

# 了解NAT的运行顺序

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[NAT 概述](#)

[NAT 配置和输出](#)

[相关信息](#)

## 简介

本文档介绍使用NAT处理事务的顺序取决于数据包在网络中内部或外部传输的方向。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 网络地址转换 (NAT)。有关 NAT 的更多信息，请参见 NAT 的工作原理。

### 使用的组件

本文档中的信息基于Cisco IOS®软件版本12.2(27)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

### 规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

## 背景信息

本文档介绍使用网络地址转换(NAT)处理事务的顺序取决于数据包是从内部网络传输到外部网络，还是从外部网络传输到内部网络。

## NAT 概述

在此表中，当 NAT 执行全局到本地或本地到全局转换时，每个数据流中的转换各不相同。

### 内部到外部

- 如果使用的是 IPsec，则检查输入访问列表
- 解密 — 对于 CET ( Cisco 加密技术 ) 或 IPsec
- 检查输入访问列表
- 检查输入速率限制
- 输入记账
- 重定向到 Web 缓存
- 策略路由
- 路由
- **NAT 内部到外部 ( 本地到全局的转换 )**
- 加密 ( 检查映射和标记是否加密 )
- 检查输出访问列表
- 检查 ( 基于上下文的访问控制 (CBAC) )
- TCP 拦截
- 加密
- 队列

### 外部到内部

- 如果使用的是 IPsec，则检查输入访问列表
- 解密 - 对于 CET 或 IPsec
- 检查输入访问列表
- 检查输入速率限制
- 输入记账
- 重定向到 Web 缓存
- **NAT 外部到内部 ( 全局到本地的转换 )**
- 策略路由
- 路由
- 加密 ( 检查映射和标记是否加密 )
- 检查输出访问列表
- 检查 CBAC
- TCP 拦截
- 加密
- 队列

## NAT 配置和输出

此示例说明运算顺序对 NAT 有何影响。在这种情况下，只会显示 NAT 和路由。

在上个示例中，路由器 A 配置为将内部本地地址 172.31.200.48 转换为 172.16.47.150，如此配置中所示。

```
!  
version 11.2  
no service udp-small-servers  
no service tcp-small-servers  
!  
hostname Router-A  
!  
enable password ww  
!  
ip nat inside source static 172.31.200.48 172.16.47.150  
  
!--- This command creates a static NAT translation  
!--- between 172.31.200.48 and 172.16.47.150 ip domain-name cisco.com ip name-server  
172.31.2.132 ! interface Ethernet0 no ip address shutdown ! interface Serial0 ip address  
172.16.47.161 255.255.255.240 ip nat inside  
  
!--- Configures Serial0 as the NAT inside interface 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  
  
!--- Configures Serial1 as the NAT outside interface no ip mroute-cache no ip route-cache ! no  
ip classless ip route 0.0.0.0 0.0.0.0 172.16.47.145  
  
!--- Configures a default route to 172.16.47.145 ip route 172.31.200.0 255.255.255.0  
172.16.47.162 ! ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 password ww login ! end  
转换表表明所需转换存在。
```

```
Router-A#show ip nat translation
```

```
Pro Inside global      Inside local      Outside local      Outside global
--- 172.16.47.150      172.31.200.48      ---                ---
```

此输出来自路由器 A，此时 debug ip packet detail 和 debug ip nat 启用，且从设备 172.31.200.48 发出的 ping 的目的地为 172.16.47.142。

**注意:** Debug 命令会生成大量输出。只有 IP 网络上的流量较低时才能使用此类命令，以避免系统上的其他活动受到负面影响。在发出 debug 命令之前，请参阅有关 debug 命令的重要信息。

```
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
```

由于上一个输出中没有 NAT 调试消息，因此不会使用当前静态转换，并且路由器的路由表中没有目的地址(172.16.47.142)的路由。不可路由数据包的结果是一个 ICMP 不可达消息，该消息将发送至内部设备。

但是，路由器 A 的默认路由为 172.16.47.145，那么，为什么该路由被视为不可路由的路由呢？

路由器 A 已配置 no ip classless，这意味着如果数据包的目的地是子网存在于路由选择表中的“主要”网络地址（在这种情况下为 172.16.0.0），那么该路由器不依靠默认路由。也就是说，如果发出 no ip classless 命令，则会关闭路由器使用最长的位匹配寻找路由的功能。为了更改此行为，您必须在路由器 A 上配置 ip classless。默认情况下，在安装有 Cisco IOS 软件版本 11.3 及更高版本的 Cisco 路由器上，ip classless 命令处于启用状态。

```
Router-A#configure terminal
```

```
Enter configuration commands, one per line. End with CTRL/Z.
```

```
Router-A(config)#ip classless
```

```
Router-A(config)#end
```

```
Router-A#show ip nat translation
```

```
%SYS-5-CONFIG_I: Configured from console by console nat tr
Pro Inside global      Inside local      Outside local      Outside global
--- 172.16.47.150      172.31.200.48      ---                ---
```

当您像之前一样重复相同的 ping 测试时，您看到数据包被转换，ping 成功。

```
Ping Response on device 172.31.200.48
```

```
D:\>ping 172.16.47.142
```

```
Pinging 172.16.47.142 with 32 bytes of data:
```

```
Reply from 172.16.47.142: bytes=32 time=10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
```

Ping statistics for 172.16.47.142:

Packets: Sent = 4, Received = 4, Lost = 0 (0%)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 10ms, Average = 2ms

Debug messages on Router A indicating that the packets generated by device 172.31.200.48 are getting translated by NAT.

Router-A#

```
*Mar 28 03:34:28: IP: tableid=0, s=172.31.200.48 (Serial0), d=172.16.47.142
(Serial1), routed via RIB
*Mar 28 03:34:28: NAT: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [160]
*Mar 28 03:34:28: IP: s=172.16.47.150 (Serial0), d=172.16.47.142 (Serial1),
g=172.16.47.145, len 100, forward
*Mar 28 03:34:28: ICMP type=8, code=0
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [160]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [161]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [161]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [162]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [162]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [163]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [163]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [164]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [164]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
```

Router-A#**undebug all**

All possible debugging has been turned off

上例说明，当信息包从内向外传输时，NAT 路由器会在继续转换数据包之前，先检查其路由选择表是否有通往外部地址的路由。因此，NAT 路由器对于外部网络具有有效路由至关重要。必须通过在路由器配置中被定义为 NAT 外部的接口来了解通向目标网络的路由。

特别需要指出的是，在返回数据包路由之前，它们已经过转换。因此，NAT 路由器的路由选择表中

还必须对内部本地地址具有有效路由。

## 相关信息

- [配置网络地址转换](#)
- [验证 NAT 的运行和基本的 NAT 故障排除](#)
- [NAT : 本地和全局定义](#)
- [组播 NAT 在 Cisco 路由器上如何工作？](#)
- [NAT 支持页](#)
- [思科技术支持和下载](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。