Configuring Static NAT in cisco router

The use of Network Address Translation (NAT) has been widespread for a number of years; this is because it is able to solve a number of problems with the same relatively simple configuration. At its most basic, NAT enables the ability to translate one set of addresses to another; this enables traffic coming from a specific host to appear as though it is coming from another and do it transparently.

NAT Concepts

There are a number of different concepts that must be explained in order to really get a good understanding of how NAT operates, which ultimately makes the configuration of NAT increasingly simple. This section reviews these different concepts and begins with an understanding of how NAT can be used. Some of the main uses for NAT include:

- Translation of non-unique addresses into unique addresses when accessing the Internet:

  This is one of the most common uses of NAT today; almost every household that has a "router" to access the Internet is using NAT on this device to translate between internal private address and public Internet addresses.

- Translation of addresses when transitioning internal addresses from one address range into another (this is common when the organization of addresses within a company is being changed):

  This is often done when a company is transitioning their IP addressing plan; common scenarios include when expanding (and the IP addressing plan was not built sufficiently when the initial addresses were assigned) and when a company is merging with another with potential overlapping addresses.

- When simple TCP load sharing is required across many IP hosts:

  This is very common, as many highly used servers are not really a single machine but a bank of several machines that utilize load balancing. In this scenario, commonly, a single public address is translated into one of several internal addresses in a round robin fashion.

This is not a complete list of every possible way that NAT can be configured but simply a list of the most common ways that it is used in modern networks.

There are a couple of main concepts that also must be reviewed and understood before configuring NAT:

- Inside and Outside Addresses
- NAT types

Inside and Outside Addresses

In typical NAT configurations, interfaces are placed into one of two categories (or locations): *inside* or *outside*. *Inside* indicates traffic that is coming from within the organizational network. O*utside* indicates traffic that is coming from an external network that is outside the organizational network.

These different categories are then used to define different types of address depending on location of the address and how it is being "seen". These different types include:

- **inside local address**: This is the inside address as it is seen and used within the organizational network.
- **inside global address**: This is the inside address as it is seen and used on the outside of the organizational network.
- **outside local address**: This is the outside address as it seen and used within the organizational network.
- **outside global address**: This is the outside address as it is seen and used on the outside of the organizational network.

NAT Types

Another important concept to be familiar with is the different types of NAT and how they are defined. On most networks there are three different types of NAT that are defined:

- **Static address translation (Static NAT):** This type of NAT is used when a single inside address needs to be translated to a single outside address or vice versa.
- **Dynamic address translation (Dynamic NAT):** This type of NAT is used when an inside address (or addresses) need to be translated to an outside pool of addresses or vice versa.
- **Overloading (Port Address Translation (PAT):** This type of NAT is a variation on dynamic NAT. With dynamic NAT, there is always a one to one relationship between inside and outside addresses; if the outside address pool is ever exhausted, traffic from the next addresses requesting translation will be dropped. With overloading, instead of a one to one relationship, traffic is translated and given a specific outside port number to communicate with; in this situation, many internal hosts can be using the same outside address while utilizing different port numbers.

Static NAT Configuration

There a few steps that are required when configuring static NAT; the number of the commands depends on whether there will be more than one static translation:

1	Enter global configuration mode.	router#**configure terminal**
2	Configure the static NAT translation (this command can be used multiple times depending on the number of static translations required). The **overload** keyword enables the use of PAT.	router(config)#**ip nat inside source static** *local-ip global-ip* [**overload**]
3	Enter interface configuration mode for the inside interface.	router(config)#**interface** *interface-id*
4	Configure the interface as the inside NAT interface.	router(config-if)#**ip nat inside**
5	Enter interface configuration mode for the outside interface.	router(config-if)#**interface** *interface-id*
6	Configure the interface as the outside NAT interface.	router(config-if)#**ip nat outside**
7	Exit configuration mode.	router(config-if)#**end**

Using NAT we can hide real ip address,we can translate private ip address to public ip address and viceversa.As we all know in internet only public ip addresses are used and some ip in every class has been reserved for use in **LOCAL AREA CONNECTION** say **LAN** and these ranges of ip are known as **Private IP Address**.Private Addresses can only be used in LAN and it can't be used in internet.But our PC with private address can communicate with PC or Machine having public ip address using **NAT**(Network Address Translation).

A public IP address is an IP address that can be accessed over the Internet. Like postal address used to deliver a postal mail to your home, a public IP address is the globally unique IP address assigned to a computing device. Private IP address on the other hand is used to assign computers within your private space without letting them directly expose to the Internet. For example, if you have multiple computers within your home you may want to use private IP addresses to address each computer within your home. In this scenario, your router get the public IP address, and each of the computers, tablets and smartphones connected to your router (via wired or wifi) get a private IP address from your router via DHCP protocol.

Internet Assigned Numbers Authority (IANA) is the organization responsible for registering IP address ranges to organizations and Internet Service Providers (ISPs). To allow organizations to freely assign private IP addresses, the Network Information Center (InterNIC) has reserved certain address blocks for private use.

The following IP blocks are reserved for private IP addresses.

Class	Starting IP Address	Ending IP Address	# of Hosts
A	10.0.0.0	10.255.255.255	16,777,216
B	172.16.0.0	172.31.255.255	1,048,576
C	192.168.0.0	192.168.255.255	65,536

What is public IP address?

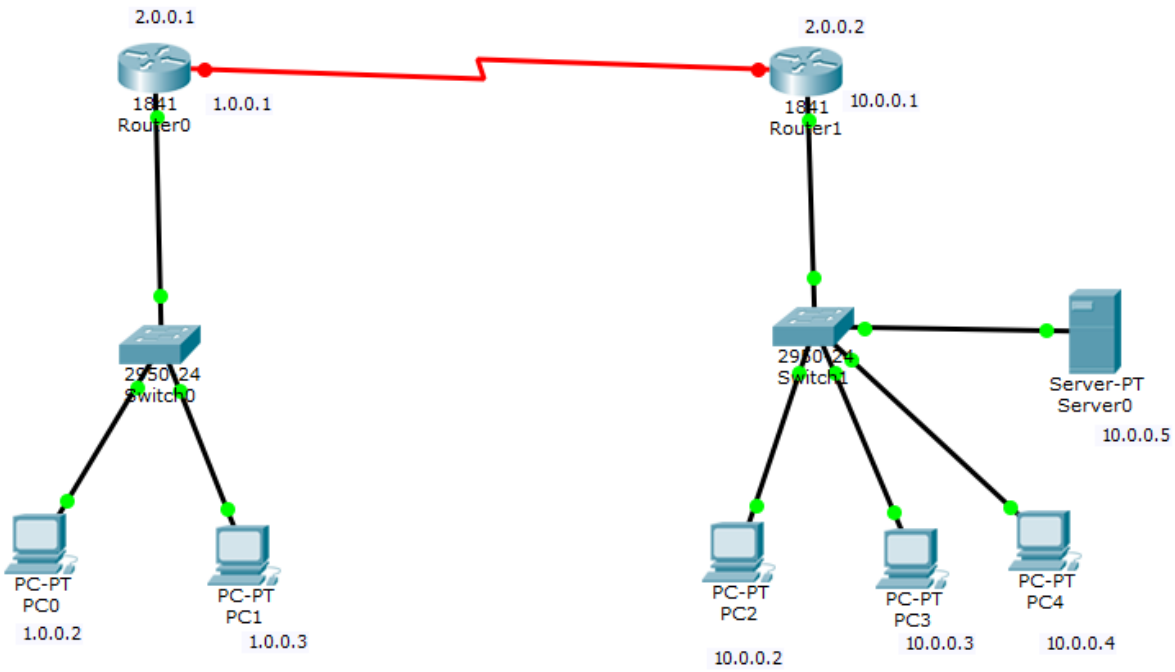
A public IP address is the address that is assigned to a computing device to allow direct access over the Internet. A web server, email server and any server device directly accessible from the Internet are candidate for a public IP address. A public IP address is globally unique, and can only be assigned to an unique device.

What is private IP address?

A private IP address is the address space allocated by InterNIC to allow organizations to create their own private network. There are three IP blocks (1 class A, 1 class B and 1 class C) reserved for a private use. The computers, tablets and smartphones sitting behind your home, and the personal computers within an organizations are usually assigned private IP addresses. A network printer residing in your home is assigned a private address so that only your family can print to your local printer.

When a computer is assigned a private IP address, the local devices sees this computer via it's private IP address. However, the devices residing outside of your local network cannot directly communicate via the private IP address, but uses your router's public IP address to communicate. To allow direct access to a local device which is assigned a private IP address, a Network Address Translator (NAT) should be used.

Now see the Example Lab Diagram through which we are going to learn how to configure STATIC NAT.



In above Diagram you can clearly see there are total 3 network used .

- Network 1.0.0.0 which is a public network.
- Network 2.0.0.0 which is also a public network.
- Network 10.0.0.0 which is a Private Network

STEP-1 Configuration on Router0

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#host r1

r1(config)#int fa0/0

r1(config-if)#ip add 1.0.0.1 255.0.0.0

r1(config-if)#no shut

r1(config-if)#exit

r1(config)#int se0/0/0

r1(config-if)#clock rate 64000

r1(config-if)#ip add 2.0.0.1 255.0.0.0

r1(config-if)#exit

r1(config)#ip route 3.0.0.0 255.0.0.0 2.0.0.2

Step-2 Configuration on Router1

Router>enable

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#host r2

r2(config)#int se0/0/0

r2(config-if)#ip add 2.0.0.2 255.0.0.0

r2(config-if)#no shut

r2(config-if)#exit

r2(config)#

r2(config)#int fa0/0

r2(config-if)#ip add 10.0.0.1 255.0.0.0

r2(config-if)#no shut

Step-3 Start configuring Private IP to Public IP

r2(config)#ip route 1.0.0.0 255.0.0.0 2.0.0.1

r2(config)#ip nat inside source static 10.0.0.2 3.0.0.2

r2(config)#ip nat inside source static 10.0.0.3 3.0.0.3

r2(config)#ip nat inside source static 10.0.0.4 3.0.0.4

r2(config)#ip nat inside source static 10.0.0.5 3.0.0.5

r2(config)#exit

r2#config t

Enter configuration commands, one per line. End with CNTL/Z.

r2(config)#int fa0/0

r2(config-if)#ip nat inside

r2(config-if)#exit

r2(config)#int se0/0/0

r2(config-if)#ip nat outside

r2(config-if)#exit

r2(config)#

Step-4 NAT testing and Troubleshooting command.

r2#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	3.0.0.2	10.0.0.2	---	---
---	3.0.0.3	10.0.0.3	---	---
---	3.0.0.4	10.0.0.4	---	---
---	3.0.0.5	10.0.0.5	---	---

You can also see NAT Statistics using below command.

r2#show ip nat statistics

Now I am on PC1 and trying to communicate or ping with private ip address mentioned above.

PC>ipconfig

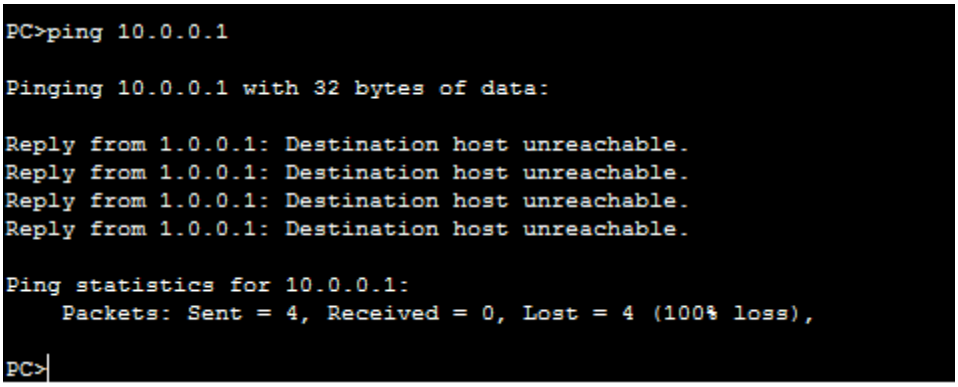
FastEthernet0 Connection:(default port)

Link-local IPv6 Address…….: FE80::210:11FF:FEA1:9244

IP Address…….: 1.0.0.3

Subnet Mask……: 255.0.0.0

Default Gateway……..: 1.0.0.1



You can see that it says destination unreachable, it means can't find private ip.

How to configure NTP Server and NTP Client on cisco Router

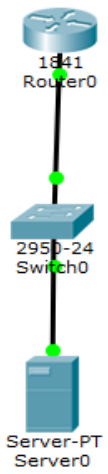
Whenever we talks about cisco routers and how to set clock or accurate time on routers it becomes so important because a variety of services depend on it. We need to monitor our routers and secure our routers through server configuration.We use to configure syslog server for monitoring routers log and incident happening over routers.The logging service shows each log entry with the date and time and all details which are directly or indirectly related to NTP Server.It becomes very critical if you're trying to track a specific incident or troubleshoot a problem.

Cisco routers have two types of clocks :

- A battery-powered hardware clock, referenced as the 'calendar' in the IOS CLI, and
- a software clock, referenced as the 'clock' in the IOS CLI.

The software clock is the primary source for time data and runs from the moment the system is up and running. The software clock can be updated from a number of sources.

Now to show ntp server-client configuration, below topology diagram is considered



Step-1:First configure ip address on routers.

Router>enable

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#host r1

r1(config)#int fa0/0

r1(config-if)#ip add 1.0.0.1 255.0.0.0

r1(config-if)#no shut

r1(config-if)#

r1(config-if)#exit

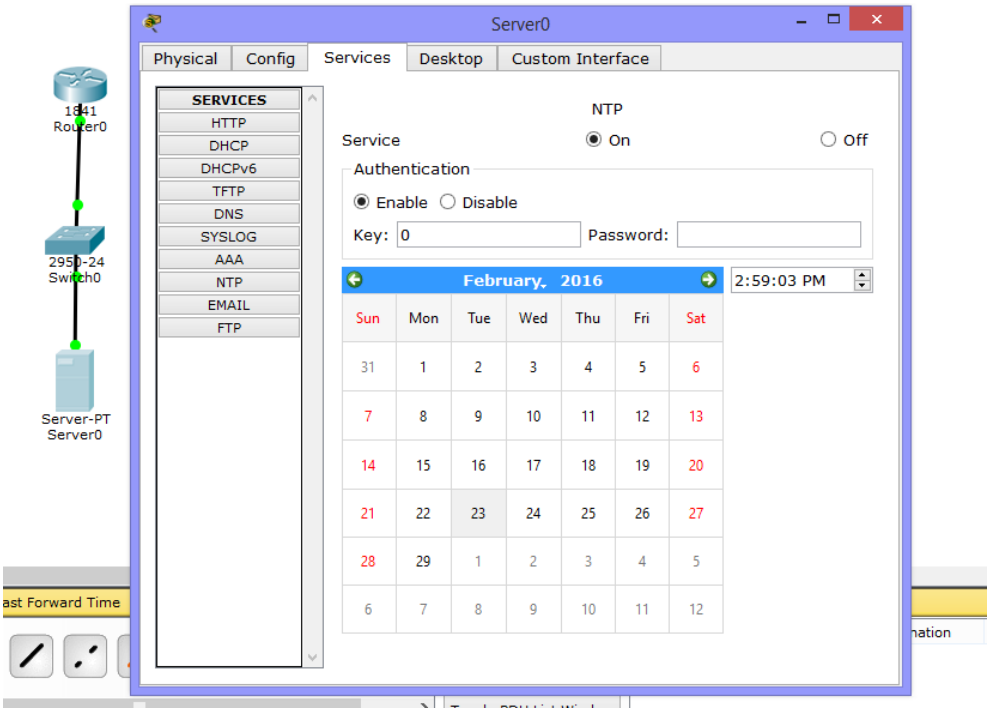
Step-2: Now see time before NTP Configuration

r1#show clock

*0:8:25.144 UTC Mon Mar 1 1993

r1#

Step-3:Now going to configure NTP Server



Step-4:Now go to Router and setup NTP Client.

r1#config t

Enter configuration commands, one per line. End with CNTL/Z.

r1(config)#ntp server 1.0.0.2

r1(config)#exit

Step-5:Now again see the time again to confirm NTP Configured or not.

```
r1#show clock
*15:2:29.448 UTC Tue Feb 23 2016
r1#

r1#show ntp status
Clock is synchronized, stratum 2, reference is 1.0.0.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is DA50B772.0000000F (15:02:10.015 UTC Tue Feb 23 2016)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec.
r1#
```