Abstract: A large number of almost all protocols merge fixes the host university relations assume, have been improved. However, in reality, this assumption no network address translators (NAT) and Firewall widely used and is valid. Especially in an environment of extreme points Edam, network firewall, NAT and extensive connections limit the impact on the multicast. In this article, Endpoints make up a large fraction because it is argued that they consider critical limits that affect the proper functioning and performance fixes to merge protocol NAT and firewall host. Basic network address translation or NAT the basic system is, IP addresses of the transparent, and another group from the map is available Users. One of method is Network Address Port Translation, or NAPT, many network addresses and their TCP / UDP (Transmission Control Protocol / User Datagram Protocol) is a single port translation Network address and TCP / UDP port. Together, providing two operations, referred to as traditional NAT, provide a mechanism the kingdom with the extra-curricular with private addresses its own unique address registered. Smartphones and other mobile devices to speed up who has addresses in mobile Internet access IPv4. IPv6 is widely seen critical for internet continues to grow and maintain, and especially, it is very important to mobile networks this document in Mobile, IPv6 deployed on the question raised by the Internet. This can be useful to refer the document served Providers and network designers.

Key words - Overlapping, Firewall, NAT

1. Introduction

Network Address Translation(NAT) is a other mechanism anywhere a device performs changes to the TCP/IP address/port number of a packet and charts the IP address from one dominion to another (frequently private IP address to public IP address and other way around). This is the Internet towards internal hosts from outgoing packets forward to this mapping, maintenance and the public Internet from inbound packet forwarding on the NAT common side temporary port number from the NAT device by working port internally for hosting some straight time by.NAT device multiple hosts public / allow users to share Internet address is established primarily to alleviate the shortage of IPv4 address space. Mapping and its character (the internal host only be mapped to

The transmission can be created), NAT device on the Internet from internal threats against the host protection/ shield of some sort to provide (for example, when only one of the home care), even when not prefer to install the IPv4 address exhaustion issue.

The need for translating the internal network IP address IP addresses of the network cannot be used for privacy outside They network invalid reason or for use outside. There are many ways out of range of local network topology can be changed. Customers may change providers, the company can be reorganized backbones, or providers may combine or fragmented. At any time external topology can changes be applied in the local domain and the time for, to address the change to reflect the external change. This type of change Changes can be hidden from users within the domain of the central Single address translation router. The dramatic growth of mobile Internet is accelerating Lack of IPv4 addresses available. It is widely accepted the continued need for maintenance and development of IPv6 Mobile internet in general and especially the Internet. While IPv6 brings many benefits, some specific challenges arise when Mobile telephone network is deployed. This document describes such Current challenges and, IPv6 and shows recommendations Deployment solutions. Therefore, it may be useful to refer document Service providers as well as for network designers. This document any new build relationship does not propose or suggest a new
carrier Specification work. In the next section two it illustrate about the background basic about the research papers and current research papers which are done.

2. Background and Related Works

NAT (Network Address Translation) is a tool where a device execute refinement to the TCP/IP, address, port number of a packet and charts the IP address from one domain to another generally from private IP address to public IP address and conversely. NAT cannot be a firewall solution since a firewall is a security solution anywhere it will protect from illegal access with a firewall. When interconnection of two inside and outside network starts there will be occurring three major problems such as overlapping between file transformations, restrictions while accessing to different networks. There are some researches which are done to prevent these issues in a private and public networks. Network Management with Overlapping IP Address Ranges by Scott Kirkwood. In this research it talks about the basic experience with network devices for an example configurations in NFS (Network File System), DNS (Domain Name System) or NIS (Notion Internet Security) all are common configurations but the network infrastructure does not regularly require more than an Ethernet cable, an IP address and an entry in the DNS server for each new Unix system. This article will be explain about the network infrastructure configuration that can make difference between a dead project and a functional architecture.

The scenario of this article contains about the service providers which always has been necessary in any enterprise WAN, proffering the telecommunications circuits and WAN bandwidth that needed to be operate in a business network. Because of the advance statements in transmission technology the competition in the telecom zone has been increased causing with having results in gluts of bandwidth available to enterprise clients for ever-decreasing costs. The enterprise network for additional services to sell has been looked deeper by the service providers and network management is the main target. The enterprise clients get benefits by reducing its need for expensive WAN savvy employees and it gives a peaceful mind that the service provider has cutting-edge NMS system monitoring its WAN twenty-four-hours. Its sounds simple until a UNIX administrator tries to apply the NMS. These case studies summarize the risks that are deep-rooted in such a system design and the network solutions that can make it all work the way the marketing advertise.

The problem of handling hundreds of individual and separate networks from a single NMS point becomes visible to be one of scale and security. The ostensibly issue seems to be having a system with enough power to monitor hundreds of thousands of network in real time. The solution for the problem requires a combination of complicated routing techniques within the network infrastructure, together with a corresponding configuration in the UNIX system. The solution is possible due mainly to the multi-tiered architecture of the NMS software deployed. Now a day’s most NMS software allows for a multi-tiered installation with multiple SNMP collection systems forwarding information to a central correlation and display engine.

Traditional IP Network Address Translator (Traditional NAT) by P. Srisuresh, K. EgevangBasic network address translation, or NAT the basic system is, IP addresses of the transparent, and another group from the map are available Users. Network Address Port Translation, or NAPT is a method by many network addresses and their TCP / UDP (Transmission Control Protocol / User Datagram Protocol) is a single port translation Network address and TCP / UDP port. Together, these two Operation, referred to as traditional NAT, provide a mechanism the kingdom with the extra-curricular with private addresses its own unique registered addresses.

Network Address Translation (NAT) Behavioral Requirements for Unicast UDP by F. Audit, Ed., C. Jennings. Glossary defines the basic information for changing the document Network type’s worn translation (NAT) service behavior Unicast, UDP, and defines a series of requirements that may many applications, such as multimedia communications or online Gaming, to work consistently. Development of NATs that meet this set Needs much this will increase the likelihood of Applications will be in place.

Overcoming NAT and Firewall Connectivity Restrictions in Overlay Multicast by Aditya GANJAM and Hoi ZHANG. Merge protocols fixes a lot of people Development, all of the University Relations assumption shall be final. However, in reality, this assumption is not valid Network Address Translator (NAT) and Firewall widely used. NAT and firewall connections limit the impact on the merge Multicast, especially in sedum-endpoint environment, and not serious consideration. In this paper, Research group argue that it is not decisive Consider limited because the NAT firewall and host connections Endpoints that make up a large fraction affects the proper Activity and fixes to merge conveyor performance. The
research group clearly consider offers several improved designs Multicast and evaluate the design limits merge True Internet broadcasts and Internet -based and space tradeoffs tested testing.

Security on Voice over Internet Protocol from Spoofing attacks by Sanjay Kumar Sonkar, Rahul Singh, Ritu Chauhan, and Ajay Pal Singh. To transmit voice conversations over a data network using IP, VoIP technology is used. Such data network may be the Internet or a corporate Intranet or managed networks which are specially used by long distance and local service traditional providers and ISPs (Internet Service Provider). Voice over Internet Protocol (VoIP) is a form of communication that allows end-user to make phone calls over a broadband internet connection. Basic VoIP access usually allows you to call others who are also receiving calls over the internet. Interconnected VoIP services also allow you to make and receive calls to and from traditional landline numbers, usually for a service fee. A special type of adapter is used in some VoIP services which required a computer and a dedicated VoIP telephone. Other services allow to end-users to use own landline phone, it is used to replace VoIP calls. All these paradigms are held by a special adapter.

Voice over Internet Protocol by Rahul Singh, Ritu Chauhan. The technology used to transmit voice conversations over a data network using IP. Such data network may be the Internet or a corporate Intranet, or managed networks typically used by long distance and local service traditional providers and ISPs (Internet Service Provider) that use VoIP. Voice over Internet Protocol (VoIP) is a form of communication that allows you to make phone calls over a broadband internet connection. Basic VoIP access usually allows you to call others who are also receiving calls over the internet. Interconnected VoIP services also allow you to make and receive calls to and from traditional landline numbers, usually for a service fee. Some VoIP services require a computer or a dedicated VoIP phone, while others allow you to use your landline phone to place VoIP calls through a special adapter.

A Comprehensive Survey of Voice over IP Security Research by Angelos D. Keromytis, Senior Member, IEEE. VoIP refers to a class of products that enable advanced communication services over data networks. While voice is a key aspect in such products, video and other capabilities (e.g., collaborative editing and whiteboard sharing, file sharing, calendaring) are supported. The key advantages of VoIP are flexibility and low cost. The former derives from the (generally) open architectures and software-based implementation, while the latter is due to new business models, equipment and network-link consolidation, and ubiquitous consumer-grade broadband connectivity. Due to these benefits, VoIP has seen rapid uptake in both the enterprise and consumer markets. An increasing number of enterprises are replacing their internal phone switches with VoIP based implementations, both to introduce new features and to eliminate redundant equipment. Consumers have embraced a slew of technologies with different features and costs, including P2P calling (Skype), Internet-to-PSTN network bridging, and wireless VoIP. These new technologies and business models are being promoted by a new generation of startup.

H.323 was designed with a good understanding of the requirements for multimedia communication over IP networks, including audio, video, and data conferencing. It defines an entire, unified system for performing these functions, leveraging the strengths of the IETF and ITU-T protocols.

SIP was designed to setup a "session" between two points and to be a modular, flexible component of the Internet architecture. It has a loose concept of a call (that being a "session" with media streams), has no support for multimedia conferencing, and the integration of sometimes disparate standards is largely left up to each vendor.

Media Gateway Control Protocols (MGCP) The communication between the separate components of a decomposed VoIP gateway is done by media gateway control protocol. It is a complementary protocol to SIP and H.323. “Call agent” is mandatory and manages calls and conferences, when the research group are using MGCP and MGC server (Figure 6). The MG endpoint is not responsible for calls and conferences. It does not maintain call states. MGs are responsible to execute commands sent by the MGC call agents. MGCP assumes that call agents will synchronize with each other sending coherent commands to MGs under.

Advantages:
- Widely adopted and deployed initially;
- Designed from the outset with multimedia communications over IP in mind;
- Provides a more precise and detailed specification of voice and multimedia functionality;
Perfect solution for real-time multimedia communication over packet-based networks;
- Umbrella protocol with a lot of protocols inside;
- Straightforward interworking with the PSTN.

Disadvantages:
- NAT and firewall restrictions;
- Hierarchical structure based on the old PSTN world;
- ASN.1 syntax for coding H.323 messages is more complex;
- Range of applications because of its restricted scope.

In the next section three it illustrate about the solutions which are given to the current problems by the research group.

3. Approach

To solve, the above-discussed problem the research group came up with the solution. Our main problem is Network Address. The main disadvantage of overlapping IP address is the outside user cannot identify the specific host which it going to communicate with. In this research paper describes how users overcome this problem in future with this researched solution. As an example NAT (Network address translation) is act as like a receptionist in a large group of company and she got all the instructions about company just like that NAT (Network address translation) is instructed when it comes from outside communications where it must be direct to. Using this research the network users can overcome disadvantages of overlapping then there work will be easier than now. The users cannot got panic about how am I going to communicate with this kind of IP address and the network engineer also can use this scenario to overcome their problem in overlapping. Translation (NAT), the research group can use for this solution.

1. SIMPLE TRAVEL OF USER DATAGRAM PROTOCOL (STUN)

When the research group considering to simple travel of user datagram protocol (STUN) its light weight protocol. This protocol allows to application discover types of NAT and firewall between and the public network. This STUN is use as a client server protocol then which server must be in public network side of Network address translation and it has a two global IP addresses. But client maybe behind the NAT. After that client try to send UDP message into the server.

Then server contains it IP address but port in the payload. After that server read the message and send back reply to client with IP address and port that already used in the header. The Figure 1 illustrate, how this SIP using STUN for NAT traversal, for more details please check [5]. Client is usually fixed in an application that need to obtain a public IP address and port to receive data and check and get IP address from STUN server. After that If the IP address is the same that it has then there is no NAT in the path between the client and STUN server. Then If IP address is different than the client starts to send another messages to the STUN server in order to learn the NAT behavior and type. After this detection process the application can use the public IP address and port that the other end should send the data to them [5].

![Figure 1: SIMPLE TRAVEL OF USER DATAGRAM PROTOCOL Operation][1]

The research group can considering about advantages such as its ease and compatibility with many types on NATs. Therefore it have many disadvantages, the most serious disadvantage is not actuality able to work with symmetric NATs which are characteristically found in business networks. Because STUN client establish totally free connection with STUN server then it will work only with cone NATS which use the same mapping for all traffic. To result in this problem a new protocol has been developed which is Traversal Using Relay NAT (TURN). STUN can also hurts from another major drawback which is the lack of help to TCP based connections and applications. But there is an extension to STUN that support TCP which is Smart Tunnel Union for NAT Traversal (STUNTS).

2. CORPERATIVE ON DEMAND OPENNING (CODO)

Let’s considering other solution for our research its name Corporative On-Demand Opening. It works with a middleware NAT/Firewall traversal system that dynamically configures NATs/Firewalls and
open holes in them so the authorized application can communicate. But CODO only allows to open authorized applications narrow holes in Firewalls when it’s needed. But the application do not need to the hole it can be closed.

CODO uses wide support between firewalls and application. That CODO enabled firewall will have a firewall agent (FA) that will communicate with client libraries (CLs). [6]

In CODO, there is no need to add fixed rules to allow application to traverse the Firewall from the time when the FA functionality which embedded with the Firewall adds and deletes the rules dynamically. FA also keeps a list of applications that can cross the Firewall and do not allow any other application cross it.

The Figure 2 illustrates, when an approved application need to open a dump in the firewall, the CL establish a secure TCP connection to the FA and informs FA of application’s need to open a assured hole, FA then modify the rules to allow such an activity. CL also informs FA with the status of the connection and when the connection is closed be the application FA modifies the rules to close the hole. CODO also address NAT traversal using similar methodology, CL make a TCP connection to FA which standby a public IP address to be used. Then client FA will ask from the server FA to allow the connection for that IP address. [6] Then the research group can see CODO can work with the most limited Firewalls and NATS and it allow only narrow and short Firewall openings. In addition to that CODO controls both arriving and outbound traffic. Another important advantage of CODO is its application approval capability which makes it very suitable for high secure systems. Whatever, CODO is not recessive compatible and it is needed to update the existing NATs and Firewalls to enable CODO to work. But, at application level only CL libraries are needed with a possibility of re-linking. [6]

4. Conclusion

System and method have been provided to support the local gateway for remote multiple overlapping networks. A plurality of overlapping connections, remote network from the IP address of a packet is including cargo each source from the local gate. For each connection, the source IP address of a bind table internal address from internal source systems across the unique source IP address is bound. A plurality of packets from the overlapping relationships will be implemented through the table to determine the destination IP address and bind to the right. IPv4 address exhaustion and its implications to mobile networks:

Mobile Phone Services conservation of its providers, begin to deploy IPv6 Internet available IPv4 address pool network implies Translate in mobile networks. At the same time, providers can use create 3GPP architecture such as APN and PDN Without affecting the leading. IPv6 introduces relations IPv4 Internet access. The IETF dual stack may be the model easily applied mobile networks.

Fixed-Mobile Convergence: Illustrations discussed Fixed and mobile network requirements change. Can be through many purposes such Access network, the primary network provider, it may sometimes for more networks into a form fit. Like cheap Convergence of services and application layers have space.

5. Future Work

The main disadvantage of overlapping IP address is the outside user cannot identify the specific host which it going to communicate with. In this research paper describes how users overcome this problem in future with this researched solution. As an example NAT (Network address translation) is act as like a receptionist in a large group of company and she got all the instructions about company just like that NAT (Network address translation) is instructed when it comes from outside communications where it must be direct to. Using this research the network users can overcome disadvantages of overlapping then there work will be easier than now. The users cannot got panic about how am I going to communicate with this kind of IP address and the network engineer also can use this scenario to overcome their problem in overlapping.
6. Acknowledgement

This research was supported by Sri Lanka Institute Of Information Technology Computing (Pvt) Ltd and lecturer Mr. Dhishan Dhammearatchi. The research group thank our colleagues from B.K. Dullewa, N.A.C. Senaviratna, K.H.H. Thenuka, G.A.L. Madushanka, B.W.P. Madushanka who provided insight and expertise that greatly assisted the research.

The research group would also like to show our gratitude to the Mr. Dhishan Dhammearatchi for sharing their pearls of wisdom with us during the course of this research, the group members are also immensely grateful to Mr. Dhishan Dhammearatchi for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons.

7. References


