# 配置网络地址转换：Getting Started

## 目录



# 简介

本文档介绍在 Cisco 路由器上配置网络地址转换 (NAT) 以用于公共网络方案。本文档的目标受众是第一次使用 NAT 的用户。

**注意**： 本文档中所提及 Internet 或 Internet 设备，都是指任何外部网络上的设备。

# 先决条件

## 要求

本文档需要读者具备与 NAT 相关的基本术语知识。某些定义可以在 NAT：本地和全局定义中找到。

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 2500 系列路由器

Cisco IOS® 软件版本 12.2(10b)

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# 配置和部署 NAT 的快速入门步骤

配置 NAT 时，往往不易知道从哪儿着手，尤其是在您不熟悉 NAT 的时候更是如此。下面的步骤将指导您定义自己希望 NAT 实现的目标，并指导您如何配置 NAT：

定义NAT内部和外部接口。

用户是否在多个接口存在？

是否有多个接口同 Internet 连接？

定义您想用 NAT 实现的目标。

您是否想允许内部用户访问 Internet？

您是否想允许 Internet 访问内部设备（如邮件服务器或者 Web 服务器）？

您是否想将 TCP 流量重定向到另一个 TCP 端口或地址？

您是否正在网络转换期间使用 NAT（例如，您更改了一台服务器的 IP 地址，并在更新所有客户端之前，希望那些未更新的客户端仍可以使用原始的 IP 地址访问该服务器，同时也允许那些已更新的客户用新地址来访问该服务器）？

您是否正使用 NAT 允许相互重叠的网络之间进行通信？

配置 NAT，以便完成您所定义的以上内容。根据您在第 2 步中定义的内容，您需要确定使用以下哪些功能：

静态 NAT

动态 NAT

超载

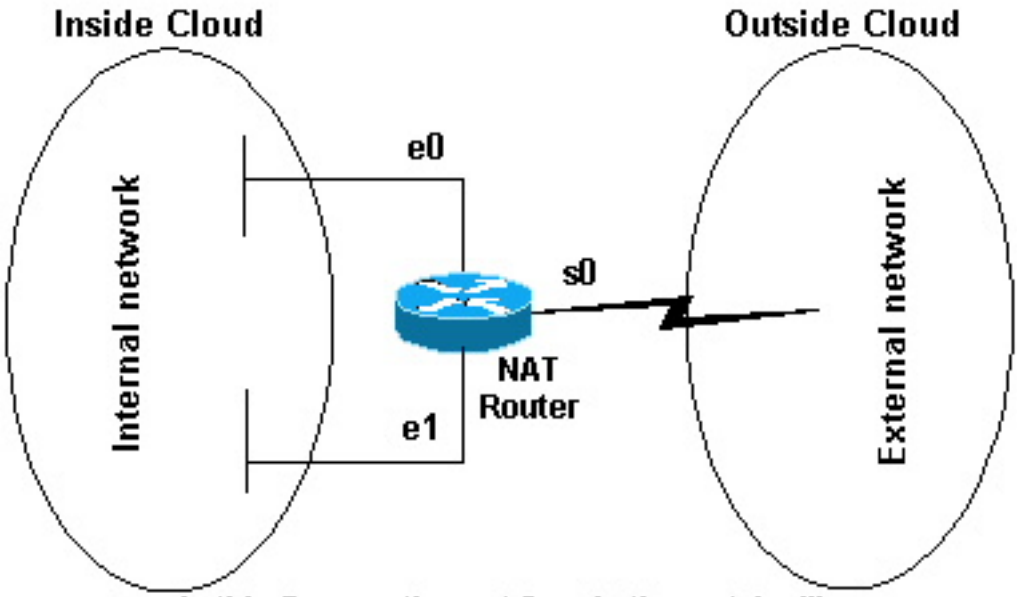
上述功能的任意组合

检验 NAT 的运行情况。

这些NAT示例中的每一通过步骤1至3上面快速开始步骤指导您。这些示例描述 Cisco 建议您部署 NAT 的一些常见情形。

## 定义NAT 内部 和 外部 接口

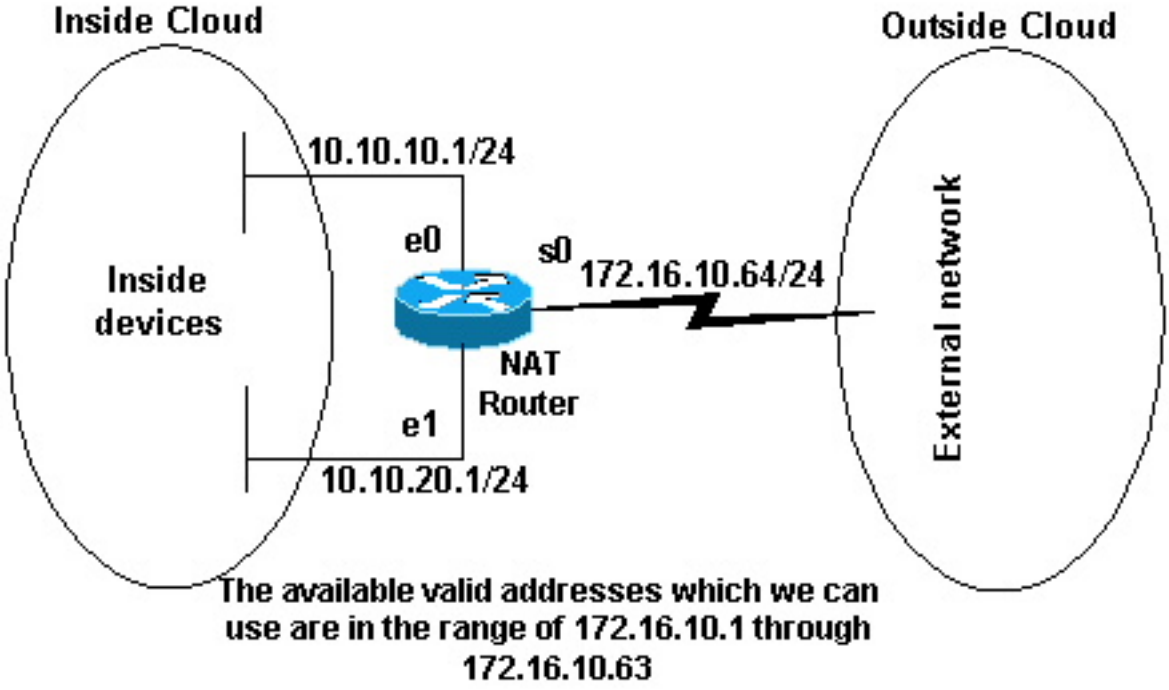
部署NAT的第一步将定义NAT内部和外部接口。您会发现，最简单的方法是将您的内部网络定义为内部接口，将外部网络定义为外部接口。不过，内部和外部这两个术语也是可以任意定义的。此图显示此的示例。




## 示例：允许内部用户访问 Internet

您可能希望允许内部用户访问 Internet，但是您可能无法为每个用户都分配一个有效地址。如果所有通信用设备在互联网里起源于内部设备，您需要单个有效地址或有效地址的池。

此图显示与作为里面和外部定义的路由器接口的一个简单网络图：




在本例中，您希望NAT允许某些设备(前31从每子网)在里面通过翻译他们的对有效地址或地址池的无效的地址产生通信用设备在外部。该地址池已定义的地址范围是从 172.16.10.1 到 172.16.10.63。

现在您已准备好配置 NAT。为了实现上面所定义的目标，请使用动态 NAT。在采用动态 NAT 时，路由器中的转换表最初是空的，一旦需要地址转换的流量通过路由器，这个列表就会填充内容。与静态NAT相对，其中转换在转换表里静态配置和安置，不用对所有流量的需要。

在本例中，您能配置NAT翻译其中每一个内部设备到唯一有效地址，或者翻译其中每一个内部设备到同一个有效地址。第二种方法叫做重载。示例如何配置每个方法给此处。

## 将 NAT 配置为允许内部用户访问 Internet

**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 强烈建议您不要将 NAT 命令参考的访问列表配置为 **permit any**。使用 **permit any** 可能会导致 NAT 消耗太多路由器资源，这可能会引发网络故障。

公告在从子网10.10.10.0的前32个地址和从子网10.10.20.0的仅前32个地址由**access-list 7**允许的先前配置里。所以，只有这些源地址可以转换。也许有有其他地址的其它设备在网络内部，但是这些没有翻译。

最后一步是验证 NAT 是否按照设置正常运行。

## 将 NAT 配置为允许内部用户使用重载访问 Internet

**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.
```

注意在上一个第二配置里， NAT池“ovrld "只有范围一个地址。ip nat inside source list 7 pool ovrld overload 这一行命令中的关键词“overload”允许 NAT 将多个内部设备转换到该池中的同一个地址中。

这条命令的另一种变化是 **ip nat inside source list 7 interface serial 0 overload**，该命令可以配置 NAT，将 NAT 地址都重载到分配给串口 0 接口的地址上。

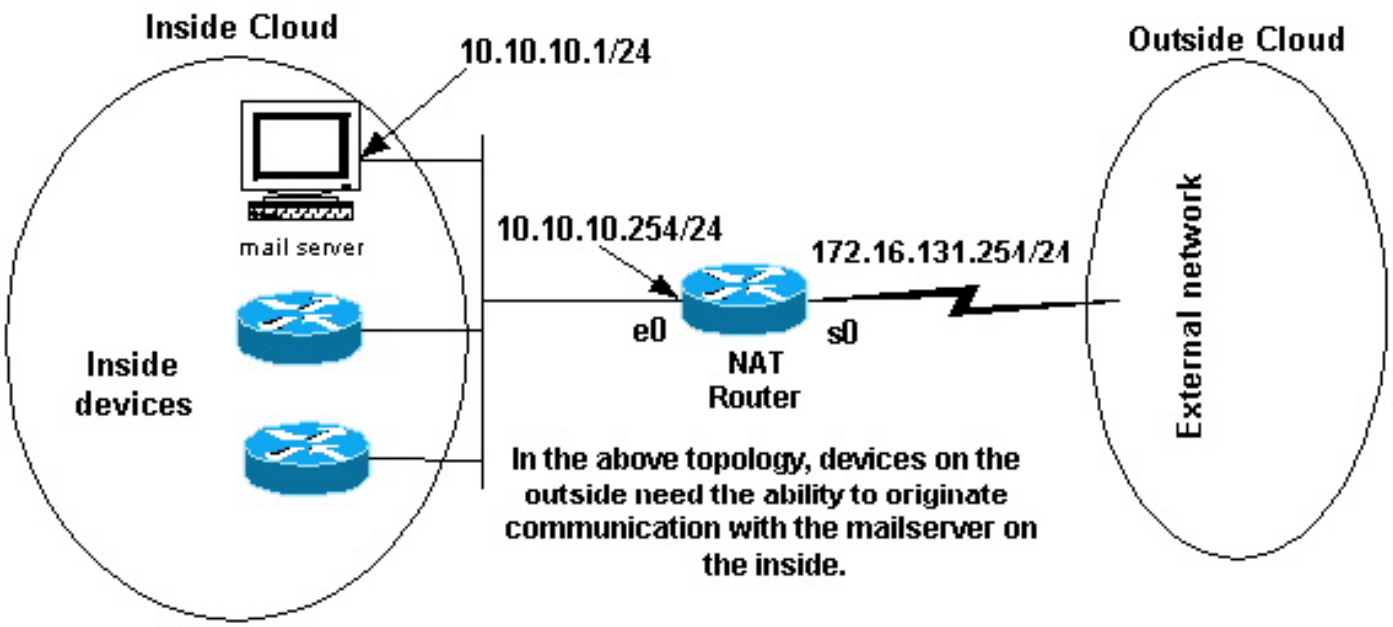
在进行重载配置时，路由器会保存来自更高层协议的足够信息（例如，TCP 或 UDP 端口数），从而将全局地址转换回正确的本地地址。要了解有关全局和本地地址的定义，请参阅 NAT：本地和全局定义。

最后一步是验证 NAT 是否按照设置正常运行。

# 示例：允许 Internet 访问内部设备

您可能需要内部设备与 Internet 上的设备交换信息，其中通信发起方为 Internet 设备，如电子邮件

。它为在互联网的设备是典型的发送电子邮件到在内部网络驻留的邮件服务器。




## 配置NAT，允许互联网访问内部设备

如上一个网络图所显示，在本例中，您首先定义了NAT内部和外部接口。

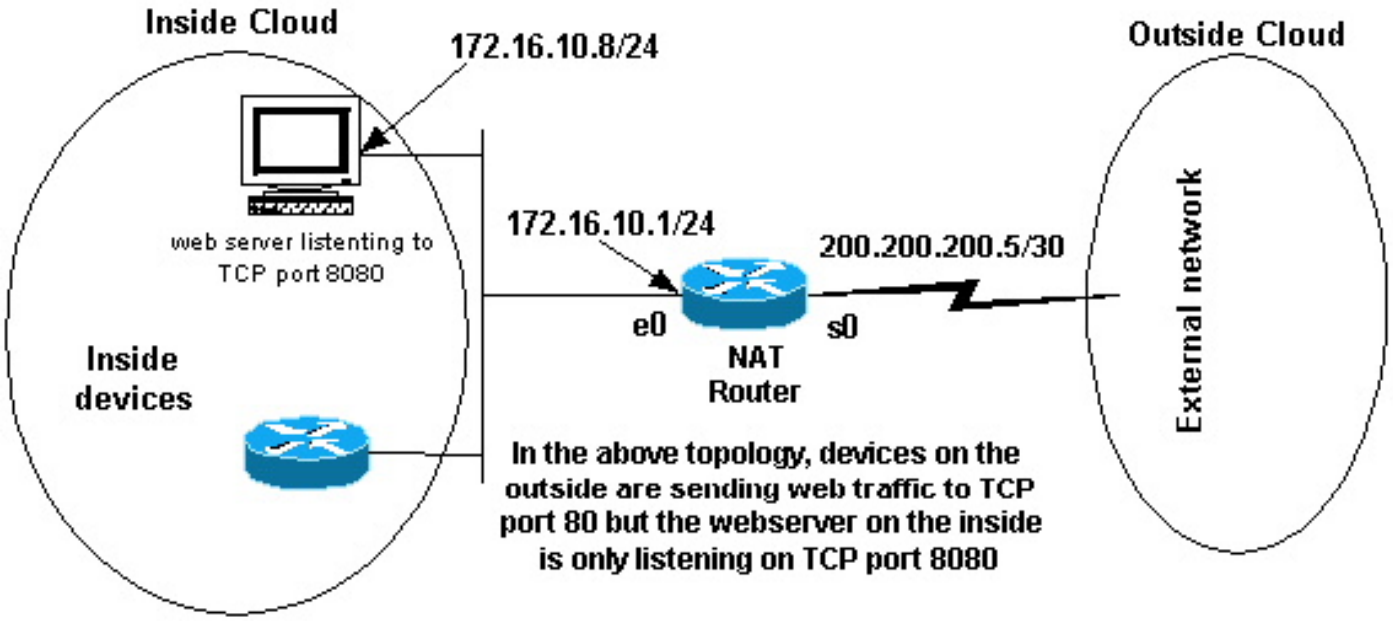
其次，您定义了您希望里面的用户能产生与外部的通信。而外部设备将只能同内部邮件服务器建立通信。

第三步是配置 NAT。要完成什么您定义，您能同时配置静态和动态NAT。有关如何配置本示例的详细信息，请参阅同时配置静态和动态 NAT。

最后一步是验证 NAT 是否按照设置正常运行。

# 示例：将 TCP 流量重定向到另一个 TCP 端口或地址

Internet 中的设备需要与内部设备建立通信连接的另外一个示例是，内部网络中存在 Web 服务器。在某些情况下，可以配置一个内部 Web 服务器，使其在一个 TCP 端口而非端口 80 上监听 Web 流量。例如，可以配置内部 Web 服务器来监听 TCP 端口 8080。在这种情况下，您可以使用 NAT 来将目的地为 TCP 端口 80 的流量重定向到 TCP 端口 8080。




如上一个网络图所显示后，在您定义了接口，您可以决定您希望NAT重定向数据包从为172.16.10.8:80到172.16.10.8:8080注定的外面。您能使用**static nat命令**为了翻译TCP端口号达到此。配置示例显示此处。

## 将 NAT 配置为将 TCP 流量重定向到另一个 TCP 端口或地址

**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
200.200.200.5 255.255.255.252 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.
```

注意静态NAT命令的配置说明指示在与源地址的内部接口接收的所有数据包为172.16.10.8:8080翻译到172.16.10.8:80。这也暗示在与目的地址的外部接口接收的所有数据包为172.16.10.8:80有目的地翻译到172.16.10.8:8080。

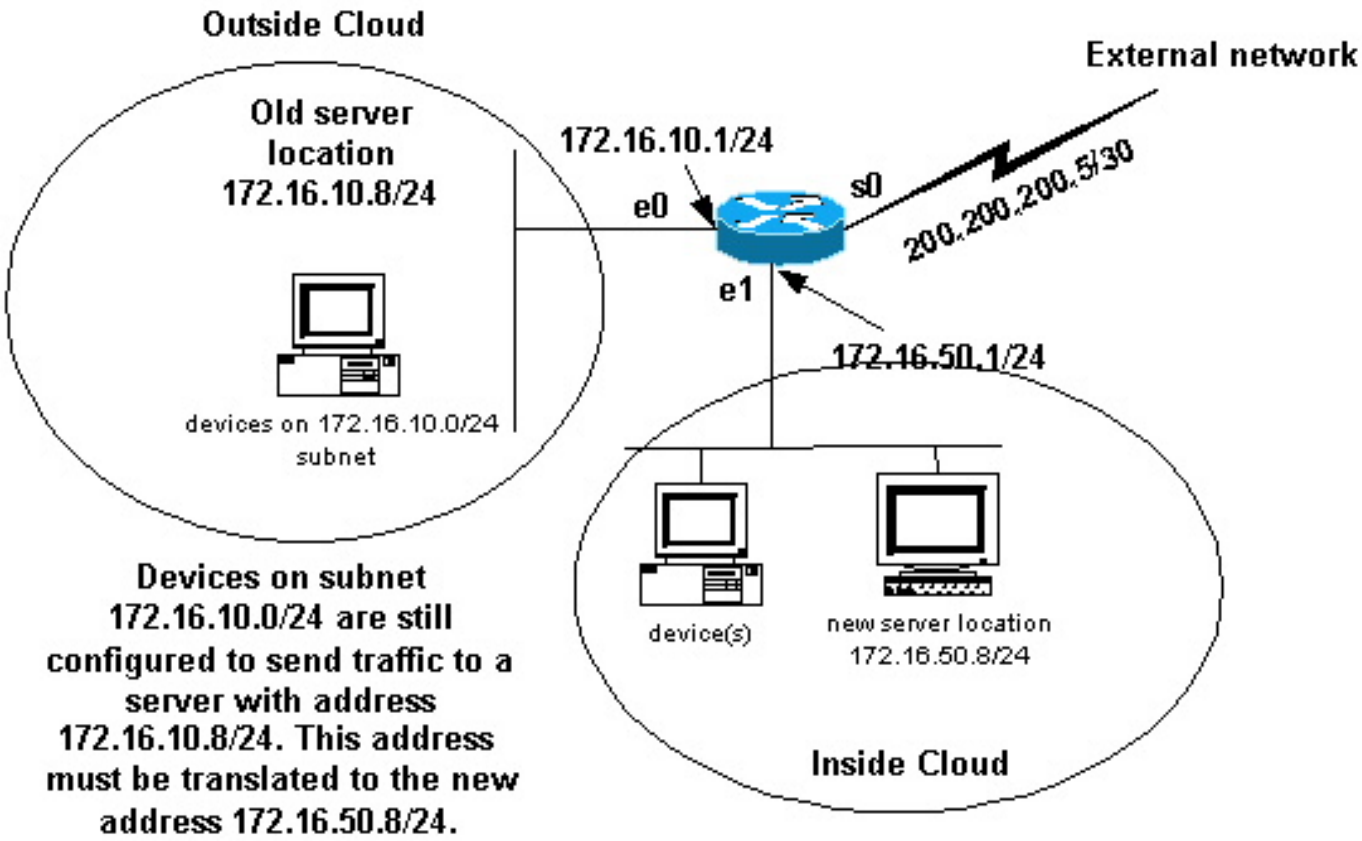
最后一步是验证 NAT 是否按照设置正常运行。

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

# 示例：在网络转换期间使用 NAT

部署NAT是有用的，当您需要再寻址在网络时的设备或，当您用别的时替换一个设备。例如，如果在网络使用的所有设备特定服务器和此服务器需要用有一个新的IP地址的新的替换，使用新的服务器地址的所有网络设备的重新配置采取一些时间。同时，您能使用NAT为了配置设备以旧有地址转

换他们的数据包用新的服务器通信。




一旦您按照上图定义了 NAT 接口，就可以确定您希望 NAT 对来自外部、目的地址为旧服务器地址 (172.16.10.8) 的数据包进行地址转换，并将其发送到新的服务器地址。注意，新服务器在另外一个 LAN 上，对于这个 LAN 上设备或者能够通过这个 LAN（在网络内部的设备）连接上的任何设备，在可能的情况下其配置都应该尽可能使用新服务器的 IP 地址。

您可以使用静态 NAT 来实现您的目的。下面是一个配置示例。

## 配置 NAT 以在网络转换期间使用

**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 200.200.200.5
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.
```

注意inside source nat命令在本例中也暗示在与172.16.10.8目的地址的外部接口接收的数据包有翻译的目的地址对172.16.50.8。

最后一步是验证 NAT 是否按照设置正常运行。

# 示例：在重叠网络中使用 NAT

当您把 IP 地址分配给已经被 Internet 中其他设备所使用的那些内部设备的时候，就生成了重叠网络。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。为此参考使用在重叠网络的NAT关于NAT的配置的更多信息。

# 一对一映射与多对多映射之间的区别

一个静态 NAT 配置创建一个一对一的映射，并将某个具体地址转换为另一个地址。只要此类配置存在且使内部和外部主机都能够建立连接，此类配置就可在 NAT 表中创建永久性条目。这对于提供应用服务（如邮件、Web、FTP 等）的主机通常很有用。例如：

```
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
```

当可用的地址数少于要转换的实际主机数时，动态 NAT 很有用。当主机建立连接并创建地址之间的一对一映射时，它会在 NAT 表中创建一个条目。但是，映射可能会有所不同，具体取决于通信时池中的可用注册地址。动态 NAT 仅允许从配置了动态 NAT 的内部或外部网络中启动会话。如果主机在可配置的特定时间内不通信，则会从转换表中删除动态 NAT 条目。然后会将地址返回到池，供另一台主机使用。

例如，请完成详细配置的以下步骤：

创建一个地址池

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

创建必须映射的内部网络的访问列表

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

将正在选择要进行网络地址转换的内部网络 10.3.2.0 0.0.0.255 的访问列表 100 与池 MYPOOLEXAMPLE 关联，然后使地址重载。

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

# 验证 NAT 的运行情况

一旦您已配置 NAT，请验证它是否按预期运行。您可以通过多种方式实现这个目的：使用网络分析器、**show** 命令或 debug 命令。有关 NAT 验证的详细示例，请参阅验证 NAT 运行情况和基本的

NAT 故障排除。

# 结论

本文档中的实例说明了有助于配置和部署 NAT 的快速入门步骤。这些快速入门步骤包括：

定义NAT内部和外部接口。

定义您想用 NAT 实现的目标。

配置 NAT 以实现您在步骤 2 中所定义的目的。

验证 NAT 的运行情况。

在其中每一前面的示例，使用了各种各样**ip nat inside命令**。您能也使用**ip nat outside命令**为了实现同样目标，但是记住NAT运算顺序。使用ip nat outside source static命令，对于使用**ip nat outside**命令的配置示例，参考配置示例使用ip nat outside source list命令和配置示例。

前面的示例也展示了这些操作：

| 命令 | 操作 |
| --- | --- |
| ip nat inside source | • 转换正从内部流往外部的 IP 数据包的源。<br>• 转换正从外部流入内部的 IP 数据包的目的。 |
| ip nat outside source | • 转换正从外部流入内部的 IP 数据包的源。<br>• 转换正从内部流往外部的 IP 数据包的目的。 |

# 相关信息

- NAT 支持页
- IP 路由协议支持页
- IP 路由支持页
- NAT 如何工作
- NAT 运行顺序
- 有关Cisco IOS NAT的常见问题
- 技术支持和文档 - Cisco Systems