CCNA / CCNP Tutorial: Introduction To NAT

By Chris Bryant, CCIE #12933

A Free Excerpt From The Bryant Advantage Ultimate CCNA Study Guide

Network Address Translation (NAT) is not only an important topic for CCNA and CCNP exams, but it's also a very commonly used technique for allowing end users access to the Internet while not revealing the end user's true IP address.

CCNA and CCNP candidates need to know how to configure NAT, and so does anyone who works in network administration. NAT is one of the most commonly used network technologies out there, and understanding how and why it is used is vital to all network personnel.

Why Do We NAT?

NAT allows private networks all over the world to use the same internal network numbers, while still allowing their users (or perhaps just some users) access to the Internet.

In this way, NAT serves as a form of IP address conservation. Imagine how many IP addresses would be necessary if every single office around the world required IP addresses that were not duplicated anywhere else in the world!

The addresses that private networks around the world use are the RFC 1918 private addresses, sometimes referred to as "1918 addresses". A word to the wise: Know these, and know them cold. I should be able to call you at 2AM and ask you what these are, and get an immediate response. :)

The RFC 1918 Private Addresses

Class A	10.0.0.0 / 8
Class B	172.16.0.0 / 12
Class C	192.168.0.0 /16

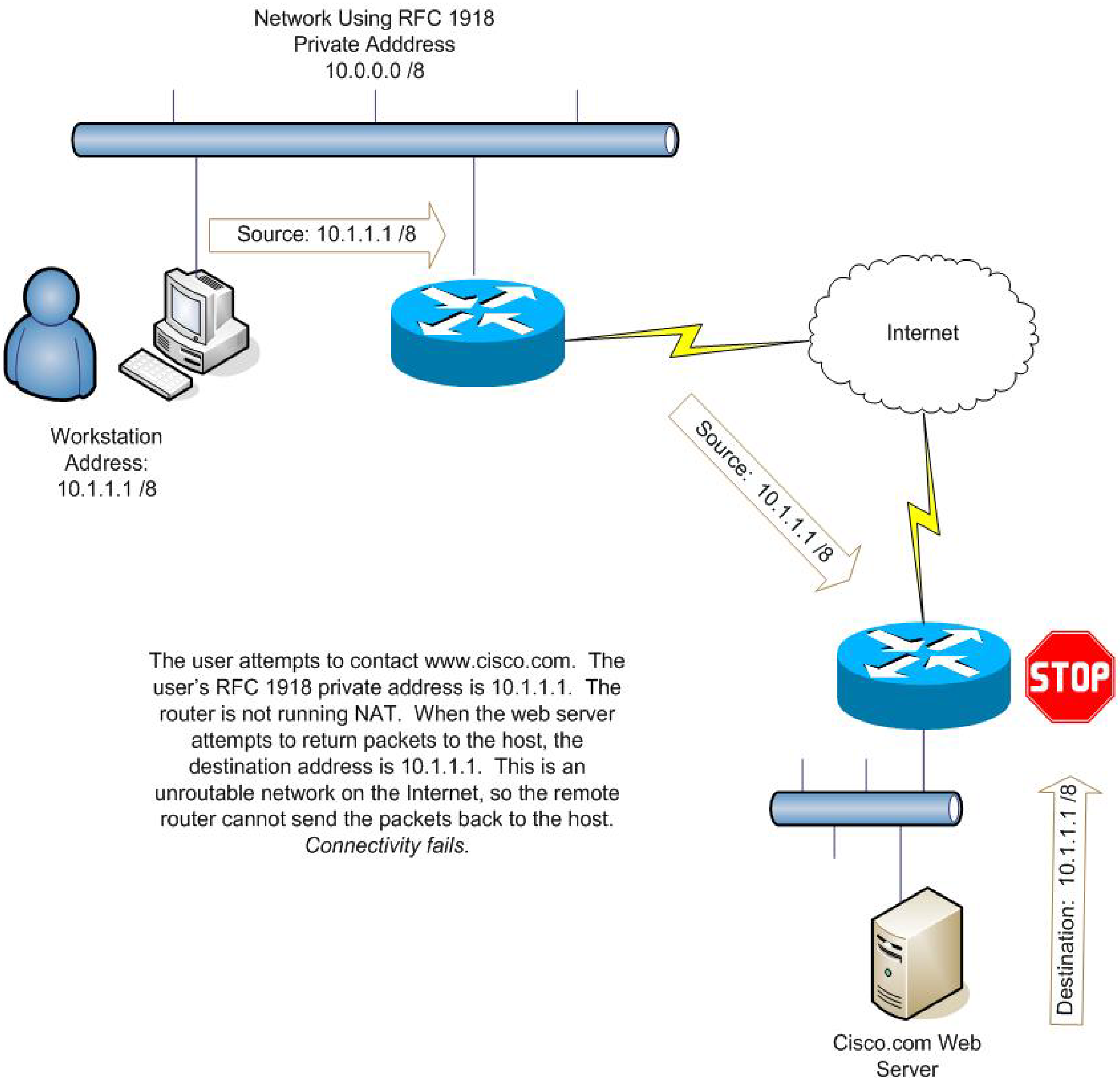
Note that the masks used with the RFC 1918 private addresses are NOT the default masks for Class A, B, and C.

These IP addresses are not used on any public networks. By public networks, we mean networks connected to the Internet.   It's my experience that the Class C 1918 addresses are the most commonly used by offices, banks, and other organizations.

If a bank and a school in your home city are both using the 192.168.0.0 /16 network on their internal networks, there's no problem *until* some of the users on either network want to access the Internet.

Internet Access and RFC 1918 Addresses

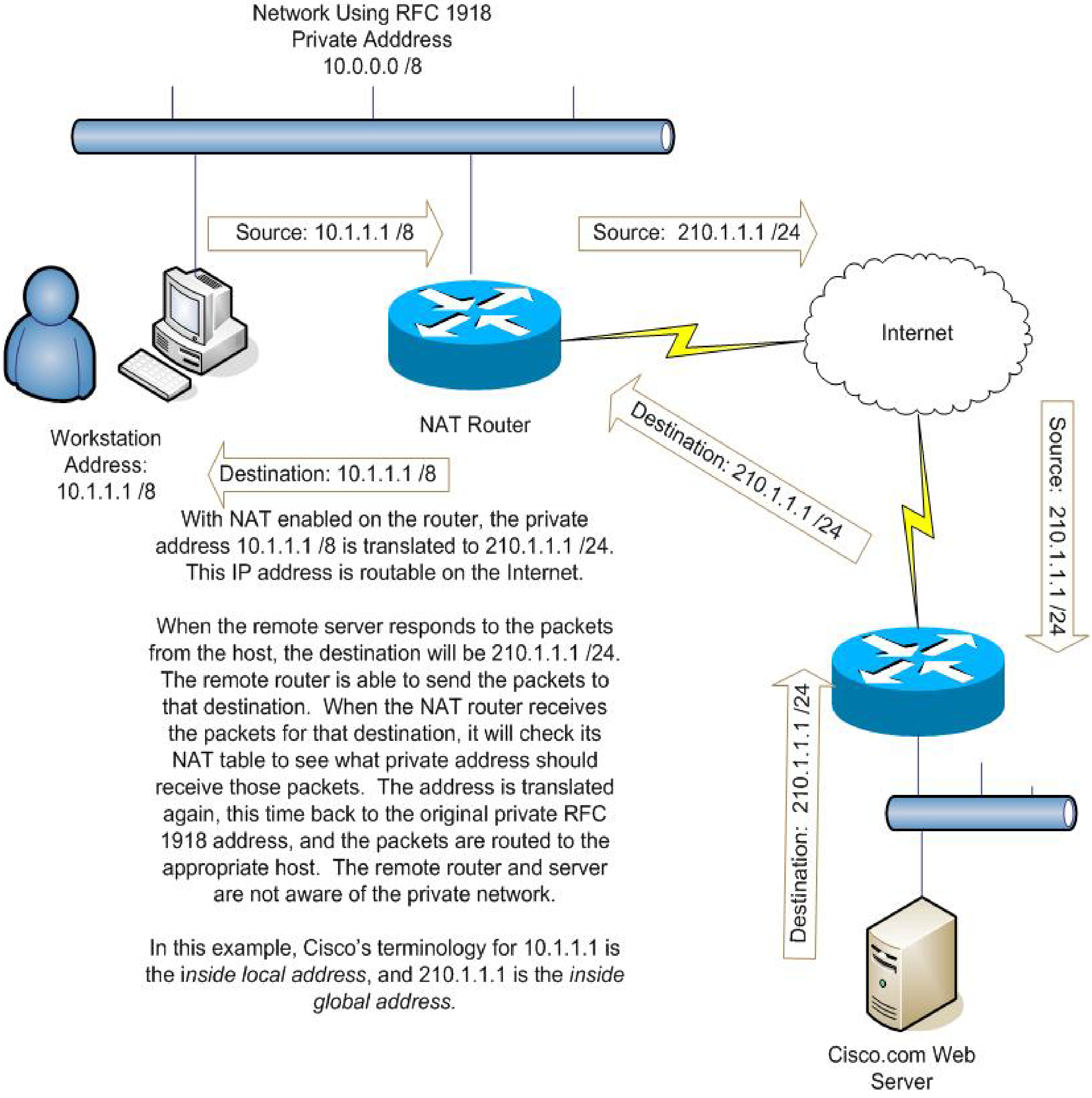
Using private addresses is fine until a host using a private address wants to communicate with a device on the Internet. Consider what happens if a workstation with a private IP address attempts to contact www.cisco.com. Cisco's web server would receive a packet from a host with a source address on an RFC 1918 network. How would the server know how to respond to the private address if it's not used anywhere on the internet? This illustration shows us where the problem would come in on a network that is not running NAT.



The user attempts to contact www.cisco.com. The user's RFC 1918 private address is 10.1.1.1. The router is not running NAT. When the web server attempts to return packets to the host, the destination address is 10.1.1.1. This is an unroutable network on the Internet, so the remote router cannot send the packets back to the host. *Connectivity fails.*

In this situation, no user on a private network can successfully communicate with an Internet host.

These networks can communicate with Internet hosts by using NAT. NAT stands for Network Address Translation, and that's exactly what is going to happen: the RFC 1918 source address is going to be translated to another address as it leaves the private network, and it will be translated back to its original address as the return data enters the private network.



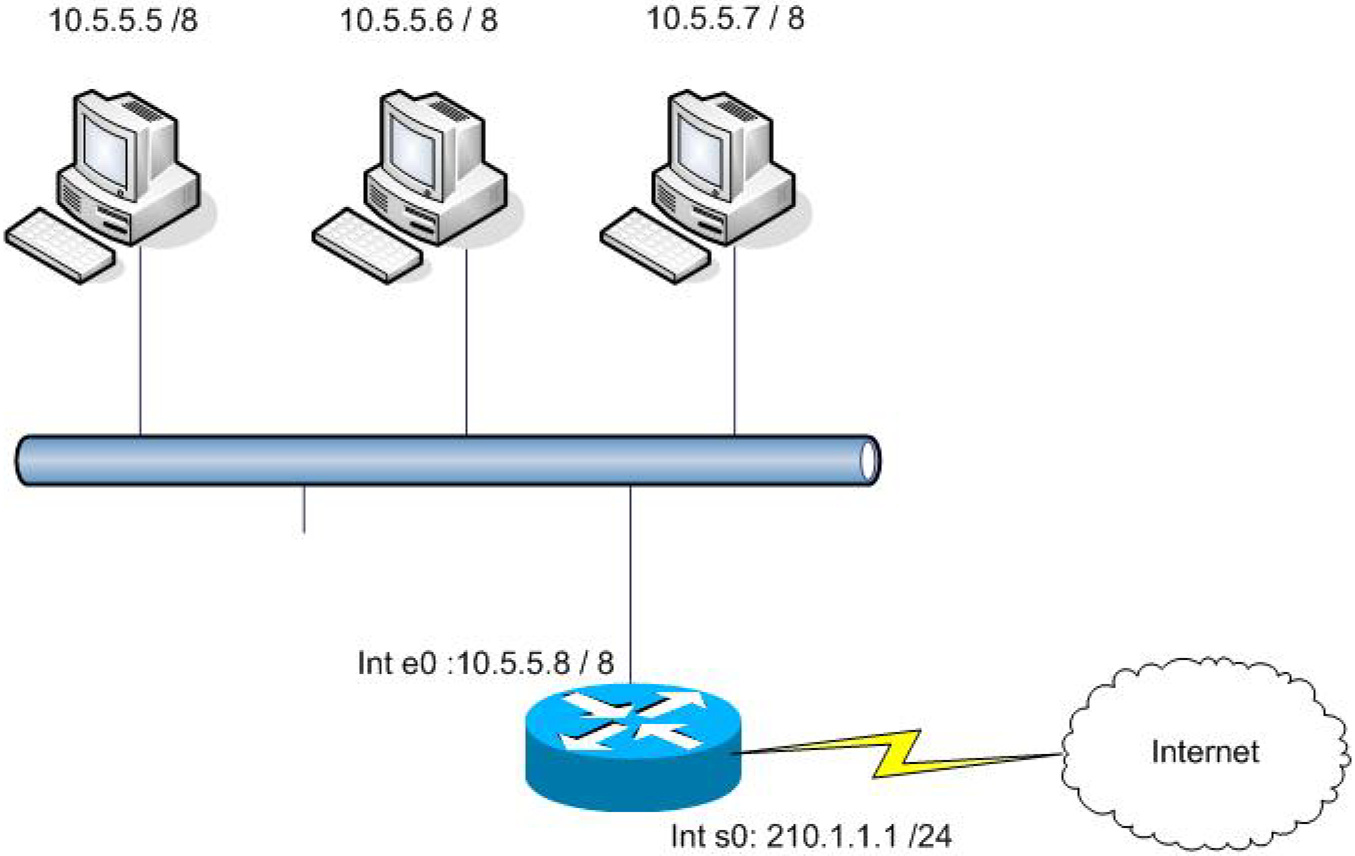
With NAT enabled on the router, the private address 10.1.1.1 /8 is translated to 210.1.1.1 /24. This IP address is routable on the Internet.

When the remote server responds to the packets from the host, the destination will be 210.1.1.1 /24. The remote router is able to send the packets to that destination. When the NAT router receives the packets for that destination, it will check its NAT table to see what private address should receive those packets. The address is translated again, this time back to the original private RFC 1918 address, and the packets are routed to the appropriate host. The remote router and server are not aware of the private network.

In this example, Cisco's terminology for 10.1.1.1 is the i*nside local address*, and 210.1.1.1 is the *inside global address.*

NAT can be defined statically or dynamically. While you need to know both for your CCNA and CCNP exams, I recommend you use dynamic NAT whenever possible. The average office has enough users to make configuring static NAT a royal pain.

If a limited number of hosts on a private network need Internet access, *static NAT* may be the appropriate choice. Static NAT maps a private address to a public one.
In this example, there are three internal PCs on an RFC1918 private network. The router's ethernet0 interface is connected to this network, and the Internet is reachable via the Serial0 interface. The IP address of the serial interface is 210.1.1.1 /24, with all other addresses on the 210.1.1.0 /24 network available.



Three static mappings are needed to use Static NAT. **The interfaces must be configured for NAT as well.**

Configuring the interfaces for Network Address Translation. The Ethernet network is the "inside" network;
the Serial interface leading to the Internet is the "outside" network.

```
R3(config)#interface ethernet0
R3(config-if)#ip address 10.5.5.8 255.0.0.0
```

```
R3(config-if)#ip nat inside
R3(config-if)#interface serial0
R3(config-if)#ip address 210.1.1.1 255.255.255.0
R3(config-if)#ip nat outside
```

The static mappings are created and verified.

```
R3#conf t
R3(config)#ip nat inside source static 10.5.5.5 210.1.1.2
R3(config)#ip nat inside source static 10.5.5.6 210.1.1.3
R3(config)#ip nat inside source static 10.5.5.7 210.1.1.4

R3#show ip nat translations
Pro Inside global     Inside local      Outside local     Outside global
--- 210.1.1.2          10.5.5.5          ---              ---
--- 210.1.1.3          10.5.5.6          ---              ---
--- 210.1.1.4          10.5.5.7          ---              ---

R3#show ip nat statistics

Total active translations: 3 (3 static, 0 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet0
Hits: 0  Misses: 0
Expired translations: 0
```

"show ip nat statistics" displays the number of static and dynamic mappings.

If you only have a few users on your RFC 1918 network that will use the Internet (or should be allowed to), static NAT will do just fine. For most networks, though, dynamic NAT is a better solution.

This article was contributed by Chris Bryant from http://www.thebryantadvantage.com