International Journal of Scientific Research in Science, Engineering and Technology (www.ijsrset.com)
© 2020 IJSRSET | Volume 7 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
DOI : https://doi.org/10.32628/IJSRSET207385

Implementation of Network Address Translation Using TCP/IP Model In Internet Communication System

Ei Ei khaing, Mya Thet Khaing, Akari Myint Soe, Shwe Sin Myat Than
Faculty of Computer Systems and Technologies, UCS (Hpa-An), Hpa-An, Kayin, Myanmar

ABSTRACT

Nowadays, many people will be used internet that for their work, communication, education, economic and organization necessary that is used today. Network address translation (NAT) is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. A network is a system of hardware and software, put together for the purpose of communication and resource sharing. A network includes transmission hardware devise to interconnect transmission media and to control transmissions and software to decode and format data. The Internet protocol suite is the computer networking model and set of communications protocols used on the Internet and similar computer networks. Knowledge on how the internet is able to communicate with internet users is a mystery to some people. Internet communication need to be TCP/IP protocol which means that TCP is Transmission Control Protocol, or what is sometimes simply used to refer to Internet Protocol, is the basic unit for communication on the internet. This can also be applied to private internet, like Ethernet and so on. Despite TCP and IP being used interchangeably, there is a slight difference between the two in relation to the roles they play IP is directly responsible for obtaining internet addresses and then it is the work of TCP to deliver the data obtained to the addresses achieved by IP. TCP/IP provides end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed and received at the destination. This paper aim is described operation and models of TCP-IP suite in data communication network.

Keywords : TCP/IP, Protocol, NAT, Internet.

I. INTRODUCTION

Before the introduction of TCP/IP, it used to be difficult to connect different computers. A computer user was not even able to pass data or applications without the ‘Sneaker Net’. TCP/IP came into existence at a time when ISO had passed certain specific guidelines for building that seven major parts be considered, which included application, session, network, presentation, physical, transport and data link. TCP would in the communication layers ensure safe delivery of applications that a packet arrives in a certain order. The development and growth of the internet required specific protocols for internet communication. Two protocols – Internet Protocol (IP) and Transmission Control Protocol (TCP) – were developed as a result. Known collectively as the TCP/IP suite, each protocol is responsible for different aspects of communication: TCP/IP is a two-layer program. The upper layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination [1]. TCP/IP uses the client/server model of communication in which a computer user requests and is provided a service by another computer in the network.

TCP/IP communication is primarily point-to-point, meaning each communication is from one point in the network to another point or host computer. TCP/IP and the higher-level applications that use it are collectively said to be "stateless". DARPA started work on a number of other data transmission technologies. In 1972, Robert E. Kahn joined the DARPA Information Processing Technology Office, where he worked on both satellite packet networks and ground-based radio packet networks, and recognized the value of being able to communicate across both. In the spring of 1973, Vinton Cerf, the developer of the existing ARPANET Network Control Program (NCP) protocol, joined Kahn to work on open-architecture interconnection models with the goal of designing the next protocol generation for the ARPANET [3]. By the summer of 1973, Kahn and Cerf had worked out a fundamental reformulation, in which the differences between network protocols were hidden by using a common internetwork protocol, and, instead of the network being responsible for reliability, as in the ARPANET, the hosts became responsible. A router is provided with an interface to each network. It forwards packets back and forth between them. Originally a router was called gateway, but the term was changed to avoid confusion with other types of gateways.

II. LAYERING MODEL OF TCP/IP

TCP/IP is mature and stable, and is the only protocol stack used on the Internet. This paper is about networking with TCP/IP. This takes a closer look at it's the layers, to how the layers work in the following explain and then show the following Table 1and Figure 1.

- **Application Layer:** Concerned with differences in internal representation, user interfaces, and anything else that the user requires. This layers is higher level protocols, such as SMTP, FTP, SSH, HTTP, operate.
- **Transport Layer:** Concerned with process-to-process delivery of information. This layer information is called segment. eg: TCP, UDP.
- **Network Layer:** Delivers data in the form of a packet from source to destination, across as many links as necessary, to non-adjacent systems. The primary protocol in this scope is the Internet Protocol, which defines IP addresses. Its function in routing is to transport datagrams to the next IP router that has the connectivity to a network closer to the final data destination.
- **Data Link Layer:** Organizes the bit stream into a data unit called a "frame" and delivers the frame to an adjacent system [6].
- **Physical Layer:** Contains all the functions needed to carry the bit stream over a physical medium to another system.

Table 1. TCP/IP 5-Layer Reference Model

	Name of Layers	**Purpose of Layers**
Layer5	Application	Specifies how a particular application uses a network.
Layer4	Transport	Specifies how to ensure reliable transport of data.
Layer3	Internet	Specifies packet format and routing.
Layer2	Network	Specifies frame organization and transmittal.
Layer1	Physical	Specifies the basic network hardware.

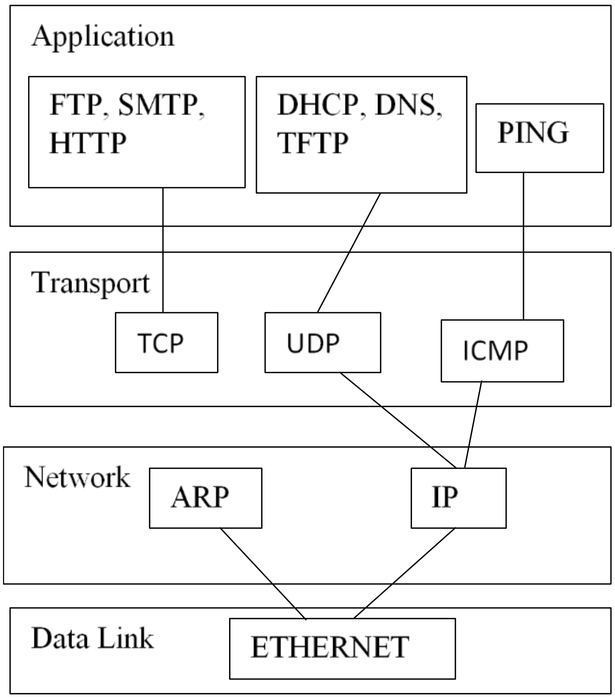

Figure 1. TCP/IP Protocol Flow

III. TCP/IP PROTOCOL STACK

TCP/IP is the protocol suite upon which all Internet communication is based. Different vendors have developed other networking protocols, but even most network operating systems with their own protocols, such as Netware, support TCP/IP. It has become the de facto standard. Protocols are sometimes referred to as protocol stacks or protocol suites. A protocol stack is an appropriate term because it indicates the layered approach used to design the networking software for each host or router in the internet must run a protocol stack. The details of the underlying physical connections are hidden by the software. The sending software at each layer communicates with the corresponding layer at the receiving side through information stored in headers. Each layer adds its header to the front of the message from the next higher layer. The header is removed by the corresponding layer on the receiving side. TCP/IP protocol stack is illustrated in the following Figure 2:

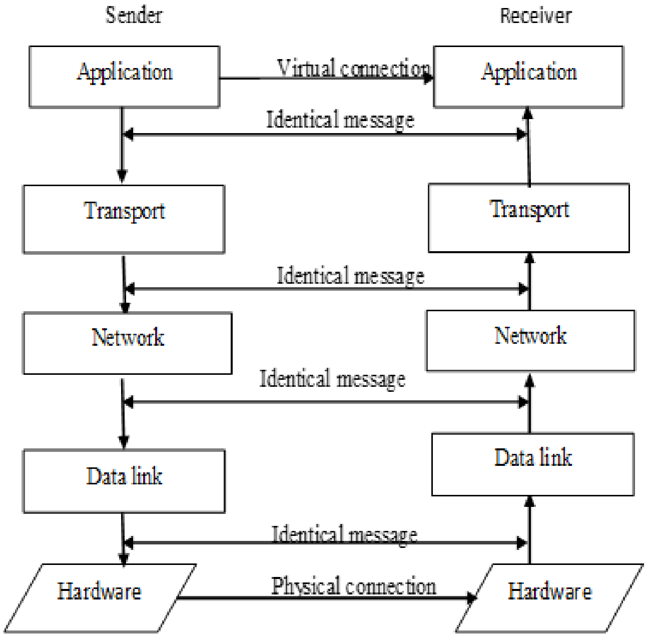

Figure 2. Flow of data between two computers using TCP/IP stacks.

A. Network Devices

Network devices are repeaters, bridges, switches and routers.in this paper, router devise are used in the system. These are all dedicated hardware devices. Network devices can also be non-dedicated systems running network software.

1) Routers

A router is a hardware device that connects two or more networks. Routers are the primary backbone device of the Internet, connecting different network technologies into a seamless whole. Each router is assigned two or more IP addresses because each IP address contains a prefix that specifies a physical network.

Before a packet is passed to the routing software, it is examined. If it is corrupted, it is discarded. If it is not corrupted, a routing table is consulted to determine where to send it next. By default, routers do not propagate broadcast packets[4]. A router can be configured to pass certain types of broadcasts.

B. Data Encapsulation

Each layer uses encapsulation to add the information its peer needs on the receiving system. The network layer adds a header to the information it receives from the transport at the sender and passes the whole unit down to the data link layer. At the receiver, the network layer looks at the control information, usually in a header, in the data it receives from the data link layer and passes the remainder up to the transport layer for further processing. This is called encapsulation because one layer has no idea what the structure or meaning of the PDU [9] is at other layers. The PDU has several more or less official names for the structure at each layer. The exception to this general rule is the data link layer, which adds both a header and a trailer to the data it receives from the network layer. T is trailer and H is header, the general flow of encapsulation in TCP/IP is shown in Figure 3.

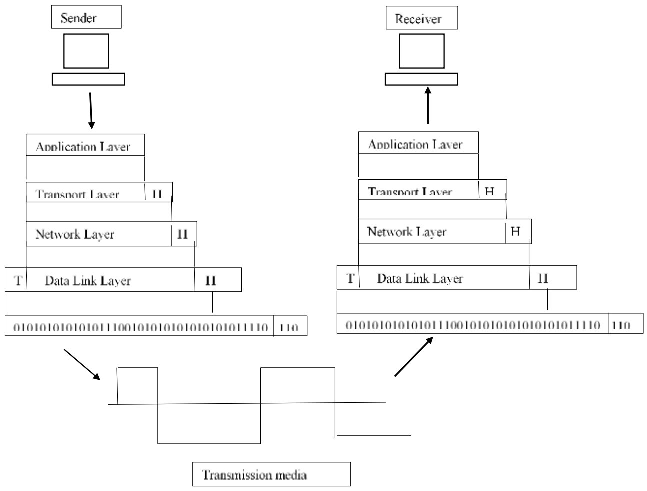

Figure 3. TCP/IP encapsulation and headers

2) TCP/IP Communication

If we want to view a webpage on the internet, the TCP/IP suite handles the communication between our device and the webpage's webserver:

- Our browser uses the Hyper Text Transfer Protocol (HTTP) to send a request to the Application Layer.
- The Application Layer protocol (HTTP) sends the request to the Transmission Control Protocol (TCP) in the Transport Layer. The TCP communicates with the Internet Layer to establish a connection with the webserver across the network(s).
- The Internet Protocol in the Internet Layer establishes the address of the webserver and converts the request into packets. The packets are sent to the Network Layer.
- The Network Layer uses its protocols to send the packets over the internet to the webserver.
- At the webserver the process is reversed. The packets are sent up through the protocols in the layers, and re-assembled into the request. The request is passed through the Application Layer protocols for the webserver to service.
- In the same manner the webserver uses the protocols in the layers to send the webpage data back to our device.

C. Advantages of TCP/IP

Here, are benefits of using the TCP/IP model in the following.

- It helps you to establish a connection between different types of computers.
- It operates independently of the operating system.
- It support many routing- protocol.
- It enables the internetworking between the organizations.
- It has a highly scalable client-server architecture.

D. Disadvantages of TCP/IP

Here, are few drawbacks of using the TCP/IP model in the following.

- It is a complicated model to set up and manage.
- The overhead of it is higher- than internetwork packet exchange (IPX).
- In this model the transport layer does not guarantee delivery of packets.
- Replacing protocol in it is not easy.
- It has no clear separation from its services, interfaces and protocols.

E. Difference between TCP / IP

TCP is a connection-oriented transport service; it provides end-to-end reliability, sequencing, and flow control. TCP enables two hosts to establish a connection and exchange streams of data, which are treated in bytes. The delivery of data in the proper order is guaranteed. TCP can detect errors or lost data and can trigger retransmission until the data is received, complete and without errors.

IP provides communication between hosts on different kinds of networks. It is a connectionless, unreliable packet delivery service. Connectionless means that there is no handshaking, each packet is independent of any other packet. It is unreliable because there is no guarantee that a packet gets delivered; higher-level protocols must deal with that.

IV. IMPLEMENTATION OF NAT

TCP/IP protocols with the operating system. Nevertheless, TCP/IP protocols are available for all widely-used operating systems today and native TCP/IP support is provided in OS/2, OS/400, all Windows versions since Windows 9x, and all Linux and UNIX variants [8]. When the user accesses a Web site on the Internet, the NAT server will translate the "private" IP address of the host (192.168.50.50) into a "public" IP address (220.16.16.5) from the pool of assigned addresses. NAT works because of the assumption that, in this system, no more than 27 of the 64 hosts will ever be accessing the Internet at a single time. A pool of IP addresses can be shared by multiple hosts using a mechanism called Network Address Translation (NAT) that private addresses; since these addresses are never seen on the Internet, this is not a problem. Consider the scenario shown in Figure 4.

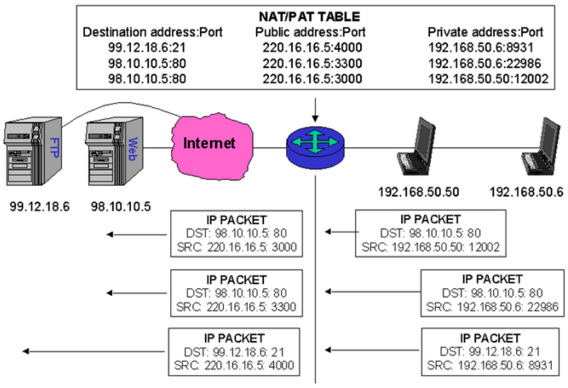

Figure 4. Configuration of NAT

Port numbers are used by higher layer protocols (e.g., TCP and UDP) to identify a higher layer application. A TCP connection, is uniquely identified on the Internet by the four values <source IP address, source port, destination IP address, destination port>. The server's port number is defined by the standards while client port numbers can be any number greater than 1023. The scenario in Figure 4 shows the following three connections:

- The client with the "private" IP address 192.168.50.50 (using port number 12002) connects to a Web server at address 98.10.10.5 (port 80).
- The client with the "private" IP address 192.168.50.6 (using port number 22986) connects to the same Web server at address 98.10.10.5 (port 80).
- The client with the "private" IP address 192.168.50.6 (using port number 8931) connects to an FTP server at address 99.12.18.6 (port 21).

PAT works in this scenario as follows. The router (running PAT software) can assign both local hosts with the same "public" IP address (220.16.16.5) and differentiate between the three packet flows by the source port. A final note about NAT and PAT. Both of these solutions work and work fine, but they require that every packet be buffered, disassembled, provided with a new IP address, a new checksum calculated, and the packet reassembled. In addition, PAT requires that a new port number be placed in the higher layer protocol data unit and new checksum calculated at the protocol layer above IP, too. The point is that NAT, and particularly PAT, results in a tremendous performance hit. One advantage of NAT is that it makes IP address renumbering a thing of the past. If a customer has an IP NET_ID assigned from its ISP's CIDR block and then they change ISPs, they will get a new NET_ID. With NAT, only the servers need to be renumbered.

V. CONCLUSIONS

In this paper, the functionality of network applications is directly related to the performance of TCP/IP. The IP is directly responsible for obtaining internet addresses and then it is the work of TCP to deliver the data obtained to the addresses obtained by IP. When this address is delivered again and again, a chain of communication is created. For data network applications to obtain data from the various websites, the two (TCP/IP) are required. Otherwise, the functionality of applications would be nearly impossible. Even though the TCP has a challenge of slow starting, when it picks the information, it is passed to the required place at a relatively high speed. One good thing about TCP is that it is very efficient compared to its competitors. It only requires that hardware and a software layer exists that is capable of sending and receiving packets on a computer network.

VI. ACKNOWLEDGMENT

I would like to express my deepest gratitude and sincere appreciation to all persons who have contributed directly towards the completion of this paper and helped make this dissertation possible.

VII. REFERENCES

[1]. S. Zaman S., F. Karray. Fuzzy ESVDF approach for Intrusion Detection System. The IEEE 23rd International Conference on Advanced Information Networking and Applications (AINA-09). May 26-29, 2009.

[2]. I. Onut and A. Ghorbani. A Feature Classification Scheme for Network Intrusion Detection. International Journal of Network Security, Page(s): 1-15, July 2007. 3A. Tamilarasan, S. Mukkamala, A. Sung, and K. Yendrapalli. Feature Ranking and Selection for Intrusion Detection Using Artificial Neural Networks and Statistical Methods. 2006 International Joint Conference on Neural Networks (IJCNN'06), Page(s):4754-4761, July 16-21, 2006.

[3]. A. Sung, S. Mukkamala. Identifying Important Features for Intrusion Detection Using Support Vector Machines and Neural Networks. Symposium on Application and Internet (SAINT'03), Page(s): 209-216, 27-31 Jan. 2003.

[4]. V. Golovko, L. Vaitsekhovich, P. Kochurko and U. Rubanau. Dimensionality Reduction and Attack Recognition using Neural Network Approaches. International Joint Conference on Neural Networks, 2007, Page(s): 2734-2739, 12-17 Aug. 2007.

[5]. S. Srinoy. Intrusion Detection Model Based On Particle Swarm Optimization and Support Vector Machine. The 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2007), Page(s): 186-192, 1-5 April 2007.

[6]. H. Gao, H. Yang, X. Wang. Ant Colony Optimization Based Network Intrusion Feature Selection and Detection. The Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, Page(s): 18-21, August 2005.

[7]. Kh. Shazzad, J. Sou Park. Optimization of Intrusion Detection through Fast Hybrid Feature

Selection. The Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005, (PDCAT'05), Page(s): 264 - 267, 05-08 Dec, 2005.

[8]. M. Yasin, and A. Awan. A Study of Host-Based IDS using System Calls. INCC 204, International Conference on Networking and communication 2004.

Cite this article as :

Ei Ei khaing, Mya Thet Khaing, Akari Myint Soe, Shwe Sin Myat Than, "Implementation of Network Address Translation Using TCP/IP Model In Internet Communication System", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 3, pp. 447-453, May-June 2020. Available at

doi : https://doi.org/10.32628/IJSRSET207385

Journal URL : http://ijsrset.com/IJSRSET207385