

Cisco ONS 15454和NAT

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[NAT](#)

[傳統NAT](#)

[雙向NAT](#)

[兩次NAT](#)

[ONS 15454和NAT相容性](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹不同型別的網路地址轉換(NAT)，並將每種型別的NAT對映到支援該型別的相關ONS 15454軟體版本。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ONS 15454
- CTC
- NAT

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ONS 15454的所有版本

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。如果您的網路正在作用，請確保您已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](#)。

背景資訊

在現場的許多情況下，不同的NAT方案正在發揮作用，無法正常工作。您可以根據症狀確定其中大多數情形。大多數問題源於網路元素(NE)無法啟動回思科傳輸控制器(CTC)工作站的連線。

通常，當CTC不支援特定的NAT配置時，CTC會以特定的時間間隔持續丟棄並重新連線到節點。在較新的版本中，CTC可以從斷開連線中恢復，而無需從檢視中丟棄。在此類版本中，您可以在通過CTC與節點互動時注意到此問題。

由於訪問清單指示安全性的外部防火牆配置不正確，也會出現相同的症狀。訪問清單不允許NE向已定義的IP地址和/或埠發起某些連線，或從這些地址和/或埠向CTC工作站發起某些連線。當外部防火牆超時設定太短時，也會發生頻繁斷開連線。

有關可用於ONS 15454的防火牆存取清單範例，請參閱[Cisco ONS 15454參考手冊5.0版](#)中的[外部防火牆](#)一節。

NAT

NAT允許單個裝置（例如路由器）作為Internet和本地網路之間的代理。本節介紹各種型別的NAT。

有關詳細資訊，請參閱[RFC 2663 - IP網路地址轉換器術語和注意事項](#)。

傳統NAT

傳統NAT允許私有網路中的主機透明地訪問外部網路中的主機。傳統NAT從專用網路發起出站會話。

本節簡要介紹傳統NAT的兩個變體：

- **基本NAT:**基本NAT保留外部地址塊。當主機發起與外部域的會話時，基本NAT使用這些地址轉換私有域中的主機地址。
- **網路位址連線埠轉譯(NAPT):**NAPT進一步擴展了翻譯的概念。NAPT還轉換傳輸識別符號，例如TCP和UDP埠號以及ICMP查詢識別符號。這種轉換將多個專用主機的傳輸識別符號多路複用到單個外部地址的傳輸識別符號中。**注意：**NAPT也稱為埠地址轉換(PAT)。

雙向NAT

外部網路上的裝置發起與內部裝置的交易。為了允許此啟動，對NAT的基本版本進行了增強以包括高級功能。這種增強通常稱為雙向NAT，但也稱為雙向NAT和入站NAT。使用雙向NAT，您可以從公共網路和專用網路中的主機啟動會話。當您在任一方向建立連線時，專用網路地址會以靜態或動態方式繫結到全域性唯一地址。

NAT在入站事務上的效能比出站NAT更困難。原因是內部網路通常知道外部裝置的IP地址，因為這些裝置是公共裝置。但是，外部網路不知道內部網路的私有地址。即使外部網路知道專用網路的IP地址，您也永遠無法指定這些IP地址作為從外部發起的IP資料包的目標，因為這些地址不可路由。

您可以使用以下兩種方法之一解決隱藏地址問題：

- 靜態對映
- TCP/IP網域名稱系統(DNS)

注意：在本檔案中，雙向NAT意味著基本NAT，但基本NAT不意味著雙向NAT。

兩次NAT

兩次NAT是NAT的變體。當資料包跨越地址領域時，兩次NAT都會修改源地址和目標地址。此概念與傳統NAT和雙向NAT相反，後者僅轉換其中一個地址（源或目標）。

ONS 15454和NAT相容性

下表顯示了ONS 15454和NAT相容性：

NAT型別	CTC Sees	閘道網路元件 (GNE)See	支援的CTC版本
基本 NAT	GNE IP	轉換後的IP	版本3.3
NAPT	GNE IP	轉換後的IP	版本4.0
雙向 NAT	轉換後的IP	CTC IP	版本5.0
兩次 NAT	轉換後的IP	轉換後的IP	版本5.0

疑難排解

如果NE和CTC之間出現通訊問題，`fhDebug`命令的輸出包含以下錯誤消息：

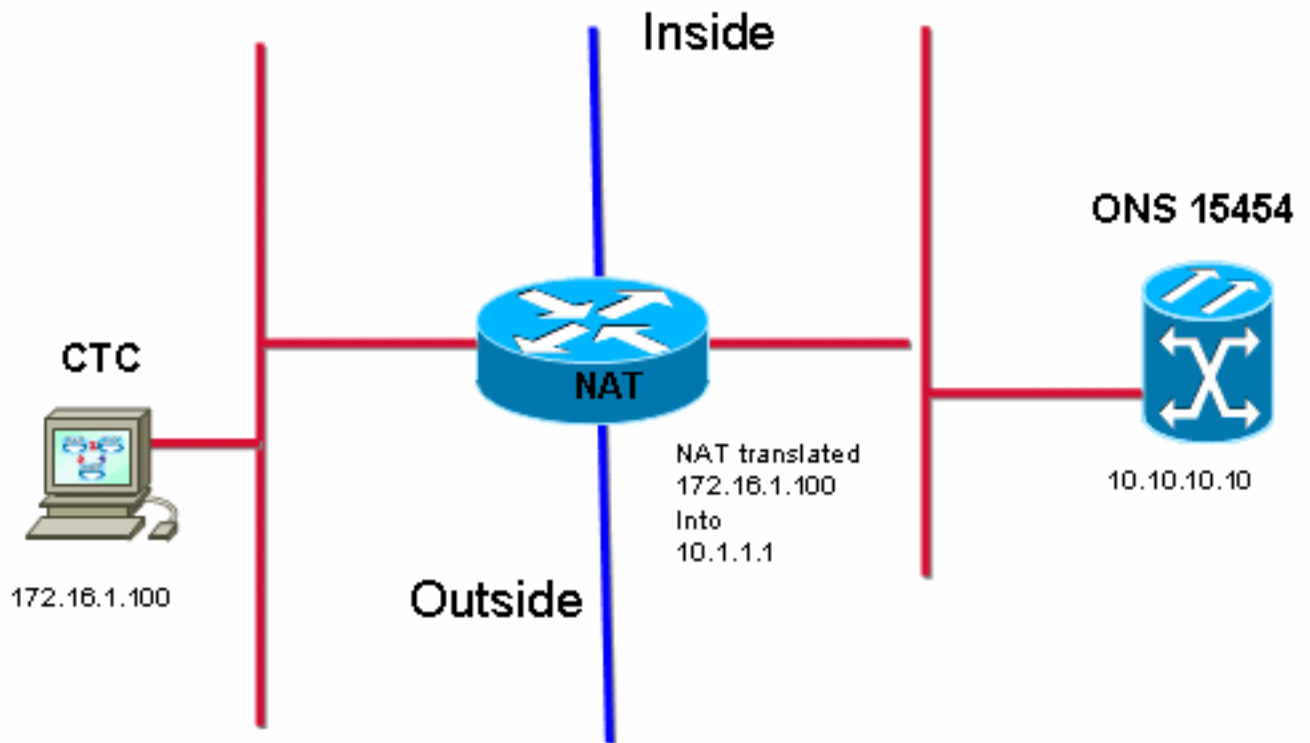
```
OCT 27 18:35:37.09 UTC ERROR      ObjectChange.cc:432    tEventMgr  
CORBA::NO_IMPLEMENT/0x3d0004 updating [192.168.1.100:EventReceiver]. Marking c
```

```
OCT 27 18:36:17.09 UTC DEBUG      AlarmImpl.cc:353      tEventMgr  
Removing corba client [192.168.1.100:EventReceiver] from auton msg list
```

導致此錯誤的原因有多種。但是，如果錯誤在正常的可預測時間間隔（通常為~2或~4分鐘）發生，則原因可能是存在CTC不支援的NAT型別，或者防火牆沒有必要的埠許可權。

請注意，172.16.1.100是CTC工作站的IP地址，10.1.1.1是NAT地址(請參見圖1)。

圖1 — 拓撲



以下是inetstatShow命令的部分輸出：

```
-> inetstatShow
Active Internet connections (including servers)
PCB      Typ Rx-Q Tx-Q Local Address      Foreign Address (state)
-----
2145984  TCP    0   0 10.10.10.10:1052  10.1.1.1:1029  SYN_SENT
21457f8  TCP    0   0 10.10.10.10:80   10.1.1.1:1246  TIME_WAIT
2145900  TCP    0   0 10.10.10.10:57790 10.1.1.1:1245  ESTABLISHED --- ISP assigned address
21453d8  TCP    0   0 10.10.10.10:80   10.1.1.1:1244  TIME_WAIT
2144f34  TCP    0   0 10.10.10.10:80   10.1.1.1:1238  TIME_WAIT
2144eb0  TCP    0   0 10.10.10.10:1080 10.1.1.1:1224  ESTABLISHED --- ISP assigned address
```

此輸出未顯示此地址的證據。輸出顯示ISP使用的公有地址，這是傳統NAT方案的證據。

為了識別雙向NAT和兩次NAT，您需要與CTC工作站來自同一網段的監聽器跟蹤。理想情況下，在CTC工作站上運行的監聽器是最合適的。

相關資訊

- [Cisco ONS 15454參考手冊，版本5.0](#)
- [技術支援與文件 - Cisco Systems](#)