設定網路位址轉譯

目錄

簡介

本文件說明如何在思科路由器上設定網路位址轉譯 (NAT)。

必要條件

需求

本文檔要求具備與NAT相關的術語的基本知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 2500系列路由器
- Cisco IOS®軟體版本12.2(10b)

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。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

配置和部署NAT的快速入門步驟

註：在本文檔中，當提及Internet或Internet裝置時，是指任何外部網路上的裝置。

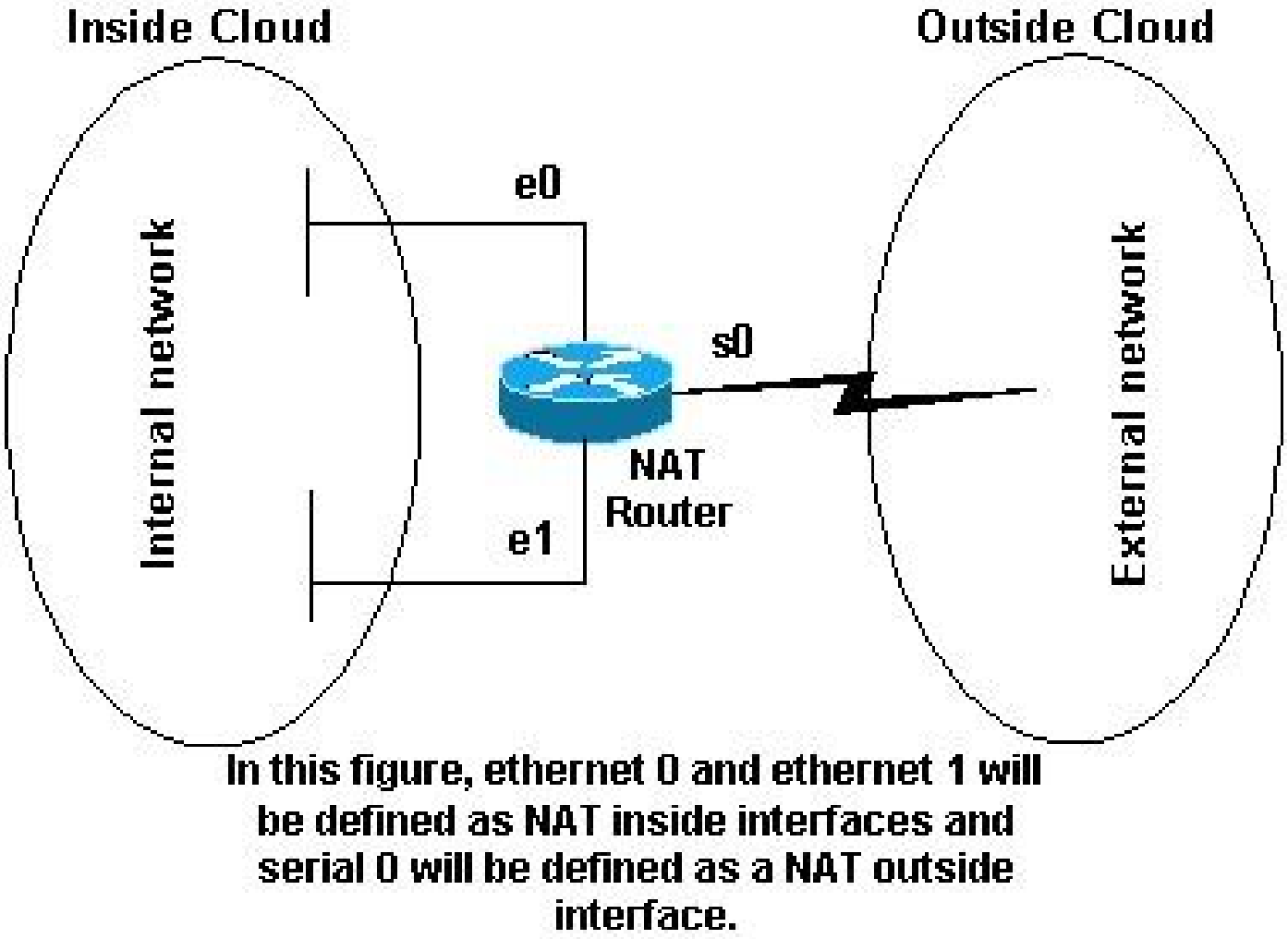
配置NAT時，有時很難知道從何處開始，特別是如果您不熟悉NAT。以下步驟指導您定義希望NAT執行的操作以及如何配置：

1. 定義NAT內部和外部介面。
    - 使用者是否存在於多個介面上？
    - 是否有多個可用於internet的介面？
2. 定義要通過NAT實現的目標。
    - 是否允許內部使用者訪問Internet?
    - 是否允許Internet訪問內部裝置（如郵件伺服器或Web伺服器）？
    - 是否要將TCP流量重定向到其他TCP埠或地址?
    - 您想在網路轉換期間使用NAT（例如，您更改了伺服器IP地址，並且直到可以更新所有希望未更新的客戶端能夠使用原始IP地址訪問伺服器並允許更新的客戶端使用新地址訪問伺服器的客戶端）嗎？
    - 是否要使用以允許重疊網路通訊?
3. 配置NAT以完成之前定義的任務。根據您在步驟2中定義的內容，您需要確定接下來要使用的功能：
    - 靜態NAT
    - 動態NAT
    - Overloading
    - 以上功能的任意組合。
4. 檢驗NAT操作。

這些NAT示例中的每一個都指導您完成上圖中的「快速啟動步驟」的第1步到第3步。這些示例說明了Cisco建議您部署NAT的一些常見場景。

定義NAT內部和外部介面

部署NAT的第一步是定義NAT內部和外部介面。您可以發現，將內部網路定義為內部，將外部網路定義為外部網路是最容易的。但是，內部和外部的條款也須接受仲裁。下圖顯示了一個示例。



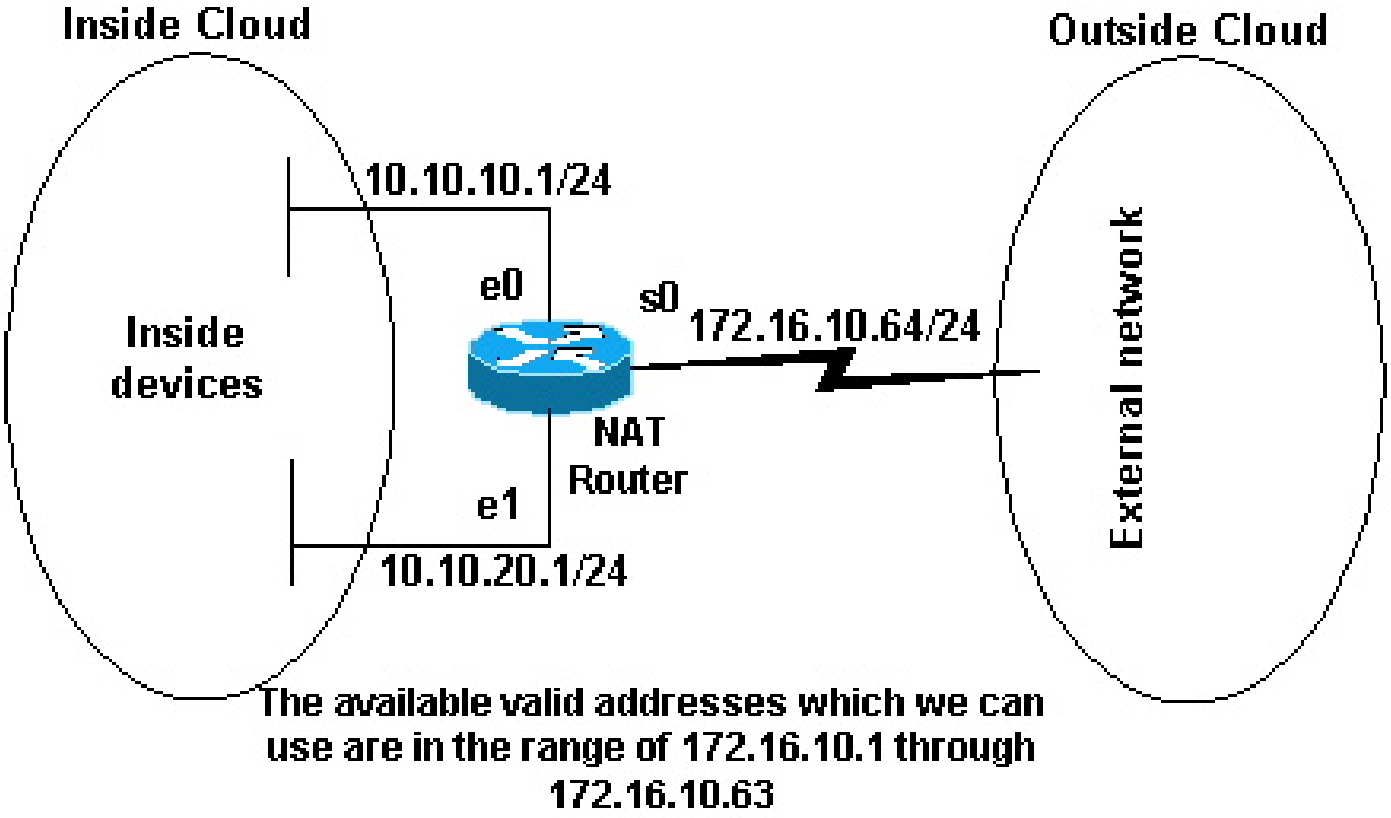
NAT拓撲

範例

1.允許內部使用者訪問網際網路

您可能希望允許內部使用者訪問Internet，但您沒有足夠的有效地址來容納所有人。如果與Internet中裝置的所有通訊均源自內部裝置，則需要單個有效地址或有效地址池。

此圖顯示路由器介面定義為inside和outside的簡單網路圖。



可用的有效地址

在本例中，您希望NAT允許內部的特定裝置（每個子網的前31個）與外部裝置發起通訊，並將它們的無效地址轉換為有效地址或地址池。地址池被定義為地址範圍172.16.10.1到172.16.10.63。

現在您可以配置NAT。為了完成前面映像中定義的內容，請使用動態NAT。使用動態NAT，路由器中的轉換表最初是空的，一旦需要轉換的流量通過路由器，就會填充轉換表。與靜態NAT相反，靜態NAT會靜態配置轉換，並將其放在轉換表中，無需任何流量。

在本示例中，您可以配置NAT將每個內部裝置轉換為唯一的有效地址，或將每個內部裝置轉換為相同的有效地址。第二種方法稱為 overloading 。這裡給出了如何配置每種方法的示例。

配置NAT以允許內部使用者訪問網際網路

NAT路由器
interface ethernet 0 ip address 10.10.10.1 255.255.255.0 ip nat inside *!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.* interface ethernet 1 ip address 10.10.20.1 255.255.255.0 ip nat inside

```
!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.


interface serial 0
 ip address 172.16.10.64 255.255.255.0
 ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.


ip nat pool no-overload 172.16.10.1 172.16.10.63 prefix 24


!--- Defines a NAT pool named no-overload with a range of addresses
!--- 172.16.10.1 - 172.16.10.63.


ip nat inside source list 7 pool no-overload


!--- Indicates that any packets received on the inside interface that
!--- are permitted by access-list 7 has
!--- the source address translated to an address out of the
!--- NAT pool "no-overload".


access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Access-list 7 permits packets with source addresses ranging from
!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

注意:Cisco強烈建議您不要使用permit any配置NAT命令引用的訪問清單。 如果您在NAT中使用permit any，則會佔用太多路由器資源，這可能會導致網路問題。

請注意，在先前的配置中，access-list 7只允許子網10.10.10.0中的前32個地址和子網10.10.20.0中的前32個地址。因此，僅轉換這些源地址。內部網路中可能有其它地址的其他裝置，但是這些裝置不會轉換。

最後一步是驗證NAT是否按預期運行。

配置NAT以允許內部使用者過載訪問網際網路

NAT路由器

```
interface ethernet 0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.


interface ethernet 1
```

```
 ip address 10.10.20.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.


interface serial 0
 ip address 172.16.10.64 255.255.255.0
 ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.


ip nat pool ovrld 172.16.10.1 172.16.10.1 prefix 24


!--- Defines a NAT pool named ovrld with a range of a single IP
!--- address, 172.16.10.1.


ip nat inside source list 7 pool ovrld overload


!--- Indicates that any packets received on the inside interface that
!--- are permitted by access-list 7 has the source address
!--- translated to an address out of the NAT pool named ovrld.
!--- Translations are overloaded, which allows multiple inside
!--- devices to be translated to the same valid IP address.

access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Access-list 7 permits packets with source addresses ranging from
!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

請注意，在之前的第二個配置中 ovrld,NAT池只有一個地址範圍。ip nat inside source list 7 pool ovrld overload 命令中使用的關鍵字overload允許NAT將多個內部裝置轉換為池中的單個地址。

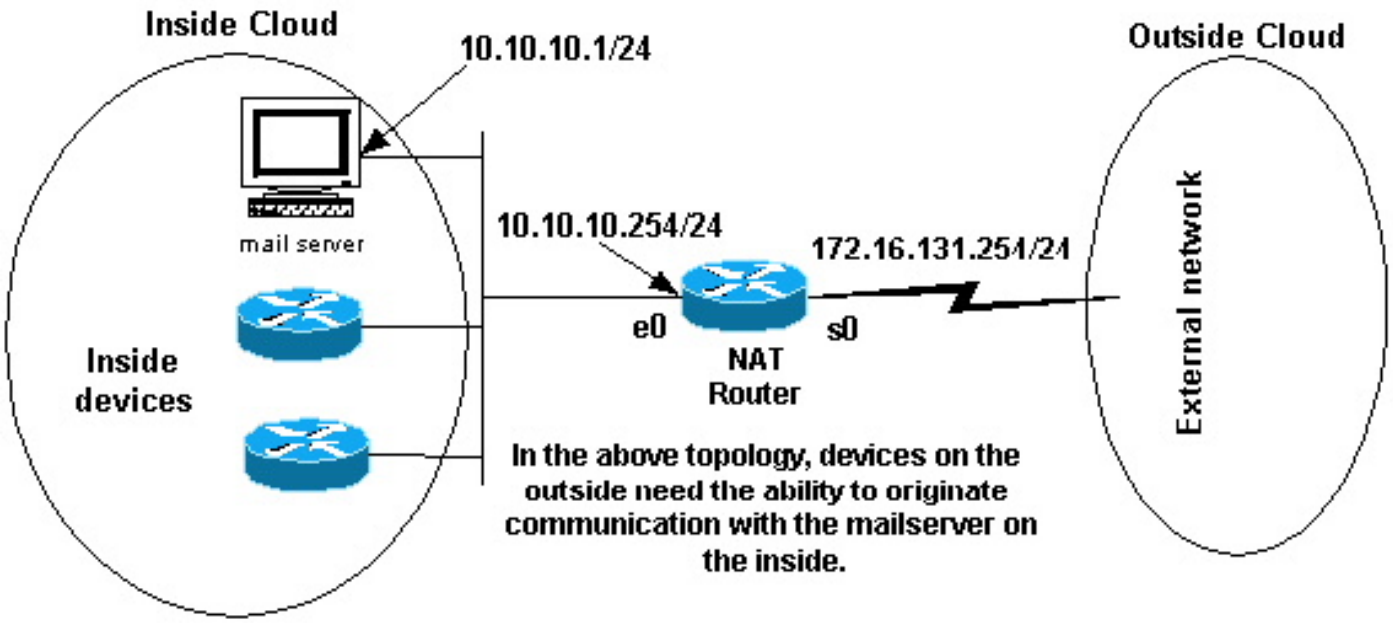
此命令isip nat inside source list 7 interface serial 0 overload的另一個變體將NAT配置為對分配給serial 0介面的地址進行過載。

設定overloading後，路由器會維護來自較高級別通訊協定（例如TCP或UDP連線埠號碼）的足夠資訊，將全域位址轉回正確的本地位址。有關全域性和本地地址的定義，請參閱NAT：全域性和本地定義。

最後一步是驗證NAT是否按預期運行。

2.允許Internet訪問內部裝置

您可能需要內部裝置與網際網路上的裝置交換資訊，從網際網路裝置（例如電子郵件）啟動通訊。Internet上的裝置通常向位於內部網路上的郵件伺服器傳送電子郵件。



Originate Communications

配置NAT以允許網際網路訪問內部裝置

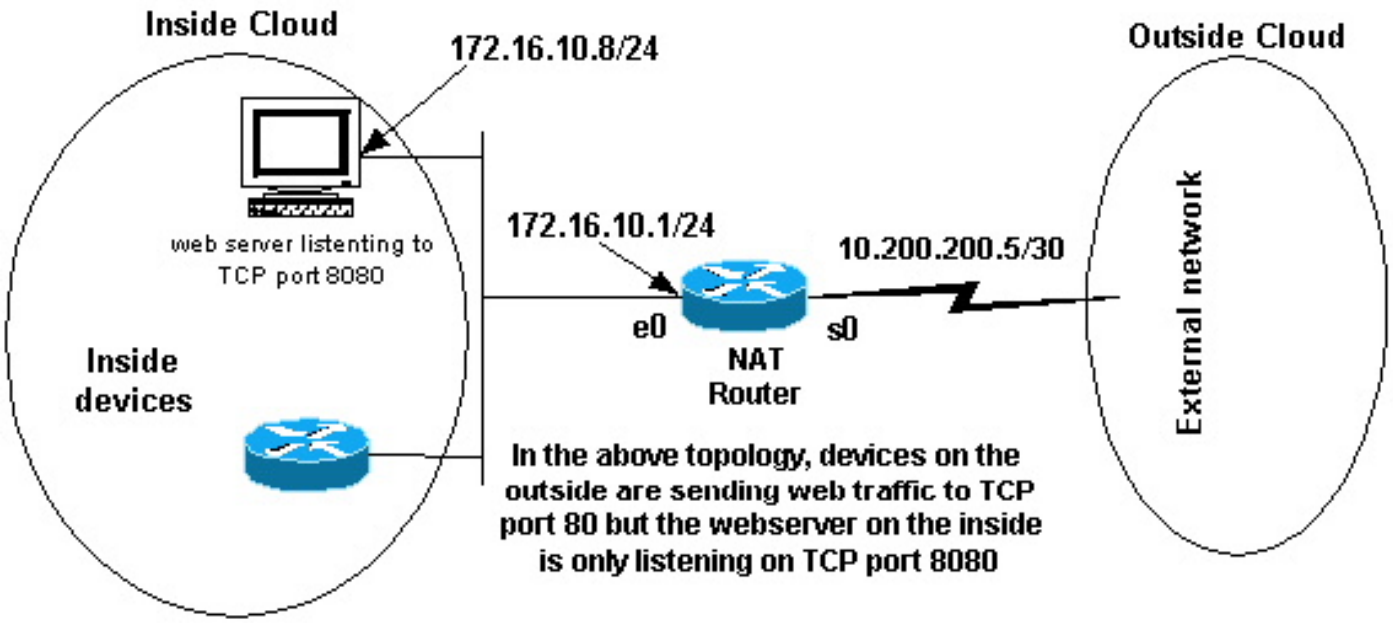
在本示例中，您首先定義NAT內部和外部介面，如前面的網路圖所示。

其次，您定義希望內部使用者能夠發起與外部的通訊。外部裝置必須能夠僅與內部郵件伺服器發起通訊。

第三步是配置NAT。為了實現您定義的功能，您可以同時配置靜態和動態NAT。有關如何配置此示例的詳細資訊，請參閱同時配置靜態和動態NAT。 最後一步是驗證NAT是否按預期運行。

3.將TCP流量重定向到另一個TCP埠或地址

內部網路上的Web伺服器是另一個示例，它說明何時需要網際網路上的裝置與內部裝置建立通訊。在某些情況下，可以將內部Web伺服器配置為偵聽TCP埠（而不是埠80）上的Web流量。例如，可以將內部Web伺服器配置為偵聽TCP埠8080。在這種情況下，您可以使用NAT將目的地為TCP埠80的流量重定向到TCP埠8080。



Web流量TCP埠

定義如前面的網路圖所示的介面後，您可以決定希望NAT將目的地為172.16.10.8:80的外部資料包重定向到172.16.10.8:8080。您可以使用static nat 命令轉換TCP埠號來實現此目的。此處顯示了一個範例組態。

配置NAT將TCP流量重定向到另一個TCP埠或地址

NAT路由器
interface ethernet 0 ip address 172.16.10.1 255.255.255.0 ip nat inside *!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.* interface serial 0 ip address 10.200.200.5 255.255.255.252 ip nat outside *!--- Defines serial 0 with an IP address and as a NAT outside interface.* ip nat inside source static tcp 172.16.10.8 8080 172.16.10.8 80 *!--- Static NAT command that states any packet received in the inside* *!--- interface with a source IP address of 172.16.10.8:8080 is* *!--- translated to 172.16.10.8:80.*

註：靜態NAT命令的配置說明表示在源地址為172.16.10.8:8080的內部介面中收到的任何資料包都將轉換為172.16.10.8:80。這也意味著在目的地址為172.16.10.8:80的外部介面上收到的

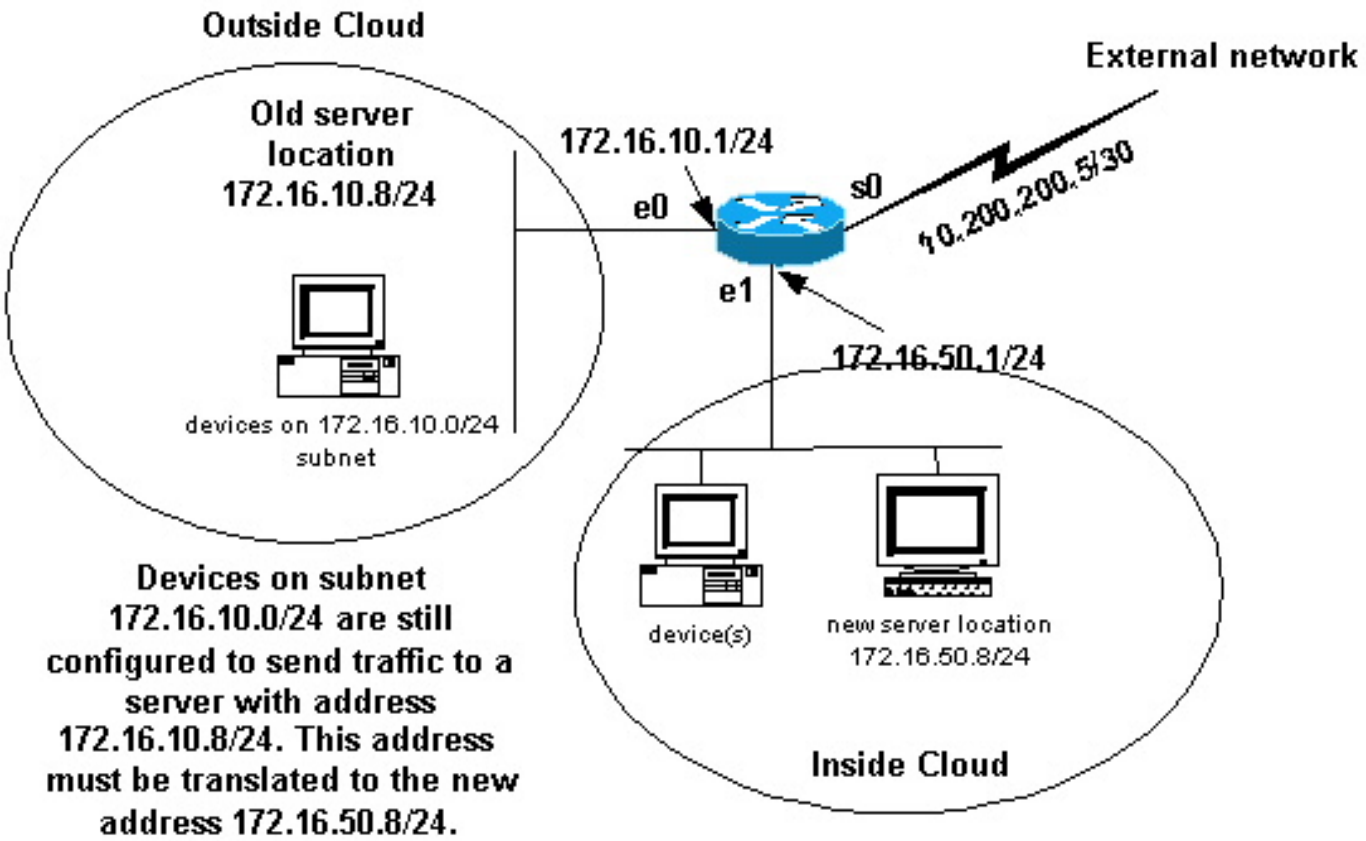
任何資料包都將目的地轉換為172.16.10.8:8080。

最後一步是驗證NAT是否按預期運行。

```
show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 172.16.10.8:80     172.16.10.8:8080   ---                ---
```

4.使用NAT進行網路過渡

當您需要重新確定網路中的裝置地址或將一台裝置替換為另一台裝置時，NAT非常有用。例如，如果網路中的所有裝置都使用特定的伺服器，並且此伺服器需要替換為具有新IP地址的新伺服器，則重新配置所有網路裝置以使用新伺服器地址將需要一些時間。同時，您可以使用NAT來配置具有舊地址的裝置，以轉換其資料包與新伺服器通訊。



NAT網路過渡

一旦定義了NAT介面（如前面的影象所示），就可以決定希望NAT允許從外部發往舊伺服器地址(172.16.10.8)的資料包被轉換並傳送到新的伺服器地址。請注意，新伺服器位於另一個LAN上，並且如果可能，必須配置此LAN上的裝置或可通過此LAN訪問的任何裝置（網路內部裝置），以使用新的伺服器IP地址。

您可以使用靜態NAT滿足您的需求。以下是組態範例。

配置NAT以通過網路轉換使用

NAT路由器

```
interface ethernet 0
 ip address 172.16.10.1 255.255.255.0
 ip nat outside

!--- Defines Ethernet 0 with an IP address and as a NAT outside interface.


interface ethernet 1
 ip address 172.16.50.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.


interface serial 0
 ip address 10.200.200.5 255.255.255.252

!--- Defines serial 0 with an IP address. This interface is not
!--- participating in NAT.


ip nat inside source static 172.16.50.8 172.16.10.8

!--- States that any packet received on the inside interface with a
!--- source IP address of 172.16.50.8 is translated to 172.16.10.8.
```

註：本示例中的內部源NAT命令還意味著在外部介面上接收的目的地址為172.16.10.8的資料包已將目的地址轉換為172.16.50.8。

最後一步是檢驗NAT是否按預期運行。

5.對重疊的網路使用NAT

當您將IP地址分配給已被Internet中的其他裝置使用的內部裝置時，網路會發生重疊。這兩個公司在其網路中都使用RFC 1918 IP地址，因此也會發生這些網路。這兩個網路需要通訊，最好不要重新定址其所有裝置。

一對一對映和多對多對映之間的區別

靜態NAT配置建立一對一對映，並將特定地址轉換為另一個地址。這種型別的配置在NAT表中建立永久條目（只要該配置存在），並使內部主機和外部主機都能啟動連線。這對於提供應用服務（如郵件、Web、FTP等）的主機最有用。舉例來說：

<#root>

```
Router(config)#
ip nat inside source static 10.3.2.11 10.41.10.12
Router(config)#
ip nat inside source static 10.3.2.12 10.41.10.13
```

當可用地址少於要轉換的實際主機數量時，動態NAT很有用。當主機發起連線並在地址之間建立一對一對映時，它會在NAT表中建立一個條目。但是，對映可能有所不同，這取決於通訊時地址池中可用的註冊地址。動態NAT僅允許從為其配置會話的內部或外部網路啟動會話。如果主機在可以配置的特定時間段內不通訊，則從轉換表中刪除動態NAT條目。然後，該地址將返回到池中以供另一主機使用。

例如，完成詳細配置的以下步驟：

1. 建立地址池。

   ```
   <#root>
   Router(config)#
   ip nat pool MYPOOLEXAMPLE 10.41.10.1 10.41.10.41 netmask 255.255.255.0
   ```

2. 為必須對映的內部網路建立訪問清單。

   ```
   <#root>
   Router(config)#
   access-list 100 permit ip 10.3.2.0 0.0.0.255 any
   ```

3. 將選擇內部網路10.3.2.0 0.0.0.255的訪問清單100關聯到池MYPOOLEXAMPLE，然後使地址過載。

   ```
   <#root>
   Router(config)#
   ip nat inside source list 100 pool MYPOOLEXAMPLE overload
   ```

檢驗NAT運行情況

配置NAT後，檢驗其是否按預期運行。您可以通過多種方式完成此操作：使用網路分析器、show命令或debug命令。有關NAT驗證的詳細示例，請參閱驗證NAT操作和基本NAT。

結論

本文檔中的示例演示了可幫助您配置和部署NAT的快速入門步驟。

這些快速入門步驟包括：

1. 定義NAT內部和外部介面。
2. 您想通過NAT實現什麼。
3. 配置NAT以完成您在步驟2中定義的操作。
4. 檢驗NAT操作。

在上述每個示例中，都使用了各種形式的ip nat insidecommand。您還可以使用ip nat outsidecommand來實現相同的目標，但請記住NAT的操作順序。有關使用ip nat outside命令的配置示例，請參閱使用IP NAT Outside Source List命令的示例配置。

前面的示例還演示了這些操作：

指令	動作
ip nat inside source	• 轉換從內部傳輸到外部的IP資料包的源。 • 轉換從外部傳送到內部的IP資料包的目的地。
ip nat outside source	• 轉換從外部傳輸到內部的IP資料包的源。 • 轉換從內部傳輸到外部的IP資料包的目的地。

相關資訊

- NAT：本地和全域性定義.
- NAT支援頁面
- IP 路由通訊協定支援頁面
- IP 路由支援頁面
- IP 定址服務
- NAT操作順序
- 有關Cisco IOS NAT的常見問題
- 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）。