRAM時不存在。因此，重新啟動後，路由器會丟失無線虛擬介面上的NAT配置。

問：Cisco IOS NAT是否可與熱備份路由器協定(HSRP)配合使用，以提供到ISP的冗餘鏈路？

是的。NAT確實提供HSRP冗餘。但是它不同於SNAT（有狀態NAT）。使用HSRP的NAT是無狀態系統。發生故障時，不會維護當前會話。在靜態NAT配置期間（當資料包與任何STATIC規則配置都不匹配時），資料包將通過傳送而不進行任何轉換。

問：Cisco IOS NAT是否支援幀中繼介面上的入站轉換？它是否支援乙太網端的出站轉換？

是的。封裝對NAT沒有影響。如果介面上有IP地址，並且介面為NAT內部或NAT外部，則可以執行NAT。NAT必須有一個內部和一個外部，才能發揮作用。如果使用NVI，必須至少有一個啟用NAT的介面。有關詳細資訊，請參閱前一個問題：如何配置NAT?。

問：一台啟用NAT的路由器是否允許某些使用者使用NAT，以及允許同一乙太網介面上的其他使用者繼續使用自己的IP地址？

是的。這可以通過使用描述需要NAT的一組主機或網路的訪問清單來實現。同一主機上的所有會話都可以轉換，也可以通過路由器而不進行轉換。

訪問清單、擴展訪問清單和路由對映可用於定義IP裝置轉換的方式。必須始終指定網路地址和相應的子網掩碼。keywordanywhere不能用來代替網路地址或子網掩碼。使用靜態NAT配置時，當資料包與任何靜態規則配置不匹配時，可以傳送資料包，而無需任何轉換。

問：配置PAT（過載）時，每個內部全域性IP地址可建立的最大轉換數是多少？

A.PAT（過載）將每個全域性IP地址的可用埠分為三個範圍：0-511、512-1023和1024-65535。PAT為每個UDP或TCP會話分配一個唯一的源埠。它會嘗試為原始請求分配相同的埠值，但如果原始源埠已被使用，它會開始從特定埠範圍的開始進行掃描，以查詢第一個可用埠，並將其分配給會話。

PAT是如何工作的？

A.PAT使用一個全域性IP地址或多個地址。

具有一個IP地址表的PAT

條件	說明
1	NAT/PAT檢查流量並將其與轉換規則匹配。
2	規則與PAT配置匹配。
3	如果PAT知道流量型別，並且該流量型別具有「它協商的一組特定埠或埠」可以使用，則PAT會將這些
4	如果沒有特殊埠要求的會話嘗試連線出去，則PAT會轉換IP源地址並檢查源埠（例如433）的可用性。
5	如果請求的源埠可用，則PAT分配源埠，會話繼續。
6	如果請求的源埠不可用，則PAT從相關組的開頭開始搜尋（TCP或UDP應用程式從1開始，ICMP從0開
7	如果連線埠可用，則會分配該連線埠，且作業階段會繼續。
8	如果沒有可用的連線埠，則封包會遭捨棄。

註：對於傳輸控制協定(TCP)和使用者資料包協定(UDP)，範圍是：1-511、512-1023、1024-65535。對於網際網路控制訊息通訊協定(ICMP)，第一個群組從0開始。

具有多個IP地址的PAT

條件	說明
1-7	前七個條件與單個IP地址相同。
8	如果在第一個IP地址上的相關組中沒有可用的埠，NAT將轉至池中的下一個IP地址，並嘗試分配請求的
9	如果請求的源埠可用，NAT將分配源埠，會話繼續進行。
10	如果請求的源埠不可用，NAT從相關組的開頭開始搜尋（TCP或UDP應用程式從1開始，ICMP從0開始
11	如果連線埠可用，則會分配該連線埠，且作業階段會繼續。
12	如果沒有可用的埠，則丟棄資料包，除非池中有其他IP地址。

問：什麼是NAT IP池？

A.NAT IP池是根據需要分配用於NAT轉換的IP地址範圍。要定義池，使用配置命令：

```
ip nat pool <name> <start-ip> <end-ip> {netmask <netmask> | prefix-length <prefix-length>} [type
{rotary}]
```

範例 1

下一個示例將從網路192.168.1.0或192.168.2.0地址的內部主機轉換為全球唯一的10.69.233.208/28網路：

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

範例 2

在下一個示例中，目標是定義虛擬地址，連線分佈在一組實際主機中。該池定義實際主機的地址。訪問清單定義虛擬地址。如果不存在轉換，則來自串列介面0（外部介面）的TCP資料包（其目標與

訪問清單匹配）將轉換為池中的地址。

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
 ip address 192.168.15.129 255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address 192.168.15.17 255.255.255.240
 ip nat inside
!
access-list 2 permit 192.168.15.1
```

問：可配置NAT IP池(ip nat pool "name")的最大數量是多少？

A.在實際使用中，可配置IP池的最大數量受特定路由器中可用DRAM數量的限制。（思科建議您配置池大小255。）每個池不得超過16位。在12.4(11)T及更高版本中，Cisco IOS引入了CCE（通用分類引擎）。這樣，NAT最多只能有255個池。

問：與NAT池上的ACL相比，路由對映有何優勢？

A.路由對映可保護不需要的外部使用者訪問內部使用者/伺服器。它還能夠根據規則將單個內部IP地址對映到不同的內部全域性地址。有關詳細資訊，請參閱使用路由對映支援多個池的NAT支援。

問：在NAT環境中，哪個IP地址是「重疊的」？

A.IP地址重疊是指兩個要互聯的位置使用同一IP地址方案的情況。這種情況並非罕見，通常發生在公司合併或被收購時。如果沒有特殊支援，兩個位置將無法連線和建立會話。重疊的IP地址可以是分配給其他公司的公有地址、分配給其他公司的私有地址，或者可以來自RFC 1918中定義的私有地址範圍。

私有IP地址不可路由，需要NAT轉換才能連線到外部世界。 此解決方案涉及從外部到內部的域名系統(DNS)名稱查詢響應的攔截、外部地址的轉換設定，並且DNS響應需要在轉發到內部主機之前修復。 NAT裝置的兩端都需要有DNS伺服器，才能解析要在兩個網路之間建立連線的使用者。

NAT能夠檢查並執行DNSA和PTR記錄內容的地址轉換，如在重疊網路中使用NAT所示。

問：什麼是靜態NAT轉換？

A.靜態NAT轉換在本地地址和全域性地址之間具有一對一對映。使用者還可以配置到埠級別的靜態地址轉換，並將IP地址的其餘部分用於其他轉換。當您執行連線埠位址轉譯(PAT)時，通常會發生這種情況。

下一個示例展示如何配置路由對映以允許靜態NAT的外部到內部轉換：

```
ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.1 0.0.0.127
route-map R1 permit 10
 match ip address ACL-A
```

問：術語*NATOverloading*是什麼意思？這是哪個PAT?

是的。NAT過載是PAT，它涉及使用包含一個或多個地址範圍的池，或將介面IP地址與埠結合使用。過載時，將建立完全擴展轉換。這是一個包含IP地址和源/目標埠資訊的轉換表條目，通常稱為PAT或過載。

PAT（或過載）是Cisco IOS NAT的一項功能，用於將*內部*（內部本地）私有地址轉換為一個或多個*外部*（內部全域性，通常註冊）IP地址。每個轉換上的唯一源埠號用於區分會話。

問：什麼是動態NAT轉換？

A. 在動態NAT轉換中，使用者可以建立本地地址和全域性地址之間的動態對映。定義要轉換的本地地址以及分配全域性地址的地址池或介面IP地址時，以及將兩者關聯時，即完成動態對映。

什麼是ALG?

A.ALG是一種應用層網關(ALG)。NAT對應用資料流中不含源IP地址和/或目標IP地址的任何傳輸控制協定/使用者資料包協定(TCP/UDP)流量執行轉換服務。

這些協定包括FTP、HTTP、SKINNY、H232、DNS、RAS、SIP、TFTP、telnet、archie、finger、NTP、NFS、rlogin、rsh、rcp。在負載中嵌入IP地址資訊的特定協定需要應用級網關(ALG)的支援。

有關詳細資訊，請參閱將應用級網關與NAT結合使用。

問：是否可以使用靜態NAT轉換和動態NAT轉換構建配置？

是的。但是，同一IP地址不能用於NAT靜態配置或用於NAT動態配置的池中。所有公有IP地址必須是唯一的。請注意，靜態轉換中使用的全域性地址不會自動排除為包含這些相同全域性地址的動態池。必須建立動態池以排除靜態條目分配的地址。有關詳細資訊，請參閱同時配置靜態和動態NAT。

問：當通過NAT路由器執行traceroute時，traceroute必須顯示NAT全域性地址還是必須洩漏NAT本地地址？

A.外部的Traceroute必須始終返回全域性地址。

問： PAT如何分配埠？

A.NAT引入了額外的埠功能：全範圍和埠對映。

- 全範圍允許NAT使用所有埠，而不管其預設埠範圍如何。
- Port-map允許NAT為特定應用保留使用者定義的埠範圍。

有關詳細資訊，請參閱使用者定義的PAT源端口範圍。

在12.4(20)T2之後，NAT為L3/L4和對稱埠引入了埠隨機化。

- 埠隨機化允許NAT為源埠請求隨機選擇任何全域性埠。

- 對稱埠允許NAT支*持點獨立*。

問： IP分段和TCP分段有何區別？

A.IP分段發生在第3層(IP);TCP分段發生在第4層(TCP)。當大於介面最大傳輸單位(MTU)的封包從此介面傳送出去時，就會發生IP分段。這些資料包從介面傳送出去時，必須將其分段或丟棄。如果Don't Fragment (DF) 封包的IP標頭中未設定位元，因此封包可以分段。如果在封包的IP標頭中設定了DF位元，則封包會遭到捨棄，而ICMP錯誤訊息會指出傳回傳送者的下一個躍點的MTU值。IP封包的所有片段在IP標頭中都有相同的識別碼，這允許最終接收者將片段重組為原始IP封包。如需詳細資訊，請參閱使用GRE和IPsec解決IP分段、MTU、MSS和PMTUD問題。

TCP分段在終端站上的應用程式傳送資料時發生。應用資料被分解為TCP認為要傳送的最大小的資料塊。從TCP傳輸到IP的這一資料單位稱為資料段。TCP資料段在IP資料包中傳送。這些IP資料包在透過網路時可能會成為IP片段，且遇到比其可容納的更低MTU連結。

TCP可以首先將此資料分段為TCP區段（根據TCP MSS值），然後增加TCP標頭並將此TCP區段傳遞到IP。然後IP可以新增IP報頭以將資料包傳送到遠端終端主機。如果具有TCP區段的IP封包大於TCP主機之間路徑上傳出介面的IP MTU，則IP可以將IP/TCP封包分段以適合大小。這些IP封包片段可以透過IP層在遠端主機上進行重組，且完整的TCP區段（最初傳送的）可以傳遞到TCP層。TCP層並不知道IP在傳輸過程中將封包分段。

NAT支援IP片段，但不支援TCP區段。

問：NAT是否支援IP分段和TCP分段順序錯誤？

A.NAT僅支援順序錯亂的IP片段，因為**ofip虛擬重組**。

問：如何調試IP分段和TCP分段？

A.NAT對IP分段和TCP分段使用相同的調試CLI:**debug ip nat frag**。

問：是否存在受支援的NAT MIB?

答案：編號沒有支援的NAT MIB，也不支援CISCO-IETF-NAT-MIB。

問：什麼是*TCP超時*？它與NAT TCP計時器有何關係？

A.如果三次握手沒有完成，並且NAT看到了TCP資料包，則NAT可以啟動60秒計時器。當三次握手完成後，NAT預設使用24小時計時器來執行NAT條目。如果終端主機傳送RESET，NAT會將預設計時器從24小時更改為60秒。對於FIN，NAT在接收FIN和FIN-ACK時將預設計時器從24小時更改為60秒。

問：是否可以從NAT轉換表中將NAT轉換的時間更改為超時？

是的。您可以更改所有條目或不同型別NAT轉換的NAT超時值（例如udp-timeout、dns-timeout、tcp-timeout、finrst-timeout、icmp-timeout、pptp-timeout、syn-timeout、port-timeout和arp-ping-timeout）。

問：如何將額外的位元組附加到每個LDAP回複資料包時，如何停止輕量型目錄訪問

協定(LDAP)?

A.LDAP設定為在處理Search-Res-Entry型別的消息時新增額外的位元組（LDAP搜尋結果）。LDAP將10個位元組的搜尋結果附加到每個LDAP回複資料包。如果此10個額外位元組的資料產生資料包，並超過網路中的最大傳輸單元(MTU)，則該資料包將被丟棄。在這種情況下，Cisco建議您使用**CLIno ip nat service append-ldap-search-rescommand關閉此LDAP行為，以便傳送和接收資料包。**

問： NAT盒上的內部全域性/外部本地IP地址的路由建議是什麼？

A.必須在NAT配置框上為NAT-NVI等功能的內部全域性IP地址指定路由。同樣，還必須在NAT框中為外部本地IP地址指定路由。在這種情況下，來自具有外部靜態規則的in-to-out方向的任何資料包都需要這種路由。在這種情況下，當它為IG/OL提供路由時，還必須配置下一跳IP地址。如果找不到下一跳配置，則這被視為配置錯誤，會導致未定義的行為。

NVI-NAT僅存在於輸出功能路徑中。如果您直接將子網與NAT-NVI或該框上配置的外部NAT轉換規則相連，則在這些情況下，您需要為下一跳提供一個虛擬下一跳IP地址和一個關聯的ARP。底層基礎架構需要此過程才能將資料包傳遞到NAT以進行轉換。

問：Cisco IOS NAT是否支援帶有*log*關鍵字的ACL?

A.配置Cisco IOS NAT進行動態NAT轉換時，會使用ACL來識別可轉換的資料包。當前的NAT體系結構不支援帶有log關鍵字的ACL。

語音 — NAT

問：NAT是否支援Cisco Unified Communications Manager(CUCM)V7附帶的瘦客戶端控制協定(SCCP)v17?

A.CUCM 7和CUCM 7的所有預設電話負載都支援SCCPv17。電話註冊時，使用的SCCP版本由CUCM和電話之間的最高通用版本確定。

NAT尚不支援SCCP v17。在實施SCCP v17的NAT支援之前，必須將韌體降級到版本8-3-5或更低版本，以便協商SCCP v16。只要使用SCCP v16,CUCM6就無法在任何電話負載上遇到NAT問題。Cisco IOS當前不支援SCCP版本17。

問： NAT支援哪些CUCM /SCCP/韌體載入版本？

A.NAT支援CUCM 6.x版和更早版本。這些CUCM版本以支援SCCP v15（或更低版本）的預設8.3.x（或更低版本）電話韌體載入發佈。

NAT不支援CUCM 7.x版或更高版本。這些CUCM版本以支援SCCP v17（或更高版本）的預設8.4.x電話韌體載入發佈。

如果使用CUCM 7.x或更高版本，則必須在CUCM TFTP伺服器上安裝舊的韌體負載，以便電話使用SCCP v15或更低版本的韌體負載，以獲得NAT支援。

問：什麼是RTP和RTCP的服務提供商PAT埠分配增強功能？

答：RTP和RTCP的服務提供商PAT埠分配增強功能可確保對SIP、H.323和Skinny語音呼叫進行分配。用於RTP流的埠號是偶數埠號，而RTCP流是下一個奇數埠號。埠號將轉換為指定範圍內的一個符合RFC-1889的埠號。如果呼叫的埠號在此範圍內，則可能導致PAT轉換到此範圍內的另一個埠號。同樣，此範圍之外的埠號的PAT轉換也不能導致到給定範圍內的某個號碼的轉換。

問：什麼是會話初始協定(SIP)，是否可以使用NAT路由SIP資料包？

A.Session Initiation Protocol(SIP)是基於ASCII的應用層控制協定，可用於建立、維護和終止兩個或多個端點之間的呼叫。SIP是由Internet工程任務組(IETF)為通過IP進行多媒體會議而開發的替代協定。Cisco SIP實施使受支援的思科平台能夠通過IP網路發出語音和多媒體呼叫設定的訊號。 SIP資料包可以進行NAT轉換。

問：什麼是對會話邊界控制器(SBC)的託管NAT遍歷支援？

答：Cisco IOS Hosted NAT Traversal for SBC功能使Cisco IOS NAT SIP應用級網關(ALG)路由器能夠充當Cisco多服務IP到IP網關上的SBC，這有助於確保順利交付IP語音(VoIP)服務。

有關詳細資訊，請參閱為會話邊界控制器配置Cisco IOS託管的NAT遍歷。

問：路由器可以通過NAT處理多少個SIP、Skinny和H323呼叫？

A.NAT路由器處理的呼叫數量取決於機箱中可用的記憶體量和CPU的處理能力。

問：NAT路由器是否支援對瘦資料包和H323資料包進行TCP分段？

A.Cisco IOS-NAT支援H323的TCP分段，以及支援SKINNY的TCP分段。

問：在語音部署中使用NAT過載配置時是否有需要注意的注意事項？

是的。當您擁有NAT過載配置和語音部署時，您需要註冊消息通過NAT並為out->in建立關聯才能到達此內部裝置。內部裝置定期傳送此註冊，NAT根據信令消息中的資訊更新此針孔/關聯。

問：在語音部署中使用clear ip nat trans *命令或clear ip nat trans forcedcommand時，是否出現任何已知的問題？

答：在語音部署中，當您發出**clear ip nat trans ***命令或**clear ip nat trans** forcedcommand並具有動態NAT時，您會清除針孔/關聯，並且必須等待來自內部裝置的下一個註冊週期來重新建立該過程。思科建議不要在語音部署中使用這些clear命令。

問： NAT是否支援語音並置解決方案？

答案：編號當前不支援同地解決方案。使用NAT的下一個部署（在同一台裝置上）被視為共置解決方案：CME/DSP-Farm/SCCP/H323。

問：NVI是否支援Skinny ALG、H323 ALG和TCP SIP ALG?

答案：編號請注意，UDP SIP ALG（用於大多數部署）不受影響。

使用VRF/MPLS的NAT

問：NAT路由器能否在VRF中的同一地址空間和全域性地址空間中支援自身？目前，當我嘗試配置以下項*時，收到此警告："% similar static entry(10.1.1.1 —> 10.2.2.2)*already exists":

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED
```

A.傳統NAT支援不同VRF上的重疊地址配置。您必須使用**match-in-**vrfoption配置重疊的at規則，並在同一VRF中為通過該特定VRF的流量設定**upip nat inside/**outside。重疊支援不包括全域性路由表。

必須為不同VRF的重疊VRF靜態NAT條目新增**match-in-vrfkeyword**。但是，不能重疊全域性和vrf NAT地址。

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

問：傳統NAT是否支援VRF-Lite（從VRF到不同VRF的路由）？

答案：編號必須在不同的VRF之間使用NVI進行NAT。您可以使用傳統NAT執行從VRF到全域性的NAT或同一VRF中的NAT。

NAT NVI

問：什麼是NAT NVI?

A.NVI代表NAT虛擬介面。它允許NAT在兩個不同的VRF之間進行轉換。必須使用此解決方案來代替單臂上的網路地址轉換。

問：是否必須使用NAT NVI在全域性介面和VRF介面之間進行路由？

A.Cisco建議您對全域性NAT(ip nat inside/out)以及同一VRF中介面之間的介面使用傳統NAT進行VRF。NVI用於不同VRF之間的NAT。

問：是否支援NAT-NVI的TCP分段？

A.不支援NAT-NVI的TCP分段。

問：NVI是否支援Skinny ALG、H323 ALG和TCP SIP ALG?

答案：編號請注意，UDP SIP ALG（用於大多數部署）不受影響。

問：SNAT是否支援TCP分段？

A.SNAT不支援任何TCP ALG（例如SIP、SKINNY、H323或DNS）。因此，不支援TCP分段。但

是支援UDP SIP和DNS。

SNAT

問：什麼是狀態NAT(SNAT)?

A.SNAT允許兩個或多個網路地址轉換器充當轉換組。轉換組的一個成員處理需要轉換IP地址資訊的流量。此外，它會在活動流發生時將其通知備份轉換器。然後，備份轉換器可以使用來自活動轉換器的資訊來準備重複的轉換表條目。因此，如果活動轉換器因嚴重故障而受阻，流量可以快速切換到備份。由於使用了相同的網路地址轉換，並且先前已定義了這些轉換的狀態，因此流量會繼續。

問：SNAT是否支援TCP分段？

A.SNAT不支援任何TCP ALG（例如SIP、SKINNY、H323或DNS）。因此，不支援TCP分段。但是支援UDP SIP和DNS。

問：SNAT是否支援非對稱路由？

A. 非對稱路由在啟用NAT時支援NAT as-queuing .預設情況下，as-queueing為啟用。然而，從12.4(24)T開始， as-queuing 不再受支援。客戶必須確保正確路由封包，並且新增適當的延遲，才能讓非對稱路由正確運作。

NAT-PT（v6到v4）

問：什麼是NAT-PT?

A.NAT-PT是用於NAT的v4到v6轉換。協定轉換(NAT-PT)是IPv6-IPv4轉換機制(如RFC 2765和RFC 2766中定義)，允許僅IPv6裝置與僅IPv4裝置通訊，反之亦然。

問：思科快速轉發(CEF)路徑是否支援NAT-PT?

A.CEF路徑不支援NAT-PT。

問：NAT-PT支援哪些ALG?

A.NAT-PT支援TFTP/FTP和DNS。在NAT-PT中不支援語音和SNAT。

問： ASR 1004是否支援NAT-PT?

A.聚合服務路由器(ASR)使用NAT64。

依賴於平台的Cisco 7600/6k

問：在SX系列的Catalyst 6500上是否提供有狀態NAT(SNAT)?

A.SNAT在SX系列的Catalyst 6500上不可用。

問：6k上的硬體是否支援VRF感知NAT?

A.此平台上的硬體不支援VRF感知NAT。

問：7600和Cat6000是否支援VRF感知NAT?

答：在65xx/76xx平台上，不支援VRF感知NAT，且CLI被阻止。

注意：如果利用在虛擬環境透明模式下運行的FWSM，則可以實施設計。

依賴於平台的Cisco 850

問：12.4T版中Cisco 850是否支援瘦身NAT ALG?

答案：編號在850系列的12.4T中不支援瘦身NAT ALG。

NAT部署

問：如何實施NAT?

A.NAT允許使用未註冊IP地址的專用IP網際網路連線到Internet。NAT將內部網路中的私人(RFC1918)位址轉譯成合法的可路由位址，然後再將封包轉送到另一個網路中。

問：如何實現帶語音的NAT?

A.語音的NAT支援功能允許通過配置了網路地址轉換(NAT)的路由器的SIP嵌入式消息轉換回資料包。應用層網關(ALG)與NAT一起用於轉換語音資料包。

問：如何將NAT與MPLS VPN整合？

A.NAT與MPLS VPN的整合功能允許在單個裝置上配置多個MPLS VPN以協同工作。即使MPLS VPN都使用相同的IP編址方案，NAT也可以區別接收IP流量的MPLS VPN。此增強功能使多個MPLS VPN客戶能夠共用服務，同時可確保每個MPLS VPN彼此完全分離。

問： NAT靜態對映是否支援HSRP以實現高可用性？

A.當對配置有網路地址轉換(NAT)靜態對映且由路由器擁有的地址觸發地址解析協定(ARP)查詢時，NAT會使用ARP指向的介面上的BIA MAC地址做出響應。兩台路由器充當HSRP主用和備用路由器。必須啟用其NAT內部介面並將其配置為屬於某個組。

問：如何實施NAT NVI?

A.NAT虛擬介面(NVI)功能取消將介面配置為NAT內部或NAT外部的要求。

問：如何使用NAT實施負載均衡？

答：使用NAT可以執行兩種負載平衡：您可以對一組伺服器的入站負載進行負載均衡，以將負載分佈到伺服器上；也可以通過兩個或多個ISP將使用者流量負載均衡到網際網路。

有關出站負載平衡的詳細資訊，請參閱Cisco IOS NAT Load-Balancing for Two ISP Connections。

問：如何將NAT與IPSec結合實施？

A.有以下方面的支援 IP Security (IPSec) Encapsulating Security Payload (ESP) through NAT 和IPSec NAT透明性。

通過NAT的IPSec ESP功能通過過載或埠地址轉換(PAT)模式配置的Cisco IOS NAT裝置支援多個併發IPSec ESP隧道或連線。 IPSec NAT透明功能引入了對通過NAT或PAT點網路的IPSec流量的支援，該功能解決了NAT和IPSec之間的許多已知不相容問題。

問：如何實施NAT-PT?

A.NAT-PT（網路位址轉譯 — 通訊協定轉譯）是一種IPv6-IPv4轉譯機制，定義見RFC 2765和RFC 2766，允許僅限IPv6的裝置與僅限IPv4的裝置通訊，反之亦然。

問：如何實施組播NAT?

A.可以對組播流的源IP進行NAT。當組播動態NAT完成時，不能使用路由對映，因此僅支援訪問清單。

如需詳細資訊，請參閱多點傳送NAT如何在Cisco路由器上運作。目標組播組使用帶有組播服務反射解決方案的NAT。

問：如何實施有狀態NAT(SNAT)?

A.SNAT為動態對映的NAT會話啟用連續服務。靜態定義的會話無需使用SNAT即可獲得冗餘的好處。在沒有SNAT的情況下，使用動態NAT對映的會話將在發生嚴重故障時中斷，並且必須重新建立。僅支援最小的SNAT配置。只有在您與思科客戶團隊溝通後，才能執行未來的部署，以便驗證與當前限制相關的設計。

建議對下一方案使用SNAT:

- 主/備份不是推薦模式，因為與HSRP相比，有一些功能缺失。
- 用於故障轉移方案和2路由器設定。也就是說，如果一個路由器崩潰，另一個路由器會無縫接管。（SNAT體系結構不是為處理介面擺動而設計的。）
- 支援非非對稱路由方案。只有在應答資料包中的延遲大於交換SNAT消息的兩台SNAT路由器之間的延遲時，才能處理非對稱路由。

目前，SNAT架構的設計不能處理魯棒性；因此，這些測試預計不會成功：

- 在有流量時清除NAT條目時。
- 發生流量時，介面引數（例如IP位址變更、shut/no-shut等）變更時。
- SNAT specificclearorshowcommand應該不能正確執行，建議不要執行。一些SNAT相關的clearandshowcommand如下所示：

```
clear ip snat sessions *
clear ip snat sessions
```

```
clear ip snat translation distributed *
clear ip snat translation peer < IP address of SNAT peer>
sh ip snat distributed verbose
sh ip snat peer < IP address of peer>
```

- 如果使用者想要清除條目，**clear ip nat trans** forcedorclear ip nat trans *命令可以使用。如果使用者要檢視條目，可以使用**show ip nat translation**、**show ip nat translations verbose**和**show ip nat stats**命令。*如果*配置了內部服務，則它還可以顯示SNAT特定資訊。
- 建議不要在備份路由器上清除NAT轉換。始終清除主SNAT路由器上的NAT條目。
- SNAT不是HA；因此，兩台路由器上的配置必須相同。兩台路由器必須運行相同的映像。此外，請確保用於兩台SNAT路由器的底層平台相同。

NAT最佳實踐

問：是否存在任何NAT最佳做法？

是的。以下是NAT最佳實踐：

1. 當使用動態和靜態NAT時，為動態NAT設定規則的ACL必須排除靜態本地主機，以便沒有重疊。
2. 如果將ACL用於帶**permit ip any**的NAT，**則可能會**得到不可預知的結果。12.4(20)T之後，NAT可以轉換本地生成的HSRP和路由協定資料包（如果它們從外部介面傳送出去），以及本地加密的與NAT規則匹配的資料包。
3. 當有重疊的NAT網路時，請使用**match-in-vrf**keyword。您必須為不同VRF的重疊VRF靜態NAT條目新增**match-in-**vrfkeyword，但無法重疊全域性和vrf NAT地址。
   ```
   Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf


   Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
   ```
4. 除非使用**match**-in-vrfkeyword，否則具有相同地址范**圍的NAT池不能**用於不同的VRF。例如：
   ```
   ip nat pool poolA 172.31.1.1 172.31.1.10 prefix-length 24
   ip nat pool poolB 172.31.1.1 172.31.1.10 prefix-length 24
   ip nat inside source list 1 poolA vrf A match-in-vrf
   ip nat inside source list 2 poolB vrf B match-in-vrf
   ```

   註：即使CLI配置有效，但沒有**match-in-vrf** 關鍵字，配置也不受支援。
5. 當部署具有NAT介面過載的ISP負載均衡時，最佳實踐是使用具有介面匹配且通過ACL匹配的路由對映。
6. 使用池對映時，不能使用兩個不同的對映（ACL或路由對映）來共用同一個NAT池地址。
7. 在故障切換場景中，當在兩個不同的路由器上部署相同的NAT規則時，必須使用HSRP冗餘。
8. 請勿在靜態NAT和動態池中定義相同的內部全域性地址。此操作可能會導致不期望的結果。

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）。