soundtraining.net
training for information technology and business professionals

Technical Brief

Configuring and Deploying NAT (Network Address Translation) on a Cisco Router

Prepared by Don R. Crawley, MCSE, CCNA-certified
President, soundtraining.net

Email: don@soundtraining.net
Telephone: 206.988.5858
Fax: 206.892.0499

On the World Wide Web at www.soundtraining.net

soundtraining.net
P.O. Box 1321
Seahurst, WA 98062-1321
USA

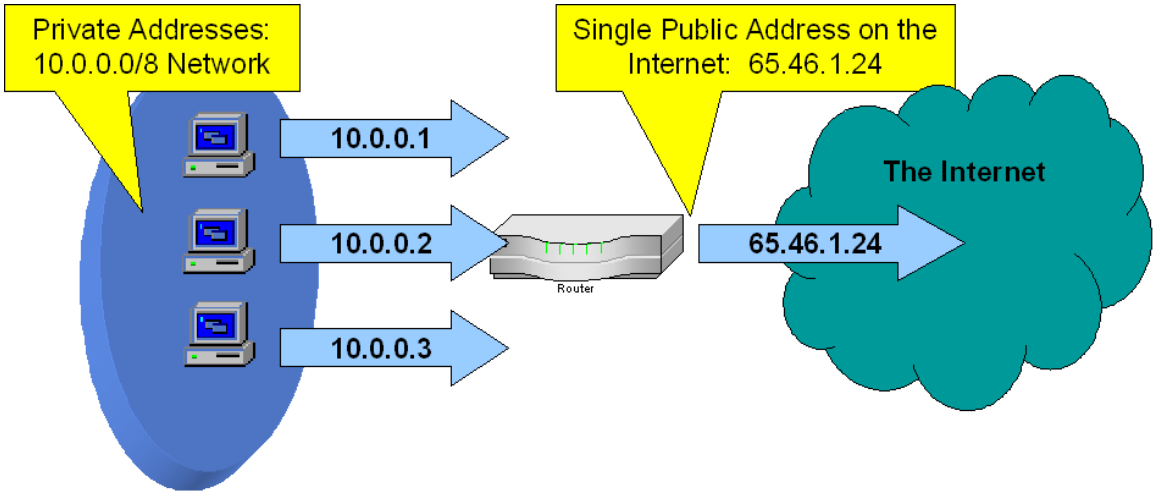
October 21, 2002

Network Address Translation on a Cisco Router

- When to use network address translation
- Types of NAT
- Configuring NAT

When to Use NAT

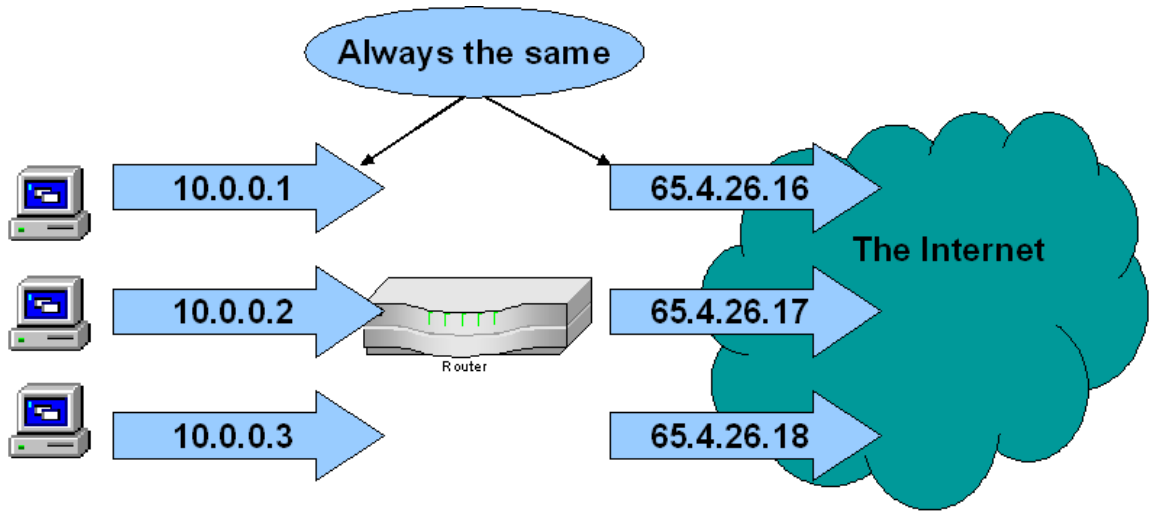
NAT connects two networks together, one private and one public. NAT is used when private addresses from the LAN need to be converted to public addresses on the Internet (or any external network). NAT allows a device such as a router or proxy server to act as an agent between private and public networks. A single address (or small range of addresses) represents an entire group of IP hosts to the public network. NAT is specified in RFC 3022.



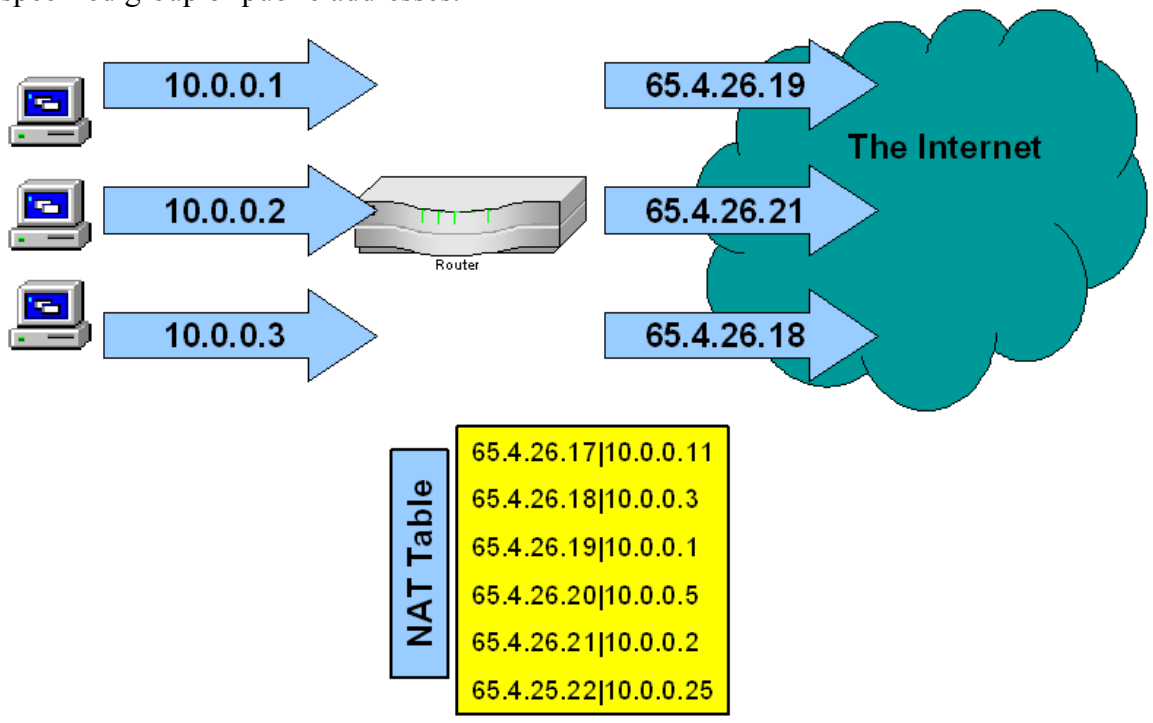
NAT serves several purposes, including the conservation of the limited public IP address space. It also provides security by making it difficult for Internet hosts to initiate connections with internal (LAN) hosts. It allows administrators to control the use of the IP address space, both internally and externally.

Types of Network Address Translation

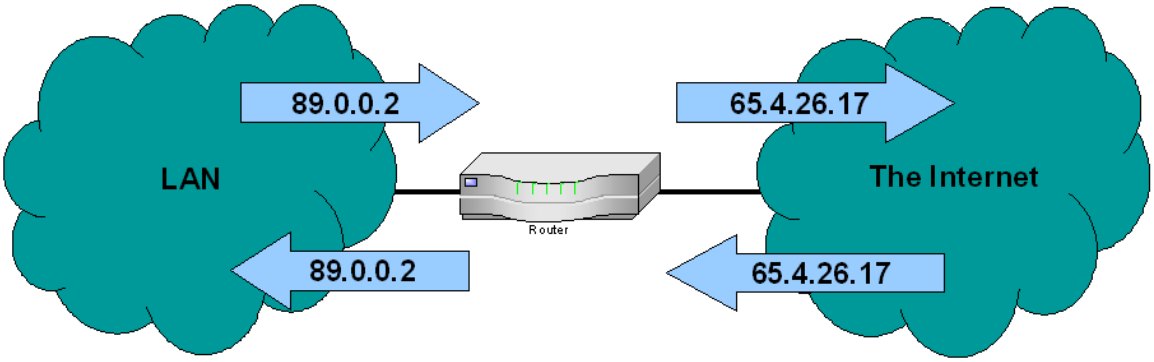
Static NAT always maps the same unregistered (private) IP address to the same registered (public) IP address. Static NAT is used when computers on private networks needs to be accessible to Internet users, as in the case of a mail or web server.



Dynamic NAT maps an unregistered (private) address to a registered (public) address from a group of public addresses. It translates to the first available address from the pre-specified group of public addresses.

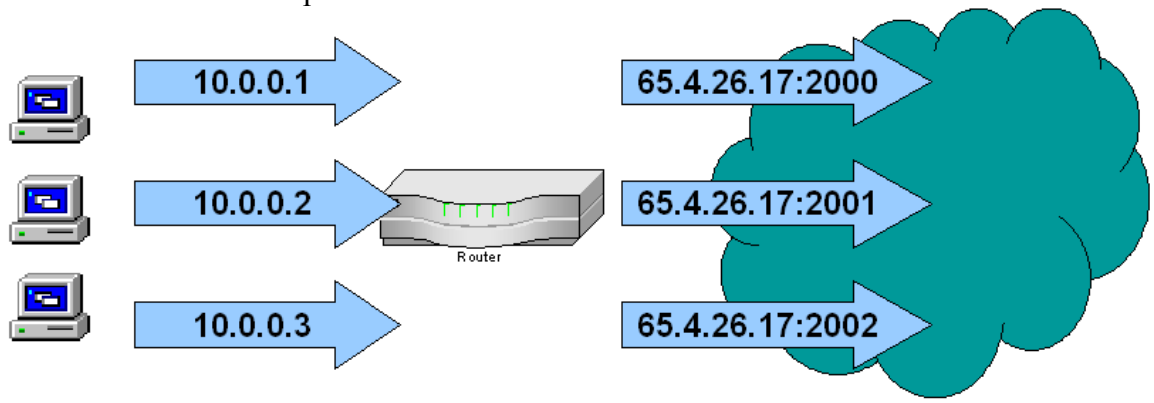


Overlapping NAT is used when the private addresses on a LAN are the same as public addresses on another network. The router maintains a "lookup table" of the "overlapping" addresses and overlapping addresses from the LAN are intercepted and replaced with unique public addresses.



Overloading NAT is a form of dynamic NAT. Interior (private) addresses are all mapped to the same public address, but with different port numbers to create unique connections. Overloading NAT is also known as:

- PAT (Port Address Translation)
- Single Address NAT
- Port-level Multiplexed NAT



NAT Overloading utilizes a feature of the TCP/IP stack called "multiplexing", which allows a host to maintain several concurrent connections with a remote computer using different TCP or UDP ports.

When using NAT Overloading, the IP packet header includes:

- Source address
- Source port (TCP or UDP port number assigned by the source computer for this connection)
- Destination address

- Destination port (TCP or UDP port number the source computer is requesting the destination computer to open)

The addresses specify the computers at each end of the connection. The port numbers ensure that the connection has a unique identifier. The combination of the four numbers identifies a unique TCP/IP connection.

Step-by-Step Guide: Configuring NAT

This step-by-step guide shows you how to configure NAT Overloading in which all internal interfaces will share one external interface (and IP address) on the Internet (or any external network).

1. Identify which interface will be external (WAN) and which will be internal (LAN). In most cases, the internal interface will be your E0 interface and the external interface will be your router's S0 interface.
2. Configure the E0 interface as the internal with the following configuration:
   Router(config)#**int e0**
   Router(config-if)#**ip nat inside**
   Router(config-if)#**int s0**
   Router(config-if)#**ip nat outside**
   Router(config-if)#**ip nat pool nattest <starting|ending address> prefix <x>** (The addresses configured here are the range of outside addresses available for use by your internal hosts. The first IP address is the beginning of the range and the second address is the end of the range. In many cases, the numbers will be the same as only a single outside address is used for the translation. The prefix is the length of the subnet mask in bits.)
   Router(config)#**ip nat inside source list 10 pool nattest overload**
   Router(config)#**access-list 10 permit <address|inverse mask>** (The first address is the network or subnet ID of the internal network which you wish to translate. The second address is the inverse mask to be used with the network or subnet address. For example, to translate the network/subnet 10.10.0.0/16, you could enter "10.10.0.0 0.0.255.255". The inverse mask is used to identify exactly which bits must match and which bits can be anything. It will be the exact inverse of the standard mask. For example, if your subnet mask is 255.255.0.0, the inverse mask would be 0.0.255.255. If your subnet mask is 255.255.192.0, the inverse mask would be 0.0.63.255 (255-192=63).
   Router(config)#**exit**

This is a sample configuration which would translate traffic from hosts within the 10.10.0.0/16 network to the 172.16.65.1 address on the outside interface.

```
router1>en
Password:
router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#int e0
router1(config-if)#ip nat inside
router1(config-if)#int s0
router1(config-if)#ip nat outside
router1(config-if)#ip nat pool nattest 172.16.65.1 172.16.65.1 prefix 22
router1(config)#ip nat inside source list 10 pool nattest overload
router1(config)#access-list 10 permit 10.10.0.0 0.0.255.255
router1(config)#exit
router1#_
```

You can watch the address translation taking place by using the following command on your router:

Router#**debug ip nat**

To turn off debugging, issue the following command:

Router#**undebug all**

You can also use **sho ip nat trans** and **show ip nat stat** to view your NAT configuration.

For more information on NAT, visit www.cisco.com and search on "NAT" or "network address translation". Also, read RFC 3022. NAT training is included in soundtraining.net's Cisco router training workshops.

About this guide…

This guide is taken from soundtraining.net's workbook for ***Unlocking the Secrets of Cisco Router Configuration and Operation 2-Day Hands-On Workshop***. You can request information concerning onsite scheduling of this fast-paced, information-packed workshop by call 206.988.5858 or emailing cisco@soundtraining.net. Onsite training can be affordable for as few as two people! Also, be sure to check online at www.soundtraining.net for information concerning our public seminars and workshops schedules.

soundtraining.net is a Seattle, Washington based training firm, specializing in training for information technology professionals and business professionals. Training programs include Microsoft and Cisco networking and desktop workshops and seminars, project management and business process analysis seminars and workshops, and our one-day ***Trends in Technology*** briefing.

Contact soundtraining.net via email at trainers@soundtraining.net, by telephone at 206.988.5858, or via postal mail at:

soundtraining.net
Box 1321
Seahurst, WA 98062-1321

soundtraining.net
training for information technology and business professionals