Design And Configuration Of Static Network Address Translation Techniques Method Using Cisco Packet Tracer Tool

Dr. Rajamohan Parthasarathy, Ms. Preethy Ayyappan

Abstract: The explosive growth of internet and increases of business and home networks mainly depends on the Network Address Translation (NAT) because the insufficient of available IP addresses. IP address is mandatorily required to communicate on the internet from one computer to another computer. In computer networks the single device of a router is acting as an agent between the local area network and internet as allowable by Network Address Translation. This technology of Network Address Translation may help in many ways for the Network System Engineers and Networks Administrators especially to reduce the cost and timing when they are configuring the part of IP addresses. The same relatively simple IP address configuration problems to be solved by this Network Address Translation techniques. The ability of NAT enable to translate from one group of or set of addresses to another group of or set addresses. The NAT enables the data traffic from a particular client or host to appear as it comes from another client or host and process it as transparently. The pool of IP addresses are provided by router and to be used by local area network and only a single IP addresses required to represent the this all group of clients or hosts. Three categories of NAT available especially in computer networks mainly that Static Network Address Translation (Static NAT), Dynamic Network Address Translation (Dynamic NAT) and Port Address Translation (PNAT). I would like to focus more on this paper on Static NAT design and configurations techniques using Cisco Packet Tracer Simulation tools for networking people.

Index Terms: Static NAT, Local IP Address, Global IP Address, Inside Local IP Address, Inside Global IP Address, Outside Local IP Address, Outside Global IP Address, IP NAT Inside and IP NAT Outside.

1 INTRODUCTION

The Network Address Translation can able to allow a network single device such as either router or firewall to acting as an agent between a private network space and a public network space. The enabled NAT agent can conceivable or possible to use a single IP address to signify or represent the entire group networked computers. Networks Address Translations may help the Networks Engineer and the Network Administrators to manage the portions of the private and public address spaces. The separation of IP address is mainly done by NAT and forming the physical device in the independent private network IP address of the hosts in the public networks. The NAT has defined well specifically in RFC (Request For Comments) 3022 [1]. The IP address allocation for private internets is also defined in RFC 1918 [2]. Principally the address of the IPv4 on the threshold was being exhausted in the middle of 1990 but enterprises and organizations required such address blocks for their private network spaces. The Block of IPv4 address are listed in Table 1 and these addresses especially reserved for private IP address and are not routable on the networks of the backbone infrastructure [2].

TABLE 1

Available Freely Address Block RFC 191

CIDR (/) Notation	Range of Address
10/8	10.0.0.0 To 10.255.255.255.255
172.16/12	172.16.0.0 To 172.31.255.255
192.168/16	192.168.0.0 To 192.168.255.255

The IP addressing scheme CIDR (Classless Inter Domain Routing) that assigns the internet addresses blocks to permit completely into number of routing table entries as smaller. CIDR as defined in RFC 1520 [3]. The address block as first one is 24 bit block, second one is 20 bit block and third one is 16 bit block. In notation of pre CIDR, the first block is empty or nothing but it has a single class A network number, a set of 16 contiguous class B networks number in second block, and a set of 256 contiguous class C networks number in third block.
The IP addresses from the address space as defined in RFC 1918 [2] is being used by any organizations or enterprises without paying or Contacting of IANA (Internet Assign Number Authority) or ISP (Internet Service Provider). An enterprise or multiple enterprises that choose the addresses within the private address space are only unique that to cooperate over this space in their own private internet to communicate each other. Static NAT that maps a single private network address into a single public network address which is typically the network server of the address. Static NAT can able to permit or allows the hosts outside of the private networks to use a public IP address to access the hosts on the private network. Static NAT security risk as potential. Network Security policy is wrongly configured means the device of private network mapped to the public IP address sure to fully shown to the public network.

2 RELATED NAT COMMANDS CONCEPTS AND APPROACHES TECHNIQUES

2.1 Network Address Translation (NAT) Concepts:

Static NAT is more useful to access the internet when a host inside a private networks as needs. The concept of static NAT is one to one mapping of a private IP address to public IP address. The operation of a networks address translation on a router to connecting two networks as simultaneously or together. Among the two networks the first one is designated as inside and these networks with either obsolete addresses

- *Dr Rajamohan Parthasarathy, Faculty of Engineering, Built Environment and Information Technology (FOEBEIT), SEGi University, Taman Sains Selangor, Kota Damansara, PJU 5, 47810 Petaling Jaya, Selangor, Malaysia. Email: parthasarathy_rajamohan@yahoo.com, prajamohan@segi.edu.my & rajamohan311098@gmail.com*
- *Ms Preethy Ayyappan, Faculty of Engineering, Built Environment and Information Technology (FOEBEIT), SEGi University, Taman Sains Selangor, Kota Damansara, PJU 5, 47810 Petaling Jaya, Selangor, Malaysia. Email: preethyayyappan@gmail.com & ayyappan@segi.edu.my*

or private addresses that required to be transformed or converted into legally addresses before the packets to another networks as forwarded and designated as outside. The operation of translation with routing as conjunction that the enabling of NAT simply on a customer side when translation is desired on a router in an internet access. The networks address translation on the router hardware as provided by RFC 1631 on a particular use of a NAT device. The functionality and the goal of NAT is provided that the globally unique addresses of the private network and the NAT device as not present. The bi-directional translation supported by Cisco IOS NAT especially on both translation of inside source and outside source simultaneously. This section explores on different concepts of NAT and understanding the usage of NAT mainly in an enterprises networks as appropriate into the benefit part as explained below [5]. When accessing the internet the translation part of non-unique addresses into unique addresses. The most common use of NAT today that all home users access the internet through router device using NAT on this device to translate between both internal private internet addresses and public internet addresses. When enterprises or company would like to transitioning the IP address planning the NAT concepts is mainly used at the time of the enterprises is merging with another company overlapping addresses as potential. When sharing of TCP loading is needed across several IP hosts. In general so many server is highly used and not a single machine but a series of several machines consume the load balancing. According to this scenario that single public address is translated into one of several internal addresses in round robin fashion.

2.2 The Address of Both Inside Address and Outside Address:

The two categories of interfaces locations are mainly in NAT configuration as inside and Outside.

2.2.1 Inside Address:

Within the organizational networks indicates the traffic is coming subject to the translation of set of networks.

2.2.2 Outside Address:

All other addresses with an external network or outside the organizational networks that indicates the traffic is coming with valid address on the internet location. The different types of addresses as defined the categories depending on the location of the address as being included as listed below.

2.2.3 Local IP Address:

The IP addresses on either internal or external as it performed or appeared and shown in the appropriate internal IP header.

2.2.4 Global IP Address:

The IP addresses on either internal or external as it performed or appeared and shown in the appropriate external IP header. Global IP address being permitted the specific network devices with a private address to be appeared or seen on the public network. The translation of static address are entered straightly in to the configuration and the translation information stored in the translation table on all time.

2.2.5 Inside Local IP Address:

The host IP address as assigned and configured on inside and as it appeared or seen and used within the boundary of organizational networks. The IP address may globally unique and be allocated out of the private address space as defined and framed by RFC 1918 or it may allocated to another office or organization as officially.

2.2.6 Inside Global IP Address:

The legitimate host IP address as assigned and configured on inside and as it appeared or seen and used on outside of the organizational networks as in the form of “Translated IP Address”. The allocated IP address from a globally unique address space classically offered by the Internet Service Provider (ISP).

2.2.7 Outside Local IP Address:

The host IP address as assigned and configured on outside and it may show and appeared inside the network and those addresses space as allocated routable on the inside and legitimate address not required as defined by RFC 1918.

2.2.8 Outside Global IP Address:

The outside host address as it is seen and used on the outside of the organizational network and it is allocated from globally routable.

Finally, The above all IP addresses as summarized as below to understand the concepts as in easy way.

Inside Local IP Address – IP address for your host
Inside Global IP Address – IP address for your public
Outside Local IP Address – IP address of remote host
Outside Global Address – IP address of remote public

2.3 Static NAT Commands Syntax and Approaches:

When we are planning to configure the part of static NAT the following steps of commands as required to full fill the static translation of network addresses.

2.3.1 Static NAT translation Configuration enable with overload keyword use of PAT:

router(config)#ip nat inside source static local-ip global-ip [overload]

2.3.2 Configure the interface as the inside NAT interface:

router(config-if)#ip nat inside

2.3.3 Enter interface configuration mode for the outside interface:

router(config-if)#interface interface-id

2.3.4 Configure the interface as the outside NAT interface:

router(config-if)#ip nat outside

3 Design And Configurations Of Static Network Address Translation Methodology

Configure the Static NAT IP services and verify the connectivity between the inside and outside addresses. The configuration tasks as carried out / done by using Cisco Packet tracer Tool such as Design the Static NAT Network topology, Perform Basic Router Configurations, Enable RIP Routing Protocol configurations, IP Address Configurations on PCs, Enable inside and outside NAT Translation and Configure Static NAT Translation.[6]-[12].

3.1 Design the Static NAT Network Topology

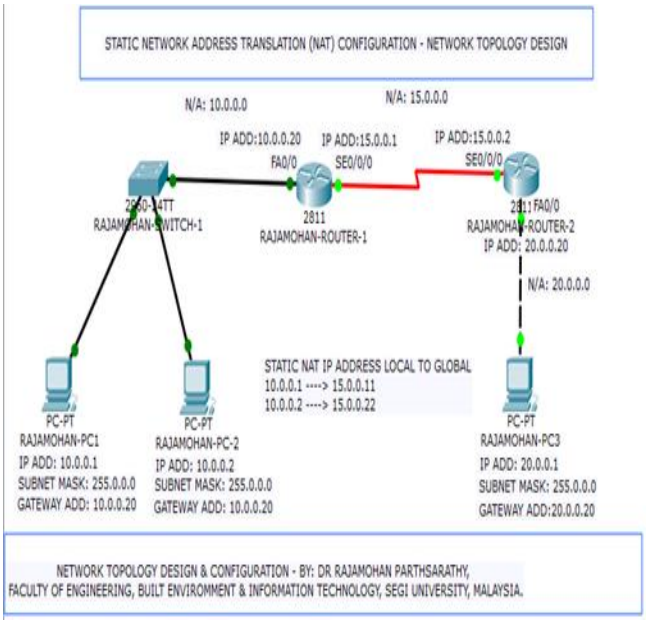


Fig. 1 *Topology of Static NAT Design with Specified IP Address Parameters*

TABLE 2

IP Address parameters for Static NAT Design

Device	Interface	IP Address	Subnet Mask	Gateway
RAJAMOHAN-ROUTER-1	Serial0/0/0	15.0.0.1	255.0.0.0	-
RAJAMOHAN-ROUTER-1	FastEthernet0/0	10.0.0.20	255.0.0.0	-
RAJAMOHAN-ROUTER-2	Serial0/0/0	15.0.0.2	255.0.0.0	-
RAJAMOHAN-ROUTER-2	FastEthernet0/0	20.0.0.20	255.0.0.0	-
RAJAMOHAN-PC1	FastEthernet0	10.0.0.1	255.0.0.0	10.0.0.20
RAJAMOHAN-PC2	FastEthernet0	10.0.0.2	255.0.0.0	10.0.0.20
RAJAMOHAN-PC3	FastEthernet0	20.0.0.1	255.0.0.0	20.0.0.20
Static NAT IP Address Local to Global				
IP Address Local		To	IP Address Global	
10.0.0.1		-	15.0.0.11	
10.0.0.2		-	15.0.0.22	

3.2 Perform Basic Router Configurations:

Basic router configurations for all the routers as below.

3.2.1 Basic IP Address Configuration on RAJAMOHAN-ROUTER-1:

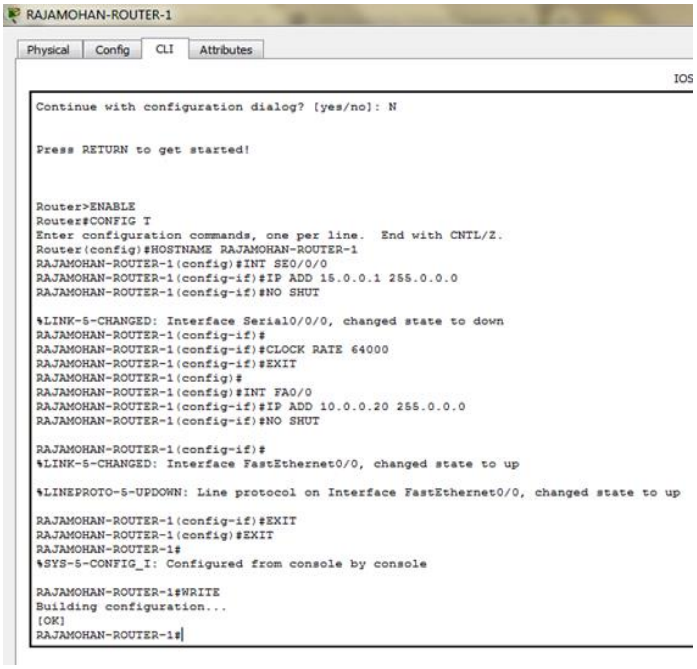


Fig. 2 *Basic IP Address Configuration on RAJAMOHAN-ROUTER-1*

3.2.2 Basic IP Address Configuration on RAJAMOHAN-ROUTER-2:

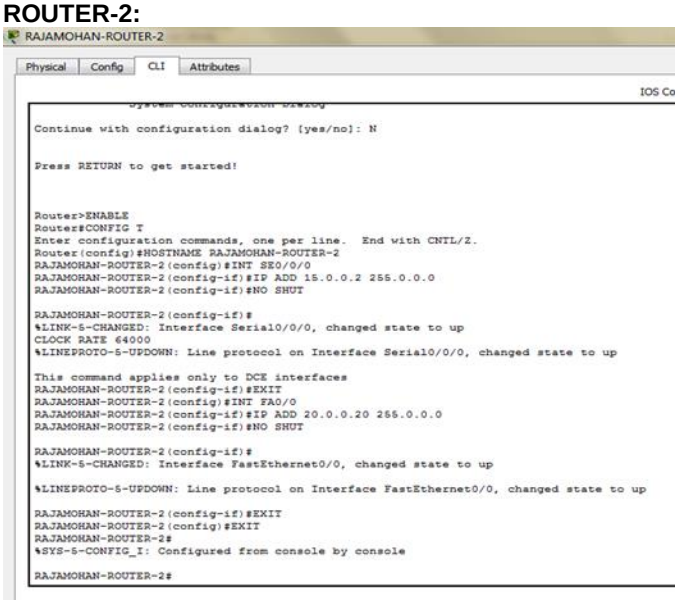


Fig. 3 *Basic IP Address Configuration on RAJAMOHAN-ROUTER-2*

3.2.3 IP Route Verification on RAJAMOHAN-ROUTER-1:

```
RAJAMOHAN-ROUTER-1>ENABLE
RAJAMOHAN-ROUTER-1#SHOW IP ROUTE
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    15.0.0.0/8 is directly connected, Serial0/0/0

RAJAMOHAN-ROUTER-1#
```

Fig. 4 *IP Route Verification on RAJAMOHAN-ROUTER-1*

3.2.4 IP Route Verification on RAJAMOHAN-ROUTER-2:

```
RAJAMOHAN-ROUTER-1>ENABLE
RAJAMOHAN-ROUTER-1#SHOW IP ROUTE
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    15.0.0.0/8 is directly connected, Serial0/0/0

RAJAMOHAN-ROUTER-1#
```

Fig. *5 IP Route Verification on RAJAMOHAN-ROUTER-2*

3.3 Enable RIP Routing Protocol Configurations:

3.3.1 Enable RIP Routing Protocol Configuration on RAJAMOHAN-ROUTER-1:

```
RAJAMOHAN-ROUTER-1>ENABLE
RAJAMOHAN-ROUTER-1#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
RAJAMOHAN-ROUTER-1(config)#ROUTER RIP
RAJAMOHAN-ROUTER-1(config-router)#NETWORK 10.0.0.0
RAJAMOHAN-ROUTER-1(config-router)#NETWORK 15.0.0.0
RAJAMOHAN-ROUTER-1(config-router)#NETWORK 20.0.0.0
RAJAMOHAN-ROUTER-1(config-router)#EXIT
RAJAMOHAN-ROUTER-1(config)#
```

Fig. *5 Enable RIP Routing Protocol Configuration on RAJAMOHAN-ROUTER-1*

3.3.2 Enable RIP Routing Protocol Configuration on RAJAMOHAN-ROUTER-2:

```
RAJAMOHAN-ROUTER-2>ENABLE
RAJAMOHAN-ROUTER-2#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
RAJAMOHAN-ROUTER-2(config)#ROUTER RIP
RAJAMOHAN-ROUTER-2(config-router)#NETWORK 10.0.0.0
RAJAMOHAN-ROUTER-2(config-router)#NETWORK 15.0.0.0
RAJAMOHAN-ROUTER-2(config-router)#NETWORK 20.0.0.0
RAJAMOHAN-ROUTER-2(config-router)#EXIT
RAJAMOHAN-ROUTER-2(config)#
```

Fig. 6 *Enable RIP Routing Protocol Configuration on RAJAMOHAN-ROUTER-2*

3.3.3 Checking the Routing Table of RAJAMOHAN-ROUTER-1:

```
RAJAMOHAN-ROUTER-1>ENABLE
RAJAMOHAN-ROUTER-1#SHOW IP ROUTE
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    15.0.0.0/8 is directly connected, Serial0/0/0
R    20.0.0.0/8 [120/1] via 15.0.0.2, 00:00:14, Serial0/0/0

RAJAMOHAN-ROUTER-1#
```

Fig. 7 *Checking the Routing Table of RAJAMOHAN-ROUTER-1*

3.3.4 Checking the Routing Table of RAJAMOHAN-ROUTER-:

```
RAJAMOHAN-ROUTER-2>ENABLE
RAJAMOHAN-ROUTER-2#SHOW IP ROUTE
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    10.0.0.0/8 [120/1] via 15.0.0.1, 00:00:19, Serial0/0/0
C    15.0.0.0/8 is directly connected, Serial0/0/0
C    20.0.0.0/8 is directly connected, FastEthernet0/0

RAJAMOHAN-ROUTER-2#
```

Fig. 8 *Checking the Routing Table of RAJAMOHAN-ROUTER-1*

3.4. IP Address Configuration on All PCs:

3.4.1 IP Address Configuration on PCs - RAJAMOHAN-PC1:

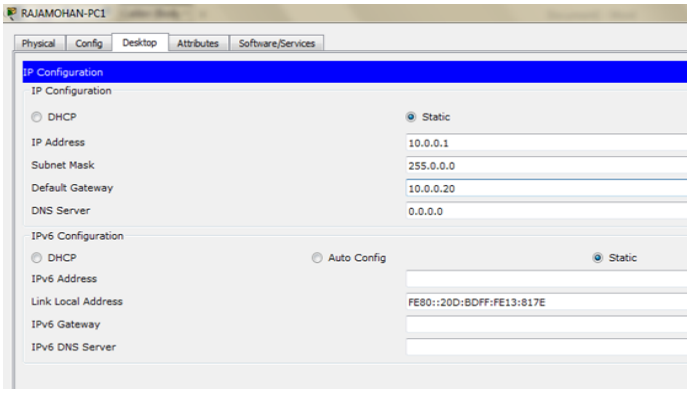


Fig. 9 *IP Address Configuration on PCs - RAJAMOHAN-PC1:*

3.4.2 IP Address Configuration on PCs - RAJAMOHAN-PC2:

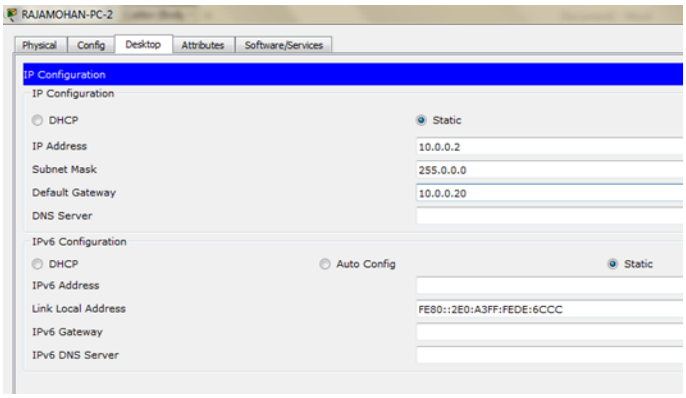


Fig. 10 *IP Address Configuration on PCs - RAJAMOHAN-PC2*

3.4.3 IP Address Configuration on PCs - RAJAMOHAN-PC3:

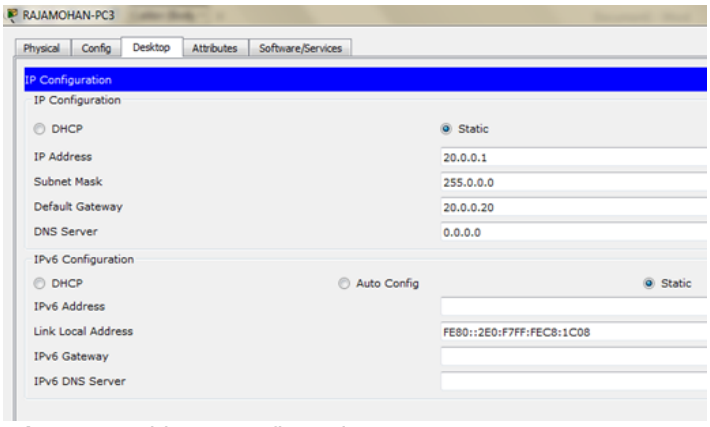


Fig. 11 *IP Address Configuration on PCs - RAJAMOHAN-PC3*

3.5 Enable Inside and Outside NAT Translation on RAJAMOHAN-ROUTER-1:

3.5.1 Enable Inside NAT Translation on RAJAMOHAN-ROUTER-1:

```
RAJAMOHAN-ROUTER-1>ENABLE
RAJAMOHAN-ROUTER-1#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
RAJAMOHAN-ROUTER-1(config)#
RAJAMOHAN-ROUTER-1(config)#INT FA0/0
RAJAMOHAN-ROUTER-1(config-if)#IP NAT INSIDE
RAJAMOHAN-ROUTER-1(config-if)#EXIT
RAJAMOHAN-ROUTER-1(config)#
```

Fig. 12 *Enable Inside NAT Translation on RAJAMOHAN-ROUTER-1:*

3.5.2 Enable Outside NAT Translation on RAJAMOHAN-ROUTER-1:

```
RAJAMOHAN-ROUTER-1>EN
RAJAMOHAN-ROUTER-1#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
RAJAMOHAN-ROUTER-1(config)#INT SE0/0/0
RAJAMOHAN-ROUTER-1(config-if)#IP NAT OUTSIDE
RAJAMOHAN-ROUTER-1(config-if)#EXIT
RAJAMOHAN-ROUTER-1(config)#
```

Fig. 13 *Enable Outside NAT Translation on RAJAMOHAN-ROUTER-1*

3.5.3 Configure Static NAT Translation on RAJAMOHAN-ROUTER-1:

RAJAMOHAN-ROUTER-1(config)#
IP NAT INSIDE SOURCE STATIC 10.0.0.1 15.0.0.11
RAJAMOHAN-ROUTER-1(config)#
IP NAT INSIDE SOURCE STATIC 10.0.0.2 15.0.0.22

```
RAJAMOHAN-ROUTER-1>EN
RAJAMOHAN-ROUTER-1#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
RAJAMOHAN-ROUTER-1(config)#IP NAT INSIDE SOURCE STATIC 10.0.0.1 15.0.0.11
RAJAMOHAN-ROUTER-1(config)#IP NAT INSIDE SOURCE STATIC 10.0.0.2 15.0.0.22
RAJAMOHAN-ROUTER-1(config)#
```

Fig. 14 *Configure Static NAT Translation on RAJAMOHAN-ROUTER-1*

4 Results And Discussions

4.1 Results and Verification on PCs Part:
(Testing Command by Ping)

4.1.1 Choose RAJAMOHAN-PC1 (IP: 10.0.0.1) and Ping to RAJAMOHAN-PC3 (IP: 20.0.0.1):

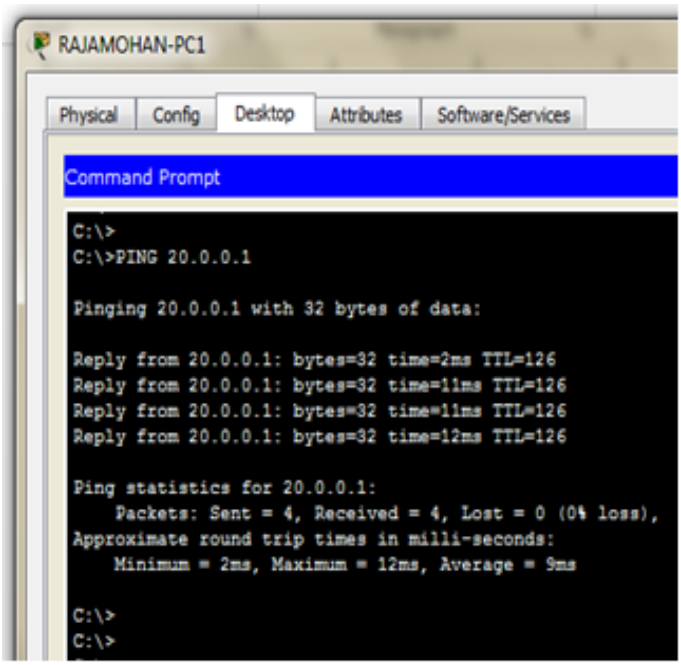
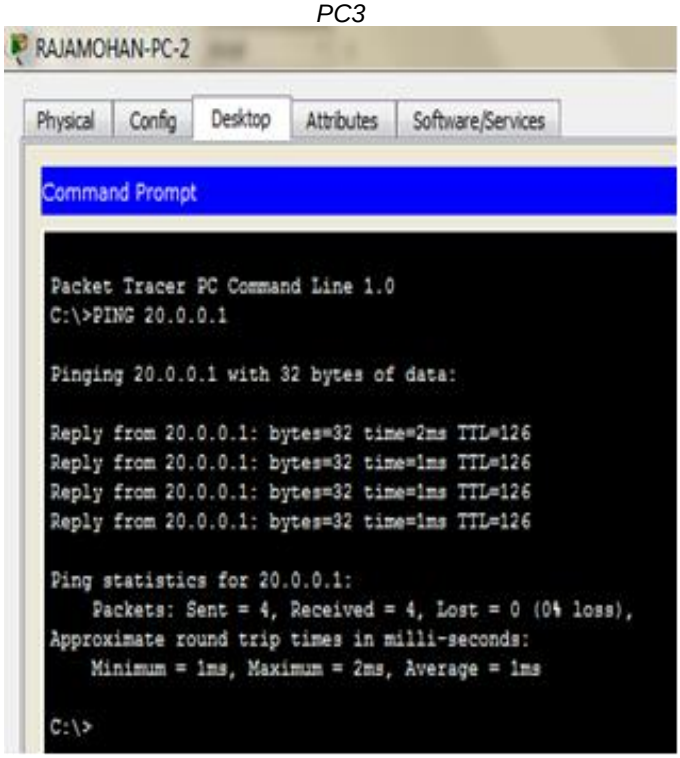


Fig. 15 *Ping Test Result Activity from RAJAMOHAN-PC1 to RAJAMOHAN-PC3*

4.1.2 Choose RAJAMOHAN-PC2 (IP: 10.0.0.2) and Ping to RAJAMOHAN-PC3 (IP: 20.0.0.1):

Fig. 16 *Ping Test Result Activity from RAJAMOHAN-PC2 to RAJAMOHAN-PC3*



4.2 Verification Static NAT on RAJAMOHAN-ROUTER-1 (Testing Command by Show IP NAT Translation)

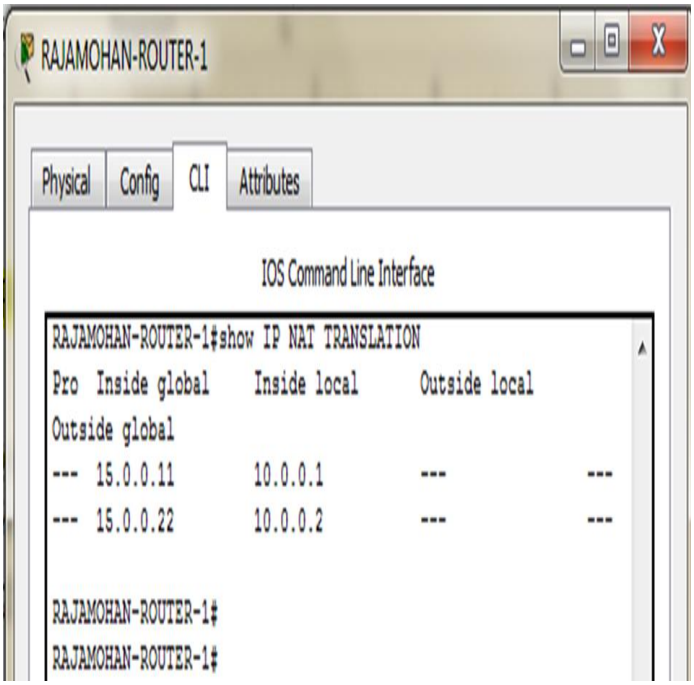


Fig. 17 *Show IP NAT Translation Test Result Activity on RAJAMOHAN-ROUTER-1*

5 CONCLUSION

Network Address Translation is one of main reason that using in networking sectors to simplifies the network administration tasks. NAT provides us in terms of flexibility by the way of assigning internal network IP addresses meanwhile it allows us to separate public network spaces from private network spaces. For example, The FTP server or Web server to another client or host, we have to change the address mapping only at the firewall to replicate the new host. Also, in case if the changes makes to the internal network that we no need to reconfiguration of the IP address for each host because the IP address of public for each device in the local of internal network either belongs to the firewall or it is linked with external network interface of the firewall. NAT is also cost effective policy to reduce the expenses of network infrastructure and time saving. The non-public routable address blocks defined in RFC 1918 and it can be reprocessed constantly without a related registration cost. NAT with hiding policy of a single network device can uses to provide network access for nodes within a private network space. NAT is only efficient capable of hiding network devices, not securing them so that we have to consider the first step to securing our network such as to install a firewall at the boundary or border of the network infrastructure.. If display equations do not fit in the two-column format, they will also be reformatted. Authors are strongly encouraged to ensure that equations fit in the given column width.

ACKNOWLEDGMENT

The authors would like to thank SEGi University Management, Dr Chia Chee Ming, Dean, Faculty of Engineering, Built Environment & Information Technology, (FOEBEIT), SEGi University, Dr Chan Mieow Kee, Deputy Dean of Research & Post Graduate Programs, Faculty of Engineering, Built

Environment & Information Technology, (FOEBEIT), SEGi University, Mr Seow Soon Loong, Deputy Head & Program Leader for Information Technology Programs and Dr Mahadevan Supramaniam, Director, Research Innovation & Management Centre (RIMC), SEGi University.

REFERENCES

[1] R P. Srisuresh, K.Egevang, “Traditional IP Network Address Translator (Traditional NAT)”, RFC 3022: January 2001. (Obsoletes RFC1631).
[2] Y. Rekhter, B. Moskowitz, D.Karrenberg, G. J. de Groot, E. Lear, RFC 1918: “Address Allocation for Private Internets”, RFC 1918: February 1996. (Obsoletes RFC1627, RFC1597).
[3] Y. Rekhter, C. Topolcic, “Exchanging Routing Information Across Provider Boundaries in the CIDR Environment”, RFC 1520:
[4] Cisco Press, White Paper, “Cisco IOS Network Address Translation”, Cisco Systems 1992–2004, pp. 1-11.
[5] Sean Wilkins, “Basic NAT Concepts and Configuration”, Cisco Press, Article is provided courtesy of Cisco Press. Date: Jul 6, 2011.
[6] Lixia Zhang, “A Retrospective View of NAT”, IETF Journal, Date: October 7, 2007.
[7] Allan Johnson, “Network Address translation for IPv4”, Cisco Press, CCENT Practice and Study Guide, Chapter 22, Cisco Press, 17 Dec 2013.
[8] Anchit Bansal, Priyanka Goel, Anchit Bansal, “Simulation and Analysis of Network Address Translation (NAT) & Port Address Translation (PAT) Techniques.”, Int. Journal of Engineering Research and Application www.ijera.com, ISSN : 2248-9622, Vol. 7, Issue 7, (Part -2) July 2017, pp.50-56
[9] Cisco Press, “IP Addressing: NAT Configuration Guide, Chapter: Configuring NAT for IP Address Conservation”, Cisco Press, IP Addressing: NAT Configuration Guide, Cisco IOS Release 15M&T, Updated 20 December 2019.
[10] Cisco Press, “IP Addressing: NAT Configuration Guide, Cisco IOS Release 15M&T, Chapter: Configuring NAT for IP Address Conservation”, Updated: November 11, 2019.
[11] Kailasam Selvaraj, Kartheeban Kamatchi, Vishalraj A V K, Pandikishore R, Ram Guru Chandar M, “Design and Development of Virtual Local Area Network and Securing Network using Network Address Translation”, International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-8 Issue-4S2, December 2019
[12] Younchan Jung, Ronnel Agulto, “Integrated Management of Network Address Translation, Mobility and Security on the Blockchain Control Plane”, Sensors (Basel)., 2020 Jan; 20(1): 69. Published online 2019 Dec 21. doi: 10.3390/s20010069, PMCID: PMC6983003, PMID: 31877695.