單臂網路地址轉換

目錄

簡介

單臂網路地址轉換(NAT)是什麼意思？術語「單臂連線」通常表示任務使用路由器的單個物理介面。就像我們可以使用同一物理介面的子介面執行交換機間鏈路(ISL)中繼一樣，我們也可以使用路由器上的單個物理介面來完成NAT。

注意：由於存在環回介面，路由器必須處理每個資料包的交換機。這會降低路由器的效能。

必要條件

需求

本文件沒有特定需求。

採用元件

此功能需要使用支援NAT的Cisco IOS® 軟體版本。使用Cisco Feature Navigator II(僅供註冊客戶使用)確定可以使用此功能的IOS版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

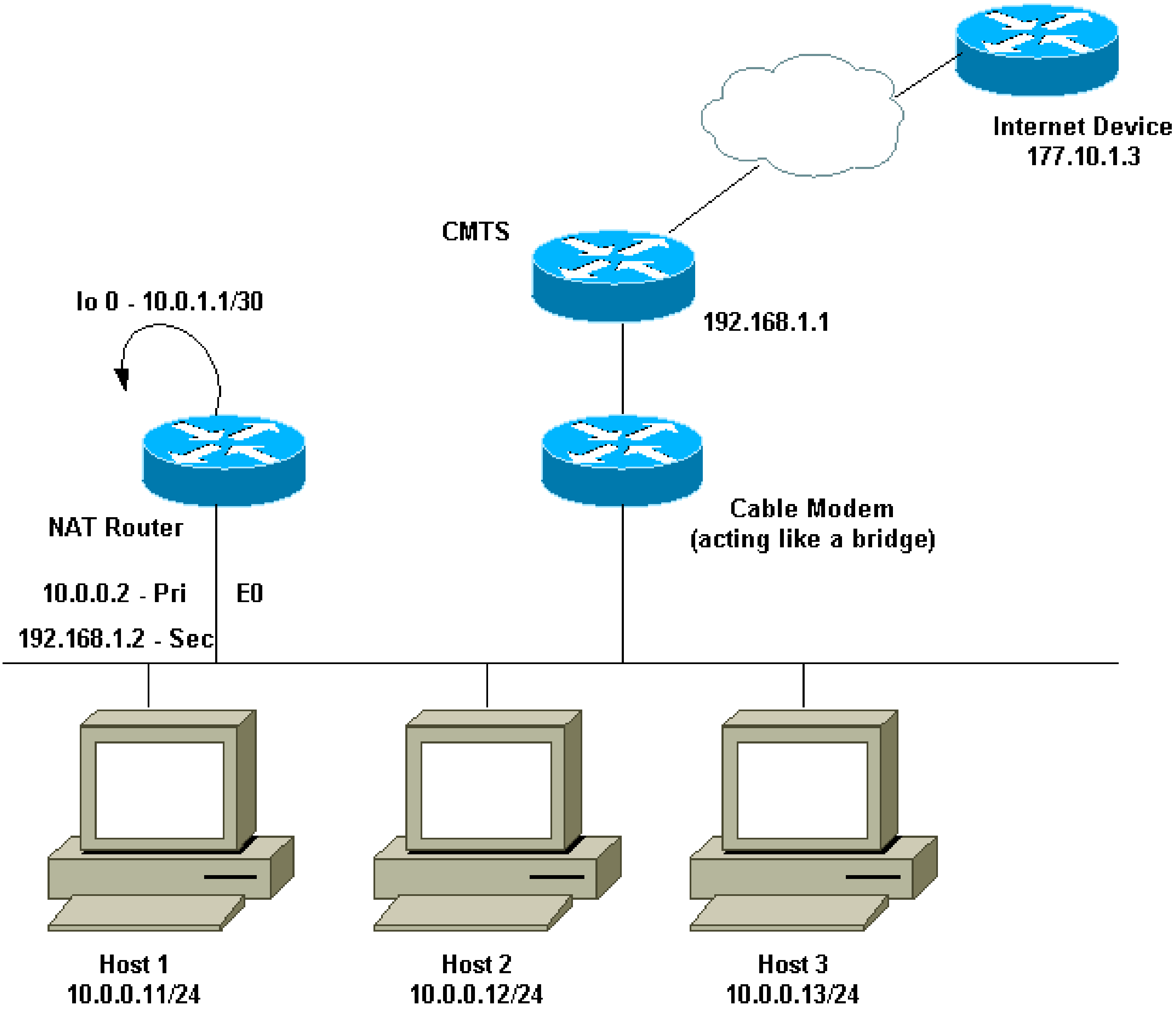
背景資訊

為了進行NAT，必須將資料包從NAT「內部」定義介面交換到NAT「外部」定義介面，反之亦然。對NAT的此要求並未改變，但本文檔演示了如何使用虛擬介面（也稱為環回介面）和基於策略的路由，使NAT在具有單個物理介面的路由器上工作。

很少需要在單臂上進行NAT。實際上，本檔案中的範例可能是需要此組態的唯一情況。雖然其他情況也出現使用者將策略路由與NAT結合使用的情況，但我們不將此情況視為單臂上的NAT，因為這些例項仍使用多個物理介面。

範例1網路圖表和組態

網路圖表



上述網路圖在電纜數據機設定中非常常見。纜線資料機終端系統(CMTS)是路由器，而纜線資料機(CM)是作用類似橋接器的裝置。我們面臨的問題是，我們的Internet服務提供商(ISP)沒有為我們提供足夠的有效地址，無法滿足訪問Internet所需的主機數量。ISP給了我們地址192.168.1.2，該地址將用於裝置。在進一步請求時，我們又收到三個地址，即192.168.2.1到192.168.2.3,NAT將地址為10.0.0.0/24範圍內的主機轉換為這些地址。

需求

我們的要求是：

- 網路中的所有主機都必須能夠訪問Internet。
- 主機2必須能夠從Internet訪問，且IP地址為192.168.2.1。
- 由於主機數可能多於合法地址，因此我們使用10.0.0.0/24子網作為內部定址。

在本文檔中，我們只顯示NAT路由器的配置。但是，我們確實提到有關主機的一些重要配置說明。

NAT路由器配置

NAT路由器配置

```
interface Loopback0
 ip address 10.0.1.1 255.255.255.252
 ip nat outside
!--- Creates a virtual interface called Loopback 0 and
assigns an !--- IP address of 10.0.1.1 to it. Defines
interface Loopback 0 as !--- NAT outside. ! ! interface
Ethernet0 ip address 192.168.1.2 255.255.255.0 secondary
ip address 10.0.0.2 255.255.255.0 ip Nat inside !---
Assigns a primary IP address of 10.0.0.2 and a secondary
IP !--- address of 192.168.1.2 to Ethernet 0. Defines
interface Ethernet 0 !--- as NAT inside. The 192.168.1.2
address will be used to communicate !--- through the CM
to the CMTS and the Internet. The 10.0.0.2 address !---
will be used to communicate with the local hosts. ip
policy route-map Nat-loop !--- Assigns route-map "Nat-
loop" to Ethernet 0 for policy routing. ! ip Nat pool
external 192.168.2.2 192.168.2.3 prefix-length 29 ip Nat
inside source list 10 pool external overload ip Nat
inside source static 10.0.0.12 192.168.2.1 !--- NAT is
defined: packets that match access-list 10 will be !---
translated to an address from the pool called
"external". !--- A static NAT translation is defined for
10.0.0.12 to be !--- translated to 192.168.2.1 (this is
for host 2 which needs !--- to be accessed from the
Internet).


ip classless
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip route 192.168.2.0 255.255.255.0 Ethernet0
 !--- Static default route set as 192.168.1.1, also a
static !--- route for network 192.168.2.0/24 directly
attached to !--- Ethernet 0 ! ! access-list 10 permit
10.0.0.0 0.0.0.255 !--- Access-list 10 defined for use
by NAT statement above.


access-list 102 permit ip any 192.168.2.0 0.0.0.255
access-list 102 permit ip 10.0.0.0 0.0.0.255 any
!--- Access-list 102 defined and used by route-map "Nat-
loop" !--- which is used for policy routing.

!
Access-list 177 permit icmp any any
 !--- Access-list 177 used for debug.

!
route-map Nat-loop permit 10
 match ip address 102
 set ip next-hop 10.0.1.2
!--- Creates route-map "Nat-loop" used for policy
routing. !--- Route map states that any packets that
match access-list 102 will !--- have the next hop set to
10.0.1.2 and be routed "out" the !--- loopback
interface. All other packets will be routed normally. !-
-- We use 10.0.1.2 because this next-hop is seen as
located !--- on the loopback interface which would
result in policy routing to !--- loopback0.
Alternatively, we could have used "set interface !---
loopback0" which would have done the same thing. ! end
NAT-router#
```

注意：所有主機的預設網關都設定為10.0.0.2，即NAT路由器。ISP和CMTS必須具有一個通往192.168.2.0/29的路由，該路由指向NAT路由器以使返回流量工作，因為來自內部主機的流量看起來是從該子網到達的。在本例中，CMTS會將用於192.168.2.0/29的流量路由到192.168.1.2（即NAT路由器上配置的輔助IP地址）。

範例1 show和debug命令輸出

本節提供的資訊可用於確認您的組態是否正常運作。

為了說明上述組態是否有效，我們已在監控NAT路由器上的**debug**輸出時執行幾次**ping**測試。您可以看到**ping**命令成功，而**debug**輸出會顯示確切的情況。

註：使用debug命令之前，請參閱有關Debug命令的重要資訊**。**

測試一

對於第一次測試，我們從實驗室定義的Internet中的裝置**ping**主機2。請記住，其中一個要求是Internet中的裝置必須能夠使用IP地址192.168.2.1與主機2通訊。以下是NAT路由器上看到的**debug**輸出。在NAT路由器上運行的debug命令是**debug ip packet 177 detail**，它使用定義的**access-list 177**、debug ip Nat和**debug ip policy**，後者向我們顯示策略路由的資料包。

以下是在NAT路由器上執行的**show ip Nat translation**命令的輸出：

```
NAT-router# show ip Nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 192.168.2.1        10.0.0.12          ---                ---
NAT-router#
```

從Internet上的裝置（本例中為路由器）**ping** 192.168.2.1，成功，如下所示：

```
Internet-device# ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/92/92 ms
Internet-device#
```

要檢視NAT路由器中發生的情況，請參閱以下**debug**輸出和註釋：

```
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1, len 100, policy match
    ICMP type=8, code=0
IP: route map Nat-loop, item 10, permit
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), Len 100, policy routed
    ICMP type=8, code=0
!--- The above debug output shows the packet with source 177.10.1.3 destined !--- to
192.168.2.1. The packet matches the statements in the "Nat-loop" !--- policy route map and is
permitted and policy-routed. The Internet !--- Control Message Protocol (ICMP) type 8, code 0
indicates that this !--- packet is an ICMP echo request packet.


IP: Ethernet0 to Loopback0 10.0.1.2
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), g=10.0.1.2, Len 100,
forward
    ICMP type=8, code=0
```

```
 !--- The packet now is routed to the new next hop address of 10.0.1.2 !--- as shown above. IP:
NAT enab = 1 trans = 0 flags = 0 NAT: s=177.10.1.3, d=192.168.2.1->10.0.0.12 [52] IP:
s=177.10.1.3 (Loopback0), d=10.0.0.12 (Ethernet0), g=10.0.0.12, Len 100, forward ICMP type=8,
code=0 IP: NAT enab = 1 trans = 0 flags = 0 !--- Now that the routing decision has been made,
NAT takes place. We can !--- see above that the address 192.168.2.1 is translated to 10.0.0.12
and !--- this packet is forwarded out Ethernet 0 to the local host. !--- Note: When a packet is
going from inside to outside, it is routed and !--- then translated (NAT). In the opposite
direction (outside to inside), !--- NAT takes place first.


IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3, Len 100, policy match
    ICMP type=0, code=0
IP: route map Nat-loop, item 10, permit
IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed
    ICMP type=0, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
!--- Host 2 now sends an ICMP echo response, seen as ICMP type 0, code 0. !--- This packet also
matches the policy routing statements and is !--- permitted for policy routing. NAT:
s=10.0.0.12->192.168.2.1, d=177.10.1.3 [52] IP: s=192.168.2.1 (Ethernet0), d=177.10.1.3
(Loopback0), g=10.0.1.2, Len 100, forward ICMP type=0, code=0 IP: s=192.168.2.1 (Loopback0),
d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100, forward ICMP type=0, code=0 IP: NAT enab = 1
trans = 0 flags = 0 !--- The above output shows the Host 2 IP address is translated to !---
192.168.2.1 and the packet that results packet is sent out loopback 0, !--- because of the
policy based routing, and finally forwarded !--- out Ethernet 0 to the Internet device. !--- The
remainder of the debug output shown is a repeat of the previous !--- for each of the additional
four ICMP packet exchanges (by default, !--- five ICMP packets are sent when pinging from Cisco
routers). We have !--- omitted most of the output since it is redundant.

IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1, Len 100, policy match
    ICMP type=8, code=0
IP: route map Nat-loop, item 10, permit
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), Len 100, policy routed
    ICMP type=8, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), g=10.0.1.2, Len 100,
forward
    ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
NAT: s=177.10.1.3, d=192.168.2.1->10.0.0.12 [53]
IP: s=177.10.1.3 (Loopback0), d=10.0.0.12 (Ethernet0), g=10.0.0.12, Len 100,
forward
    ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3, Len 100, policy match
    ICMP type=0, code=0
IP: route map Nat-loop, item 10, permit
IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed
    ICMP type=0, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
NAT: s=10.0.0.12->192.168.2.1, d=177.10.1.3 [53]
IP: s=192.168.2.1 (Ethernet0), d=177.10.1.3 (Loopback0), g=10.0.1.2, Len 100,
forward
    ICMP type=0, code=0
IP: s=192.168.2.1 (Loopback0), d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100,
forward
    ICMP type=0, code=0
IP: NAT enab = 1 trans = 0 flags = 0
```

測試二

我們的另一個要求是允許主機與Internet通訊。對於此測試，我們從Host 1 **ping** Internet裝置。下面

是生成的show和debug命令。

最初NAT路由器中的NAT轉換表如下所示：

```
NAT-router# show ip Nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 192.168.2.1        10.0.0.12          ---                ---
NAT-router#
```

從Host 1發出ping命令後，我們看到：

```
Host-1# ping 177.10.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 177.10.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/92/96 ms
Host-1#
```

我們以上看到ping成功。NAT路由器中的NAT表現在如下：

```
NAT-router# show ip Nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.2.2:434   10.0.0.11:434      177.10.1.3:434     177.10.1.3:434
icmp 192.168.2.2:435   10.0.0.11:435      177.10.1.3:435     177.10.1.3:435
icmp 192.168.2.2:436   10.0.0.11:436      177.10.1.3:436     177.10.1.3:436
icmp 192.168.2.2:437   10.0.0.11:437      177.10.1.3:437     177.10.1.3:437
icmp 192.168.2.2:438   10.0.0.11:438      177.10.1.3:438     177.10.1.3:438
--- 192.168.2.1        10.0.0.12          ---                ---
NAT-router#
```

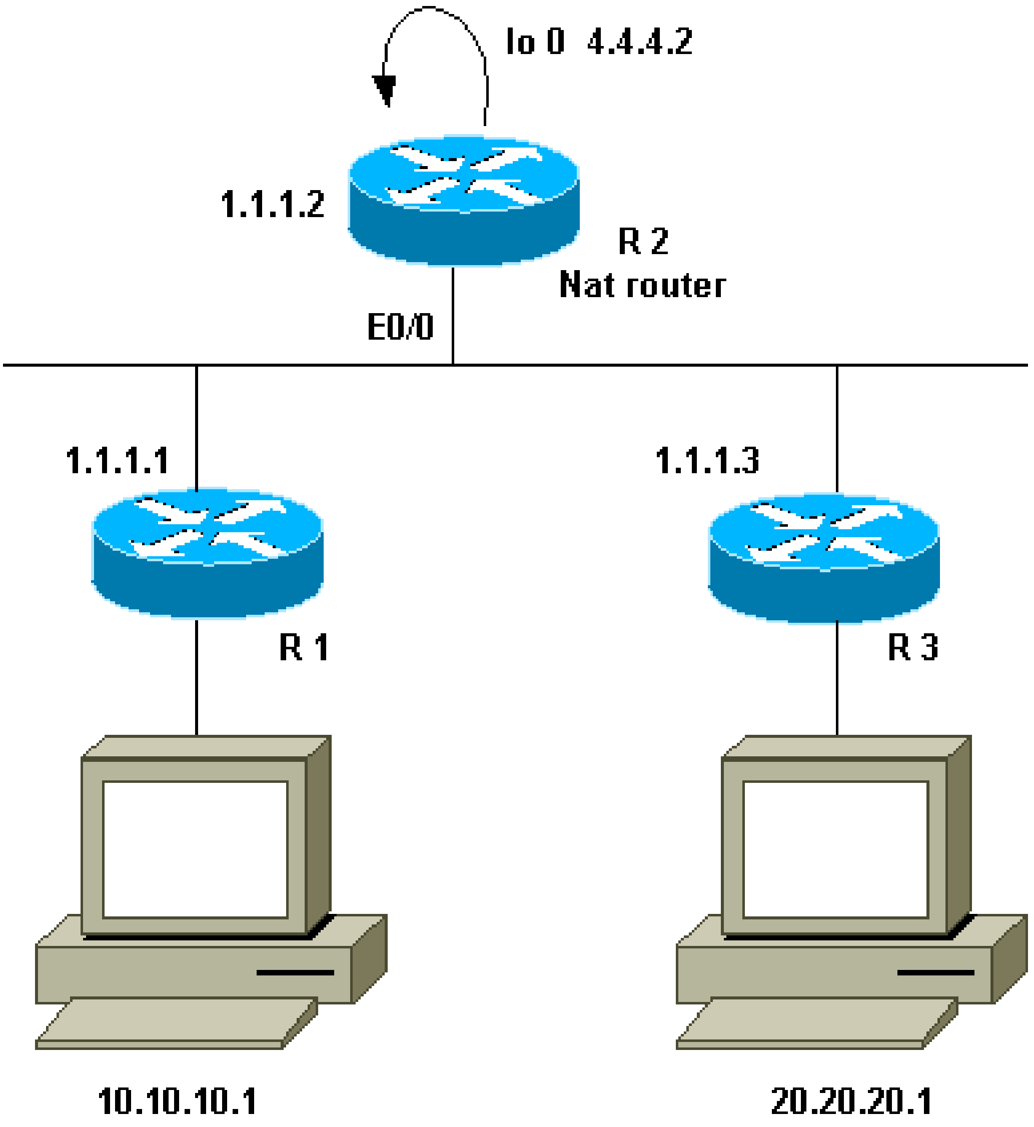
現在上面的NAT轉換表顯示了由動態NAT配置（與靜態NAT配置相反）產生的其他轉換。

以下debug輸出顯示了NAT路由器上發生的情況。

```
IP: NAT enab = 1 trans = 0 flags = 0
IP: s=10.0.0.11 (Ethernet0), d=177.10.1.3, Len 100, policy match
    ICMP type=8, code=0
IP: route map Nat-loop, item 10, permit
IP: s=10.0.0.11 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed
    ICMP type=8, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
!--- The above output shows the ICMP echo request packet originated by !--- Host 1 which is
policy-routed out the loopback interface. NAT: s=10.0.0.11->192.168.2.2, d=177.10.1.3 [8] IP:
s=192.168.2.2 (Ethernet0), d=177.10.1.3 (Loopback0), g=10.0.1.2, Len 100, forward ICMP type=8,
code=0 IP: s=192.168.2.2 (Loopback0), d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100, forward
ICMP type=8, code=0 IP: NAT enab = 1 trans = 0 flags = 0 !--- After the routing decision has
been made by the policy routing, !--- translation takes place, which translates the Host 1 IP
address of 10.0.0.11 !--- to an address from the "external" pool 192.168.2.2 as shown above. !--
- The packet is then forwarded out loopback 0 and finally out Ethernet 0 !--- to the Internet
device. IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2, Len 100, policy match ICMP type=0, code=0
IP: route map Nat-loop, item 10, permit IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2 (Loopback0),
Len 100, policy routed ICMP type=0, code=0 IP: Ethernet0 to Loopback0 10.0.1.2 IP: s=177.10.1.3
(Ethernet0), d=192.168.2.2 (Loopback0), g=10.0.1.2, Len 100, forward ICMP type=0, code=0 !---
The Internet device sends an ICMP echo response which matches our !--- policy, is policy-routed,
and forward out the Loopback 0 interface. IP: NAT enab = 1 trans = 0 flags = 0 NAT:
s=177.10.1.3, d=192.168.2.2->10.0.0.11 [8] IP: s=177.10.1.3 (Loopback0), d=10.0.0.11
(Ethernet0), g=10.0.0.11, Len 100, forward ICMP type=0, code=0 !--- The packet is looped back
into the loopback interface at which point !--- the destination portion of the address is
translated from 192.168.2.2 !--- to 10.0.0.11 and forwarded out the Ethernet 0 interface to the
local host. !--- The ICMP exchange is repeated for the rest of the ICMP packets, some of !---
which are shown below. IP: NAT enab = 1 trans = 0 flags = 0 IP: s=10.0.0.11 (Ethernet0),
d=177.10.1.3, Len 100, policy match ICMP type=8, code=0 IP: route map Nat-loop, item 10, permit
IP: s=10.0.0.11 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed ICMP type=8,
code=0 IP: Ethernet0 to Loopback0 10.0.1.2 NAT: s=10.0.0.11->192.168.2.2, d=177.10.1.3 [9] IP:
s=192.168.2.2 (Ethernet0), d=177.10.1.3 (Loopback0), g=10.0.1.2, Len 100, forward ICMP type=8,
code=0 IP: s=192.168.2.2 (Loopback0), d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100, forward
ICMP type=8, code=0 IP: NAT enab = 1 trans = 0 flags = 0 IP: s=177.10.1.3 (Ethernet0),
d=192.168.2.2, Len 100, policy match ICMP type=0, code=0 IP: route map Nat-loop, item 10, permit
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2 (Loopback0), Len 100, policy routed ICMP type=0,
code=0 IP: Ethernet0 to Loopback0 10.0.1.2 IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2
(Loopback0), g=10.0.1.2, Len 100, forward ICMP type=0, code=0 IP: NAT enab = 1 trans = 0 flags =
0 NAT: s=177.10.1.3, d=192.168.2.2->10.0.0.11 [9] IP: s=177.10.1.3 (Loopback0), d=10.0.0.11
(Ethernet0), g=10.0.0.11, Len 100, forward ICMP type=0, code=0
```

範例2網路圖表和組態

網路圖表



需求

我們希望兩個站點（R1和R3）後面的某些裝置能夠通訊。這兩個站點使用未註冊的IP地址，因此當它們相互通訊時，我們必須轉換這些地址。在本例中，主機10.10.10.1被轉換為200.200.200.1，主機20.20.20.1將被轉換為100.100.100.1。因此，我們需要在兩個方向上進行轉換。出於會計考慮，這兩個站點之間的流量必須通過R2。總之，我們的要求是：

- 位於R1後面的主機10.10.10.1需要與R3後面的主機20.20.20.1進行通訊，並使用其全域性地址。
- 這些主機之間的流量必須通過R2傳送。
- 對於我們的情況，我們需要靜態NAT轉換，如下面的配置所示。

NAT路由器配置

NAT路由器配置

```
interface Loopback0
 ip address 4.4.4.2 255.255.255.0
 ip Nat inside
!--- Creates a virtual interface called "loopback 0" and
assigns IP address !--- 4.4.4.2 to it. Also defines for
it a NAT inside interface. ! Interface Ethernet0/0 ip
address 1.1.1.2 255.255.255.0 no ip redirects ip Nat
outside ip policy route-map Nat !--- Assigns IP address
1.1.1.1/24 to e0/0. Disables redirects so that packets
!--- which arrive from R1 destined toward R3 are not
redirected to R3 and !--- visa-versa. Defines the
interface as NAT outside interface. Assigns !--- route-
map "Nat" used for policy-based routing. ! ip Nat inside
source static 10.10.10.1 200.200.200.1 !--- Creates a
static translation so packets received on the inside
interface !--- with a source address of 10.10.10.1 will
have their source address !--- translated to
200.200.200.1. Note: This implies that the packets
received !--- on the outside interface with a
destination address of 200.200.200.1 !--- will have the
destination translated to 10.10.10.1.


ip Nat outside source static 20.20.20.1 100.100.100.1
!--- Creates a static translation so packets received on
the outside interface !--- with a source address of
20.20.20.1 will have their source address !---
translated to 100.100.100.1. Note: This implies that
packets received on !--- the inside interface with a
destination address of 100.100.100.1 will !--- have the
destination translated to 20.20.20.1.


ip route 10.10.10.0 255.255.255.0 1.1.1.1
ip route 20.20.20.0 255.255.255.0 1.1.1.3
ip route 100.100.100.0 255.255.255.0 1.1.1.3
!
access-list 101 permit ip host 10.10.10.1 host
100.100.100.1
route-map Nat permit 10
 match ip address 101
 set ip next-hop 4.4.4.2
```

範例2 show和debug命令輸出

注意：輸出直譯器工具支援某些show命令，該工具允許您檢視show命令輸出的分析。使用**debug**指令之前，請先參閱有關Debug指令的重要資訊。

測試一

如以上配置所示，我們具有兩個靜態NAT轉換，在R2上使用**show ip Nat translation**命令可以看到這些轉換。

以下是在NAT路由器上執行的**show ip Nat translation**命令的輸出：

```
NAT-router# show ip Nat translation
Pro Inside global       Inside local       Outside local      Outside global
--- ---                 ---                100.100.100.1      20.20.20.1
--- 200.200.200.1       10.10.10.1         ---                ---
R2#
```

在本測試中，我們從R1背後的裝置(10.10.10.1)發出**ping**，且目的地為R3背後裝置(100.100.100.1)的全域性位址。在R2上執行**debug ip Nat**和**debug ip packet**將導致以下輸出：

```
IP: NAT enab = 1 trans = 0 flags = 0
IP: s=10.10.10.1 (Ethernet0/0), d=100.100.100.1, Len 100, policy match
    ICMP type=8, code=0
IP: route map Nat, item 10, permit
IP: s=10.10.10.1 (Ethernet0/0), d=100.100.100.1 (Loopback0), Len 100, policy
routed
    ICMP type=8, code=0
IP: Ethernet0/0 to Loopback0 4.4.4.2
!--- The above output shows the packet source from 10.10.10.1 destined !--- for 100.100.100.1
arrives on E0/0, which is defined as a NAT !--- outside interface. There is not any NAT that
needs to take place at !--- this point, however the router also has policy routing enabled for
!--- E0/0. The output shows that the packet matches the policy that is !--- defined in the
policy routing statements. IP: s=10.10.10.1 (Ethernet0/0), d=100.100.100.1 (Loopback0),
g=4.4.4.2, Len 100, forward ICMP type=8, code=0 IP: NAT enab = 1 trans = 0 flags = 0 !--- The
above now shows the packet is policy-routed out the loopback0 !--- interface. Remember the
loopback is defined as a NAT inside interface. NAT: s=10.10.10.1->200.200.200.1, d=100.100.100.1
[26] NAT: s=200.200.200.1, d=100.100.100.1->20.20.20.1 [26] !--- For the above output, the
packet is now arriving on the loopback0 !--- interface. Since this is a NAT inside interface, it
is important to !--- note that before the translation shown above takes place, the router !---
will look for a route in the routing table to the destination, which !--- before the translation
is still 100.100.100.1. Once this route look up !--- is complete, the router will continue with
translation, as shown above. !--- The route lookup is not shown in the debug output.


IP: s=200.200.200.1 (Loopback0), d=20.20.20.1 (Ethernet0/0), g=1.1.1.3, Len 100,
forward
    ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
!--- The above output shows the resulting translated packet that results is !--- forwarded out
E0/0.
```

這是來自路由器3後方裝置且目的地為路由器1後方裝置的響應資料包所導致的輸出：

```
NAT: s=20.20.20.1->100.100.100.1, d=200.200.200.1 [26]
NAT: s=100.100.100.1, d=200.200.200.1->10.10.10.1 [26]
 !--- The return packet arrives into the e0/0 interface which is a NAT !--- outside interface. In this direction (outside to inside), translation !--- occurs before routing. The above output shows the translation takes place. IP: s=100.100.100.1 (Ethernet0/0), d=10.10.10.1 (Ethernet0/0), Len 100, policy rejected -- normal forwarding ICMP type=0, code=0 IP: s=100.100.100.1 (Ethernet0/0), d=10.10.10.1 (Ethernet0/0), g=1.1.1.1, Len 100, forward ICMP type=0, code=0 !--- The E0/0 interface still has policy routing enabled, so the packet is !--- check against the policy, as shown above. The packet does not match the !--- policy and is forwarded normally.
```

摘要

本文檔演示了如何使用NAT和基於策略的路由來建立「單臂上的NAT」場景。請務必注意，此配置可能會降低運行NAT的路由器的效能，因為資料包可能會通過路由器進行進程交換。

相關資訊

- NAT支援頁面
- 技術支援 - Cisco Systems