Configure Network Address Translation

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Quick Start Steps to Configure and Deploy NAT

Define NAT Inside and Outside Interfaces

Examples

- 1. Allow Internal Users to Access the Internet
  - Configure NAT to Allow Internal Users to Access the Internet
  - Configure NAT to Allow Internal Users to Access the Internet with Overload
- 2. Allow the Internet to Access Internal Devices
  - Configure NAT to Allow the Internet to Access Internal Devices
- 3. Redirect TCP Traffic to Another TCP Port or Address
  - Configure NAT to Redirect TCP Traffic to Another TCP Port or Address
- 4. Use NAT For a Network Transition
  - Configure NAT for Use Through a Network Transition
- 5. Use NAT for Networks that Overlap

Difference between One-to-One and Many-to-ManyMapping

Verify the NAT Operation

Conclusion

Related Information

Introduction

This document describes how to configure the Network Address Translation (NAT) on a Cisco router.

Prerequisites

Requirements

This document requires a basic knowledge of the terms used in connection with NAT.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2500 Series Routers
- Cisco IOS® Software Release 12.2 (10b)

The information in this document was created from the devices in a specific lab environment. All of the

devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Quick Start Steps to Configure and Deploy NAT

Note: In this document, when the internet, or an internet device is referred to, it means a device on any external network.

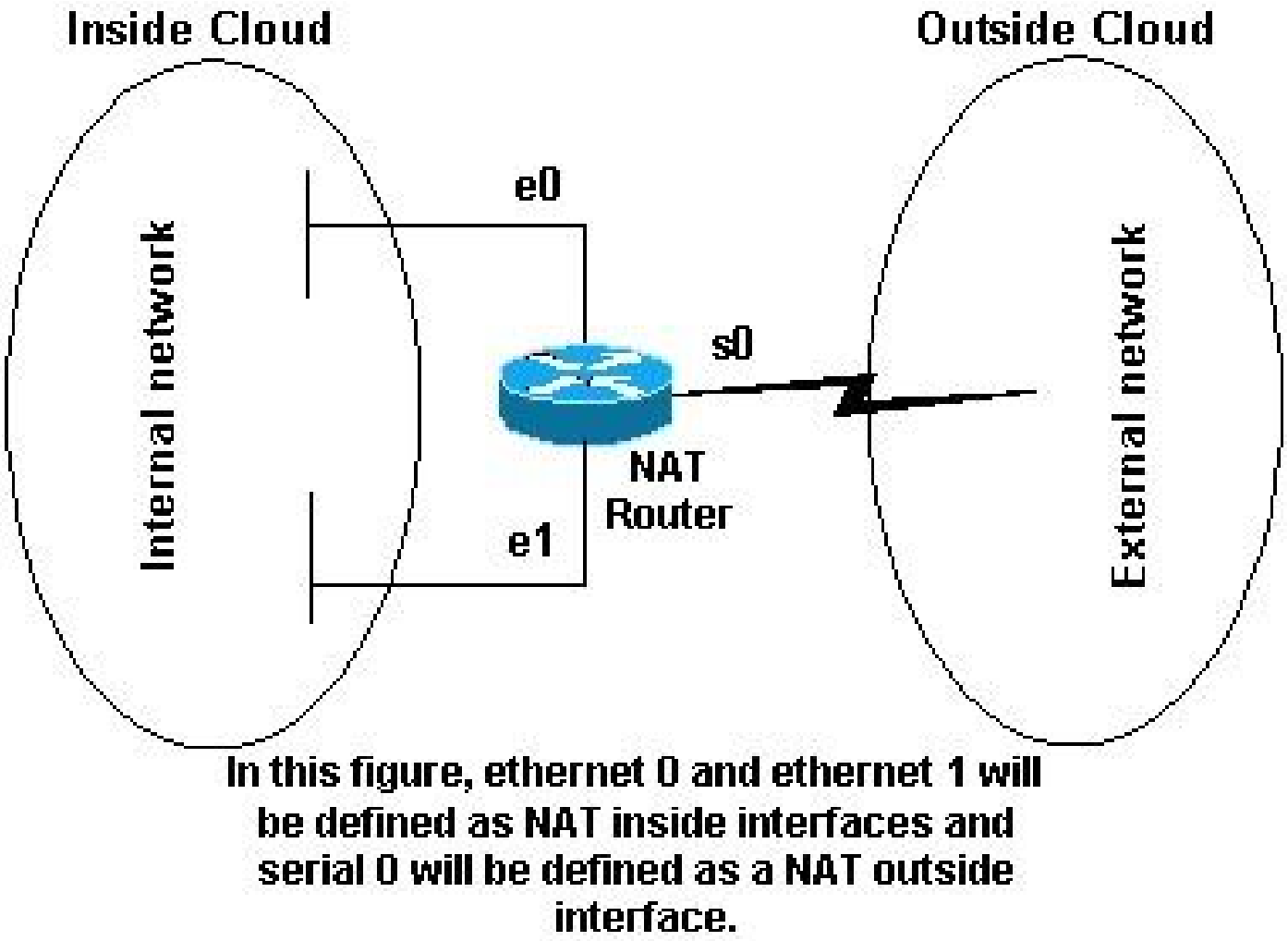
When you configure NAT, it is sometimes difficult to know where to begin, especially if you are new to NAT. These steps guide you to define what you want NAT to do and how to configure it:

1. Define NAT inside and outside interfaces.
    - Do users exist off multiple interfaces?
    - Are there multiple interfaces available to the internet?
2. Define what you want to accomplish with NAT.
    - Do you want to allow internal users to access the internet?
    - Do you want to allow the internet to access internal devices(such as a mail server or web server)?
    - Do you want to redirect TCP traffic to another TCP port or address?
    - Do you want to use NAT during a network transition(for example, you changed a server IP address and until you can update all the clients, you want the non-updated clients to be able to access the server with the original IP address as well as allow the updated clients to access the server with the new address)?
    - Do you want to allow networks that overlap to communicate?
3. Configure NAT in order to accomplish what you defined previously. Based on what you defined in step 2, you need determine which of the next features to use:
    - Static NAT
    - Dynamic NAT
    - Overloading
    - Any combination of these features.
4. Verify the NAT operation.

Each of these NAT examples guides you through steps 1 through 3 of the Quick Start Steps in the previous image. These examples describe some common scenarios in which Cisco recommends you deploy NAT.

Define NAT Inside and Outside Interfaces

The first step to deploy NAT is to define NAT inside and outside interfaces. You can find it easiest to define your internal network as inside, and the external network as outside. However, the terms internal and external are subject to arbitration as well. This figure shows an example of this.



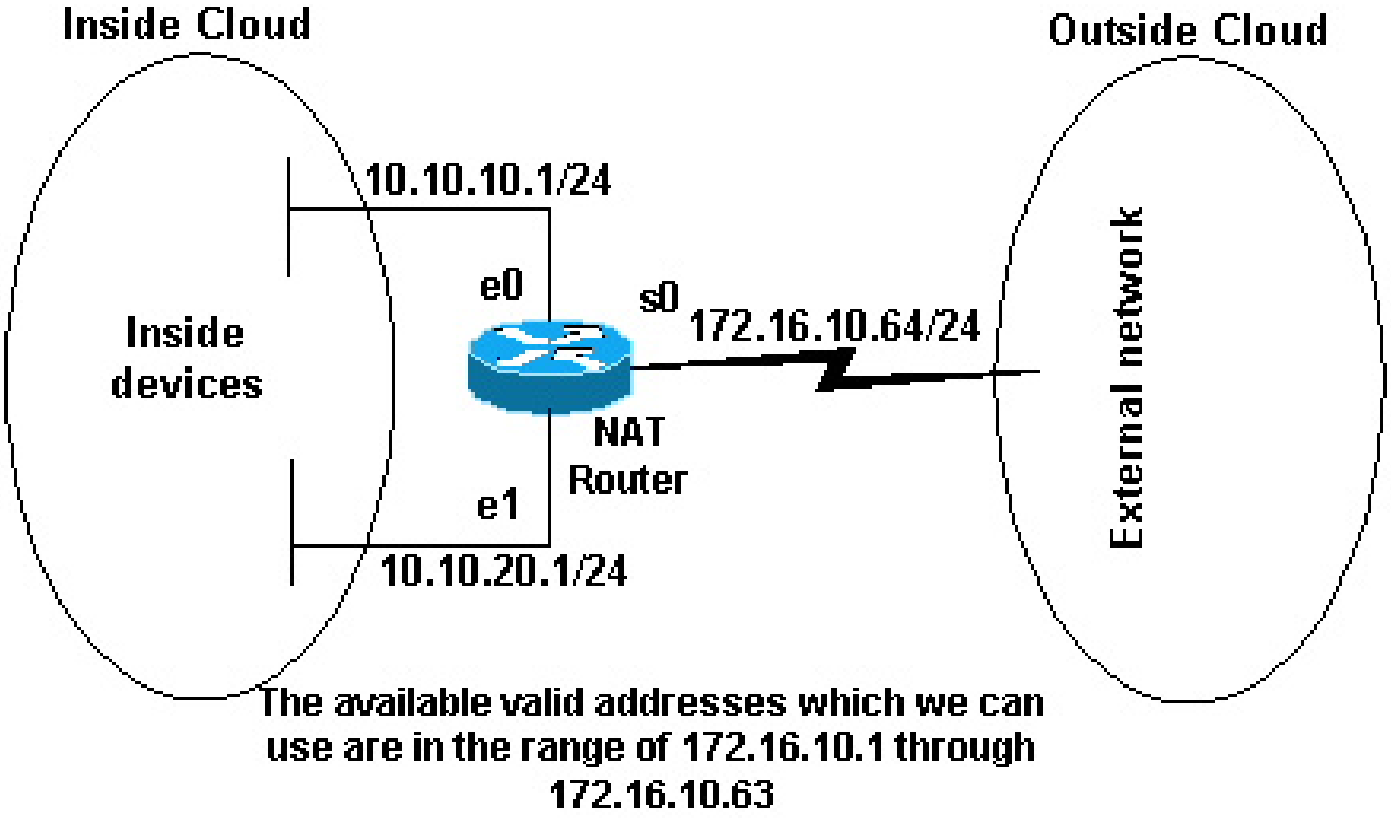
NAT Topology

Examples

1. Allow Internal Users to Access the Internet

Is it possible that you want to allow internal users to access the internet, but you do not have enough valid addresses to accommodate everyone. If all communication with devices in the internet originate from the internal devices, you need a single valid address or a pool of valid addresses.

This image shows a simple network diagram with the router interfaces defined as inside and outside.



Available Valid Addresses

In this example, you want NAT to allow certain devices (the first 31 from each subnet) on the inside to originate communication with devices on the outside and translate their invalid address to a valid address or pool of addresses. The pool has been defined as the range of addresses 172.16.10.1 through 172.16.10.63.

You can now configure NAT. In order to accomplish what is defined in the previous image, use dynamic NAT. With dynamic NAT, the translation table in the router is initially empty and gets populated once traffic that needs to be translated passes through the router. As opposed to static NAT, where a translation is statically configured and is placed in the translation table without the need for any traffic.

In this example, you can configure NAT to translate each of the inside devices to a unique valid address, or to translate each of the inside devices to the same valid address. This second method is known as overloading. An example of how to configure each method is given here.

Configure NAT to Allow Internal Users to Access the Internet

NAT Router

`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.
```



Note: Cisco highly recommends that you do not configure access lists referenced by NAT commands with **permit any**. If you use **permit any** in NAT, it consumes too many router resources which can cause network problems.

Notice in the previous configuration that only the first 32 addresses from subnet 10.10.10.0 and the first 32 addresses from subnet 10.10.20.0 are permitted by access-list 7. Therefore, only these source addresses are translated. There can be other devices with other addresses on the inside network, but these are not translated.

Configure NAT to Allow Internal Users to Access the Internet with Overload

NAT Router

```
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.
```

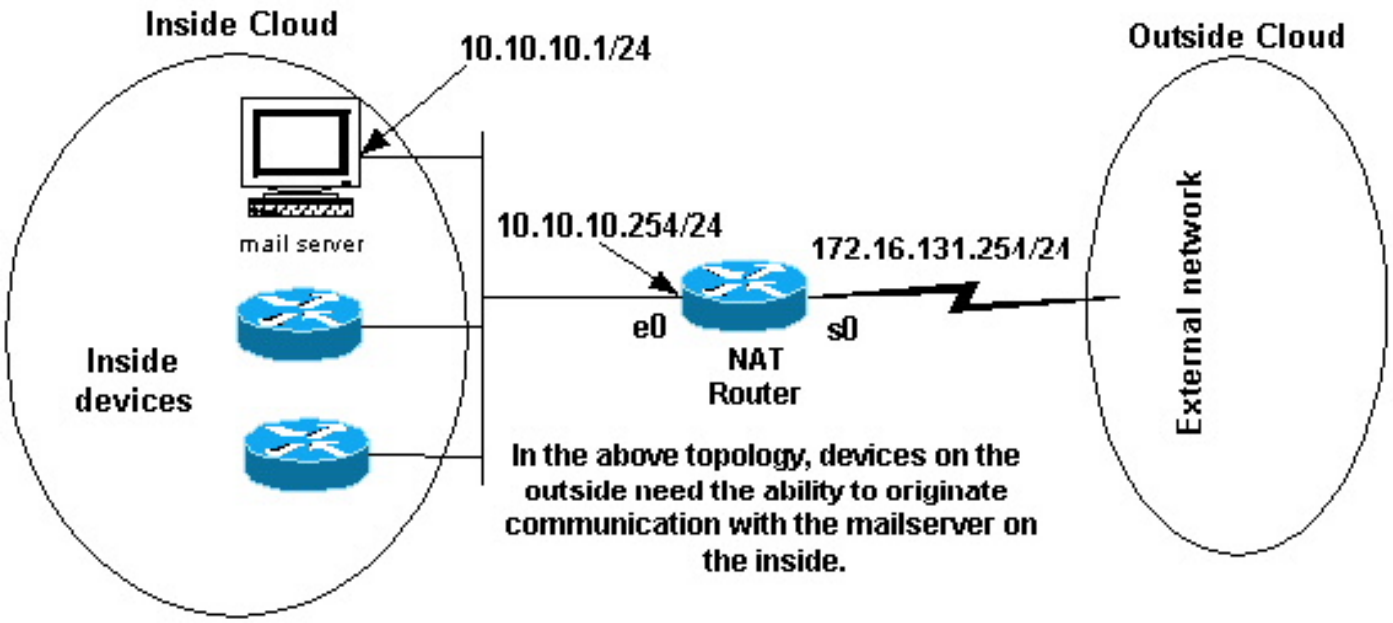
Notice in the previous second configuration, the NAT pool ovrld only has a range of one address. The keyword overload used in the **ip nat inside source list 7 pool ovrld overload** command allows NAT to translate multiple inside devices to the single address in the pool.

Another variation of this command is**ip nat inside source list 7 interface serial 0 overload**, which configures NAT to overload on the address that is assigned to the serial 0 interface.

When overloading is configured, the router maintains enough information from higher-level protocols (for example, TCP or UDP port numbers) to translate the global address back to the correct local address. For definitions of global and local address, refer toNAT: Global and Local Definitions.

2. Allow the Internet to Access Internal Devices

You can need internal devices to exchange information with devices on the internet, where the communication is initiated from the internet devices, for example, email. It is typical for devices on the internet to send email to a mail server that resides on the internal network.



Originate Communications

Configure NAT to Allow the Internet to Access Internal Devices

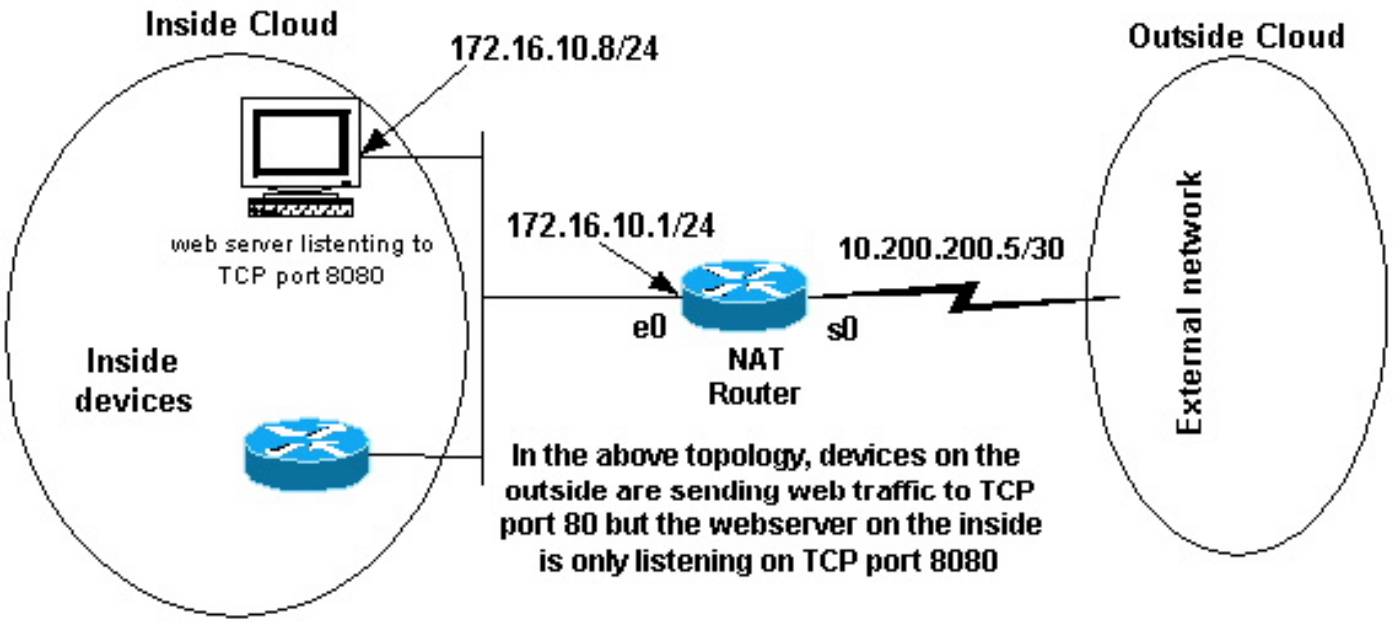
In this example, you first define the NAT inside and outside interfaces, as shown in the previous network diagram.

Second, you define that you want users on the inside to be able to originate communication with the outside. Devices on the outside must be able to originate communication with only the mail server on the inside.

The third step is to configure NAT. To accomplish what you have defined, you can configure static and dynamic NAT together. For more information on how to configure this example, refer toConfigure Static and Dynamic NAT Simultaneously.

3. Redirect TCP Traffic to Another TCP Port or Address

A web server on the internal network is another example of when it can be necessary for devices on the internet to initiate communication with internal devices. In some cases, the internal web server can be configured to listen for web traffic on a TCP port other than port 80. For example, the internal web server can be configured to listen to TCP port 8080. In this case, you can use NAT to redirect traffic destined to TCP port 80 to TCP port 8080.



Web Traffic TCP Port

After you define the interfaces as shown in the previous network diagram, you can decide that you want NAT to redirect packets from the outside destined for 172.16.10.8:80 to 172.16.10.8:8080. You can use a **static nat** command in order to translate the TCP port number to achieve this. A sample configuration is shown here.

Configure NAT to Redirect TCP Traffic to Another TCP Port or Address

NAT Router

`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.`

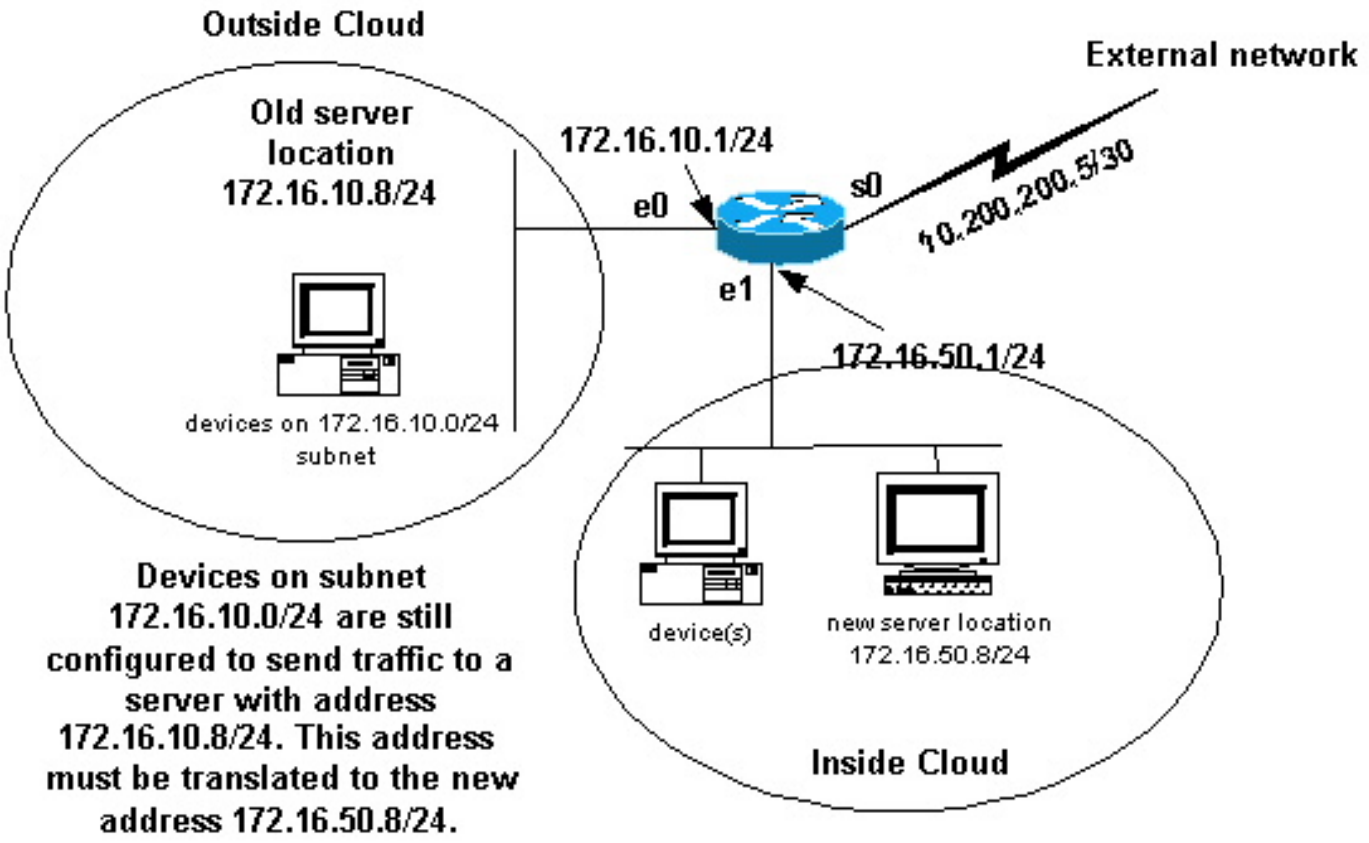
Note: The configuration description for the static NAT command indicates any packet received in the inside interface with a source address of 172.16.10.8:8080 is translated to 172.16.10.8:80. This also

implies that any packet received on the outside interface with a destination address of 172.16.10.8:80 has the destination translated to 172.16.10.8:8080.

```
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. Use NAT For a Network Transition

NAT is useful when you need to readdress devices on the network or when you replace one device with another. For instance, if all devices in the network use a particular server and this server needs to be replaced with a new one that has a new IP address, the reconfiguration of all the network devices to use the new server address takes some time. In the meantime, you can use NAT in order to configure the devices with the old address to translate their packets to communicate with the new server.



NAT Network Transition

Once you have defined the NAT interfaces as the previous image illustrates, you can decide that you want NAT to allow packets from the outside destined for the old server address (172.16.10.8) to be translated and sent to the new server address. Be aware that the new server is on another LAN, and devices on this LAN or any devices reachable through this LAN (devices on the inside part of the network), must be configured to use the new server IP address if possible.

You can use static NAT to accomplish what you need. This is a sample configuration.

Configure NAT for Use Through a Network Transition

NAT Router

```
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.
```

Note: The inside source NAT command in this example also implies that packets received on the outside interface with a destination address of 172.16.10.8 has the destination address translated to 172.16.50.8.

5. Use NAT for Networks that Overlap

Networks that overlap result when you assign IP addresses to internal devices that are already used by other devices within the internet. These networks also result when two companies, both of whom use RFC 1918 IP addresses in their networks, merge. These two networks need to communicate, preferably without all of their devices readdressed.

Difference between One-to-One and Many-to-Many Mapping

A static NAT configuration creates a one-to-one mapping and translates a specific address to another address. This type of configuration creates a permanent entry in the NAT table as long as the configuration is present and enables both inside and outside hosts to initiate a connection. This is mostly useful for hosts that provide application services like mail, web, FTP and so forth. For example:

<#root>

```
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
```

Dynamic NAT is useful when fewer addresses are available than the actual number of hosts to be translated. It creates an entry in the NAT table when the host initiates a connection and establishes a one-to-one mapping between the addresses. But, the mapping can vary and it depends upon the registered address available in the pool at the time of the communication. Dynamic NAT allows sessions to be initiated only from inside or outside networks for which it is configured. Dynamic NAT entries are removed from the translation table if the host does not communicate for a specific period of time which is configurable. The address is then returned to the pool for use by another host.

For example, complete these steps of the detailed configuration:

1. Create a pool of addresses.

```
<#root>

Router(config)#

ip nat pool MYPOOLEXAMPLE 10.41.10.1 10.41.10.41 netmask 255.255.255.0
```

2. Create an access-list for the inside networks that has to be mapped.

```
<#root>

Router(config)#

access-list 100 permit ip 10.3.2.0 0.0.0.255 any
```

3. Associate the access-list 100 that select the internal network 10.3.2.0 0.0.0.255 to be natted to the pool MYPOOLEXAMPLE and then overload the addresses.

```
<#root>

Router(config)#

ip nat inside source list 100 pool MYPOOLEXAMPLE overload
```

Verify the NAT Operation

Once you have configured NAT, verify that it operates as expected. You can do this in a number of ways: with a network analyzer, **show** commands, or **debug** commands. For a detailed example of NAT verification, refer to Verify NAT Operation and Basic NAT.

Conclusion

The examples in this document demonstrate quick start steps that can help you configure and deploy NAT.

These quick start steps include:

1. Define NAT inside and outside interfaces.
2. What do you want to accomplish with NAT.
3. Configure NAT in order to accomplish what you defined in Step 2.
4. Verify the NAT operation.

In each of the previous examples, various forms of the **ip nat inside**command were used. You can also use the **ip nat outside**command in order to accomplish the same objectives, but keep in mind the NAT order of operations. For configuration examples that use the **ip nat outside**commands, refer to Configure IP NAT Outside Source List Command.

The previous examples also demonstrated these actions:

Command	Action
ip nat inside source	• Translates the source of IP packets that travel inside to outside. • Translates the destination of the IP packets that travel outside to inside.
ip nat outside source	• Translates the source of the IP packets that travel outside to inside. • Translates the destination of the IP packets that travel inside to outside.

Related Information

- NAT: Local and Global Definitions.
- NAT Support Page
- IP Routed Protocols Support Page
- IP Routing Support Page
- IP Addressing Services
- NAT Order of Operation
- Frequently Asked Questions about Cisco IOS NAT
- Technical Support & Documentation - Cisco Systems