

# 在重叠网络中使用 NAT

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

本文档介绍如何使用网络地址转换 (NAT) 重叠网络。当您将一个IP地址分配给网络上的设备，但该IP地址已经被互联网或外部网络上的其他设备合法拥有时，会产生重叠网络。在各自网络中都使用 [RFC 1918](#) IP 地址的两个公司合并的时候，也会产生重叠网络。 [这两个网络需要进行通信，但最好不要重新为其所有设备分配地址。](#)

## 先决条件

### 要求

对IP编址、IP路由和域名系统(DNS)信息的基本了解对理解本文内容有用。

### 使用的组件

NAT的支持在Cisco IOS软件版本11.2开始。有关平台支持的详细信息，请参阅 [NAT 常见问题](#)。

### 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 配置

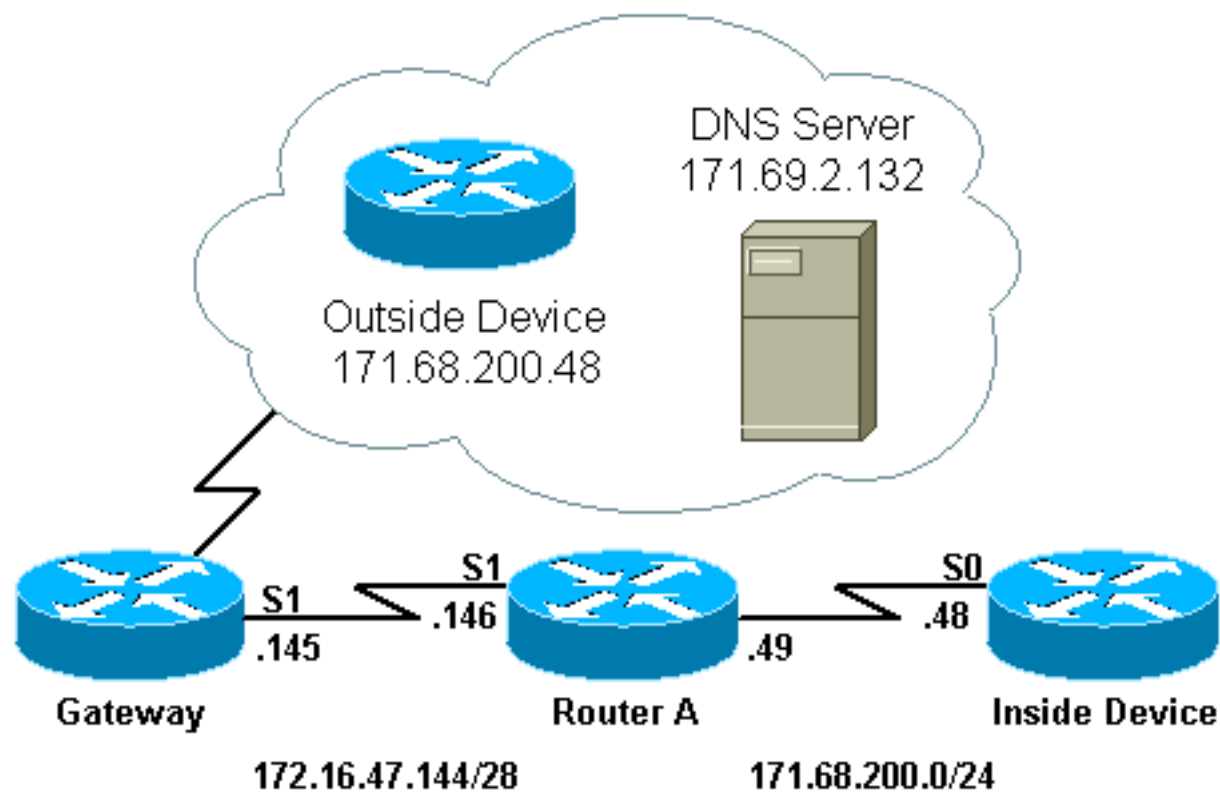
本部分提供有关如何配置本文档所述功能的信息。

**注意：**要查找本文档所用命令的其他信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

## 网络图

本文档使用下图所示的网络设置。

注意：内部设备和它希望与之通信的外部设备有相同的IP地址。



## 配置

路由器A为NAT配置，这样它将内部设备转换到来自池"测试环路"的地址，把外部设备转换到来自"test-dns"池的地址。有关此配置如何帮助重叠的说明，请参阅以下配置表。

路由器 A
<pre>! 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</pre>

```

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

```

为了让上述配置帮助完成内部设备与外部设备通信时的重叠，必须使用外部设备域名。

内部设备不能使用外部设备的IP地址，因为它与分配到自身(内部设备)的地址相同。因此，内部设备将发送对外部设备域名的 DNS 查询。内部设备的IP地址将是此查询的来源，并且由于已经配置了ip nat inside source list命令，该地址将被转换为来自"测试环路"池的一个地址。

DNS服务器回复来自池"测试环路"的地址，同时提供与信息包有效载荷中的外部设备域名相关IP地址。"应答数据包的目的地址转换回内部设备的地址，并且由于ip nat outside source list命令，应答数据包有效载荷地址被转换为来自池""test-dns""的地址。"因此内部设备获悉该外部设备的IP地址来自"test-dns"池，并且再与外部设备通信时，它将使用此地址。此时，运行 NAT 的路由器负责转换。

**故障排除**部分对此进程进行了详细介绍。使用重迭地址的设备不使用DNS也能够彼此连通，但在这种情况下，必须配置静态NAT。以下提供了如何完成此进程的示例。

#### 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
```

有了上述配置，当内部设备想与外部设备通信时，它可以使用IP地址172.16.47.177，但不需要DNS。如上所述，内部设备的地址的转换仍然要动态完成，这意味着创建转换之前路由器必须从内部设备得到信息包。为此，内部设备必须首次启动所有连接，以便让内部设备和外部设备进行通信。如果外部设备必须启动内部设备连接，那么内部设备地址也必须静态配置。

## 验证

当前没有可用于此配置的验证过程。

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

内部设备使用DNS与外部设备进行通信的流程（如上所述）可以通过下列故障排除流程详细查看。

当前用show ip nat translations命令看到的转换表里没有发生转换过程。以下示例改为使用 debug ip packet 和 debug ip nat 命令。

**注意：** debug 命令会产生大量输出。只有在IP网络的数据流很低时才能使用它，以便系统上的其他操作不会受到负面影响。

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

当内部设备向驻留再NAT域外面的DNS服务器发送DNS查询时，由于ip nat inside命令，DNS查询的源地址(内部设备地址)将被转换。此内容可在以下 debug 输出中显示。

```
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
```

在DNS服务器发送DNS回复时，由于ip nat outside命令存在，所以DNS回复的有效载荷可以进行转换。

**注意：** 除非转换发生在应答数据包的IP头上，否则NAT不查看DNS回复的有效载荷。请参阅以上路由器配置中的 ip nat outside source list 7 pool 命令。

下面调试输出的第一NAT消息表示，路由器认可DNS回复，并且将有效载荷的IP地址转换到

172.16.47.177。第二个NAT消息显示路由器转换DNS回复的目的地，因此它能将回复转发到执行最初DNS 查询的内部设备上。报头的目标部分（内部全局地址）将转换为内部本地地址。

DNS 应答的有效负载进行了转换：

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

DNS 应答数据包中 IP 报头的目标部分进行了转换：

```
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
```

让我们看一下另一个 DNS 查询和应答：

```
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
```

现在DNS的有效载荷已被转换，我们的转换表有一个外部设备的外部本地和全局地址条目。有了表中这些条目，我们现在可以完全转换在内外设备之间交换的ICMP信息包头。让我们在以下 debug 输出中看一下此交换。

以下输出显示了正在转换的源地址（内部设备的地址）。

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

此处，目标地址（外部设备的外部本地地址）进行了转换。

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

转换之后，IP 数据包如下所示：

```
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
```

下列输出显示，源地址(外部设备地址)正在返回信息包上转换。

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

此时，返回数据包的目标地址（内部设备的全局地址）进行了转换。

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

转换之后，返回数据包如下所示：

```
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
```

数据包的交换继续在内部设备和外部设备之间进行。

```
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
```

一旦外部和内部之间的信息包交换完成，我们就能查看带有三个条目的转换表。当内部设备发出DNS查询时，将会创建第一个条目。当对DNS应答的有效负载进行转换时，将会创建第二个条目。在内部设备和外部设备之间交换ping时，创建了第三个条目。第三个条目是前二个条目的汇总，被用来提高转换效率。

```
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
```

值得注意的是，当您试图通过在单个Cisco路由器上运行动态NAT建立二个重叠网络之间的连接时，您必须使用DNS创建外部本地到外部全局的转换。如果您不使用DNS，可以使用静态NAT来建立连接，但管理起来更加困难。

## 相关信息

- [NAT 支持页](#)
- [技术支持 - Cisco Systems](#)