在重疊網路中使用NAT

目錄

簡介

本檔案將示範如何對重疊網路使用網路位址轉譯(NAT)。當您將某個IP地址分配給您網路中的裝置（該裝置已經合法擁有並分配給Internet或外部網路上的其他裝置）時，就會產生重疊網路。當兩家公司(兩家公司在其網路中都使用RFC 1918 IP地址)合併時，也會產生重疊網路。這兩個網路需要通訊，最好無需重新定址其所有裝置。

必要條件

需求

瞭解IP定址、IP路由和網域名稱系統(DNS)的基本知識有助於瞭解本檔案的內容。

採用元件

對NAT的支援開始於Cisco IOS®軟體版本11.2。有關平台支援的詳細資訊，請參閱NAT常見問題。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定

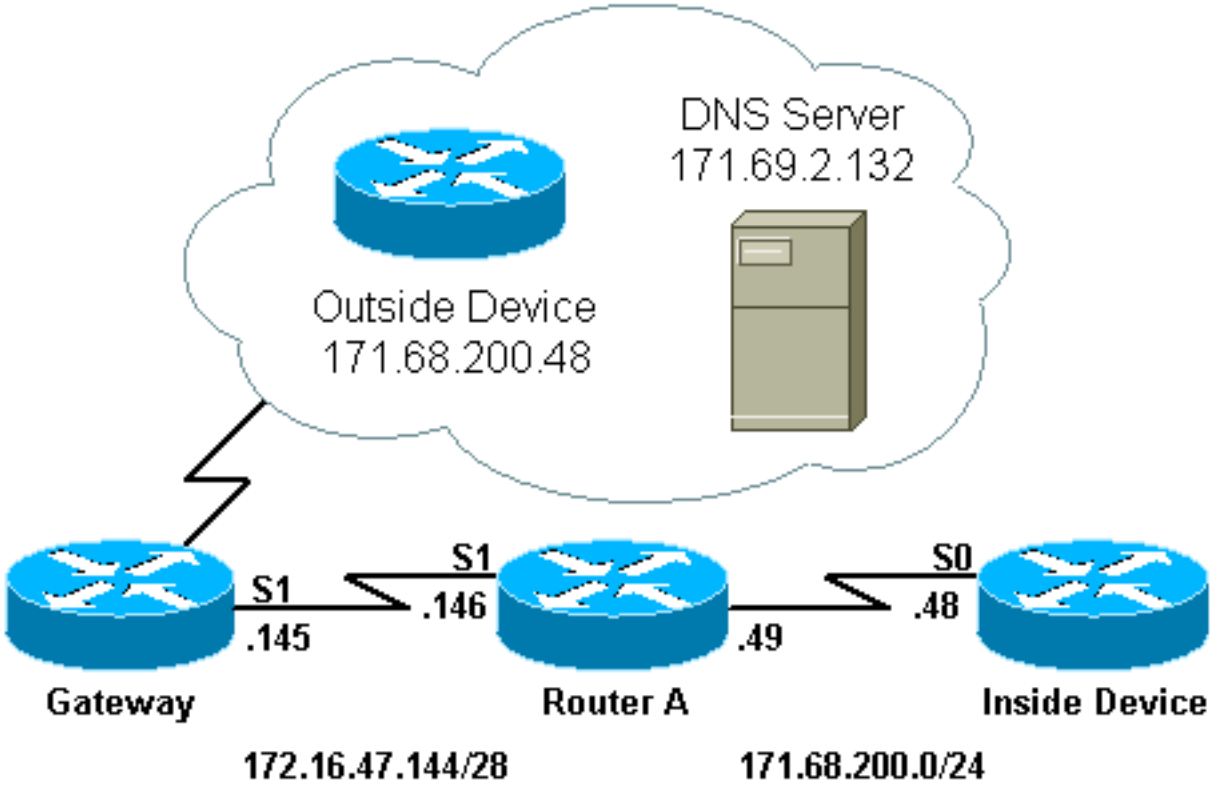
本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本文檔使用下圖所示的網路設定。

請注意，內部裝置的IP地址與希望與之通訊的外部裝置相同。



組態

路由器A配置了NAT，以便它將內部裝置轉換為地址池的「test-loop」，並將外部裝置轉換為地址池的「test-dns」。 有關此配置如何幫助重疊的說明，請參閱下面的配置表。

路由器A
!   version 11.2   no service udp-small-servers   no service tcp-small-servers   !   hostname Router-A   !   !   ip domain-name cisco.com   ip name-server 171.69.2.132   !   interface Loopback0   ip address 1.1.1.1 255.0.0.0   !   interface Ethernet0   ip address 135.135.1.2 255.255.255.0   shutdown   !   interface Serial0   ip address 171.68.200.49 255.255.255.0   ip nat inside

```
 no ip mroute-cache
 no ip route-cache
 no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside
 no ip mroute-cache
 no ip route-cache
!
ip nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat pool test-dns 172.16.47.177 172.16.47.180 prefix-
length 28
ip nat inside source list 7 pool test-loop
ip nat outside source list 7 pool test-dns
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
access-list 7 permit 171.68.200.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

為了讓上述配置在內部裝置與外部裝置通訊時幫助實現重疊，必須使用外部裝置的域名。

內部裝置無法使用外部裝置的IP地址，因為它與分配給其自身（內部裝置）的地址相同。 因此，內部裝置將傳送DNS查詢來查詢外部裝置的域名。內部裝置的IP地址將是此查詢的源，該地址將轉換為「測試循環」池中的地址，因為已配置**ip nat inside source list**命令。

DNS伺服器使用與資料包負載中的外部裝置域名關聯的IP地址來回覆來自池「test-loop」的地址。應答資料包的目的地址被轉換回內部裝置的地址，然後由於**ip nat outside source list**命令，應答資料包的負載中的地址被轉換為池「test-dns」中的地址。因此，內部裝置獲知外部裝置的IP地址是來自「test-dns」池的地址之一，並且在與外部裝置通訊時將使用此地址。此時運行NAT的路由器負責轉換。

此過程可在疑難排解一節中詳細看到。使用重疊地址的裝置可以不使用DNS相互通訊，但在這種情況下，必須配置靜態NAT。以下是如何進行此操作的示例。

路由器A

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
!

ip domain-name cisco.com
ip name-server 171.69.2.132
!
```

```
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 no ip mroute-cache
 no ip route-cache
 no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside
 no ip mroute-cache
 no ip route-cache
!
ip nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat inside source list 7 pool test-loop
ip nat outside source static 171.68.200.48 172.16.47.177
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
ip route 172.16.47.160 255.255.255.240 Serial0
!--- This line is necessary to make NAT work for return
traffic. !--- The router needs to have a route for the
pool to the inside !--- NAT interface so it knows that a
translation is needed. access-list 7 permit 171.68.200.0
0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

通過上述配置，當內部裝置想與外部裝置通訊時，它現在可以使用IP地址172.16.47.177，並且無需使用DNS。如上所述，內部裝置地址的轉換仍以動態方式完成，這意味著路由器必須在建立轉換之前從內部裝置獲取資料包。因此，內部裝置必須啟動所有連線，以便內部裝置和外部裝置通訊。如果需要外部裝置啟動與內部裝置的連線，則必須靜態配置內部裝置的地址。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

如前所述，內部裝置使用DNS與外部裝置通訊的過程可通過以下故障排除過程詳細檢視。

目前，使用**show ip nat translations**命令看不到轉換表中的任何轉換。以下範例改用**debug ip**

packet和debug ip nat指令。

註：debug命令會產生大量輸出。僅當IP網路上的流量較低時才使用它，這樣系統上的其他活動就不會受到負面影響。

```
Router-A# show ip nat translations
Router-A# show debug
Generic IP:
  IP packet debugging is on (detailed)
  IP NAT debugging is on
```

當內部裝置將其DNS查詢傳送到位於NAT域之外的DNS伺服器時，由於**ip nat inside命令，DNS查詢的源地址（內部裝置的地址）會被轉換。**這可以在下面的調試輸出中看到。

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=6988, dst=53
```

當DNS伺服器傳送DNS回覆時，由於**ip nat outside命令，將轉換DNS回覆的**負載。

注意：NAT不會檢視DNS應答的負載，除非在應答資料包的IP報頭上進行轉換。請參閱上述路由器配置中的**ip nat outside source list 7 pool**命令。

以下調試輸出中的第一個NAT消息顯示路由器識別DNS應答並將負載中的IP地址轉換為172.16.47.177。第二個NAT消息顯示路由器轉換DNS應答的目的地，以便可以將應答轉發回執行初始DNS查詢的內部裝置。報頭的目的地部分（內部全域性地址）將轉換為內部本地地址。

DNS回覆的負載會轉換：

```
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
```

DNS應答資料包中IP報頭的目的地部分將被轉換：

```
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65371]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=6988
```

現在來看看另一個DNS查詢和回覆：

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=7419, dst=53
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65388]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=7419
```

現在DNS的負載已經轉換，我們的轉換表包含外部裝置的外部本地和全域性地址條目。有了表中的這些條目，我們現在可以完全轉換在內部裝置和外部裝置之間交換的ICMP資料包的報頭。下面的debug輸出中讓我們來看一下此交換。

以下輸出顯示正在轉換的源地址（內部裝置的地址）。

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [406]
```

在這裡，目標地址（外部裝置的外部本地地址）被轉換。

```
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [406]
```

轉換後，IP資料包如下所示：

```
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

以下輸出顯示在返回資料包上轉換的源地址（外部裝置的地址）。

```
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16259]
```

現在，返回資料包的目標地址（內部裝置的全域性地址）被轉換。

```
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16259]
```

轉換後，返回資料包如下所示：

```
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

資料包交換在內部裝置和外部裝置之間繼續進行。

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [407]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [407]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16262]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16262]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [408]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [408]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16267]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16267]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [409]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [409]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16273]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16273]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [410]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [410]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16277]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16277]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

完成外部和內部之間的資料包交換後，我們可以檢視包含三個條目的轉換表。第一個條目是在內部裝置傳送DNS查詢時建立的。第二個條目是在轉換DNS回覆的負載時建立的。第三個條目是在內部

裝置和外部裝置之間交換ping時建立的。第三個條目是前兩個條目的摘要，用於更高效的翻譯。

```
Router-A# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.161      171.68.200.48      ---                ---
--- ---                ---                172.16.47.177      171.68.200.48
--- 172.16.47.161      171.68.200.48      172.16.47.177      171.68.200.48
```

請注意，當您試圖通過在單個Cisco路由器上運行動態NAT在兩個重疊網路之間建立連線時，必須使用DNS建立外部本地到外部全域性轉換。如果不使用DNS，可以使用靜態NAT建立連線，但更難管理。

相關資訊

- NAT支援頁面
- 技術支援 - Cisco Systems