配置网络地址转换

目录

简介

本文档介绍如何在思科路由器上配置网络地址转换 (NAT)。

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。

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

NAT 配置和部署的快速入门步骤

注意：本文档中提及的互联网或互联网设备是指任何外部网络上的设备。

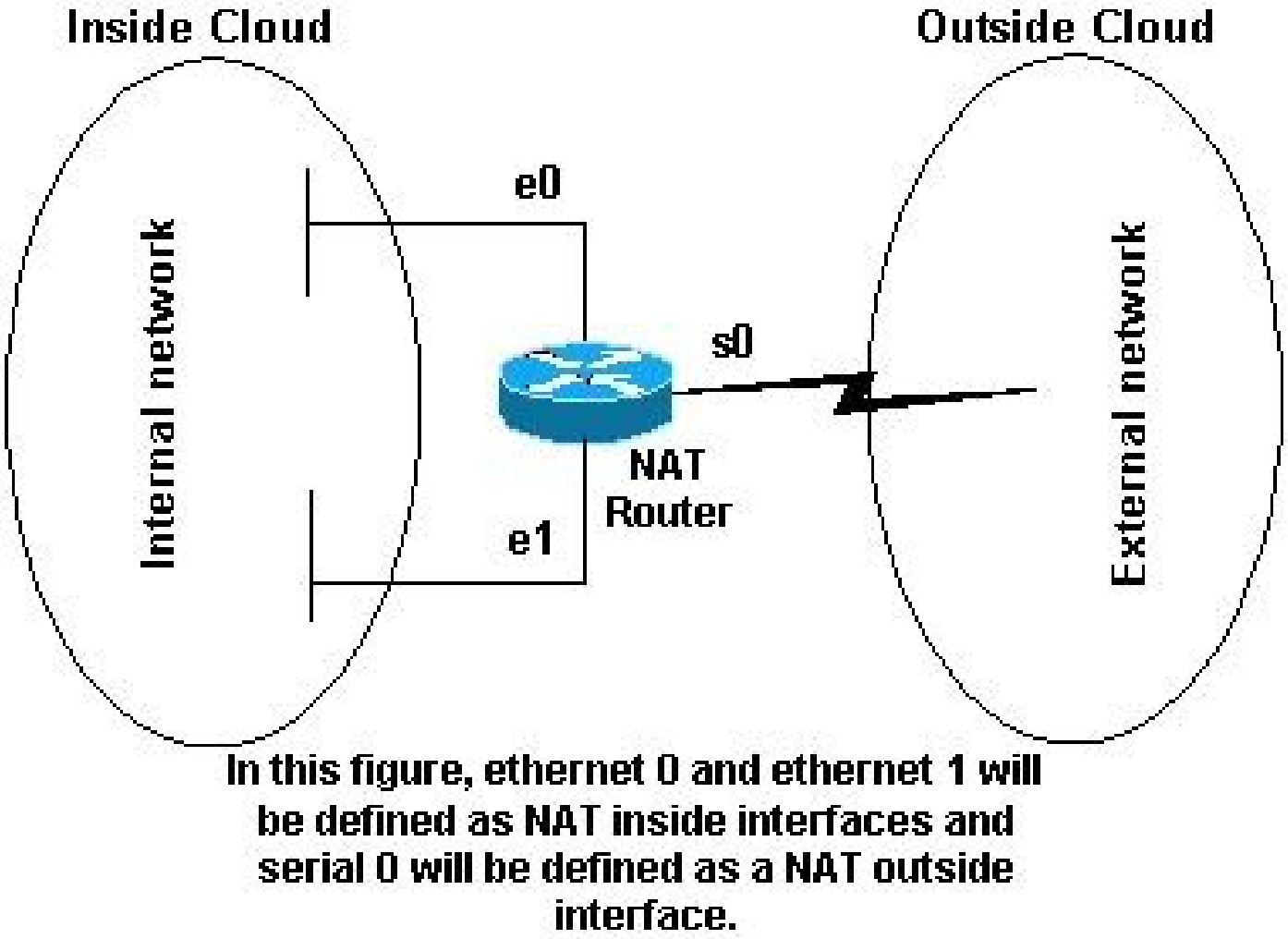
配置 NAT 时，往往不易知道从哪儿着手，尤其是在您不熟悉 NAT 的时候更是如此。下面的步骤将指导您定义自己希望 NAT 实现的目标，并指导您如何配置 NAT：

1. 定义NAT内部和外部接口。
    - 用户是否在多个接口存在？
    - 是否有多个可用于互联网的接口？
2. 定义要使用 NAT 完成的任务。
    - 是否要允许内部用户访问互联网？
    - 是否要允许互联网访问内部设备（例如邮件服务器或 Web 服务器）？
    - 是否要将 TCP 流量重定向到其他 TCP 端口或地址？
    - 是否要在网络过渡期间使用 NAT（例如，您更改了服务器 IP 地址，在更新完所有客户端之前，您希望未更新的客户端能够访问具有原始 IP 地址的服务器，并且已更新的客户端能够访问具有新地址的服务器）？
    - 是否要使用以允许重叠网络通信?
3. 配置 NAT 以完成您之前定义的任务。根据在第 2 步中的定义，您需要确定要使用以下哪些功能：
    - 静态 NAT
    - 动态 NAT
    - Overloading
    - 这些功能的任意组合。
4. 检验 NAT 的运行情况。

这些 NAT 示例将指导您完成上图中快速入门步骤的第 1 步到第 3 步。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 的第一步是定义 NAT 内部和外部接口。您会发现最简单的方法是将内部网络定义为内部，将外部网络定义为外部。不过，内部和外部这两个术语也是可以任意定义的。此图显示了一个示例。



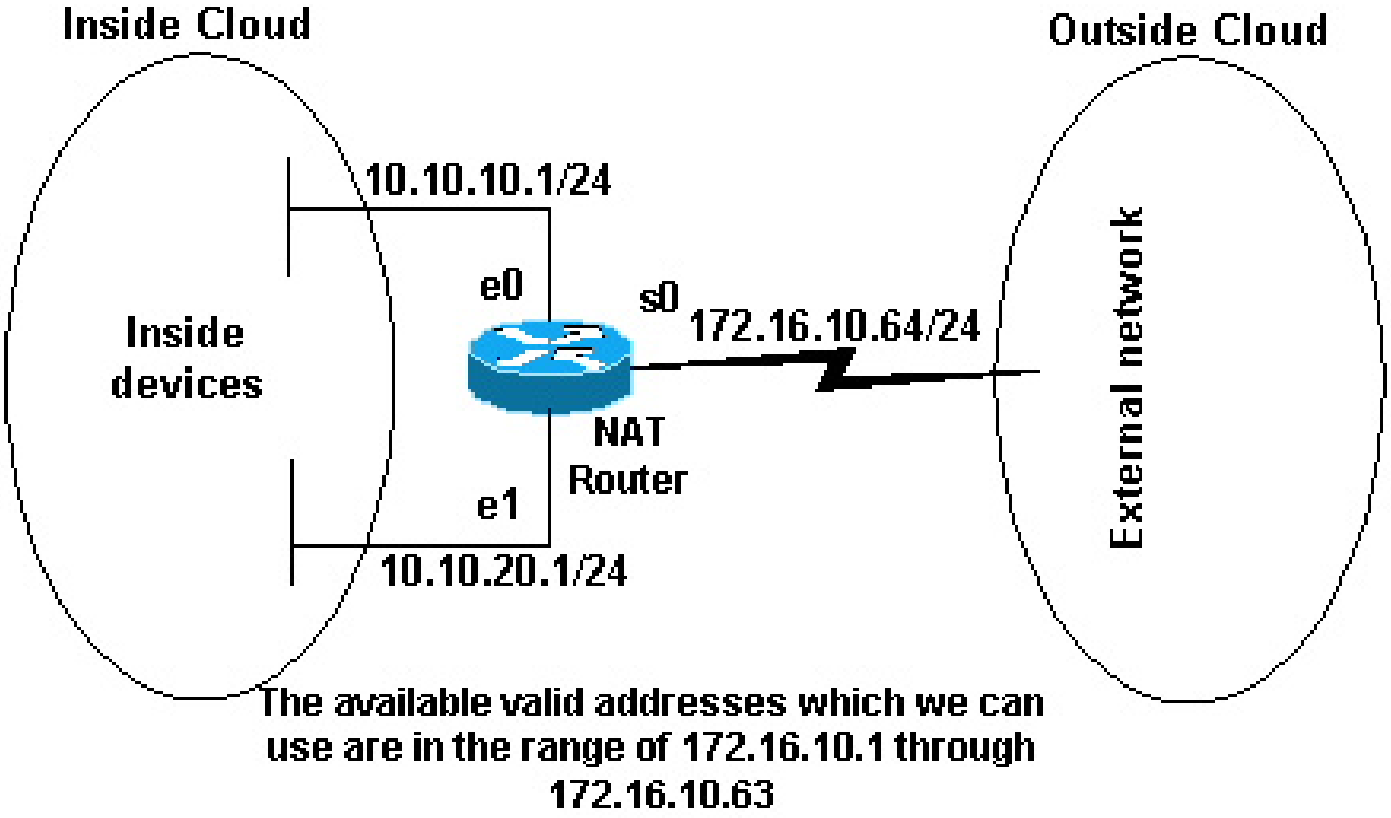
NAT 拓扑

Examples

1. 允许内部用户访问互联网

您可能希望允许内部用户访问互联网，但没有足够的有效地址来满足所有用户的需求。如果与互联网中的设备的所有通信均来自内部设备，则需要独立的有效地址或使用有效地址池。

此图显示了一个简单的网络示意图，其中定义了内部和外部路由器接口。



可用的有效地址

在本示例中，您希望 NAT 允许内部的特定设备（每个子网的前 31 台设备）发起与外部设备的通信，并将其无效地址转换为有效地址或地址池。该地址池已定义的地址范围是从 172.16.10.1 到 172.16.10.63。

现在即可配置 NAT。要完成上图中定义的任务，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。这完全不同于静态 NAT。静态 NAT 会将静态配置的转换放置在转换表中，而无需任何流量。

在本示例中，您可以将 NAT 配置为将每个内部设备转换为唯一的有效地址，或将每个内部设备转换为相同的有效地址。第二种方法称为 overloading 。此处提供了如何配置每种方法的示例。

配置 NAT 以允许内部用户访问互联网

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：思科强烈建议不要使用 permit any 来配置 NAT 命令引用的访问列表。 如果在 NAT 中使用 permit any，则会消耗过多的路由器资源，从而导致网络问题。

请注意，在之前的配置中，access-list 7 仅允许来自子网 10.10.10.0 的前 32 个地址和来自子网 10.10.20.0 的前 32 个地址。所以，只有这些源地址可以转换。内部网络上可能有其他设备具有别的地址，但这些地址没有转换。

最后一步是验证 NAT 是否按预期运行。

配置 NAT 以允许内部用户过载访问互联网

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.
```

请注意，在之前的第二个配置中 ovrld,NAT地址池只有一个地址范围。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。

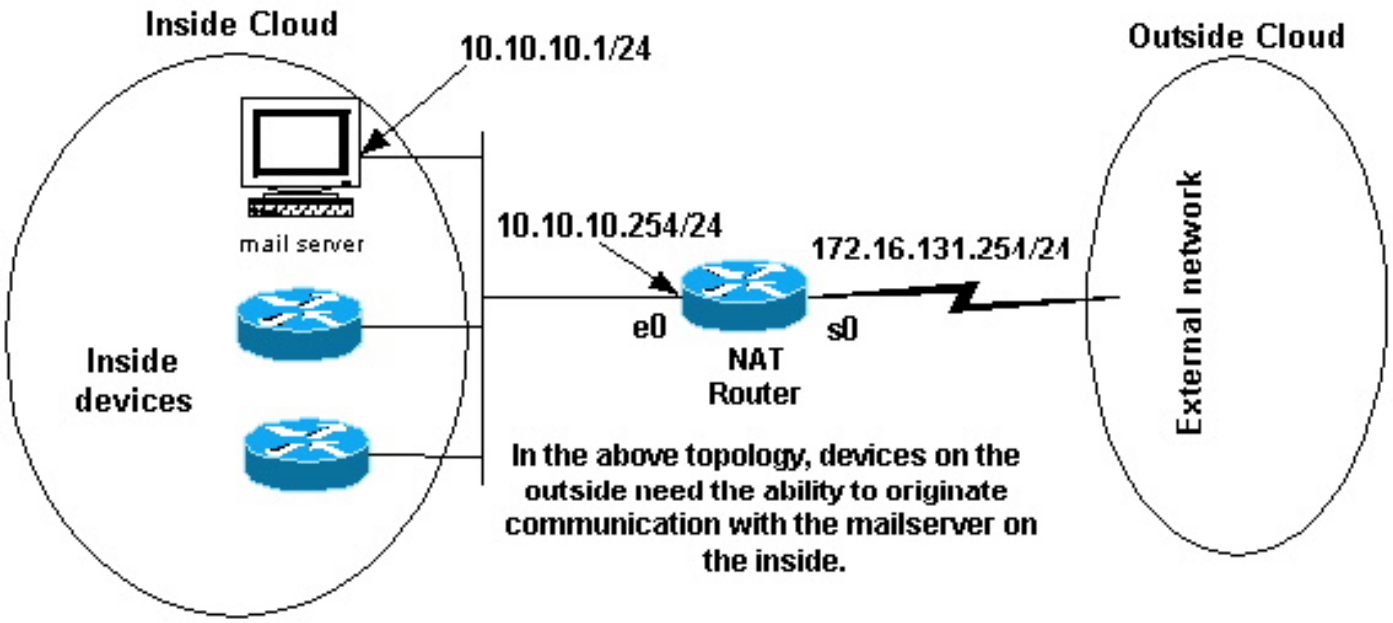
此命令的另一种变体是 ip nat inside source list 7 interface serial 0 overload，用于将 NAT 配置为在分配给 serial 0 接口的地址上过载。

配置overloading后，路由器会维护来自较高级别协议（例如，TCP或UDP端口号）的足够信息，以便将全局地址转换回正确的本地地址。有关全局和本地地址的定义，请参阅 NAT：全局和本地定义。

最后一步是验证 NAT 是否按预期运行。

2. 允许互联网访问内部设备

有时您可能需要内部设备与互联网上的设备交换信息，从互联网设备发起通信，例如电子邮件。互联网上的设备通常会将邮件发送至位于内部网络上的邮件服务器。



发起通信

配置 NAT 以允许互联网访问内部设备

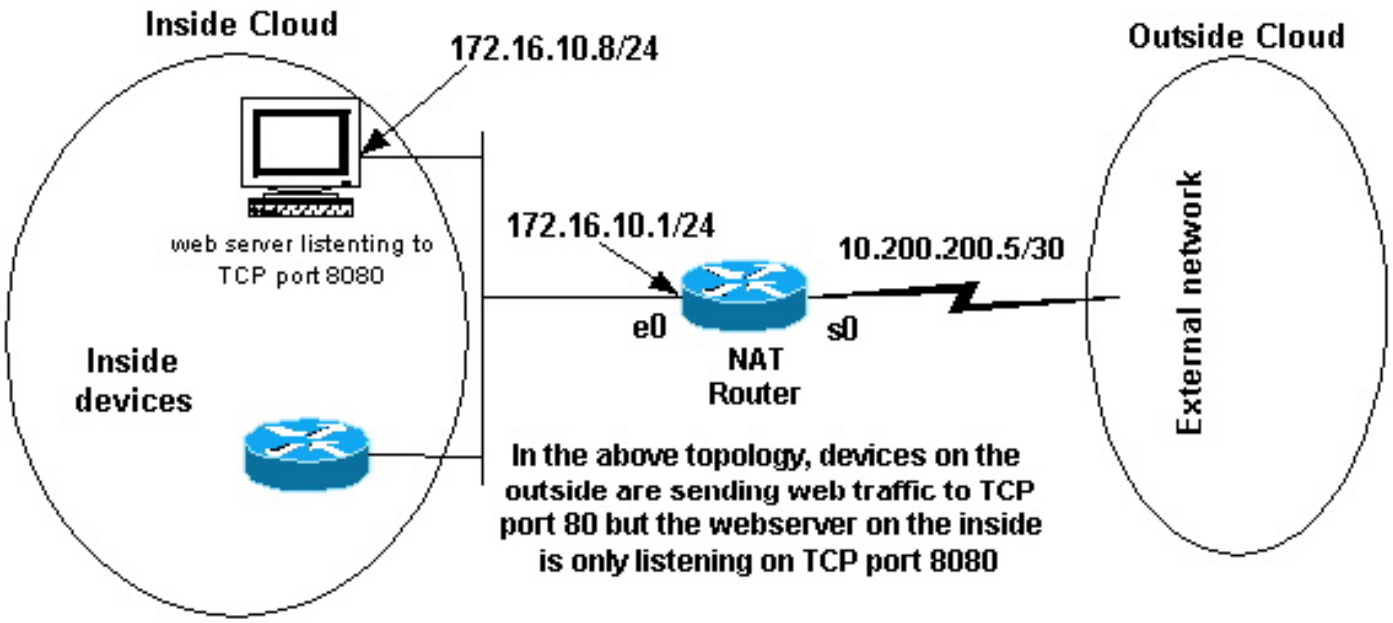
在本示例中，首先定义 NAT 内部接口和外部接口，如上述网络示意图所示。

然后，定义内部用户能够发起与外部的通信。外部设备必须能够发起仅与内部邮件服务器的通信。

第三步是配置 NAT。要完成所定义的操作，可以同时配置静态和动态 NAT。有关如何配置此示例的更多信息，请参阅同时配置静态和动态 NAT。 最后一步是验证 NAT 是否按预期运行。

3. 将 TCP 流量重定向到其他 TCP 端口或地址

互联网上的设备可能需要发起与内部设备的通信，这一点也可以通过内部网络上的 Web 服务器来说明。在某些情况下，可以配置内部 Web 服务器侦听除端口 80 以外的 TCP 端口上的 Web 流量。例如，可以配置内部 Web 服务器侦听 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。



Web 流量 TCP 端口

在定义上述网络示意图所示的接口之后，您可以决定是否想要 NAT 将发往 172.16.10.8:80 的外部数据包重定向至 172.16.10.8:8080。为此，您可以使用 static nat 命令来转换 TCP 端口号。下面显示了配置示例。

配置 NAT 以将 TCP 流量重定向到其他 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 10.200.200.5 255.255.255.252
 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 命令的配置描述表明，在内部接口中收到的源地址为 172.16.10.8:8080 的任何数据包都将被转换为 172.16.10.8:80。这也意味着在外部接口上收到的目的地地址为

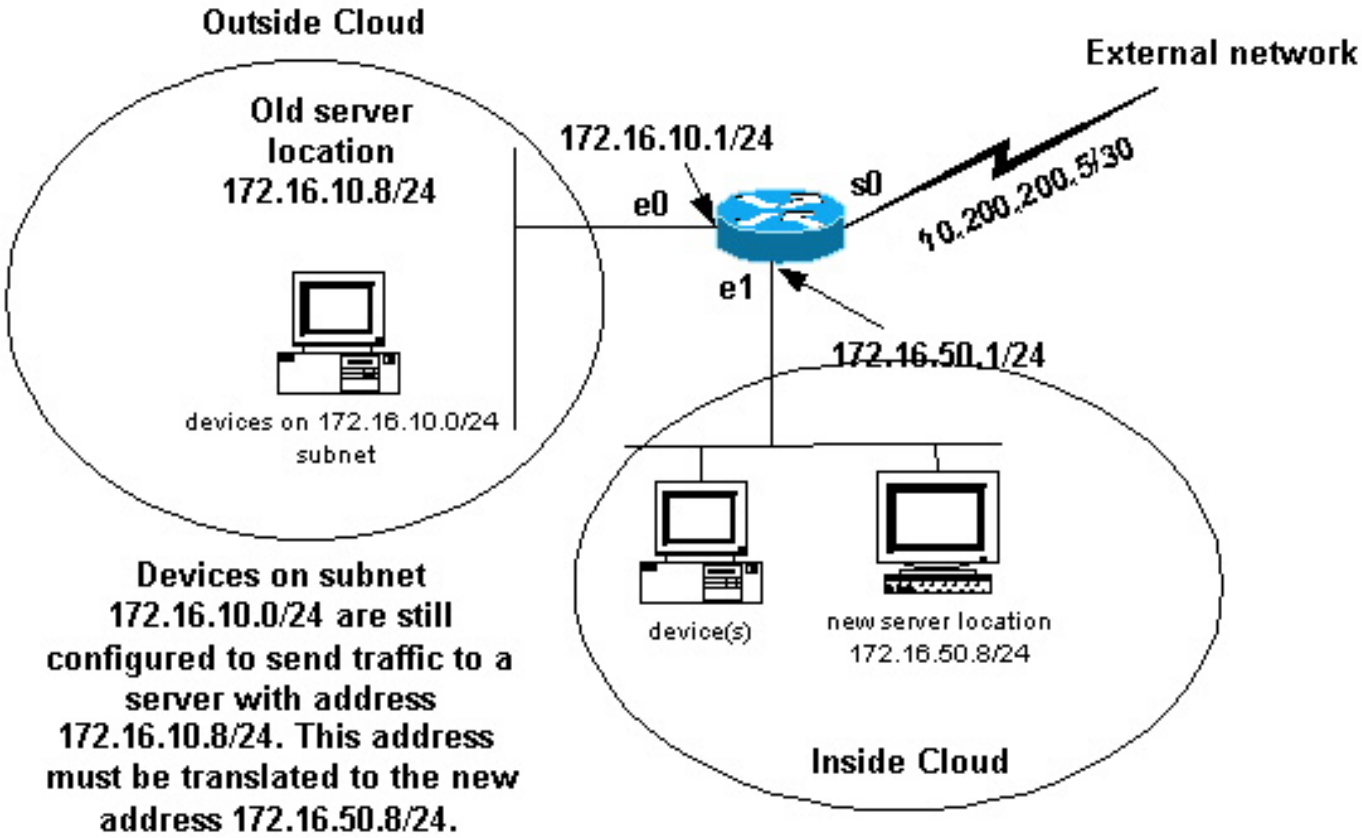
172.16.10.8:80 的任何数据包都会将目的地地址转换为 172.16.10.8:8080。

最后一步是验证 NAT 是否按预期运行。

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

4. 将 NAT 用于网络过渡

当需要对网络上的设备重新寻址时，或进行设备替换时，NAT 可发挥重要作用。例如，如果网络中的所有设备均使用特定服务器，而需要将此服务器替换为具有新 IP 地址的新服务器，则重新配置所有网络设备使用新服务器地址会花费一些时间。同时，您可以使用 NAT 来配置具有旧地址的设备，通过转换其数据包来与新服务器通信。



NAT 网络过渡

按照上图所示定义 NAT 接口后，您可以决定是否想要 NAT 允许对外部发往旧服务器地址 (172.16.10.8) 的数据包进行转换并发送到新服务器地址。请注意，新服务器位于另一局域网上，对于此局域网上的设备或可通过此局域网访问的任何设备（网络内部的设备），必须尽可能配置为使用新的服务器 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 以便用于网络过渡

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 10.200.200.5 255.255.255.252 !--- 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：本示例中的内部源 NAT 命令也可表明，在外部接口上收到的目的地地址为 172.16.10.8 的数据包的目的地地址会转换为 172.16.50.8。

最后一步是验证 NAT 是否按预期运行。

5. 将 NAT 用于重叠网络

为内部设备分配 IP 地址时，如果这些 IP 地址已经被互联网中的其他设备使用，就会导致网络重叠。当两家公司（两者都在其网络中使用 RFC 1918 IP 地址）合并时，也会产生重叠网络。这样的两个网络需要通信，但最好不要对其所有设备重新寻址。

一对一映射和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：

1. 创建一个地址池.

   <#root>

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

2. 创建必须映射的内部网络的访问列表.

   <#root>

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

3. 将 access-list 100（选择内部网络 10.3.2.0 0.0.0.255 进行 NAT 操作）关联到池 SYPOOLEXAMPLE，然后过载地址。

   <#root>

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

验证 NAT 操作

配置 NAT 后，请验证其是否按预期运行。您可以通过多种方式执行此操作：使用网络分析仪、show 命令或 debug 命令。有关 NAT 验证的详细示例，请参阅验证 NAT 操作和基本 NAT。

结论

本文档中的示例演示了可帮助您配置和部署 NAT 的快速入门步骤。

这些快速入门步骤包括：

1. 定义NAT内部和外部接口。
2. 您要使用 NAT 完成什么任务。
3. 配置 NAT 以完成您在第 2 步中定义的任务。
4. 检验 NAT 的运行情况。

之前的各示例使用了各种不同形式的 ip nat inside 命令。您还可以使用 ip nat outside 命令来实现相同的目标，但请记住 NAT 的操作顺序。有关使用 ip nat outside 命令的配置示例，请参阅使用 ip nat outside source list 命令的示例配置。

之前的示例还演示了以下操作：

命令	操作
ip nat inside source	• 转换从内部传输到外部的 IP 数据包的源。 • 转换从外部传输到内部的 IP 数据包的目标。
ip nat outside source	• 转换从外部传输到内部的 IP 数据包的源。 • 转换从内部传输到外部的 IP 数据包的目标。

相关信息

- NAT：本地和全局定义.
- NAT 支持页
- IP 路由协议支持页
- IP 路由 支持页
- IP 编址服务
- NAT 运行顺序
- 有关Cisco IOS NAT的常见问题
- 技术支持和文档 - Cisco Systems

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）。