查看網路位址轉譯 (NAT) 的常見問題

目錄

簡介

本文說明網路位址轉譯 (NAT) 的常見問題。

通用NAT

問：什麼是NAT？

A.網路地址轉換(NAT)旨在保護IP地址。它允許使用未註冊的IP地址的專用IP網路連線到Internet。NAT在路由器上運行，通常將兩個網路連線在一起，並將內部網路中的私有（非全局唯一）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，可以將NAT配置為僅向外部世界通告整個網路的一個地址。這樣可以有效地將整個內部網路隱藏在該地址後面，從而提供更高的安全性。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。

問題： 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以外的任何裝置。

問題： 如何配置NAT？

答：要配置傳統NAT，您需要使路由器上的至少一個介面（NAT外部）和路由器上的另一個介面（NAT內部）以及一組用於轉換資料包報頭（如果需要，還包括負載）中的IP地址的規則需要配置。要配置Nat虛擬介面(NVI)，您至少需要一個配置了NAT enable的介面以及上述規則集。

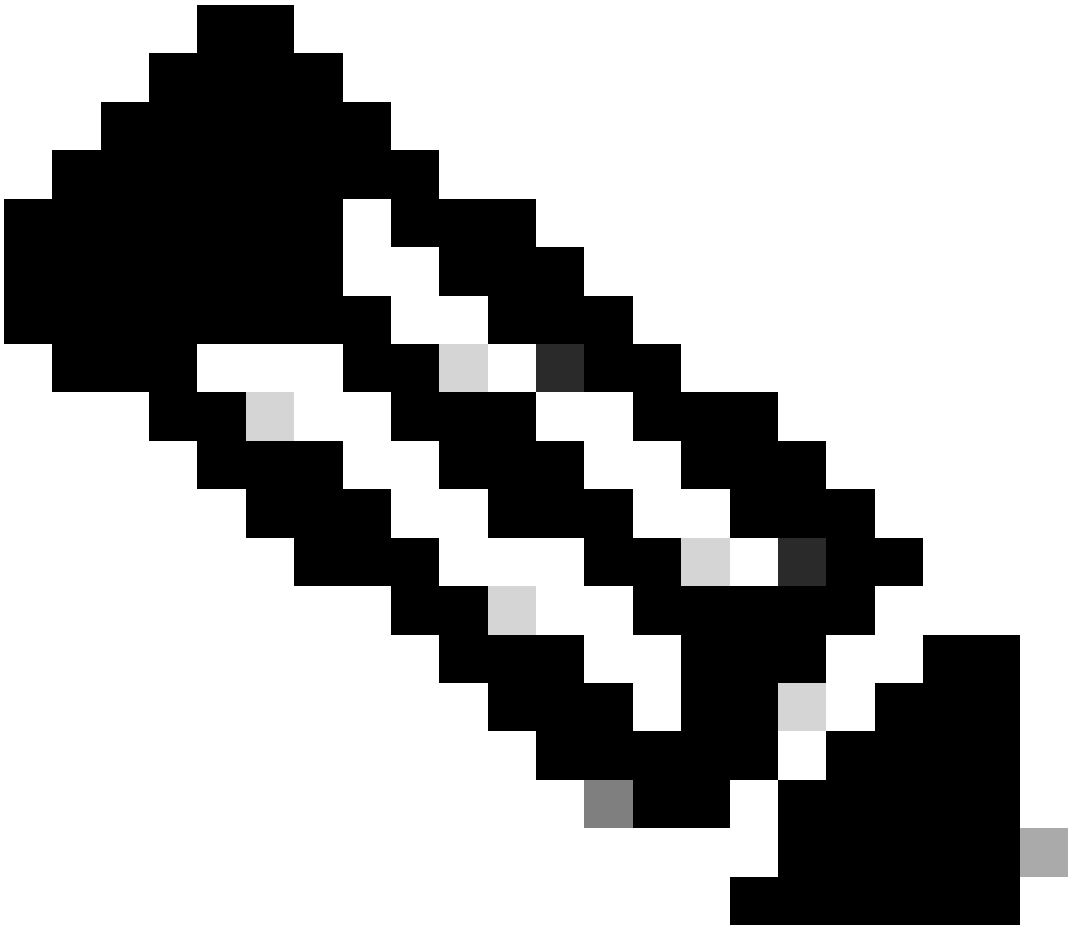
有關詳細資訊，請參閱Cisco IOS® IP定址服務配置指南或配置NAT虛擬介面。

問題： Cisco IOS軟體和Cisco PIX安全裝置實施NAT的主要區別是什麼？

答：基於Cisco IOS軟體的NAT與Cisco PIX安全裝置中的NAT功能沒有本質區別。主要的差異包括實施中支援的不同流量型別。有關在Cisco PIX裝置（包括支援的流量型別）上配置NAT的詳細資訊，請參閱NAT配置示例。

問題： Cisco IOS NAT在哪些思科路由硬體上可用？如何訂購硬體？

答：Cisco Feature Navigator工具使客戶能夠辨識功能(NAT)，並找到此Cisco IOS軟體功能的可用版本和硬體版本。要使用此工具，請參閱Cisco Feature Navigator。



附註：只有完成註冊的思科使用者能存取思科內部工具與資訊。

問題： NAT發生在路由之前還是之後？

A.使用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。路由之後發生內部到外部轉換，路由之前發生外部到內部轉換。有關詳細資訊，請參閱NAT運行順序。

問題： 能否在公共無線LAN環境中部署NAT？

答：是的。NAT -靜態IP支援功能為具有靜態IP位址的使用者提供支援，讓這些使用者能夠在公用無線LAN環境中建立IP作業階段。

問題： NAT是否為內部網路上的伺服器執行TCP負載均衡？

答：是的。使用NAT，您可以在內部網路上建立一個虛擬主機，以協調實際主機之間的負載共用。

問題： 是否可以對NAT轉換的數量進行速率限制？

答：是的。速率限制NAT轉換功能可限制路由器上併發的NAT操作的最大數量。除了讓使用者更好地控制NAT地址的使用方式外，速率限制NAT轉換功能還可用於限制病毒、蠕蟲和拒絕服務攻擊的影響。

問題： 如何為NAT使用的IP子網或地址獲取或傳播路由？

A.在下列情況下，可以察覺由NAT建立的IP地址的路由：

- 內部全局地址池從下一跳路由器的子網中生成。
- 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。

當內部全局地址與本地介面匹配時，NAT會安裝一個IP別名和一個ARP條目，在這種情況下，路由器可以為這些地址代理ARP。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。

問題： 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位元組。因此，10,000個轉換（比通常在單個路由器上處理的要多）消耗約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。

問題： 使用Cisco IOS NAT時可以預期哪種路由效能？

A. Cisco IOS NAT支援Cisco快速轉發交換、快速交換以及進程交換。對於12.4T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
- IP地址是否嵌入
- 交換和檢查多個報文
- 需要源埠
- 轉換數目
- 當時正在運行的其他應用程式
- 硬體和處理器的型別

問題： Cisco IOS NAT能否應用於子介面？

答：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（包括撥號程式介面）。無法使用無線虛擬介面配置NAT。寫入NVRAM時無線虛擬介面不存在。因此，重新啟動後，路由器會丟失無線虛擬介面上的NAT配置。

問題： Cisco IOS NAT能否與熱備用路由器協定(HSRP)配合使用來提供到ISP的冗餘鏈路？

答：是的。NAT確實提供HSRP冗餘。但是，它與SNAT（有狀態NAT）不同。使用HSRP的NAT是無狀態系統。發生失敗時，不會維持目前的作業階段。在靜態NAT配置期間（當資料包與任何靜態規則配置都不匹配時），資料包將透過傳送而不進行任何轉換。

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

答：是的。NAT不考慮封裝問題。在介面上有IP地址且介面為NAT內部或NAT外部的情況下，可以執行NAT。NAT必須具備內部和外部才能正常運行。如果使用NVI，必須至少有一個啟用了NAT的介面。有關詳細資訊，請參閱如何配置NAT？。

問題： 一台啟用NAT的路由器能否允許某些使用者使用NAT，而同一乙太網介面上的其他使用者繼續使用自己的IP地址？

答：是的。這可以透過使用描述需要NAT的主機或網路集的訪問清單來實現。

訪問清單、擴展訪問清單和路由對映均可用於定義IP裝置轉換的規則。必須始終指定網路地址和適當的子網掩碼。不能使用關鍵字any代替網路地址或子網掩碼。使用靜態NAT時，當資料包與任何靜態規則配置都不匹配時，將傳送資料包而不進行任何轉換。

問題： 配置PAT（過載）時，每個內部全局IP地址可建立的最大轉換數是多少？

A.PAT（過載）將每個全局IP地址的可用埠分成三個範圍：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，但如果已經使用了原始源埠，它會從特定埠範圍的開始開始開始掃描，以查詢第一個可用埠並將其分配給會話。12.2S程式碼基礎有一個例外。12.2S代碼庫使用不同的埠邏輯，並且沒有埠保留。

問題： PAT如何工作？

A. PAT使用一個全局IP地址或多個地址。

使用一個IP地址的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其使用的「一組特定埠或協商埠」，PAT會將它

	們放置一旁，並且不將它們分配為唯一識別符號。
4	如果沒有特殊埠要求的會話嘗試連線，則PAT轉換IP源地址並檢查源源埠（例如433）的可用性。 注意：傳輸控制通訊協定(TCP)和使用者資料包通訊協定(UDP)的範圍是：1-511、512-1023、1024-65535。對於網際網路控制消息協定(ICMP)，第一組從0開始。
5	如果請求的源埠可用，則PAT會分配源埠，會話繼續進行。
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開始）。
7	如果有可用的連線埠，則會指派該連線埠，作業階段會繼續。
8	如果沒有可用的連線埠，封包就會遭捨棄。

使用多個IP地址的PAT

條件	說明
1-7	前七個條件與使用單個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埠，NAT將轉到池中的下一個IP地址並嘗試分配請求的原始源埠。
9	如果請求的源埠可用，則NAT分配源埠，會話繼續。
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，則會指派該連線埠，且作業階段會繼續。
12	如果沒有可用的連線埠，除非集區中有另一個IP位址可用，否則封包會被捨棄。

問題： 什麼是NAT IP池？

A. NAT IP池是根據需要為NAT轉換所分配的IP地址範圍。要定義池，可使用配置命令：

<#root>

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

範例 1

下一個示例在從192.168.1.0或192.168.2.0網路定址的內部主機之間轉換到全球唯一的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

在本示例中，目標是定義虛擬地址，連線在一組實際主機之間分配。該池定義了實際主機的地址。訪問清單定義虛擬地址。如果轉換不存在，則來自串列介面0（外部介面）且目標與訪問清單匹配的TCP資料包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
```

問題： 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。（思科建議您配置一個池大小255。）每個池不能超過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。在12.2S代碼庫中，沒有最大池數限制。

問題： 在NAT池上使用路由對映與ACL相比有何優點？

A.路由對映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局地址。有關詳細資訊，請參閱使用路由對映對多個池提供NAT支援。

問題： NAT環境中重疊的IP地址是什麼？

A. IP地址重疊是指兩個要互聯的位置使用相同的IP地址方案。這種情況並不罕見，通常發生在公司合併或被收購時。如果沒有特殊支援，這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，也可以來自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。該解決方案包括攔截從外部到內部的域名系統(DNS)名稱查詢響應、為外部地址設定轉換，以及在將DNS響應轉發到內部主機之前對其進行修

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能夠對DNS A和PTR記錄的內容進行檢查並執行地址轉換，如在重疊網路中使用NAT中所述。

問題： 什麼是靜態NAT轉換？

A. 靜態NAT轉換在本地地址和全局地址之間具有一對一的對映關係。使用者還可以配置到埠級別的靜態地址轉換，並將剩餘的IP地址用於其他轉換。當您執行埠地址轉換(PAT)時，通常會發生這種情況。

下一個示例顯示如何配置routemap以允許靜態NAT進行外部到內部轉換：

<#root>

```
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 10.1.10.128 0.0.0.127'

route-map R1 permit 10
match ip address ACL-A
```

問題： 術語NATOverloading是什麼意思；這是PAT嗎？

答：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，或者將介面IP地址與埠結合使用。過載時，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（內部全局，通常註冊）IP地址。每個轉換上的唯一源埠號用於區分會話。

問題： 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局地址之間的動態對映。動態對映是透過定義要轉換的本地地址以及要從中分配全局地址的地址池或介面IP地址並將兩者關聯來完成的。

問題： 什麼是ALG？

A. ALG是應用層網關(ALG)。NAT對應用資料流中不攜帶源和/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)資料流執行轉換服務。

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

有關詳細資訊，請參閱將應用層網關與NAT結合使用。

問題： 能否同時使用靜態和動態NAT轉換來構建配置？

答：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局地址不會自動與包含這些相同全局地址的動態池一起排除。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。

問題： 當透過NAT路由器執行traceroute時，traceroute是顯示NAT全局地址還是洩漏NAT本地地址？

A.來自外部的Traceroute必須始終返回全局地址。

問題： 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，無論其預設埠範圍如何。
- 埠對映允許NAT為特定應用保留使用者定義的埠範圍。

有關詳細資訊，請參閱用於PAT的使用者定義的源埠範圍。

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局埠。
- 對稱埠允許NAT支援點獨立。

問題： 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)。當大於介面的最大傳輸單元(MTU)的資料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。如果沒有在封包的IP標頭中設定不分段(DF)位元，則會將封包分段。如果封包的IP標頭中設定了DF位元，則會捨棄封包，並向傳送者傳回表示下一個躍點的MTU值的ICMP錯誤訊息。IP封包的所有片段在IP標頭中都有相同的Ident，因此最終接收者可以將片段重組為原始IP封包。有關詳細資訊，請參閱解決GRE和IPsec中的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認為要傳送的最大的資料塊。從TCP傳輸到IP的這一資料單元稱為資料段。TCP資料段在IP資料包中傳送。然後，這些IP資料包在透過網路時，可能會成為IP分段，並且會遇到比它們可容納的更低的MTU鏈路。

TCP首先將此資料分段為TCP資料段（基於TCP MSS值），然後增加TCP報頭並將此TCP資料段傳遞到IP。然後，IP協定增加IP報頭，將資料包傳送到遠端終端主機。如果含有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會將IP/TCP封包分段以符合大小。這些IP封包片段是由IP層在遠端主機上進行重組，且完整的TCP區段（最初傳送的）會傳遞給TCP層。TCP層不知道IP在傳輸過程中將資料包分段。NAT支援IP分段，但它不支援TCP分段。

問題： NAT是否支援IP分段和TCP分段順序混亂？

A.由於存在ip virtual-reassembly，NAT僅支援無序的IP分段。

問題： 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。

問題： 是否存在受支援的NAT MIB？

答：不能。不支援的NAT MIB，包括CISCO-IETF-NAT-MIB。

問題： TCP超時是什麼？它與NAT TCP計時器的關係有如何關係？

A.如果三次握手沒有完成，並且NAT看到一個TCP資料包，則NAT將啟動60秒計時器。當三次握手完成後，NAT預設情況下對NAT條目使用24小時計時器。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。就FIN而言，NAT在收到FIN和FIN-ACK時將預設計時器從24小時更改為60秒。

問題： 是否可以將NAT轉換從NAT轉換表中超時所需的時間量？

答：是的。您可以更改所有條目或不同型別的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）。

問題： 如何阻止輕量級目錄訪問協定(LDAP)向每個LDAP應答資料包附加額外的位元組？

A. LDAP設定在處理型別為Search-Res-Entry的消息時增加額外的位元組（LDAP搜尋結果）。LDAP將10個位元組的搜尋結果附加到每個LDAP應答資料包。如果這10個額外位元組的資料導致資料包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CLI命令no ip nat service append-ldap-search-res停用此LDAP行為，以便正常傳送和接收資料包。

問題： 對於NAT裝置上的內部全局/外部本地IP地址，路由建議是什麼？

A. 對於NAT-NVI之類的功能，必須在為內部全局IP地址配置的NAT框中指定路由。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，任何使用外部靜態規則從輸入到輸出方向的資料包都需要這種路由。在這種情況下，在為IG/OL提供路由的同時，還必須配置下一跳IP地址。如果缺少下一跳配置，則將其視為配置錯誤，並導致不確定的行為。

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，則在這些場景中，您需要提供虛擬下一跳IP地址以及下一跳的關聯ARP。底層基礎設施需要此配置才能將資料包傳遞給NAT進行轉換。

問題： Cisco IOS NAT是否支援帶有log關鍵字的ACL？

A. 當您為動態NAT轉換配置Cisco IOS NAT時，會使用ACL標識可以轉換的資料包。當前NAT架構不支援帶有log關鍵字的ACL。

語音NAT

問：NAT是否支援Cisco Unified Communications Manager (CUCM) V7隨附的Skinny Client Control Protocol (SCCP) v17？

A. CUCM 7和CUCM 7的所有預設電話載入都支援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。

在建立本文檔時，NAT尚未支援SCCP v17。在實施對SCCP v17的NAT支援之前，必須將韌體降級為版本8-3-5或更早版本，以便協商SCCP v16。只要使用SCCP v16，CUCM6就不會遇到任何電話負載的NAT問題。Cisco IOS當前不支援SCCP版本17。

問題： NAT支援哪些CUCM /SCCP/韌體載入版本？

A. NAT支援CUCM版本6.x及更早版本。這些CUCM版本使用支援SCCP v15（或更早版本）的預設8.3.x（或更早版本）電話韌體載入發佈。

NAT不支援CUCM版本7.x或更高版本。這些CUCM版本隨支援SCCP v17（或更高版本）的預設8.4.x電話韌體載入一起發佈。

如果使用CUCM 7.x或更高版本，則必須在CUCM TFTP伺服器上安裝較舊的韌體載入，以便電話使用SCCP v15或更早版本的韌體載入，以獲得NAT支援。

問題： 什麼是RTP和RTCP的服務提供商PAT埠分配增強？

A. RTP和RTCP功能的服務提供商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流是下一個後續的奇數埠號。埠號將轉換為符合RFC-1889的指定範圍內的一個號碼。如果呼叫的埠號在此範圍內，則會將PAT轉換到此範圍內的另一個埠號。同樣，對於此範圍之外的埠號的PAT轉換不會導致到給定範圍內的號碼的轉換。

問題： 什麼是會話初始協定(SIP)？SIP資料包可以進行NAT轉換嗎？

答：會話初始協定(SIP)是基於ASCII的應用層控制協定，可用於建立、維持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)為透過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Cisco平台能夠透過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。

問題： 什麼是會話邊界控制器(SBC)的託管NAT遍歷支援？

A. Cisco IOS託管的SBC NAT遍歷功能使Cisco IOS NAT SIP應用級網關(ALG)路由器可以充當Cisco多業務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，請參閱配置會話邊界控制器的Cisco IOS託管NAT遍歷。

問題： 路由器記憶體和CPU可以透過NAT處理多少SIP、精簡和H323呼叫？

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

問題： NAT路由器是否支援Skinny和H323資料包的TCP分段？

答：Cisco IOS-NAT支援12.4主線中針對H323的TCP分段，並且從12.4(6)T開始支援SKINNY的TCP分段。

問：在語音部署中使用NAT過載配置時需要注意哪些注意事項？

答：是的。如果您有NAT過載配置和語音部署，則需要註冊消息透過NAT並為傳出->傳入建立一個關聯以到達此內部裝置。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：在語音部署中發出clear ip nat trans *命令或clear ip nat trans forced命令是否會導致已知問題？

A.在語音部署中，如果發出clear ip nat trans *命令或clear ip nat trans forced命令並且使用動態NAT，則會清除針孔/關聯，必須等待來自內部裝置的下一個註冊週期才能重新建立針孔/關聯。Cisco建議不要在語音部署中使用這些clear命令。

問題： NAT是否支援語音協同定位解決方案？

A.否。目前不支援協同定位解決方案。使用NAT的下一個部署（在同一台裝置上）被視為一個協同定位解決方案：CME/DSP-Farm/SCCP/H323。

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

答：否。請注意，UDP SIP ALG（用於大多數部署）不受影響。

NAT與VRF/MPLS

問：NAT路由器是否曾支援NAT在VRF中使用相同的地址空間，同時在全局地址空間使用NAT？目前，當我嘗試配置此命令時，我收到了「% similar static entry (10.1.1.1 —> 10.210.2.2)already exists」警告：

<#root>

72UUT(config)#

ip nat inside source static 10.1.1.1 10.210.2.2

72UUT(config)#

ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED

A.傳統NAT支援不同VRF上的重疊地址配置。對於特定VRF上的流量，您必須使用match-in-vrf選項在規則中配置重疊，並在同一VRF中設定ip nat inside/outside。重疊支援不包括全局路由表。

對於不同的VRF，必須為重疊VRF靜態NAT條目增加match-in-vrf關鍵字。但是，不能重疊全局和vrf NAT地址。

<#root>

72UUT(config)#

ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED match-in-vrf

72UUT(config)#

ip nat inside source static 10.1.1.1 10.210.2.2 vrf BLUE match-in-vrf

問題： 傳統NAT是否支援VRF-Lite（從VRF到其他VRF的NAT）？

答：不能。您必須使用NVI在不同的VRF之間進行NAT轉換。您可以使用傳統NAT執行從VRF到全局的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。此解決方案必須代替單介面網路地址轉換。

問：在全局介面和VRF中的介面之間執行NAT時，是否必須使用NAT NVI？

A. Cisco建議您對全局NAT(ip nat inside/out)以及同一VRF中的介面之間使用VRF的傳統NAT。NVI用於不同VRF之間的NAT。

問題： 是否支援NAT-NVI的TCP分段？

A. NAT-NVI不支援TCP分段。

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

答：否。請注意，UDP SIP ALG（用於大多數部署）不受影響。

問題： 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：何謂有狀態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，因此流量傳輸會繼續。

問題： 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。

問題： 非對稱路由是否支援SNAT？

A.透過啟用為隊列，非對稱路由支援NAT。預設情況下，as-queueing為啟用狀態。但是，從12.4(24)T開始，不再支援as-queuing。客戶必須確保正確路由封包並新增適當的延遲，才能讓非對稱路由正確運作。

NAT-PT（v6至v4）

問：什麼是NAT-PT？

A. NAT-PT是用於NAT的4到v6轉換。協定轉換(NAT-PT)是IPv6-IPv4轉換機制(如RFC 2765 和RFC 2766 中所定義)，它允許僅IPv6裝置與僅IPv4裝置通訊，反之亦然。

問題： Cisco Express Forwarding (CEF)路徑是否支援NAT-PT？

A. CEF路徑不支援NAT-PT。

問題： NAT-PT中支援哪些ALG？

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

問題： ASR 1004是否支援NAT-PT？

A.聚合服務路由器(ASR)使用NAT64。

與平台相關的思科7300/7600/6k

問：有狀態NAT (SNAT)在SX系列的Catalyst 6500上是否可用？

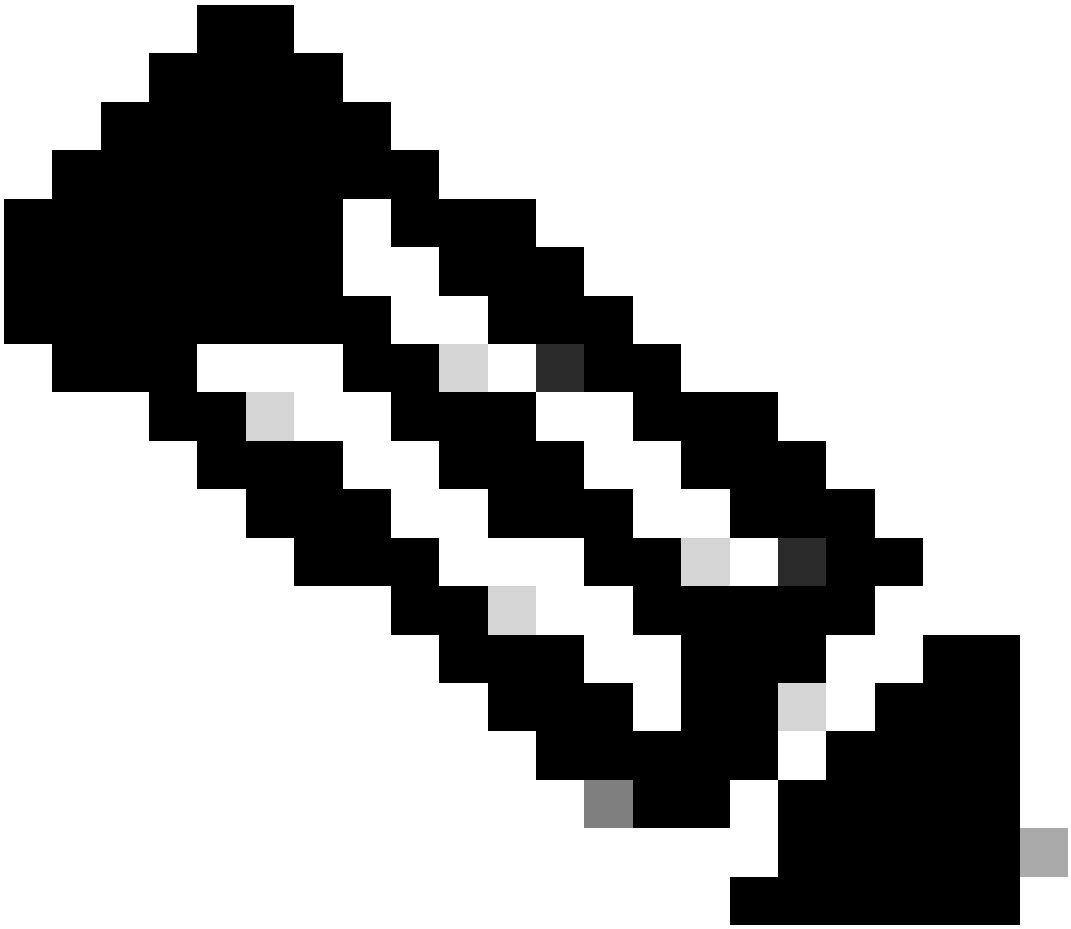
A. SNAT在Catalyst 6500的SX系列上不可用。

問題： 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。

問題： 7600和Cat6000是否支援VRF感知NAT？

A. 在65xx/76xx平台上，不支援VRF感知NAT，且CLI受到阻止。



注意：可以利用在虛擬環境透明模式下運行的FWSM實施設計。

與平台相關的思科850

問：Cisco 850在版本12.4T中是否支援Skinny NAT ALG？

答：不支援。在850系列上，12.4T不支援Skinny 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網際網路連線到網際網路。在將資料包轉發到另一個網路之前，NAT將內部網路中的私有(RFC1918)地址轉換為合法的可路由地址。

問題： 如何實施帶語音的NAT？

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

問題： 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全部使用相同的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，同時確保每個MPLS VPN彼此完全獨立。

問題： NAT靜態對映是否支援HSRP以實現高可用性？

A.當使用網路地址轉換(NAT)靜態對映配置且歸路由器所有的地址觸發地址解析協定(ARP)查詢時，NAT將使用ARP指向的介面上的BIA MAC地址作出響應。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。

問題： 如何實施NAT NVI？

A. NAT虛擬介面(NVI)功能取消了將介面配置為NAT內部介面或NAT外部介面的要求。

問題： 如何使用NAT實施負載均衡？

答：使用NAT有兩種負載均衡方式：一種是入站負載均衡到一組伺服器，將負載分佈到伺服器上；另一種是透過兩個或多個ISP將使用者流量負載均衡到網際網路。

有關出站負載均衡的更多資訊，請參閱兩個ISP連線的Cisco IOS NAT負載均衡。

問題： 如何將NAT與IPSec結合使用？

A.支援透過NAT和IPSec NAT透明模式封裝IP安全(IPSec)安全有效載荷(ESP)。

透過NAT功能的IPSec ESP支援透過配置在過載或埠地址轉換(PAT)模式下的Cisco IOS NAT裝置同時支援多個IPSec ESP隧道或連線。

IPSec NAT透明功能透過解決NAT和IPSec之間的許多已知不相容問題，支援IPSec流量透過網路中的NAT或PAT點。

問題： 如何實施NAT-PT？

答： NAT-PT（網路地址轉換—協定轉換）是一種IPv6-IPv4轉換機制，如RFC 2765和RFC 2766中所定義，它允許僅IPv6裝置與僅IPv4裝置通訊，反之亦然。

問題： 如何實施組播NAT？

A. 可以對多播流的源IP進行NAT。對組播執行動態NAT時不能使用路由對映，因此僅支援訪問清單。

有關詳細資訊，請參閱組播NAT如何在Cisco路由器上運行。目標組播組使用組播服務反射解決方案進行NAT。

問題： 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。靜態定義的會話在無需使用SNAT的情況下即可獲得冗餘的好處。在沒有SNAT的情況下，使用動態NAT對映的會話將在出現嚴重故障時中斷，並且必須重新建立。僅支援最小的SNAT配置。只有在諮詢您的思科客戶團隊後，才能驗證設計是否符合當前限制，才能執行未來的部署。

建議在以下情況下使用SNAT：

- 主要/備份不是建議的模式，因為與HSRP相比，缺少某些功能。
- 用於故障轉移方案和2路由器設定。也就是說，如果一台路由器崩潰，另一台路由器將無縫接管。（SNAT架構並非設計用於處理介面抖動。）
- 支援非非對稱路由方案。只有在應答資料包中的延遲高於2台SNAT路由器之間交換SNAT消息的延遲時，才能處理非對稱路由。

目前SNAT架構的設計不能處理穩健性；因此，這些測試預計不會成功：

- 在有流量時清除NAT條目。
- 在有流量時更改介面引數（如IP地址更改、關閉/不關閉等）。
- SNAT特定的clear或show命令應當不會正常執行，也不推薦使用。

  與SNAT相關的部分clear< /strong>和show命令如下所示：

  <#root>

  ```
  clear ip snat sessions *

  clear ip snat sessions <ip address of the peer>

  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>
  ```

- 如果使用者要清除條目，可以使用clear ip nat trans forced< /strong>或clear ip nat trans *命令。
- 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。如果已配置內部服務，它也會顯示SNAT特定的資訊。
- 不建議在備用路由器上清除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同一個映像。還要確保用於兩個SNAT路由器的底層平台相同。

NAT最佳實踐

問：是否有NAT最佳做法？

答：是的。以下是NAT最佳實踐：

1. 同時使用動態和靜態NAT時，為動態NAT設定規則的ACL必須排除靜態本地主機，這樣就不會有重疊。
2. 將NAT的ACL與permit ip any any配合使用時要謹慎，因為您會獲得不可預知的結果。在12.4(20)T之後，如果本地生成的HSRP和路由協定資料包是從外部介面傳送出去的，NAT將轉換這些資料包，以及與NAT規則匹配的本地加密資料包。
3. 如果將重疊網路用於NAT，請使用match-in-vrf關鍵字。

   對於不同的VRF，必須為重疊VRF靜態NAT條目增加match-in-vrf 關鍵字，但不能重疊全局和VRF NAT地址。

   <#root>

   ```
   Router(config)#
   ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED match-in-vrf
   ```

   <#root>

   ```
   Router(config)#
   ip nat inside source static 10.1.1.1 10.210.2.2 vrf BLUE match-in-vrf
   ```

4. 除非使用match-in-vrf關鍵字，否則不能在不同的VRF中使用地址範圍相同的NAT池。

   舉例來說：

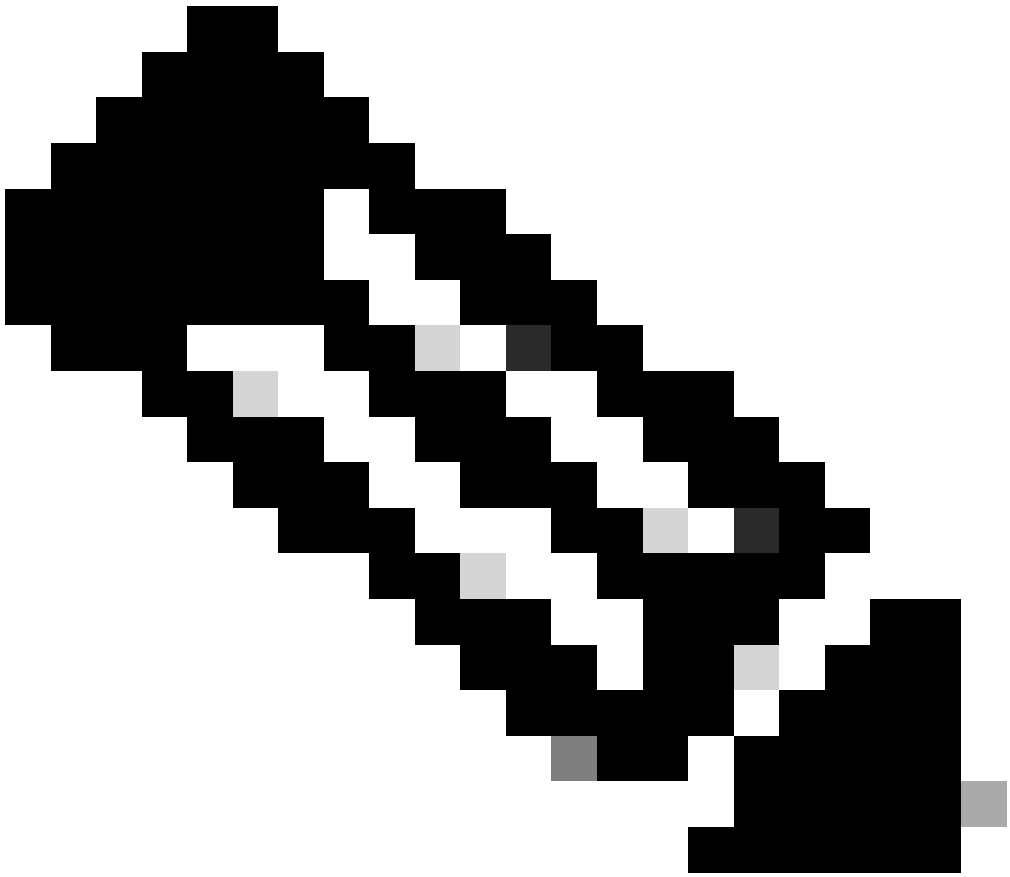
<#root>

```
ip nat pool poolA 1710.1.1.1 1710.1.1.10 prefix-length 24

ip nat pool poolB 1710.1.1.1 1710.1.1.10 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
```



注意：即使CLI配置有效，但不支援沒有match-in-vrf關鍵字的配置。

---

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（而不是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）來共用相同的NAT池地址。

7. 在故障轉移場景中，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局地址。此操作可能導致不理想的結果。

相關資訊

- 思科技術支援與下載

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）。