Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación

TRABAJO FIN DE MÁSTER

ANALISIS DE TÉCNICAS PARA ATRAVESAR NAT/FIREWALLS EN UNA RED EXTREMO - EXTREMO

Gabriela Alexandra Coppiano Marin

2011

Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación

Máster Universitario en
Ingeniería de Redes y Servicios Telemáticos

TRABAJO FIN DE MÁSTER

ANALISIS DE TÉCNICAS PARA ATRAVESAR NAT/FIREWALLS EN UNA RED EXTREMO - EXTREMO

Autor
Gabriela Alexandra Coppiano Marin

Director
Enrique Vázquez

Departamento de Ingeniería de Sistemas Telemáticos

2011

Resumen

Con el paso del tiempo la implementación de tecnologías se ha vuelto un recurso óptimo y necesario para llevar a cabo la distribución, implementación y en especial la comunicación en un entorno de trabajo cada vez más globalizado y competitivo. Esta última situación ha producido también el mal uso de la misma, por lo que muchas empresas han visto la necesidad de obstaculizar ciertos accesos a su información, haciendo que sus redes sean solo de uso exclusivo interno, requiriendo que una mínima cantidad de terminales tengan acceso a redes externas. Además, el rápido agotamiento de las direcciones IP públicas hace que adquirirla sea costoso, razón por la cual, las redes privadas usan un direccionamiento basado en direcciones IP reservadas que son inválidas para su uso fuera de la red interna

Las empresas pueden tener acceso a redes externas o a Internet, cuando exista una traducción de direcciones que permita que con una sola conexión acceda a la red de redes y unas cuantas direcciones IP válidas, de esta manera implementar el uso de Firewalls y NAT puede tener un buen control de seguridad de la red y sobre el tipo de información intercambiada con redes externas.

Los NAT constituyen sistemas para bloquear el acceso no autorizado con el objetivo de controlar todas las comunicaciones que pasan de una Red a otra, cuya funcionalidad se basa en un cliente y en un servidor. Sin embargo, no siempre se tiene la simplicidad de permitir la comunicación, por lo que es necesario en ciertas ocasiones desarrollar aplicaciones que descubran la presencia de estas barreras y/o cooperen con estas.

Los problemas no se producen por NAT, sino por estar detrás del NAT especialmente cuando hay varias aplicaciones para varios equipos, aplicaciones del mismo nivel e IPSec de NAT-T; aunque la mayoría de técnicas NAT eludan la política de la empresa, es necesario implementar estas técnicas para la cooperación en la obtención de información. Las soluciones que se proponen en este documento, están basadas en las soluciones especialmente para NAT Transversal y situaciones con cierta complejidad que suele presentarse en los clientes privados al acceder a Webs Públicas o Servidores Externos, es decir, en una situación de Internet de Extremo a Extremo, fragmentado en cuatro capítulos.

La presentación de este documento, se enfoca en el análisis y descripción de métodos y técnicas para atravesar NAT, aportaría a solventar la necesidad de elección de dichas tecnologías a la hora de incorporarlas; por ejemplo, el desarrollo de técnicas como STUN y TURN son necesarias para muchos NATs existentes en una Red para encontrar las direcciones públicas.

Este trabajo no presenta los costos de incorporación de cada tecnología descrita, tan solo representa un análisis investigativo de los métodos para atravesar NAT.

Abstract

The implementation of technologies has become an excellent and necessary resource to carry out the distribution, implementation and communication especially in a work environment globalize and competitive, the situation has also evil using it, so, many companies have seen the need to block access to certain information, making their networks are just internal use only, requiring a minimum number of terminals with access to external networks. Moreover, the fast depletion of public IP addresses makes it expensive to acquire; the solution could be privatize the networks based in routing using reserved IP addresses that are invalid for use outside the internal network. The Companies can access external networks or Internet, where there is an address translation that allows a single connection to access the Net and few valid IP addresses, thus implementing the use of Firewalls and NAT may have a good control of network security and the type of information exchanged with external networks.

NATs are systems to block unauthorized access in order to monitor all communications that pass from one network to another, whose functionality is based on a client and a server. However, it always has the simplicity to allow communication, so it is sometimes necessary to develop applications that discover the presence of these barriers or cooperate with them.

The problems are not caused by NAT, but, being behind the NAT especially when there are multiple applications for several teams, level applications and IPSec NAT-T, although the majority of NAT techniques circumvent the policy of the company, it is necessary to implement these techniques for cooperation in obtaining information.

The solutions proposed in this document are based on special solutions for NAT Traversal and situations with a certain complexity that often occurs in private clients to access public Websites or External Servers, in a situation of Internet End-to-End, edited into four chapters.

The presentation of this paper focuses on the analysis and description of methods and techniques to traverse NAT / Firewalls, would contribute to solving the need for choice of these technologies when to incorporate, for example, the development of techniques such as STUN and TURN are required for many existing NATs in a network to find the public addresses.

This work does not present the costs of incorporation of each technology, only it described a analysis of solutions NAT.

Índice General

Resumen ..... - 1 -

Abstract ..... - 2 -

Índice General ..... - 3 -

Índice de Figuras ..... - 6 -

Siglas ..... - 7 -

1. INTRODUCCIÓN ..... - 9 -

1.1 Contexto ..... - 9 -

1.2 Objetivos ..... - 10 -

1.2.1 Objetivo General ..... - 10 -

1.2.2 Objetivos Específicos ..... - 10 -

1.3 Estructura del Documento ..... - 11 -

2. RED EXTREMO – EXTREMO/INTERNET ..... - 13 -

2.1 Evolución de Internet ..... - 13 -

2.1.1 Historia ..... - 13 -

2.2 Funcionamiento de Internet ..... - 15 -

2.3 Servicios y Aplicaciones de Internet ..... - 16 -

2.4 Infraestructura de Internet ..... - 17 -

2.5 Topología actual del Internet ..... - 17 -

2.6 Direccionamiento ..... - 18 -

3. ANOMALIAS Y OBSTACULOS EN LA RED ..... - 19 -

3.1 FIREWALLS ..... - 19 -

3.1.1 Tipos de Firewalls ..... - 21 -

3.2 NAT – NETWORK ADDRESS TRANSLATION ..... - 22 -

3.2.1 Introducción ..... - 22 -

3.2.2 Objetivos ..... - 22 -

3.2.3 Justificación ..... - 23 -

3.2.4 Funcionamiento NAT ..... - 23 -

3.2.5 Simulación NAT ..... - 25 -

3.2.6 Clasificación de NAT ..... - 30 -

3.2.7 Tipos de NAT basados en la Traslación ..... - 31 -

3.2.8 Condiciones de NAT frente a la escases de Direcciones IPV4 ..... - 32 -

3.2.8.1 Traducción de Direcciones IPv4 – IPv6: Network Address Translation - Protocol Translation (NAT – PT) ..... - 34 -

3.2.8.2 Operaciones de Traducciones en NAT-PT: ..... - 36 -

4. PROBLEMAS Y SOLUCIONES NAT ..... - 40 -

4.1 NAT y la seguridad ..... - 40 -

4.2 Problemas del uso de un servidor tras un NAT ..... - 41 -

4.2.1 Aplicaciones para varios equipos ..... - 41 -

4.2.3 NAT-T (NAT Transversal) de IPSec ..... - 43 -

4.3 Técnica para solventar los problemas de NAT ..... - 45 -

4.3.1 STUN ..... - 45 -

4.3.2 TURN ..... - 47 -

4.3.3 UNIVERSAL PLUG AND PLAY - UPnP ..... - 48 -

4.3.4 INTERACTIVE CONNECTIVITY ESTABLISHMENT (ICE) ..... - 48 -

4.3.5 VIRTUAL INTRANET PLATFORM (VIP) ..... - 51 -

4.3.6 ADVANCE NAT TRANSVERSAL SERVICE – ANTS ..... - 51 -

4.3.7 MULTIPLE SUBSCRIBER VIDEOCONFERENCING SYSTEM ..... - 52 -

4.3.8 TRAVERSAL OF NON – PROTOCOL AWARE FIREWALLS AND NATS - 53 -

4.3.9 MASMCT - MULTI-AGENT SYSTEM FOR MULTIMEDIA COMMUNICATION TRAVERSING NAT AND FIREWALL ..... - 53 -

4.3.10 A NEW TUNNEL SCHEMME FOR MULTIMEDIA COMMUNICATIONS TRAVERSING NAT IN NGN ..... - 54 -

4.3.11 NAT FRIENDLY SIP ..... - 54 -
4.3.12 MIDCOM – UNAWARE NAT/FRIENDLY TRAVERSAL ..... - 54 -
4.3.13 APLICATION LEVEL GATEWAY – ALG ..... - 55 -
4.3.14 MIDDLEBOX COMMUNICATION (MIDCOM) ..... - 57 -
5. CONCLUSIONES Y OBSERVACIONES ..... - 59 -
5.1 Trabajos Futuros ..... - 60 -
6. ANEXOS ..... - 61 -
6.1 ANEXO1. ..... - 61 -
6.2 ANEXO 2. ..... - 62 -
7. BIBLIOGRAFIA ..... - 65 -

Índice de Figuras

Figura 1. Estructura de los Protocolos de Red 15

Figura 2. Infraestructura de Internet 17

Figura 3. Esquema Conceptual de un Firewall 19

Figura 4. Comunicación NAT 23

Figura 5. Esquema de la Comunicación..... 26

Figura 6. Simulación NAT R1/R2..... 29

Figura 7. Simulación NAT R2/R1..... 29

Figura 8. Estructura de los Protocolos de Red 33

Figura 9. Traducción de Protocolos..... 34

Figura 10. Aplicaciones del mismo nivel 42

Figura 11. NAT-T de IPSec 43

Figura 12. Diagrama TURN 47

Figura 13. Protocol Aware Firewall 56

Índice de Tablas

Tabla 1. Clase de Direcciones IP 18

Siglas

ARPA	Agencia de Proyectos de Investigación Avanzada.
ARPANET	Advanced Research Projects Agency Network.
BGP	Border Gateway Protocol
DNS	Domain Name Server
H.323	Recomendación del ITU-T
IGP	Internal Gateway Protocol
IRC	Internet Relay Chat
ISP	Session Initiation Protocol
NGN	Next Generation Network
NSFNET	National Science Foundation
NuFW	Filtrado basado en Netfilter
PPP	Point to Point Protocol
RIR	Regional Internet Registry
RTP	Real-Time Transport Protocol
SDP	Session Description Protocol
SIIT	Stateless IP/ICMP Translator
SLIP	Serial Line Internet Protocol.
Softswitch	Dispositivo de Next Generation Network

1. INTRODUCCIÓN

El usar una IP pública para toda una red privada imposibilita el uso de muchas aplicaciones en la Intranet como se ha estado mencionando continuadamente, dado que muchos protocolos son incapaces de atravesar NAT en tiempo real.

La idea fundamental es crear conexiones sin modificar configuraciones en los equipos de barrera como los Firewalls que contienen NAT y de no entrar en gastos de nuevas tecnologías que utilicen elementos intermedios. Por lo que es necesario estipular cuales y como se implementan, funcionan las técnicas que ayudan a solucionar estos obstáculos.

Este proyecto busca brindar un documento que contemple las soluciones para atravesar NAT, para lo cual previamente se debe dar una pequeña introducción de la trascendencia de Internet, un análisis del funcionamiento de NAT y sus aplicaciones, problemas que principalmente suceden al estar detrás de un NAT y la seguridad que conlleva esto.

1.1 Contexto

La evolución y transcendencia que ha tenido Internet o Web Pública en los últimos tiempos, ha impulsado a crear y ampliar su red como tal, desde el punto de vista de migrar de IPv4 a IPv6 como alternativa ante la escasez de direcciones. Además, el exorbitante aumento de direcciones ha conllevado al descontrol de las mismas, permitiendo el acceso y uso legal e ilegal; razón por la cual se han creado mecanismos y recursos que puedan brindar seguridad y estabilidad al usar Internet conocida como la Red Mundial.

Un gran método diseñado ha sido NAT o Traductor de Direcciones, que permite usar una sola IP Pública para toda una Red Privada, sin embargo, esto en la práctica imposibilita el uso de muchas aplicaciones, que quedan relegadas a su uso en la Red Interna o Intranet, dado que muchos protocolos son incapaces de atravesar los dispositivos NAT, especialmente utilizados en comunicaciones de extremo a extremo como voz y video (aplicaciones P2P). Estos dispositivos de red que ejecutan NAT aportan privacidad a la red al "esconder" las IP internas y posee una sola conexión a su red vecina.

NAT en su papel de privatizar las redes internas sigue conservando el esquema de direccionamiento y aumenta la flexibilidad de las conexiones de la Red Pública. No

obstante, también presenta pérdida en la funcionalidad con cualquier protocolo o aplicación, lo cual implica que el envío de información de dirección IP dentro del payload IP requiere que NAT tenga más funcionalidades.

Al buscar soluciones para atravesar NAT, existen muchas alternativas, por lo que este documento objeta la idea de crear una guía de mecanismos considerados hasta la actualidad, tales como STUN, TURN, ICE y otros que se mencionan en el desarrollo del trabajo escrito.

1.2 Objetivos

1.2.1 Objetivo General

Presentar el estudio y análisis de técnicas, aplicaciones y/o estándares para futuros trabajos relacionados con NAT, Firewalls o implementaciones en las Redes que presenten problemas de accesibilidad hacia una Red Pública y situaciones complejas con sus ventajas y desventajas.

1.2.2 Objetivos Específicos

Entender que es una Red Extremo – Extremo y Pública, como es el caso de Internet.

Realizar un estudio de la Traducción de Direcciones.

Analizar las condiciones emergentes frente a la escasez de direcciones IPv4 y explicar el concepto de la traducción a IPv6 con una extensión de NAT.

Simular un ejemplo de NAT, para observar y analizar la traducción de direcciones al acceder desde una Intranet o Red Interna-Privada hacia una Web Pública y a un Servidor Externo.

Investigar los distintos métodos existentes actualmente para atravesar NAT y/o Firewalls.

Anexar el estudio de otros proyectos involucrados con las técnicas para atravesar NAT, para una mejor visión del tema.

1.3 Estructura del Documento

El presente Trabajo de Finalización de Máster se divide en los siguientes capítulos:

El primer capítulo se refiere a la introducción, objetivos generales y específicos como se ha descrito.

El segundo capítulo realiza un estado del arte de lo que es INTERNET, su evolución, funcionamiento, aplicaciones, infraestructura y las tipologías para las distintas áreas y asignaciones de direcciones a los clientes alrededor del mundo, para entender lo que ha llevado a la creación de tecnologías que detengan el flujo de información.

El tercer capítulo está enfocado hacia las anomalías que hay en Internet, los cuales generan obstáculos, como los Firewalls y/o NAT, de los cuales se resalta los conceptos básicos de estas dos barreras; haciendo énfasis principalmente en el funcionamiento de NAT para posteriormente realizar una simulación con la ayuda del software Packet Tracer y de acuerdo a los tipos y clases de NAT con el objetivo de entender la traducción de direcciones y que en momento es óptimo realizarlo. Además, se estima las condiciones de la escasez de las direcciones IPv4, lo cual ha llevado a implementar mecanismos de traducción a IPv6 (NAT- PT) como una extensión de NAT para aplacar el agotamiento de las direcciones con el uso del direccionamiento privado en las redes para acceder a Internet, a través de un router con una sola dirección IP pública; aunque este método se considere obsoleto como se señala en el RFC 4966, es preciso mencionar los conceptos de NAT-PT como ejemplo de NAT en el cambio de IPv4 a IPv6 debido al incremento de direcciones y la importancia que tiene cada vez más el acceso a Internet.

Al describir el funcionamiento, aplicaciones y los fines lucrativos que ha llevado a NAT a su uso efusivo, no se puede dejar aún lado los problemas que trae consigo su seguridad, el uso de un servidor detrás de un NAT e IPSec en NAT - Transversal (NAT - T) descritos en el cuarto capítulo y las soluciones respectivas como STUN, TURN, ICE, VIP, ANTS y entre otros que son el objetivo de este trabajo, con la finalidad de aportar cierta ayuda o respaldo en temas relacionados a la traducción de direcciones, la accesibilidad a la Web Pública cuando existe Firewalls y/o NAT, los problemas que estos ocasionan y sobre todo como solventar o atravesarlas para obtener la información.

En el cuarto capítulo y último de este documento se realiza las respectivas conclusiones y posteriores trabajos.

2. RED EXTREMO – EXTREMO/INTERNET

2.1 Evolución de Internet

Internet se define como una red interconectada de redes de computadores, de carácter Internacional e Intercontinental, que une a servidores de todo el mundo y que se comunica a través de diversos canales, como lo son las líneas telefónicas, el cable coaxial, las microondas, fibra óptica y los satélites.

Hay dos momentos sustanciales que marcan la historia del desarrollo de Internet; el primero tiene directa relación con medidas de defensa militar, y el otro se refiere, por consecuencia directa, al desarrollo de las economías nacionales a través del planeta y la búsqueda de la integración mercantil y financiera. Este proceso lo conocemos como globalización.

2.1.1 Historia

Internet (INTERconnected NETworks) como se conoce en la actualidad, se define como la Infraestructura de la Sociedad y como un conjunto de ordenadores que pueden interconectarse que permiten compartir recursos, distinguiéndose dos tipos de redes principales:

Intranets: redes con fines específicos, acceso restringido y controladas por un servidor central.

Internet: red con libre acceso y múltiples servidores.

Internet es una red de redes, la red de comunicaciones más grande del mundo, con millones de ordenadores conectados y una creciente importancia social.

Sus primeros pasos o su origen se da a partir de los años 60', cuando en los Estados Unidos se estaban buscando alternativas de mantener una forma de comunicación en el posible caso de una Guerra Nuclear con la creación de ARPA marcando la historia del Internet.

Pensar en una red descentralizada y que esté diseñada para poder llevar a cabo operaciones en situaciones difíciles quitando cualquier tipo de autoridad centralizada.

Cada máquina conectada debía constar del mismo estatus y la misma capacidad para recibir información y a la vez enviarla, entonces se decidió que los mensajes tenían que ser divididos en pequeñas porciones de información o paquetes (conmutación de paquetes), éstos contendrían la dirección de destino sin especificar la ruta de arribo, cada paquete debía buscar la manera de llegar al destinatario según las rutas disponibles. El destinatario sería el encargado de reensamblar los paquetes individuales para construir el mensaje original.

Para 1968 se realiza en el Laboratorio Nacional de Física de Gran Bretaña el primer experimento de una Red de Conmutación Distribuida en Inglaterra con la finalidad de ofrecer máxima resistencia ante un ataque enemigo; al siguiente año, el Pentágono de los Estados Unidos, decidió que era hora de financiar su propio proyecto, y es en 1969, en que se establece la primera red en la Universidad de California, de esta forma nacía ARPANET.

Para años 70' el tiempo que poseían las computadoras para procesar datos era un recurso escaso ya que constaban con tan solo 15 nodos y 23 ordenadores host (centrales); para 1972 ARPANET acumulaba 37 redes. Lo curioso aquí, es que se empezó a notar que la mayor parte del tráfico informático era constituido por mensajes personales y noticias, y no por procesos informáticos.

En los años 80' surge las primeras aplicaciones TCP/IP, y en 1984 la Fundación para la Ciencia introduce el DNS y da comienzo a una nueva red de redes, vinculando en su primera etapa a los centro de cómputos en los Estados Unidos mediante nuevas y más rápidas conexiones, esta red se la conoció como NSFNET. El crecimiento exponencial de dicha red así como el incremento de la capacidad de transmisión de datos, hizo que la mayor parte de los miembros de ARPANET optaran por conectarse a esta nueva red y es en 1989 en donde ARPANET se disuelve. Las redes que se sitúan fuera de los Estados Unidos eligieron identificarse por su localización geográfica, mientras que otros integrantes de NSFNET se agruparon bajo seis básicas categorías: "mil", "gov", "edu", "org", "net" y "com"; como todos saben hoy en día, estas extensiones se han expandido a raíz de la demanda creciente de dominios, llegando a los "info", "us", "name", etc; lo cual ha conllevado a la creación de una "RED DE REDES", en la que un ordenador de una red puede intercambiar información con otro situado en una red remota.

En gran parte, este espectacular crecimiento se debe a la notable mejora en la facilidad de uso de los servicios ofrecidos, dado que aun manteniéndose los servicios originales de transferencia de ficheros, correo electrónico o acceso remoto, la irrupción de la 'TELARAÑA MUNDIAL', World Wide Web (www), un servicio de consulta de documentos hipertextuales, ha sido el paso definitivo hacia la popularidad de la que actualmente goza.

2.2 Funcionamiento de Internet

Internet es una red mundial que se ha formado al unirse las redes nacionales e internacionales que estaban previamente aisladas dentro de una misma red; esta comunicación se logra gracias a las direcciones MAC (Control de Acceso al Medio); físicamente lo hacen por medio del protocolo DLL (Data Link Layer, es decir, Ethernet) y la comunicación entre los ordenadores conectados a diferentes redes se consigue gracias al protocolo TCP/IP.

Protocolos de red

Un protocolo es un conjunto de reglas que definen si se debe realizar una comunicación entre ordenadores, y cómo codificarse y transmitirse la información.

Cuando se transfiere información entre ordenadores ésta se transmite en forma de paquetes pequeños de información, que deben atravesar diversos ordenadores y dispositivos que hacen posible la transmisión como se muestra en la Fig.1.

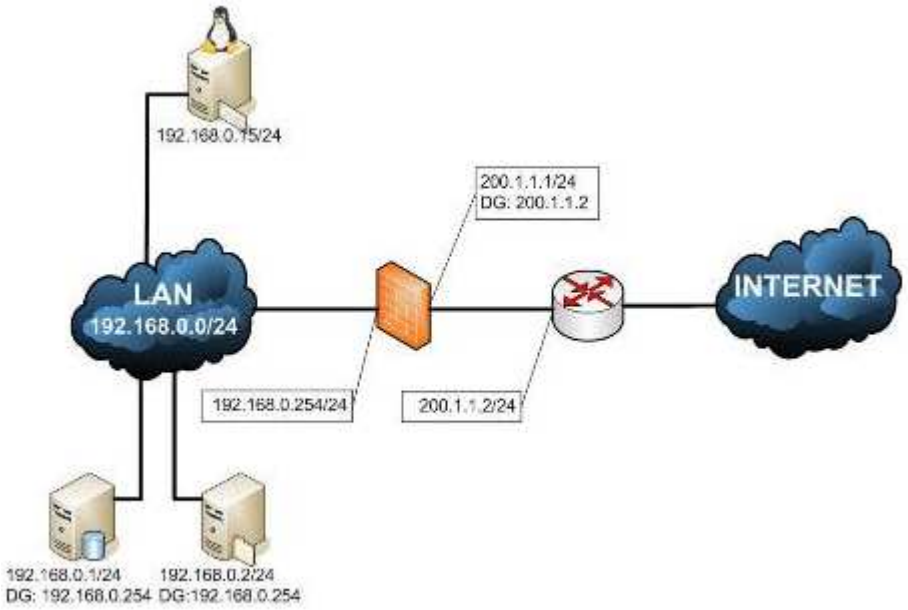


Figura. 1. Estructura de los Protocolos de Red

Los routers son sistemas que conectan las diferentes redes que forman Internet y que redirigen los paquetes de información hacia la dirección adecuada.

El protocolo TCP/IP es el encargado de identificar cada paquete de manera que llegue a su destino, es decir, es un protocolo de transmisión de paquetes.

Cada ordenador conectado tiene una dirección IP que lo distingue de los demás. Sin embargo, éste no es el único protocolo de Internet, los usuarios pueden también

conectarse con su proveedor de servicios usando protocolos PPP (Point to Point Protocol) o el SLIP (Serial Line Internet Protocol).

2.3 Servicios y Aplicaciones de Internet

Debido a su amplia difusión y utilidad para los usuarios de la red, se las conoce también como servicios de Internet y constituyen una serie de servicios básicos de Internet, como: Correo Electrónico, World Wide Web, FTP, Grupos de Noticias, IRC y Servicios de Telefonía.

El Correo Electrónico - email, nos permite intercambiar mensajes, generalmente textuales, entre usuarios, este correo es casi instantáneo, a diferencia del correo normal, y además muy barato.

La World Wide Web - WWW, se inventó a finales de los 80 en el CERN, el Laboratorio de Física de Partículas más importante del Mundo. Se trata de un sistema de distribución de información tipo revista y es el servicio de Internet que más usuarios concentran y que más ha popularizado la red, nos permite el acceso a todos los recursos del Internet en un sistema hipertextual.

El FTP - File Transfer Protocol, permite la obtención y/o envío de copias de archivos entre ordenadores conectados a la red.

Los Grupos de Noticias, basados en el servicio de Correo Electrónico.

Servicio IRC - Internet Relay Chat, nos permite tener una conversación en tiempo real con una o varias personas por medio de texto y envío de imágenes u otro tipo de ficheros mientras se dialoga.

Servicios de Telefonía, se basan en conexiones de voz a través de Internet sin tener que pagar el coste de la llamada internacional con aplicaciones multimedia como las conocidas Videoconferencia.

Internet también posee otros servicios como:

Archie que es un complemento del FTP para buscar ficheros concretos por la Red.

Gopher es el antecesor de la WWW para obtener información sin los elementos multimedia como imágenes y sonido principalmente.

X.500 y WOIS son servicios de búsqueda de personas y datos sobre esas personas, usado principalmente en Instituciones públicas como las Universidades.

Telnet que se basa en una conexión a un ordenador remoto estableciendo una sesión interactiva. Prácticamente en desuso, superada por la Web.

2.4 Infraestructura de Internet

La infraestructura de Internet, Fig.2, no es más que un conjunto de redes IP y enrutadores bajo el control de una o varias organizaciones con una política de encaminamiento común [1], mediante la interconexión de Sistemas Autónomos (AS) utilizando un protocolo de pasarela interno IGP como OSPF o RIP y otro protocolo de frontera como BGP.

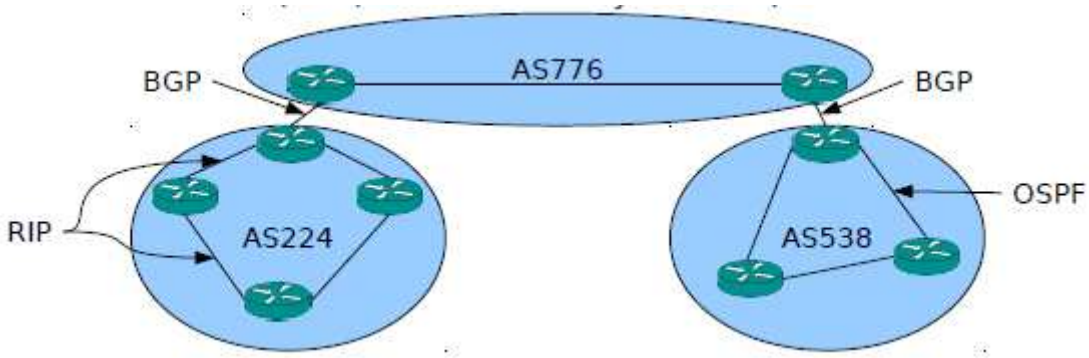


Figura 2. Infraestructura de Internet

Cada Sistema Autónomo está identificado con un número único denominado ASN (Autonomus System Number) delegados por IANA (Internet Asigned Number Authority) y los RIR (Regional Internet Registries) por bloques y cada uno de estos se asigna un ASN a cada organización ofreciendo 32 bits y para los ASN del 65512 al 65534 están reservados para uso privado.

Los ASs se pueden comunicar de la siguiente manera:

Proveedor – Cliente (Transit): El proveedor proporciona servicios de tránsito al cliente.

De igual a igual (Peering): Intercambio directo entre sistemas pertenecientes a los ASs o sus clientes.

2.5 Topología actual del Internet

Referente a las asignaciones y registros, se tiene hasta el momento cinco Registros Regionales correspondientes a diferentes continentes, tales como:

AfriNIC: África

APNIC: Asia y Pacífico

ARIN: Norte América

LACNIC: América Latina y Caribe

RIP NCC: Europa, Oriente Medio y Asia Central.

2.6 Direccionamiento

En [2] se define los estándares para las direcciones IP, que consiste en un par de números:

Dirección IP = <número de red><número de host>

Las direcciones son números de 32 bits comúnmente representadas en forma decimal, así por ejemplo: la dirección 128.2.7.9 es una dirección IP siendo 128.2 el número de red y 7.9 el número de host.

El formato binario de la dirección IP 128.2.7.9 es:

10000000 00000010 00000111 00001001

Existen cinco clases de direcciones IP en una totalidad de 4000 millones, cuyo sistema se basa en clases muy ineficientes por la falta de flexibilidad en la asignación de rangos de direcciones. Las cincos clases son:

Clase	Net	Host	Nº Direc.	Hosts	Asignadas	Crecimiento
A	1 octeto	3 octeto	126	16387064	115	0
B	2 octeto	2 octeto	16383	64516	8361	Muy alto
C	3 octeto	1 octeto	1097151	254	128709	alto
D	MULTICAST					
E	RESERVADO					

Tabla 1. Clases d Direcciones IP

Debido al crecimiento explosivo de Internet, el uso de las direcciones IP asignadas empiezan a ser demasiado inflexibles para permitir cambios sencillos en las configuraciones de red local, en consecuencia se percibe:

Agotamiento de direcciones clase B a corto plazo.

Agotamiento del espacio total de direcciones IP a medio plazo.

3. NOMALIAS Y OBSTACULOS EN LA RED

3.1 FIREWALLS

En muchos casos, se preguntan ¿Qué es son los Firewalls? O ¿Qué puede hacer en mi máquina u ordenador? Y entre otras.

Brevemente realizando un paréntesis e introducción se puede decir que cada ordenador que se conecta a Internet y, a cualquier red puede ser víctima de ataques, ya sean mediante el envío aleatorio de paquetes de datos en busca de un ordenador conectado con el propósito de buscar un punto débil en el sistema de seguridad para explotarlo y tener acceso a los datos de la máquina. Ver Fig. 3.

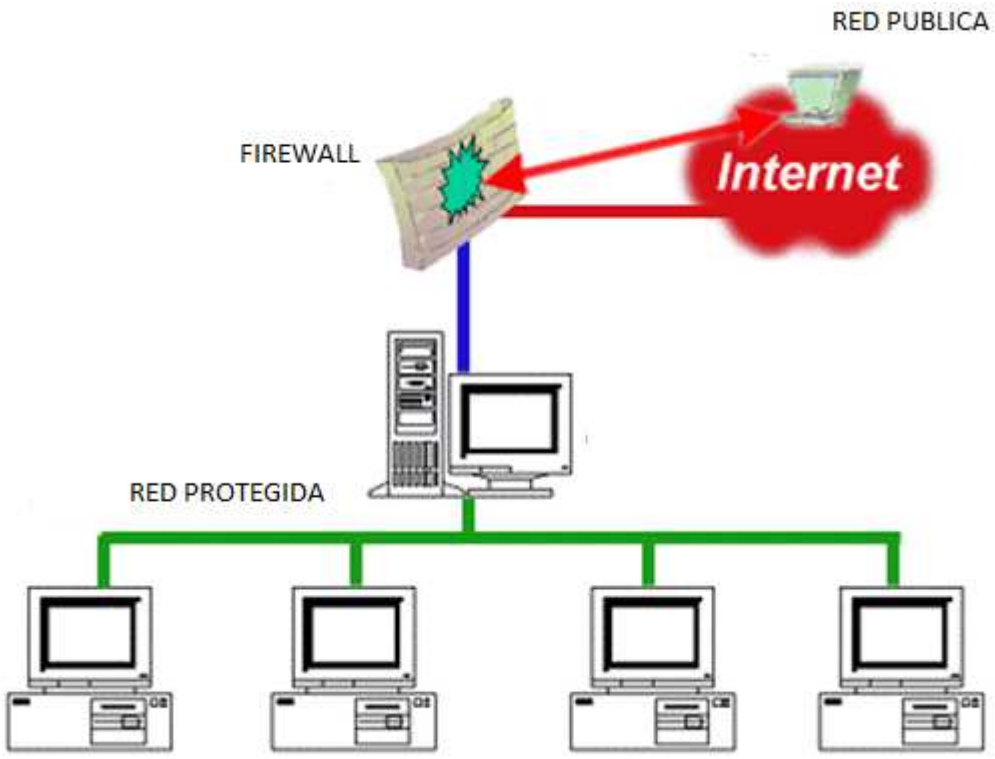


Figura 3. Esquema Conceptual de un Firewall

Un Firewall entre redes es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo o denegando al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Por lo tanto un Firewall es simplemente un dispositivo, software o hardware que se conecta entre la red y el cable de la conexión a Internet, es decir un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sea, permite o deniega su paso. Para permitir o denegar una comunicación el Firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el Firewall decide si lo permite o no. Además, el Firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no. De este modo un Firewall puede permitir desde una red local hacia Internet servicios de web, correo y FTP. También se puede configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que sea accesible desde Internet). Dependiendo del Firewall que se tenga también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

La tecnología de los Firewalls surgió a finales de 1980, cuando Internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad usando routers que mantenían a las redes separadas una de otras, de allí que tenemos Firewalls de:

Primera Generación: Conocidos como Firewalls de red y basados en el filtrado de paquetes, que actuaba sobre las tres primeras capas del modelo de referencia OSI (trabajo realizado entre la red y las capas físicas).

Segunda Generación: Firewalls de Aplicación y actúan sobre actúan sobre la capa de aplicación del modelo OSI. Permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial

Ejemplo: Un Firewall de aplicación puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP y TFTP (GSS).

Tercera Generación: Firewalls de Estado, esta tecnología se basa en la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el Firewalls, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. Este tipo de Firewalls pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

Este tipo de Firewall en su funcionalidad de inspección profunda de paquetes en los actuales Firewalls puede ser compartida por los sistemas de prevención de intrusiones (IPS), por lo que hasta el momento, IETF está trabajando en la estandarización de protocolos para la gestión de Firewalls que proporcionen características tales como

unir a las identidades de usuario con las direcciones IP o MAC; como el Firewalls NuFW, que brinda características de identificación real solicitando la firma del usuario para cada conexión.

3.1.1Tipos de Firewalls

Nivel de aplicación de pasarela: Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

Circuito a nivel de pasarela: Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

Firewalls de capa de red o de filtrado de paquetes: Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de Firewalls se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

Firewalls de capa de aplicación: Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder.

Un Firewalls a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los computadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

Firewalls personal: Es un caso particular de Firewalls que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red. Se usa por tanto, a nivel personal.

3.2 NAT – NETWORK ADDRESS TRANSLATION

3.2.1 Introducción

El rol que cumple NAT en los ambientes multimedia, se ha convertido en tema de investigación de Redes de Nueva Generación. Cuando NAT se introdujo inicialmente, no se tomó encuenta todas las leyes o restricciones que podían causar la transición a IPv6.

En este capítulo se realiza la explicación de los conceptos básicos de NAT, tipos de NAT para la traducción de direcciones y sus respectivas aplicaciones (por ejemplo en el cambio de IPv4 a IPv6) con el propósito de comprender la necesidad de este mecanismo.

La idea básica que hay detrás de NAT es traducir las IP privadas de la red en una IP publica para que la red pueda enviar paquetes al exterior; y traducir luego esa IP publica, de nuevo a la IP privada del PC que envió el paquete, para que pueda recibirlo una vez llega la respuesta. Sin embargo, nos cuesta creer que el NAT tenga inconvenientes, ya que muchas aplicaciones no pueden funcionar detrás del NAT y cada vez se vuelve más destacado este tema, por lo cual se ha llegado a considerar en este documentos dos puntos: el primero consiste en evitar NATs para aplicaciones multimedia donde se trata posibles problemas de seguridad, y en segundo lugar tratar de explicar un método adecuado de NAT Transversal. Ambas consideraciones podría traer resultados adecuados y resolver problemas particulares. Mientras que el primero no parece ser siempre aplicable, el segundo, dependiendo de la aplicación elegida podría resolver los problemas de NAT, hasta un nivel de descenso.

Además se da un enfoque de la relevancia de NAT en la migración de IPv4 a IPv6 como parte fundamental de la traducción de direcciones frente a la escasez de las mismas. Y para concluir, se presenta las posibles técnicas existentes para atravesar NAT (NAT Traversal) que son requeridas especialmente por aplicaciones cliente-cliente como Peer to Peer y VoIP dependiendo del comportamiento del NAT empleado. De allí que la mayoría de las técnicas basadas en NAT eluden la política de seguridad de las empresas, por lo que se prefieren técnicas que explícitamente cooperan con NAT y los firewalls.

3.2.2 Objetivos

1. El objetivo fundamental de NAT es aparentar usar una red de IP con direcciones diferentes a las que realmente usa, permitiendo así convertir espacios de IP no ruteables en direcciones ruteables y cambiar la ISP de forma amigable.

2. La misión de NAT es aplacar el agotamiento de las direcciones IPv4 permitiendo el uso del direccionamiento privado en la redes para acceder a Internet, a través de un router con una sola dirección IP pública.

3.2.3 Justificación

NAT permite que una red IP parezca hacia el exterior que emplea un espacio de direcciones diferente del que en realidad usa. La utilidad más típica es hacer que una red que emplea direccionamiento privado pueda conectarse a Internet convirtiendo las direcciones IP en los paquetes que envía a direcciones públicas.

3.2.4 Funcionamiento NAT

El crecimiento masivo de las redes ha creado nuevas alternativas que hacen difícil el funcionamiento de algunas aplicaciones. Hoy en día la arquitectura de Internet (Fig. 4) consiste en una dirección global y muchas direcciones privadas interconectadas por NAT; esto conlleva a que los equipos que tengan direcciones públicas puedan fácilmente conectarse a otros en la red, ya que poseen una única, global y ruteable dirección IP; mientras, que los equipos de las redes privadas pueden conectarse entre sí o pueden establecer conexiones TCP o UDP con equipos que pertenezcan a la red pública.

Figura 4. Comunicación NAT

Los dispositivos que realizan NAT traducen la dirección y puertos de los paquetes que provienen de las redes privadas hacia las redes públicas, es decir, los NAT solo permiten conexiones salientes y cualquier tráfico entrante o a su vez la comunicación cliente/servidor para el caso típico donde el cliente se encuentre en la red privada y el servidor en la red pública, esto resulta una comunicación difícil especialmente para el caso de las redes P2P que pertenecen a distintas redes privadas.

NAT es necesario cuando la cantidad de direcciones IP que nos haya asignado nuestro proveedor de Internet sea inferior a la cantidad de ordenadores que queramos que accedan a Internet [7].

La traducción de direcciones es un método utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo, de esta manera NAT se encarga de la siguiente información:

- Dirección IP de Origen
- Puerto TCP o UDP de Origen

NAT por Origen o Source NAT – SNAT

Se produce cuando el router altera el origen del paquete, es decir, cambia parámetros del lugar de donde viene, se realiza siempre después de los encadenamientos justo antes de que el paquete salga del router.

NAT por Destino o Destination NAT (DNAT)

Se produce cuando el router altera el destino del paquete, es decir, cambia los parámetros del lugar a donde va, siempre se realiza antes del encadenamiento, cuando el paquete entra al router.

Funcionamiento NAT

NAT se puede dividir en varias formas según se modifiquen parámetros del destino o parámetros del origen, como se verá más adelante. NAT propone un método de traducción que consiste en:

1. Los paquetes deben aparentar que se han originado y provienen de la pasarela NAT y de esta forma poder registrar los cambios en su tabla de estado y así poder:

_ Invertir los cambios en los paquetes devueltos
_ Asegurar que los paquetes pasen a través del Firewall.

2. Puede ocurrir que la IP de origen sea sustituida con la dirección externa de la pasarela NAT y que el puerto de origen sea sustituido por un puerto no en uso en la pasarela; esto permite al equipo interno deducir que el sistema NAT sea una simple pasarela a Internet. Para el equipo público los paquetes parecen venir directamente de la pasarela NAT, sin darse cuenta de que existe una estación interna.

3. Cuando el anfitrión de Internet responde a los paquetes internos de la máquina, este los direcciona a la IP externa de la pasarela NAT y a su puerto de traducción y ahí ésta pasarela busca la tabla de estado para determinar si los paquetes de respuesta concuerdan con alguna conexión establecida.

4. Considerando la aplicación básica de NAT para que una red privada tenga acceso a Internet, esta red debe ser por medio de un dispositivo ubicado en la frontera de las dos redes que tenga configurado NAT para la traducción de direcciones, en estos casos lo más conveniente es poner a un router para que los paquetes sean enviados hacia él como se explica en el siguiente apartado.

Para hacer énfasis en lo estipulado anteriormente, se ha visto la necesidad de realizar una simulación de NAT, ver Fig. 5., como se explica a continuación.

3.2.5 Simulación NAT

NAT brinda seguridad de red, aunque, las redes privadas no publicitan sus direcciones o topología interna, éstas son razonablemente seguras cuando se las utiliza en conjunto con NAT para tener un acceso externo controlado. Sin embargo, NAT no reemplaza los firewalls. En el siguiente ejemplo, NAT entra en la función para obtener host con direcciones IP válidas para poder tener acceso ya sea a un servidor web o a un host externo, como se explica a continuación:

Procedimiento:

_ Se configura una ACL que permita NAT
_ Se configura la NAT estática y dinámica
_ Se configura el router y conectividad
_ Por último se procede a configurar el NAT

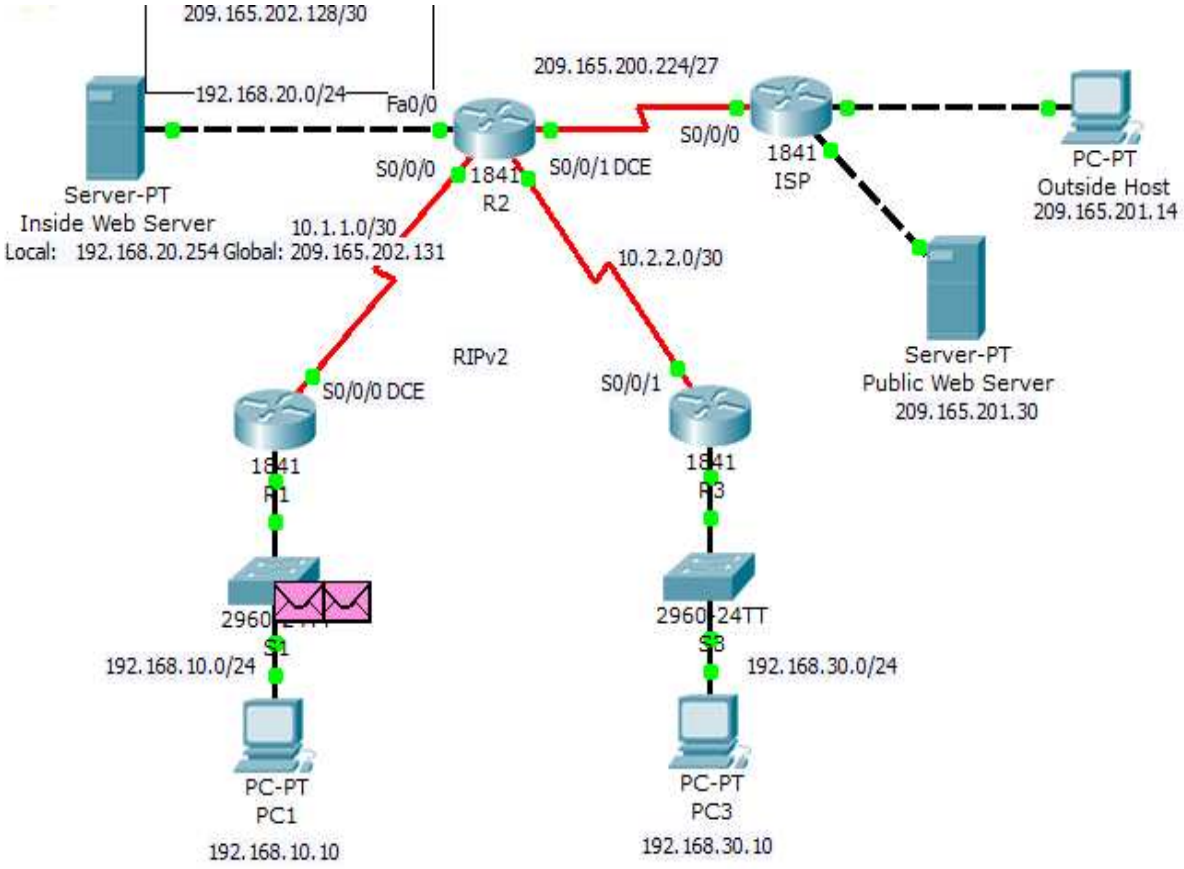


Figura 5. Esquema de la Configuración NAT

La simulación se llevó a cabo con la ayuda de Packet Tracer, procediendo de la siguiente manera:

1. Definir las direcciones internas que se traducen a direcciones públicas en el proceso NAT, y se crea una ACL estándar nombrada, llamada R2NAT.

   _PC1: 192.168.10.10
   _PC3: 192.168.30.10
   _R1: 192.168.10.1
   _R2; 192.168.20.1
   _R3: 192.168.30.1
   _Host Externo: 209.165.201.14
   _Servidor Web Público: 209.265.201.30

2. Configurar NAT estática para un servidor web interno que debe tener la dirección pública que no debe cambiar, y definir las direcciones internas que se traducen a direcciones públicas en el proceso NAT, esto crea una ACL estándar

nombrada, llamada R2NAT. La configuración de una dirección NAT estática permite la configuración del servidor Web con una dirección interna privada. Luego, el proceso NAT asigna paquetes mediante la dirección pública del servidor a la dirección privada.

3. Configurar NAT dinámica con sobrecarga para la dirección IP pública asignada al servidor Web interno, en este caso el ISP asigna tres direcciones públicas para que las use. Estas direcciones se asignan a todos los demás hosts internos que acceden a Internet.

4. Permitir que más de tres hosts internos accedan a Internet al mismo tiempo, se configura la NAT con sobrecarga para incorporar los hosts adicionales. NAT con sobrecarga, llamada también Traducción de la Dirección del Puerto (PAT), utiliza números de puerto para distinguir paquetes de diferentes hosts que se asignan a la misma dirección IP pública.

5. Configurar una ISP con ruta estática a R2.

Para la simulación se procedió a enviar un paquete desde el PC1 hasta el Host Externo y otro hacia el Servidor Web Público.

Configuración Router 2:

R2(config)#ip access-list standard R2NAT

R2(config-std-nacl)#permit 192.168.10.0 0.0.0.255

R2(config-std-nacl)#permit 192.168.20.0 0.0.0.255

R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255R2(config-std-nacl)#exit

R2(config)#ip nat inside source static 192.168.20.254 209.165.202.131

R2(config)#ip nat pool R2POOL 209.165.202.128 209.165.202.130 netmask 255.255.255.252

R2(config)#ip nat inside source list R2NAT pool R2POOL overload

R2(config)#exit

Configuración del ISP:

ISP>enable

ISP#config

Configuring from terminal, memory, or network [terminal]?

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

ISP(config)#ip route 209.165.202.128 255.255.255.224 serial0/0/0

Configuración NAT:

R2(config)#interface fa0/0

R2(config-if)#ip nat inside

R2(config-if)#interface serial 0/0/0

R2(config-if)#ip nat inside

R2(config-if)#interface serial 0/0/1

R2(config-if)#ip nat inside

R2(config-if)#interface serial 0/1/0

R2(config-if)#ip nat outside

R2(config-if)#exit

Resultado de la conectividad y visualización de NAT cuando pasa de R1 a R2:

Cuando se transfieren de R1 a R2:

- Dirección de Origen: 192.168.10.10
- Dirección de Destino: 209.165.201.14

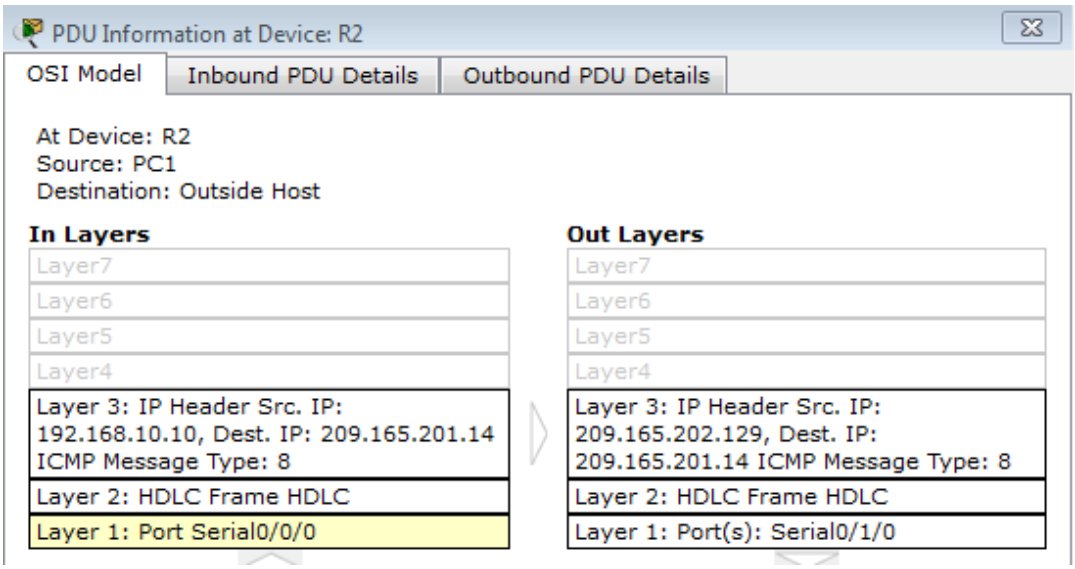


Figura 6. Simulación NAT – R1/R2

Se puede visualizar que cuando la información se transfiere de R1 a R2, la dirección de origen de la PDU entrante es 192.168.10.10 cambia a la dirección de origen 209.165.202.129 de la PDU saliente, lo cual señala que en este periodo se realiza la traducción de direcciones (NATEO) para poder acceder al Host Externo.

Resultado de la conectividad y visualización de NAT cuando pasa de R2 a R1:

Cuando se transfieren de R2 a R1:

- Dirección de Origen: 192.168.10.10
- Dirección de Destino: 209.165.201.30

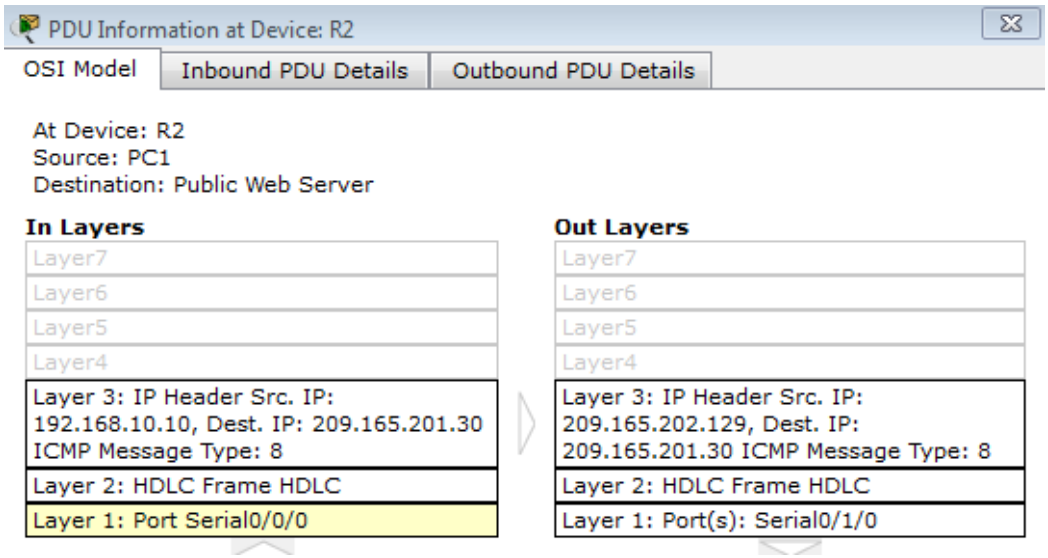


Figura 7. Simulación NAT - R2/R1

Al igual que se direccionó al Host Externo, se lo hizo hacia el Servidor Web Público, obteniendo la siguiente traducción de direcciones de 192.168.10.10 a 209.165.202.129 en la PDU entrante y saliente respectivamente.

El problema radica cuando los dispositivos de la red interna (PC1 en este caso) de comunicación con el Servidor Web Público y/o Host Externo al cambiar la dirección de origen de las solicitudes de salida a la del dispositivo de NAT y las respuestas de la retransmisión de nuevo al dispositivo de origen. Esto deja a la red interna inadecuada para los servidores host, ya que el dispositivo NAT no tiene un método automático para determinar el host interno para que los paquetes entrantes sean destinados. Esto no es un problema para los usuarios domésticos detrás de dispositivos NAT haciendo acceso a la web en general y el correo electrónico. Sin embargo, para las aplicaciones como Peer-to-Peer para compartir archivos, servicios VoIP y los servicios en línea de la actual generación de consolas de videojuegos requiere que los clientes sean servidores, así, lo que plantea un problema para los usuarios detrás de dispositivos NAT, ya que las solicitudes de entrada no puede ser fácilmente correlacionado al host interno apropiado. Además, muchos de estos tipos de servicios llevan la dirección IP y la información de número de puerto en los datos de aplicación, la sustitución o puedan requerir técnicas especiales para atravesar NAT.

En este ejemplo se detalla la fácil transición al Servidor Web Público basándose en una simulación de una red doméstica hacia una red privada, en la cual se presencia el cambio de direcciones (NATEO) como se explicó anteriormente; no obstante, cuando se trata de una red como VoIP, es necesario tener herramientas y/o técnica para permitir el acceso a la red pública.

3.2.6 Clasificación de NAT

En general existen tres tipos de funcionamiento de NAT:

NAT estático

Es un tipo de NAT en el cuál se mapea una dirección IP privada con una dirección IP pública de forma estática. De esta manera, cada equipo en la red privada debe tener su correspondiente IP pública asignada para poder acceder a Internet. La principal desventaja de este esquema es que por cada equipo que se desee tenga acceso a Internet se debe contratar una IP pública. Además, es posible que haya la existencia de direcciones IP públicas sin usar, por ejemplo que los equipos que las tienen asignadas están apagados o que no puedan tener acceso a Internet porque no tienen ninguna IP pública mapeada.

NAT dinámico

Este tipo de NAT pretende mejorar varios aspectos del NAT estático dado que utiliza un pool de IP públicas para un pool de IP privadas que serán mapeadas de forma dinámica y a demanda, por lo tanto establece la conexión entre direcciones IP registradas y no registradas. La ventaja de este esquema es que si se tienen por ejemplo 5 IPs públicas y 10 máquinas en la red privada, las primeras 5 máquinas en conectarse tendrán acceso a Internet. Si suponemos que no más de 5 máquinas estarán encendidas de forma simultánea nos garantiza que todas las máquinas de nuestra red privada tendrán salida a Internet eventualmente.

NAT con sobrecarga

El caso de NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos y el más usado. Es un método en el cual muchas direcciones de red y sus puertos TCP/UDP son traducidos en una dirección de red y en sus puertos respectivos TCP/UDP; considerando en utilizar una única dirección IP pública para mapear múltiples direcciones IP privadas.

La principal ventaja está enfocada cuando el cliente necesita contratar una sola dirección IP pública para que las máquinas de su red tengan acceso a Internet, lo que supone un importante ahorro económico, ahorrando de esta manera un número importante de IP públicas, lo que demora el agotamiento de las mismas.

La pregunta casi obvia es cómo puede ser que con una única dirección IP pública se mapeen múltiples IP privadas. Bien, como su nombre lo indica, PAT hace uso de múltiples puertos para manejar las conexiones de cada host interno.

3.2.7 Tipos de NAT basados en la Traslación

NAT se clasifica de acuerdo a los procesos de traducción en cuatro tipos. Para las direcciones internas los tres primeros tipos de NAT mantienen un tipo de traducción de dirección independiente de la dirección de destino y el cuarto tipo de NAT creará un tipo de traducción independiente por cada conexión con el destinatario.

En el caso de que el NAT tenga una tabla de traducción estática, la traducción se inicia cuando el primer paquete es enviado desde el cliente a través del NAT y este será válido por cierto tiempo hasta que se deje de enviar paquetes a esa IP y puerto.

Full Conexión: En este tipo de conexión cuando la traducción está establecida, cualquier equipo detrás del NAT, necesita solo conocer la dirección y el puerto de donde el tráfico está siendo enviado.

Conexión Restringida: Para el caso de conexión restringida, la IP y el puerto externo son abiertos cuando el equipo de la red privada envía tráfico saliente a una dirección IP específica, y así quedaría bloqueado el acceso para una dirección distinta.

Conexión Restringida por puerto: La conexión restringida por puertos es idéntica a la conexión restringida, pero en este caso solo el NAT bloqueará todo el tráfico, a menos que el cliente haya enviado antes tráfico a una IP y a un puerto específico, entonces ahí, esa IP en su puerto tendrá acceso a la red privada. Por ejemplo al enviar múltiples direcciones y puertos, la información se enviará a la dirección señala con anticipación.

Simétrico: Este tipo de NATs es muy diferente a los tres que se ha señalado anteriormente, ya que en este caso la traducción de la IP pública a la privada depende de la IP de destino donde ha sido enviado el tráfico y en el caso de existir tráfico de otro equipo, consecuentemente será rechazado.

3.2.8 Condiciones de NAT frente a la escases de Direcciones IPV4

No todas las aplicaciones se prestan fácilmente a la traducción de direcciones de los dispositivos NAT, especialmente, las aplicaciones que llevan la dirección IP y puerto, que sería el caso de NAPT, dentro de la carga útil.

La conversión de direcciones de red o NAT se puede utilizar en la traducción de protocolos IPv4 a IPv6 especialmente para nuevos tipos de dispositivos de Internet para resolver la falta de direcciones IP con el protocolo IPv4.

La traducción de IPv4 a IPv6 se considera una extensión de las técnicas NAT, convirtiendo no sólo direcciones sino también la cabecera. De hecho, en las direcciones IPv4 la cantidad de direcciones IP enrutables (que son únicas en el mundo) no son suficientes para permitir que todos los equipos que lo requieran estén conectados a Internet.

Sin embargo, la alternativa para evitar que se estanque el crecimiento de la red sin direcciones IP o que no se pueden crear nuevas subredes, ni identificar dispositivos que se conecten a las mismas, es considerar la renumeración y reasignación de los espacios de direccionamiento, aunque no sea tan sencillo ya que es impensable que algunas redes puedan coordinarse y sobre todo a escala mundial. **Y otra alternativa ha sido hasta el momento proporcionar direcciones IP privadas mediantes mecanismos NAT usando una sola IP pública para toda una red privada y por último migrar al protocolo IPv6**, que con sus 128 bits de longitud admite 340 sextillones de direcciones y con más de 1500 direcciones por metro cuadrado como se indica en la Fig. 8.

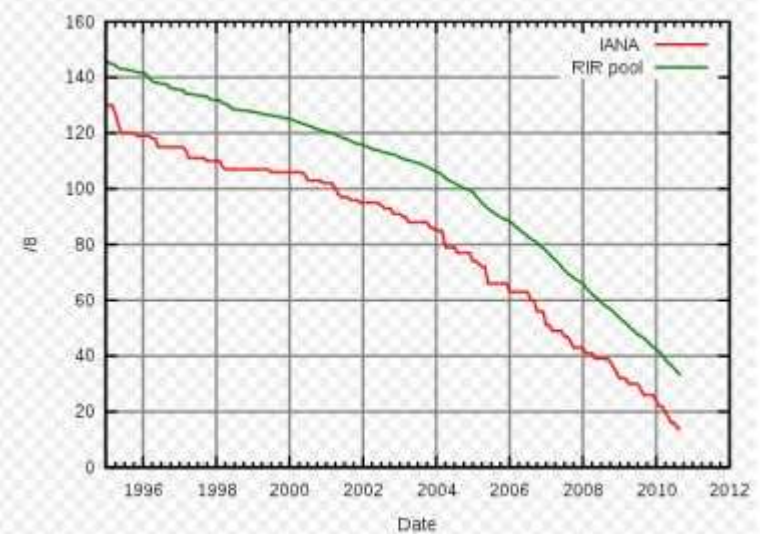


Figura 8. Decremento de IPv4

La función de los nodos IPv6 detrás de un traductor tienen la funcionalidad de IPv6 cuando hablan con otro nodo IPv6 y obtienen la funcionalidad habitual de NAT cuando se comunican con dispositivos IPv4; además, los métodos que comúnmente se utilizan para mejorar el rendimiento de NAT pueden ser usados para mejorar el rendimiento de la traducción IPv4-IPv6.

Para emplear la traducción de direcciones de IPv4 a IPv6, existen varios métodos para traducir en un elemento de red los paquetes de un formato a otro:

_ Sin estado (Stateless):

Stateless IP/ICMP Translation Algorithm (SIIT)

Bump in the Stack (BIS/MBIS)

Bump in the API (BIA)

_ Con estado (Stateful):

NAT-PT

SOCKS64

Transport Relay Translator (TRT)

Application Level Gateways (ALG)

El proceso de traducción implica llevarlo a cabo con Stateful (con estado) y el más conocida es NAT-PT, que actúa como un nodo intermedio (router) que modifica las cabecera de IPv4 a IPv6 y el tratamiento de paquetes es complejo, como se indica en el siguiente diagrama de la Fig. 9:

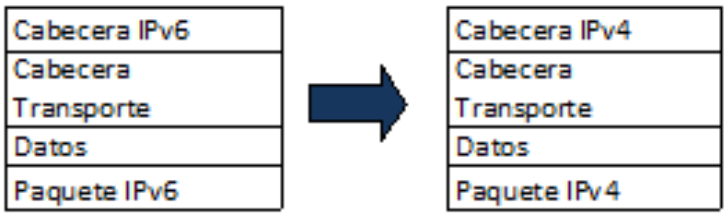


Figura 9. Traducción de Protocolos

La clave para la traducción es la compatibilidad con la base instalada de dispositivos de IPv4 conjuntamente con el mecanismo NAT para permitir usar infraestructuras IPv4 para IPv6 y viceversa. Sin embargo, es considerada como la peor solución, puesto que la traducción no es perfecta y requiere soporte de ALGs en el caso de NAT- IPv4 (DNS, FTP, VoIP).

3.2.8.1 Traducción de Direcciones IPv4 – IPv6: Network Address Translation - Protocol Translation (NAT – PT)

Definido en [12] y en un principio surge como solución a la escases de direcciones, con lo cual se define como un conjunto de la red-capa de traducción y mecanismos diseñados para permitir que los nodos de IPv4 puedan comunicarse con nodos de IPv6, durante la transición a la utilización de IPv6 en Internet. Sin embargo se ha aportado un nuevo documento [8] y que deja obsoleto a [12] en ciertos argumentos.

En esta sección se especifica NAT-PT básico, en el que sólo se ocupa la función de traducido, y la dirección de red Port Traductor (NAPT-PT) queda descartada de acuerdo a [8].

Para la traducción mediante NAT-PT, es necesario de los paquetes de salida IPv6, las direcciones IP y los otros campos como TCP, UDP, las cabeceras ICMP y el cheksum sean traducidos al igual que los paquetes de entrada.

Para NAT-PT existe un paso más que consiste en trasladar los identificadores de transporte utilizando el estado IP/ICMP como se indica en el Algoritmo SIIT.

SIIT (Stateless IP/ICMP Translator)

El algoritmo SIIT definido en [11], dispone de una conversión directa (traducción) de protocolos entre IPv4 e IPv6 de manera bidireccional incluyendo una transformación tanto del encabezado como de la carga útil, incluyendo los encabezados ICMP, conlleva a la traducción en diferentes capas de la pila incluyendo la capa red, transporte y aplicación. Este algoritmo puede utilizarse como parte de una solución que permite host IPv6 que no tienen una dirección IPv4 permanentemente asignada, y sirve de base para diferentes métodos de transición.

SIIT no específica cómo se realiza la conversión entre direcciones IPv4 e IPv6, sin embargo lleva a cabo la traducción de la siguiente manera:

IPv4 a IPv6 y viceversa

El traductor IPv4 a IPv6 recibe un datagrama IPv4 porque está configurado para conocer el grupo de direcciones de IPv4 que representan los nodos de IPv6 anteriores y sabe que el paquete necesita la traducción; de allí que recurre a quitar la cabecera IPv4 y la reemplaza con una cabecera IPv6 traduciendo toda la información.

En el caso de tener la traducción de IPv6 a IPv4, el traductor mantiene reglas similares de la traducción de IPv4 a IPv6, remueve la cabecera IPv6 y la reemplaza con la cabecera IPv4.

ICMPv4 a ICMPv6 y viceversa

Para los mensajes ICMPv4, el traductor tiene que computar un cheksum válido, porque esta es requerida para ICMPv6, de esta misma manera se realiza para la traducción de mensajes ICMPv6 a ICMPv4. A más de esto, el tipo de valores tienen que ser traducidos, y para los mensajes de error, las cabeceras IPv6 incluidas también deben ser traducidas.

Ejemplo:

Traduce los números de puertos TCP y UDP y los identificadores ICMP, permitiendo así que un conjunto de puertos IPv6 compartan una dirección simple IPv4 y combinar con NAT-PT Básico y así las direcciones externas son usadas en conjunto con los puertos de traslación.

NAT-PT para los paquetes de salida de IPv6 trasladaría la dirección IP, los identificadores de las capas de transporte y los campos relacionados como IP, TCP, UDP y el cheksum de la cabecera ICMP; en este caso los identificadores de transporte puede ser un puerto TCP/UDP o un identificador de consulta ICMP, y para los paquetes de entrada la dirección de destino IP, los identificadores de transporte de destino e IP y el cheksum de la cabecera de transporte son traducidos.

Para NAT-PT bidireccional las sesiones pueden iniciarse en los hosts de la redes de IPv4 como en redes de IPv6, los host IPv4 solo tienen acceso a los hosts IPv6 usando el DNS para la resolución de direcciones [8]. Un DNS-ALG debe ser empleado en conjunto con el NAT-PT bidireccional para facilitar el nombre en la asignación de direcciones, es decir debe ser capaz de trasladar las direcciones de IPv6 en consultas DNS y responder dentro sus enlaces de direcciones de IPv4 y viceversa como paquete DNS como paquete entre IPv6 e IPv4.

PT Protocol Translation

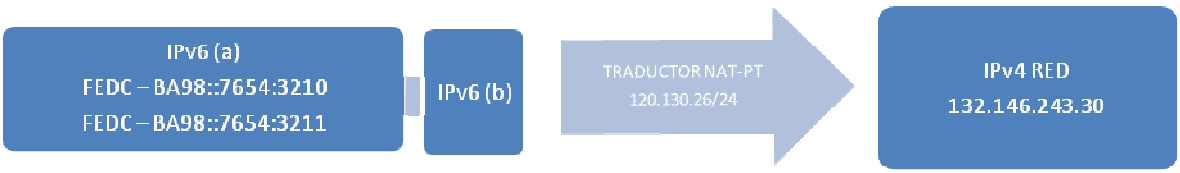
Descrito en SIIT-2765, y se refiere a la translación de los paquetes IPv4 dentro de un paquete IPv6 semánticamente equivalente.

3.2.8.2 Operaciones de Traducciones en NAT-PT:

a. NAT-PT BASICO

Permite traducir las direcciones/protocolos IPv4 en IPv6 y viceversa sin cambios en las aplicaciones.

Ejemplo:



En este ejemplo, el paquete de IPv6 es enrutado a NAT-PT Gateway y ahí es traducido a IPv4.

b. Traducción de Cabeceras

- **IPv4 a IPv6**

Las direcciones de destino IPv4 son reemplazadas por las direcciones retenidas IPv6 en la asignación.

- **IPv6 a IPv4**

Las direcciones IPv6 son reemplazadas por las direcciones IPv4 retenidas en tal asignación.

Los paquetes IPv6 que son traducidos, en este caso las direcciones IPv6 son copiadas a las direcciones IPv4.

c. TCP/UDP/ICMP Cheksum Update IPv4-IPv6

- **Cuando el Checksum UDP≠0**

NAT: El TCP Cheksum puede ser recalculado para reflejar o para cambiar las direcciones de IPv4 a IPv6.

NAT-PT: TCP/UDP Cheksum puede ser ajustado.

- **Cuando el Cheksum =0**

NAT: Se ensambla una parte no fragmentada y se evalúa el Cheksum en su totalidad para traducir el paquete UDP de IPv6.

d. ICMPv4 – ICMPv6 USA PSEUDO CABECERAS

El Cheksum ICMPv6 header es computado (SIIT) y necesita ser ajustado para tener encuenta las pseudo cabeceras y los ajustes deben ser tanto en la dirección de de origen como en la dirección de destino, y en el caso de NAT – PT los identificadores TCP/UDP/ICMP de la carga útil.

e. TCP/UDP/ICMP IPv6 –IPv4

NAT: Igual que IPv4 – IPV6.

NAT – PT: TCP/UDP deben ser ajustados para tomarlos encuenta para cambiar las direcciones y puertos TCP/UDP que van desde IPv6 a IPv4. Como opción los paquetes UDP, el Cheksum puede ser cambiado a cero, y el cálculo del Cheksum de las cabeceras ICMPv4 deben derivarse de las cabeceras ICMPv6.

f. Aplication Level Gateway - ALG

Es un agente específico de aplicación que permite a los nodos de IPv6 comunicarse con los nodos de IPv4 y viceversa. Este agente podría trabajar con NA-PT para proveer soporte a muchas aplicaciones, especialmente es requerido para proveer niveles de aplicación transporte para una aplicación popular de Internet. Se explica mas detallado en el siguiente capítulo.

Ventajas y Desventajas de FTP - ALG

NAT-PT tiene como propósito la comunicación extremo a extremo de la capa de red, pero la siguiente no es posible.

IPSec en end to end no es posible ya que atraviesa varias direcciones, ya que los dos nodos extremos deben soportar IPv4 o IPv6 y es difícil buscar una red segura IPSec.

NAT – PT combinado con DNS-ALG provee conectividad bidireccional entre IPV6 e IPv4.

NAT en la conversión de IPv4 a IPv6 limita la capacidad de trabajar alrededor de los límites permitidos y NAT-PT constituye un mecanismo diferente de transición para IPv6, pero que no contrasta el desarrollo de las aplicaciones IPv6.

PROBLEMAS DE NAT-PT

NAT-PT de acuerdo a [8] resuelve:

Que el DNS es parte integral de NAT-PT para proporcionar la información necesaria para el mapeado.

Que puede ser aplicado a cualquier red de capa esquema de traducción, incluyendo cualquier SIIT basado en el algoritmo [8]. En el caso de que las nuevas formas de traductor se desarrollan como alternativa a NAT-PT.

Los protocolos que incrustan direcciones IP en sus payloads o carga útil no pueden trabajar a través de NAT y requieren especificaciones ALG para traducir los payloads en línea con sus direcciones y puertos; de igual manera ocurre con NAT-PT, ya que IPv6 e IPv4 son de diferente longitud.

NAT-PT fue creado a razón de NAT como mecanismo suave para manejar las direcciones y puertos para que se opere autónomamente (sin clientes), pero se complica cuando se trata de traducir para varios hosts IPv6.

Existen desajustes en la equivalencia en IPv4 para el campo de flujo etiquetado de la cabecera IPv6. No obstante, las extensiones de las cabeceras IPv6 proponen flexibilidad para mejoras futuras del protocolo IP.

En conclusión NAT-PT no es la única y mejor solución, sino al contrario, hay que apoyarse de que hasta el momento se disponen cerca de 20 mecanismos de transición, traducción e implementaciones disponibles entre ellos y experimentación práctica tanto en redes experimentales como en proyectos de investigación en escenario como:

- GPP son servicios móviles para dispositivos de pequeño tamaño con ancho de banda modest.

- Se presenta escenarios GPRS en estudio (draft-soininen-ngtrnas 3gpp-cases), conllevando a conectar los siguientes casos:
- Dual UE que se conecte a nodos IPv4 e IPv6.
- IPv6 UE que se conecte a nodo IPv6 a través de una red IPv4.
- IPv4 UE que se conecte a nodo IPv4 a través de una red IPv6.

REDES NO GESTIONADAS - UNMANAGED: Redes domésticas o de pequeñas empresas sin personal técnico que las gestione. Esto permite que una única subred se conecte a Internet a través de un único ISP (draft-ietf-ngtrans-unmanscope), lo cual es aplicado para:

- Entornos domésticos o pequeñas empresas SOHO.
- Plug and Play.
- Aplicaciones locales, cliente, P2P.
- Migración de aplicaciones a IPv6 (draft-huitemangtrans-unmaneval

REDES GESTIONADAS - MANAGED: Redes corporativas gestionadas por personal cualificado.

PROVEEDOR DE SERVICIO DE INTERNET (ISP): Pueden ser redes de un proveedor que da servicio utilizando diferente tecnologías de red como DSL, HFC, dial – up, etc. No obstante, aun no se establece recomendaciones clara para aquellos que deseen comenzar con la transición, como es el caso de los ISPs, redes corporativas o de campus, redes domésticas, etc.

Resaltando la disposición de direcciones y crecimiento de la Internet, IPv6 fue diseñado para ofrecer una seguridad mejor que IPv4. Sin embargo, la seguridad sigue siendo una edición en nuevas instalaciones debido a la escasez de las herramientas de seguridad para estos protocolos debido a que el número de dispositivos que filtran y dificultan las comunicaciones extremo a extremo, siendo proporcional al crecimiento de la red. Para ello podemos hacer uso de los Firewalls actuales.

4. PROBLEMAS Y SOLUCIONES NAT

Cuando hablamos de NAT, debemos tener en cuenta que en primer lugar no permite encontrar host internos con alguna relación a lo enviado con lo que es posible desarrollar ciertas aplicaciones que descubran la presencia de NAT y/o Firewalls; no obstante, esto conlleva a invadir la privacidad o viole la seguridad, por ejemplo con ataques o envíos de spams.

Al establecer la comunicación entre dos puntos externos, NAT tiene la función de obstaculizar o poner barreras con el propósito de evitar anomalías en la comunicación de las mismas.

La traducción de direcciones [17] de red rompe la conectividad entre los dos puntos finales y se puede llevar a cabo la intercepción y modificación de tráfico de manera transparente en ausencia de cifrado seguro y autenticación; teniendo en cuenta que la mayoría de las técnicas de NAT eluden la política de las empresas, por lo que es neceario contar con aplicaciones que cooperen con NAT y Firewalls.

4.1 NAT y la seguridad

Como los NAT rechazan todo el tráfico que no coincida con una entrada de la tabla de traducción, son considerados dispositivos de seguridad. Sin embargo, los NAT no pueden sustituir a los servidores de seguridad. Normalmente, hay dos conjuntos de puertos TCP y UDP abiertos en el NAT:

- El conjunto de puertos correspondiente al tráfico que se traduce, especificado en la tabla de traducción. Contiene los puertos dinámicos que abren los clientes situados tras el NAT y los puertos estáticos configurados para los servidores situados tras el NAT.
- El conjunto de puertos correspondiente a aplicaciones y servicios en ejecución en el NAT.

Los puertos estáticos para los servidores situados tras el NAT y los puertos para las aplicaciones y servicios que se ejecutan en el NAT los hace vulnerable a los ataques.

Los puertos dinámicos no son tan vulnerables porque es difícil que un atacante adivine cuando se abrirán. Si el NAT es un equipo en lugar de un dispositivo dedicado (por ejemplo, un dispositivo de puerta de enlace de Internet), el equipo está expuesto a los ataques.

Por lo tanto, es recomendable que el NAT se use combinado con un servidor de seguridad y que los clientes de la red privada usen también servidores de seguridad basados en host para evitar la difusión de software malintencionado en la red privada.

4.2 Problemas del uso de un servidor tras un NAT

Los equipos clientes que usen NAT y tengan acceso a servidores conectados a Internet no suelen tener problemas. Por el contrario, sí se pueden producir problemas si los servidores se encuentran tras un NAT en las situaciones siguientes:

- Aplicaciones para varios equipos
- Aplicaciones del mismo nivel
- NAT-T de IPSec

4.2.1 Aplicaciones para varios equipos

Las aplicaciones para varios equipos son aquellas en que varios equipos acuerdan comunicarse juntos a través de un servidor central para una finalidad concreta. Se pueden citar como ejemplos una aplicación de colaboración o un juego en red para varios jugadores. Si el servidor central y algunos de los clientes están tras el NAT, el uso de direcciones privadas puede crear problemas de configuración.

Por ejemplo, un servidor de colaboración está situado tras un NAT y hay ciertos clientes situados tras el mismo servidor y otros que están situados en Internet. Como consecuencia del espacio de direcciones privado situado tras el NAT y el servidor situado tras el NAT, se debe configurar lo siguiente:

- Entradas estáticas en la tabla de traducción que asignen la dirección pública del NAT y los números de puerto de la aplicación del servidor a la dirección privada del servidor y los números de puerto de la aplicación del servidor.
- Para que los clientes conectados a Internet tengan acceso al servidor mediante su nombre DNS, se deben agregar entradas al DNS de Internet, de manera que el nombre del servidor se puedan resolver como la dirección pública del NAT.
- Para que los clientes conectados a la red privada tengan acceso al servidor mediante su nombre DNS, se deben agregar entradas al DNS de la red privada, de manera que el nombre del servidor se pueda resolver como la dirección privada del servidor.

La configuración de DNS no es necesaria si se usa la dirección privada o pública real del servidor al iniciar la conexión desde los equipos cliente. Con todo, el uso de direcciones para establecer conexiones con servidores es complicado para los usuarios finales; hay que garantizar que se indica a los clientes de Internet que utilicen la

dirección pública y a los clientes situados tras el NAT que utilicen la dirección privada. Incluso cuando se ha definido toda esta configuración, los clientes situados tras el NAT y los clientes conectados a Internet no utilizan la misma dirección del servidor. Si la aplicación informática de colaboración debe usar una dirección común por razones de configuración, sincronización o seguridad, se pueden seguridad produciendo problemas de comunicación.

4.2.2 Aplicaciones del mismo nivel

Otro problema de los NAT es cómo afectan a las aplicaciones del mismo nivel. En el modelo de comunicación del mismo nivel, los equipos del mismo nivel pueden actuar como cliente o como servidor y comunicarse enviando paquetes directamente uno a otro. Si un equipo del mismo nivel está tras un NAT, tiene dos direcciones asociadas, las direcciones privada y pública.

A continuación se examina una configuración sencilla en la que los NAT pueden crear problemas en aplicaciones del mismo nivel. La siguiente figura (Fig. 10) muestra una red privada con un NAT en el extremo.

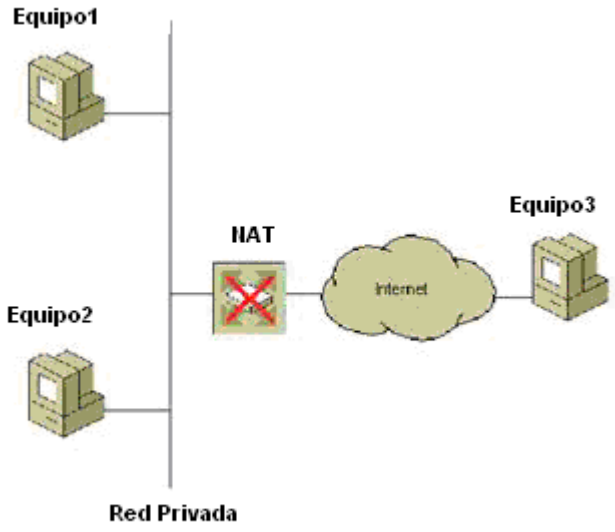


Figura 10. Aplicaciones del mismo nivel

Para una aplicación del mismo nivel que se ejecuta en todos los equipos del mismo nivel, el Equipo1 puede iniciar una sesión con el Equipo2 (accesible directamente en su subred) y con el Equipo3. Sin embargo, el Equipo1 no puede comunicar al Equipo3 la dirección pública del Equipo2 porque no la sabe. Además, el Equipo3 no puede iniciar una sesión con el Equipo1 ni el Equipo2 sin configurar manualmente el NAT con una entrada estática de la tabla de traducciones que convierta los paquetes de petición de

conexión entrantes en la dirección privada o el puerto del Equipo1 o el Equipo2. Incluso con dicha entrada en la tabla, el Equipo3 no puede iniciar una sesión con el Equipo1 ni el Equipo2, porque ambos host usan la misma dirección pública y el mismo número de puerto de aplicación.

Si se quiere complicar las cosas, es más frecuente que haya equipos del mismo nivel de Internet tras dos NAT distintos. Por ejemplo, en la figura anterior, el Equipo3 se encuentra tras un NAT. Para garantizar que la aplicación del mismo nivel pueda funcionar en cualquier configuración con NAT, se debe modificar para que sea compatible con NAT, lo que aumenta la complejidad de la aplicación.

4.2.3 NAT-T (NAT Transversal) de IPSec

La seguridad del Protocolo Internet (IPSec) de NAT Transversal (NAT-T) permite que los equipos del mismo nivel de IPSec situados tras un NAT detecten la presencia del NAT, negocien las asociaciones de seguridad IPSec y envíen datos protegidos mediante Carga de Seguridad Encapsuladora (ESP), a pesar de que las direcciones de los paquetes protegidos mediante IPSec cambien. La siguiente figura (Fig. 11) muestra un ejemplo de configuración.

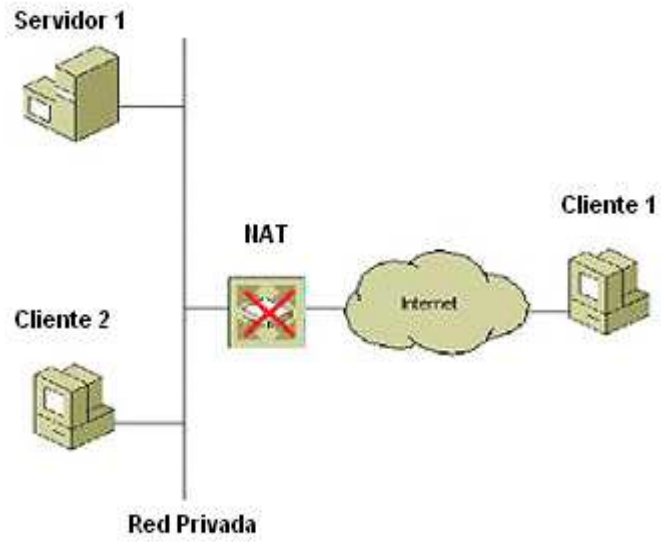


Figura 11. NAT-T de IPSec

Para garantizar que el Servidor 1 está accesible tras el NAT para el tráfico de IPSec, se debe configurar el NAT con entradas estáticas de traducción que asignen el tráfico de Intercambio de claves de Internet (IKE) y de IPSec NAT-T al Servidor 1.

En esta configuración se puede producir la situación siguiente:

- El Cliente 1, ubicado en Internet, usa IPSec NAT-T para establecer asociaciones de seguridad bidireccionales con el Servidor 1. El NAT reenvía el tráfico de IKE e IPSec NAT-T entre el Servidor 1 y el Cliente 1, como consecuencia de las entradas estáticas de la tabla de traducción.

- El Cliente 2 usa IPSec NAT-T para establecer asociaciones de seguridad bidireccionales con el Cliente 1. Cuando el Cliente 2 inicia la comunicación con el Cliente 1, el NAT crea un conjunto de entradas dinámicas en la tabla de traducción, lo que permite el intercambio de tráfico de IKE e IPSec NAT-T entre los clientes 2 y 1.

- Si el NAT elimina las entradas dinámicas de la tabla de traducción creadas por el Cliente 2 y se produce una situación que haga que el Cliente 1 vuelva a establecer asociaciones de seguridad con el Cliente 2.

Los problemas con NAT se radican principalmente en el caso de: aplicaciones para varios equipos, aplicaciones del mismo nivel y seguridad del NAT; los cuales pueden ser aplicados en estos tres casos, que se describen a continuación:

Cuando se usa direcciones específicas en el payload como el Protocol Session Initiation – SIP para establecer y modificar las sesiones, que usa una dirección para transportar junto a su payload señalando de esta forma donde espera una respuesta. El NAT simple no opera en la capa cuatro por lo que la solución más idónea sería utilizar una Application Layer Gateway – ALG, pero falla cuando se usa encriptación.

Cuando se trata por ejemplo aplicaciones P2P, en donde, la conexión se establece entre cliente y servidores reales y cada conexión viene de cada cliente interno; en esta situación el NAT puede añadir un mapeo a la tabla, no obstante, puede suceder un desenlace cuando varios peers se conectan, por lo que es posible que escuchen la conexión. La solución es establecer cierta seguridad, es decir, que el peer localizado establezca la comunicación siempre y cuando la política de privacidad permita dicha conexión.

Y cuando se tiene la combinación de los dos casos anteriores como sería en el caso de FTP o SIP/SDP que tienen aplicaciones con sesiones incluidas en su payload referidas especialmente como sesión de control y de datos. El problema está en que no solo existe una dirección IP específica de un Internet público hacia un host privado, en lo que NAT no permite realizar este direccionamiento, por lo que es factible solventar con ciertas técnicas para resolver los problemas de NAT-T (NAT Transversal) como SIP, incluido Universal Plug and Play - UPnP, Simple Transversal of UDP through

NAT - STUN, Traversal Using Relay - TURN y Interactive Connectivity Establishment - ICE. Y entre otros.

4.3 Técnica para solventar los problemas de NAT

4.3.1 STUN

Simple Transversal of UDP, es un protocolo de red del tipo cliente/servidor que permite a clientes NAT encontrar su dirección pública y descubrir la presencia de NAT y/o Firewalls entre ellos e Internet. STUN trabaja con muchos NAT existentes y no requiere ningún comportamiento especial. Como resultado se obtiene una red variada de aplicaciones que pueden funcionar a través de la infraestructura NAT, como se indica en el algoritmo del Anexo 1.

[18] señala que está compuesto por un programa STUN servidor que tiene que estar disponible en la Internet, y por el cliente STUN que tiene que ser alojado dentro de la red que se encuentra tras el dispositivo NAT o Firewall. El cliente STUN genera peticiones STUN y este puede ser utilizado por un PC o puede ser ejecutado como elemento de red; y el servidor STUN es una entidad que recibe peticiones STUN y envía respuestas STUN como se indica en el ejemplo del Anexo 2.

Las principales características de STUN son:

- STUN activa un dispositivo para encontrar su dirección pública y tipo de NAT que da acceso a Internet.
- STUN opera en los puertos TCP y UDP.
- STUN se usa principalmente como complemento de protocolos como SIP como: señalización de tráfico de sonido, video y texto sobre Internet, sin embargo, no es soportado por todos los dispositivos VoIP.
- STUN puede usar registros DNS SVR para encontrar servidores STUN unidos al dominio.

Funcionamiento de STUN

Las peticiones de STUN especifican tres parámetros:

- Dirección de Respuesta
- IP cambiada
- Puerto cambiado

El cliente STUN envía una petición al servidor STUN y este enviará una respuesta a la dirección IP y puerto abierto por NAT, si se tiene:

- Que el campo no se encuentra definido, el servidor enviará la respuesta a la dirección IP y al puerto donde recibió la petición.
- Que la dirección IP de cambio y el puerto de cambio no están definidos, el servidor STUN responderá desde la dirección IP y puerto donde el paquete inicial fue enviado.
- Que la dirección IP está definida, el servidor responderá desde una dirección IP diferente.
- Que el puerto de cambio está definido, el servidor STUN responderá desde un puerto diferente.

La respuesta STUN contendrá la siguiente información:

- ***Dirección Mapeada:*** La dirección IP y puerto del cliente que es vista por el servidor STUN afuera del NAT, una vez recibida la petición STUN.
- ***Dirección Cambiada:*** La dirección IP que debería ser fuente de la respuesta recibida, si la petición tiene activada el flag de cambio de la dirección IP.
- ***Dirección Fuente:*** La dirección IP y el puerto donde la respuesta STUN fue enviada.
- ***Tipo de de NAT en uso.***

Cuando se usa una serie de peticiones hacia el servidor STUN, un cliente puede determinar:

- Si el equipo se encuentra disponible para conectarse a Internet.
- Si el equipo se encuentra detrás de un Firewall que bloquea UDP.
- Si el equipo se encuentra detrás de un NAT y qué tipo de NAT es.

STUN es aplicable para casos cuando NAT trabaja con Full Conexión, Conexión Restringida, Conexión Restringida por Puerto; ya que NAT creará un mapeo basado en una IP interna y número de puerto y consecuentemente ejecutará su función de acuerdo a la situación del cliente para traspasar entornos con NAT, por ejemplo: El cliente STUN bajo Linux se ejecuta colocando solamente la dirección IP del servidor STUN y el servidor STUN requiere dos interfaces de red con sus respectivas direcciones IP públicas configuradas.

4.3.2 TURN

Transversal Using Relay NAT – TURN, es un simple protocolo cliente – servidor y se entiende como una extensión de STUN para interceptar y modificar el tráfico para realizar de forma transparente la comunicación en la ausencia de cifrado y autentificación segura a través de conexiones TCP/UDP con direcciones IP y puertos diferentes, cuyo objetivo es dar solución a los problemas de NAT Transversal simétrico y Firewalls.

La solución consiste en un servidor TURN, el cual puede recibir y enviar respuestas TURN primero recibiendo datos con la dirección que provee el cliente para luego enviar estas a sus respectivos clientes.

TURN opera de la siguiente manera, como se indica en el siguiente diagrama de la Fig. 12.

Un cliente TURN se conecta a una red privada (red 1) y esta a su vez se conecta con otra (red 2) a través de NAT para conectarse respectivamente al Internet público, que en este caso será un servidor TURN que hace de repetidor o relé.

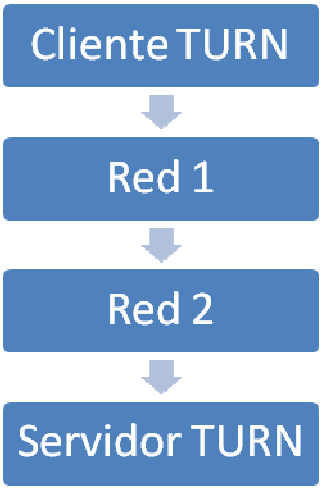


Figura 12. Diagrama TURN

Cuando se establece la comunicación entre el cliente TURN y el servidor TURN, el nuevo cliente TURN establecido envía una respuesta exploratoria que contiene tanto las direcciones IP mapeadas como los puertos del cliente para establecer los mensajes en ambos SIPs permitidos.

El servidor TURN empieza a enviar paquetes al cliente siempre y cuando este envíe paquetes de datos a la dirección IP y puerto mapeado.

TURN es útil cuando hay elementos detrás de un NAT simétrico o Firewall que quieren estar en el lado de recepción de una conexión con otro elemento exterior. Pero

la gran desventaja del protocolo TURN, es su costo para el proveedor del servidor TURN, ya que necesita un gran ancho de banda para la conexión con Internet; que por dependencia se refiere a la cantidad de tráfico transmitido tanto del tráfico que va al servidor como el que se envía del mismo hacia el objetivo SIP.

4.3.3 UNIVERSAL PLUG AND PLAY - UPnP

UPnP es un conjunto de protocolos de red para todas las redes residenciales sin dispositivos de clase empresarial que permite controlar la red de dispositivos, como ordenadores personales, impresoras, pasarelas de Internet, Wi-Fi de los puntos de acceso y dispositivos móviles para descubrir a la perfección la presencia del otro en la red y establecer funcionales los servicios de red para el intercambio de datos, comunicaciones y entretenimiento. La tecnología UPnP es probablemente uno de los métodos más confiables para UDP y TCP que permite controlar Internet Gateway Device [20].

Desafortunadamente UPnP posee una fuerte seguridad que a menudo es desactivada y que no puede ser usada por muchos NAT, la arquitectura UPnP como tal soporta el trabajo de una red sin configurar y automáticamente detecta cualquier dispositivo que se conecte a esta. De acuerdo a las pruebas realizadas por [21] en cuanto a las técnica para NAT Transversal con UPnP resulta que tan solo 36.42% de los dispositivos NATs permiten esta técnica.

La principal ventaja de UPnP sobre otras tecnología es que permite la fácil implementación de nuevos mapeos, y estos no necesitan ser consientes de las conexiones establecidas para especificar que puertos externos están encaminados hacia los puertos internos, lo cual simplifica a esta tecnología candidata idónea para descubrir y configurar ciertos dispositivos obteniendo su dirección IP, un nombre lógico y el NAT que puede ser establecido por el protocolo UPnP para informar a los demás de sus funciones y capacidad de procesamiento.

4.3.4 INTERACTIVE CONNECTIVITY ESTABLISHMENT (ICE)

ICE es una forma de NAT Transversal Peer to Peer para facilitar las comunicaciones de dos dispositivos SIP con la capacidad de mantener una sesión multimedia salvando todas las dificultades que el NAT pueda poner de por medio.

Cuando existe la convertibilidad de IPv4 a IPv6, se puede encontrar con diferentes escenarios que utilizan diferentes espacios de direcciones y redes privadas conectadas a Internet a través de NAT. Por ende, ICE permite que los dispositivos involucrados en

la sesión SIP prueben distintos medios o rutas para comunicarse entre sí y acuerden uno común. Por ejemplo:

Es posible con ICE, que dos terminales que se encuentran en la misma LAN envíen el tráfico RTP de manera local, en lugar de utilizar un relay como MediaProxy o RTP Proxy, sin realizar ninguna configuración exótica en el servidor. La inteligencia está en los terminales.

Entonces ICE funciona de acuerdo a nueve pasos, tales como:

a. OBTENSION DE CANDIDATOS

Antes de que se haga un acceso universal se obtiene la dirección IP y la combinación de puertos de dos candidatos tanto para los candidatos de host – host candidates (se incluyen enlaces VPN) como para los candidatos obtenidos al realizar consultas a un servidor STUN server – reflexive – candidates para poder leer la dirección IP pública y puerto permitidos por el NAT para el candidato. Finalmente se obtiene los contactos del cliente y candidatos transmitidos.

b. PRIORIDADES

Se aplican prioridades, para que exista preferencia entre candidatos; es preferible que el candidato del host sea más prioritario que uno de tipo transmitido.

c. INICIO - INVITACION

Se envía la invitación – INVITE al usuario correspondiente que se obtuvo de acuerdo a la prioridad, para que el SIP atraviese el NAT con mecanismos tradicionales.

d. OBTENCION DE CANDIDATOS - LLAMADO

Una vez que se recibe el INVITE, el llamado procede a detectar los posibles candidatos (host y server reflexive) de la misma manera que lo hizo el llamante y poder aplicar prioridades y construir la Sesión de la Descripción del Protocolo – SDP de la misma manera que se produjo con el llamante.

e. INFORMACION

Se procede a responder el INVITE por parte del usuario llamado (provisional o definitivo) y en su SDP habrá incluido información de sus candidatos.

f. VERIFICACION

Luego se emparejan los candidatos de ambos host (llamado y llamante) con los candidatos remotos para formar parejas de candidatos entre ambos. Estas parejas serán evaluadas por cierto orden de prioridad descendente por un controlador (el que hace la llamada). Posteriormente se empieza a realizar pruebas de conectividad mediante paquetes especiales STUN que contienen binding request y así se definirá el candidato idóneo. Cuando uno de los host involucrados en la sesión se encuentra tras un NAT simétrico, esto será detectado al ver la diferencia entre el candidato del servidor publicado y el origen del binding request que mandará. Entonces se crea un nuevo candidato de tipo peer reflexive, que contiene la dirección IP y puerto de la prueba de conectividad que se hacen enviando paquetes STUN a los puertos. Gracias a esto es posible que un usuario tras NAT simétrico y otro tras un NAT no simétrico hablen entre sí con audio de router a router.

Tras la negociación ambos agentes involucrados en ella han de terminar con un par de candidatos válidos por cada componente.

g. COORDINACION

El llamante elegirá un candidato. A éste proceso se le llama nominación. Para validar éste candidato se envía otra binding request (STUN) pero en esta ocasión se incluye un flags. Tanto el llamado como el llamante utilizarán el par de candidatos que ha pasado las pruebas de conectividad y que además esté nominado.

Hay que recordar que el proceso descrito por ICE ha sido realizado por los agentes utilizando paquetes STUN entre sí, sin ninguna interacción por parte del servidor.

h. COMUNICACIÓN

Ahora que el llamado y el llamante saben cómo comunicarse, ya pueden empezar la comunicación, y tenemos garantizado que habrá comunicación bidireccional, ya que las pruebas de conectividad se realizan en ambas direcciones.

i. CONFIRMACION

Aunque toda la negociación entre el llamante y el llamado, es posible y/o habitual que haya otros agentes externos en el medio de la señalización, como por ejemplo proxys. Para que los proxys o las middle-boxes entre el llamado y el llamante estén al tanto de lo sucedido, se enviará un re-INVITE o un UPDATE con el resultado de la negociación en el caso de que el candidato seleccionado no sea el candidato por defecto.

Aunque ICE trabaja con STUN y TURN sin sus desventajas, no lo hace un mecanismo perfecto a la hora de realizar la negociación para transmitir la información.

4.3.5 VIRTUAL INTRANET PLATFORM (VIP)

La Plataforma Virtual de Intranet nos ayuda a resolver problemas en los cuales muchos usuarios se encuentran de tras de un NAT o Firewall y que difícilmente puedan tener una dirección IP pública. Así, algunos hosts que se encuentran detrás de la NAT no pueden ser accedidos por los hosts que están detrás de otros NATs. No obstante, algunos sistemas P2P puede resolver este tipo de problemas, pero por desgracia, estos mecanismos solo se centran en aplicaciones específicas autónomas, contenidos particularmente en aplicaciones como: Skipe, BitTorrent. Por lo tanto, los mecanismos P2P y NAT Transversal no pueden ser reutilizados por otras aplicaciones directamente.

La solución para este tipo de problemas se centra en una plataforma para comunicaciones P2P para solventar problemas de NAT Transversal como VIP (Virtual Intranet Platform) con el uso de servicios público DHT – Open DHT como la información distribuida de la dirección y puerto.

No es necesario realizar cambios en la configuración del NAT, ya que todas las redes y los servicios de aplicaciones distribuidas detrás del NAT pueden hacer uso del VIP para comunicarse con otros servicios fuera del NAT.

VIP es mejor en rendimientos respecto a otras plataformas de tipo cliente/servidor en cuanto a ancho de banda, perdida de datos y problemas de transmisión. VIP es una Plataforma P2P más robusta y escalable, ya que no hay puntos de fallo en la plataforma, la estructura es de distribución y la mayoría de los datos de tráfico entre dos hosts detrás de la NAT se pueden transferir directamente sin necesidad de reinstalación.

4.3.6 ADVANCE NAT TRANSVERSAL SERVICE – ANTS

La idea principal de [22] de ANTS es usar previamente los conocimientos adquiridos acerca del comportamiento de NAT y los servicios para establecer nuevas conexiones. El concepto de ANTS está basado en el concepto de disociación del trabajo realizado por la técnica de NAT Transversal, es decir los procesos de recolección (gathering) desde el inicio de la utilización de dicha técnica; dando lugar a determinar el comportamiento del NAT y detectar los puntos finales de trabajo para cada aplicación y conexión establecida separadamente.

El establecimiento de conexiones ANTS depende de las entidades disponibles (hosts), por ejemplo cuando se tiene dos host comunicándose en dicha aplicación, un

servidor externo preguntará para intercambiar la información específica para posteriormente utilizar una técnica de NAT Transversal para crear el respectivo mapeo y establecer la conexión directamente.

La conexión tan solo se establece una vez en cada host y el proceso ANTS emplea por lo general servidores STUN, transmisión de datos y nodos de señalización para informar los servicios de los recursos de conexión disponibles (URI – Uniform Resource Identifier), que luego define una categoría de servicio en el SIP asignada en el DNS para establecer la técnica de NAT Transversal, la cual dependerá de muchos factores como el comportamiento del NAT, número de solicitantes (no todos están preparados para ANTS) y el rol de la de la aplicación. En resumen, el URI cumple con el papel de identificar un host detrás del NAT de acuerdo a la dirección establecida, este servicio – Service Request preguntará por un puerto en este host para realizar el mapeo correspondiente y enviar los endpoint públicos al solicitante (cliente).

La principal ventaja de ANTS es que está basado en XML y puede ser fácilmente usado con un gran número de infraestructuras de señalización como SIP y XMPP (Javer) [25], lo que lo convierte en un protocolo para la coordinación de casos distribuidos; y en comparación a ICE, es más flexible y rápido gracias a la verificación de conectividad desasociada.

4.3.7 MULTIPLE SUBSCRIBER VIDEOCONFERENCING SYSTEM

Representa un sistema, método y dispositivo para video conferencia. Este sistema incluye un switch instalado para videoconferencias como un punto de acceso a redes IP y suscriptores registrados para servicios de videoconferencia, cada uno tiene pluralidad de endpoints.

Este método incluye establecimientos de subscritores específicos para recibir y ser aplicados en múltiples llamadas de videoconferencia desde varios endpoints asociados con cada subscritor. Además este método incluye un almacenamiento de subscritores específicos establecidos para acceder al switch, y poder configurar el switch para conectar con llamadas desde los endpoints a cada subscritor basado en su correspondiente subscritor establecido.

Para el caso de NAT o Firewalls, este tipo de sistema se basa en presubscritores básicos configurados sin el switch para proveer servicios NAT desde un grupo consistente de SIP – NAT y H.232 – NAT. La aplicación H.232/SIP inicia el control da datos abriendo y cerrando puertos para el control de tráfico, la información que se obtiene dese el inicio es enviada al hardware de la red de datos. Al configurar los Firewall se incluye la información de las direcciones añadidas dentro de un contenedor (gatekeeper) para la zona, estableciendo puertos o canales que están estáticamente abiertos y estableciendo seguridad de inicio.

Para el modulo de NAT H.232, se configura el modulo NAT al iniciar la cabecera de los paquetes y la carga útil de los datos de control de Q.931/H.245 durante el establecimiento de la llamada. Además el modulo de NAT es configurado con el propósito de sustituir las direcciones IP y puertos de los endpoints no ruteables con sus propias direcciones IP de los proxys y números de puertos. Para el caso de los datos entrantes, los sustitutos del NAT no ruteables o las direcciones IP de los endpoints internos y puertos usan direcciones IP y/o puertos almacenados en la información del mapeo.

4.3.8 TRAVERSAL OF NON – PROTOCOL AWARE FIREWALLS AND NATS

Este método se basa en los métodos antes descritos, añadiéndole otro esquema llamado Traversal of Non – Protocol Aware Firewalls and NATs. Esta solución usa una combinación de técnicas incluyendo túneles y paquetes para atravesar NAT. El sistema no requiere que los Firewalls o NATs sean actualizados, y constituye un método seguro por usar técnica de tunneling.

4.3.9 MASMCT - MULTI-AGENT SYSTEM FOR MULTIMEDIA COMMUNICATION TRAVERSING NAT AND FIREWALL

La existencia de redes IP, compromete cada día a garantizar las comunicaciones multimedia para NATs y Firewalls. La existencia de métodos para atravesar NAT no son adecuados para proveedores del servicio en cuanto al establecimiento de un sistema real en NGN – Next Generation Networks.

Multi-agent System for Multimedia Communication Traversing NAT and Firewall es dado para resolver problemas a larga escala en NGN tanto para empresas como para subscritores, su arquitectura consiste de dos capas multi – agentes y puede ser clasificado como agente – cliente y agente – servidor, los cuales en el MASMCT son transparentes para usuarios endpoints y softswitch. Su función consiste en capturar y transmitir llamadas señalizando mensajes y mediadatos entre los endpoints y softswitch.

MASMCT tiene como aspecto clave su mecanismo y funcionalidad para establecer la comunicación de forma segura y fácil para los proveedores de servicio en NGN, ya que este método no necesita actualizar la existencia de los dispositivos como Firewalls, NATs o simples endpoint de lo subscritores; es así, que MASMCT al compararlo con otras soluciones es fiable, usando una buena seguridad en TLS - Transport Layer Security y técnica tunnel.

MASMCT está preparado para soportar protocolos que empleen TCP, por ejemplo H.323.

4.3.10 A NEW TUNNEL SCHEMME FOR MULTIMEDIA COMMUNICATIONS TRAVERSING NAT IN NGN

Este método es considerado de nueva generación y con mejoras respecto al MASMCT básico (Multi-agent System for Multimedia Communications Traversing NAT). Esta técnica moviliza el agente controlador dentro de una red privada incorpora la función de señalización en una red pública en el softswitch. Además este método realiza algunas transmisiones para establecer tiempos de llamadas gracias al desempeño que cumple el agente de llamadas del cliente (CCA – Call Client Agent) basado en MASMCT.

4.3.11 NAT FRIENDLY SIP

NAT Friendly SIP, [26] permite atravesar NAT que usen TCP y UDP sobretodo cuando el NAT está en el cliente y los proveedores quieren y/o necesitan el SIP, la solución sería realizar protocolos de NATs amigables.

De acuerdo a lo estipulado y propuesto en [27], este método busca ignorar las direcciones IP en el SIP/SDP donde sean posibles (obteniendo la información desde la conexión de transporte de estos), además busca realizar aplicaciones peer to peer como cliente servidor, y necesariamente debe depender del DNS. De allí que:

- SIP en UDP no es NAT Friendly, y utiliza puertos para establecer la conexión.
- SIP en TCP es NAT Friendly, y realiza envíos de respuesta de la existencia de conexión.

La conexión se establece cuando se registra al cliente usando la dirección IP y el puerto de donde ha venido (responde al INVITE), siendo esta conexión algo persistente sobre TCP; posteriormente los clientes deben escuchar el interfaz por header para que las llamadas sean ruteadas al destino a través de NAT.

NAT Fiendly tiene por objetivo manipular el SIP, para notificar la existencia de NATs para integrar un SIP ALG dentro de empresas NATs y así parar la circulación inconsciente de productos comerciales NATs. Este método propuesto en [27] es recomendable en empresas NATs y NATs residenciales que no tengan que configurar los dispositivos o sus configuraciones para conseguir SIPs adecuados para la transmisión de información.

4.3.12 MIDCOM – UNAWARE NAT/FRIENDLY TRAVERSAL

Este método tiene dos piezas claves para solucionar los problemas de NAT Transversal, tales como:

- Un servidor Proxy Signaling para la señalización de la trayectoria a seguir.
- Un servidor Proxy Media para la trayectoria media de la conexión.

La trayectoria o ruta señalizada dependerá del servidor Proxy SIP llamado Back – to – Back – User – Agent (BBUA) y para la ruta media es un servidor Proxy RTP, respectivamente para el establecimiento de las conexiones SIP y RTP. Estos dos componentes utilizan un protocolo de control para usuarios finales.

La ruta señalizada debe estar siempre abierta a través del NAT para mantener un mecanismo activo, ya que la dirección IP y puerto permitidos por el NAT deben ser retornados al header del contacto del cliente, que previamente han sido enviados por el servidor Proxy. Así esto permite, que la UA o estaciones de servicio realizar la detección de NAT y/o Firewalls en un tiempo prolongado y para el cambio de direcciones IP para NAT Transversal.

4.3.13 APLICATION LEVEL GATEWAY – ALG

El mecanismo en el cual los dispositivos Firewalls y NATs son construidos, necesita conocer la dirección IP para enviar y recibir datos. Además necesita tener conocimiento de los protocolos de donde pueda extraer, usar o alterar la dirección IP y puerto. De aquí que la forma de realizar esto es a nivel de aplicación, sería la utilización de ALG – Aplication Layer Gateway, el cual debe ser diseñado para ser un protocolo – aware para especificar protocolos en SIP basados en ambientes multimedia (VoIP).

Usualmente ALG se fusiona con el NAT para:

- Crear el mapeo de información de las IP privadas a públicas.
- Posteriormente usa este mapeo para traducir los mensajes SIP.

Lleva un control de las nuevas llamadas entrantes para mantener una lista de acceso configurable de las direcciones de entidades multimedia, para llevarlas a direcciones IP públicas, puertos, los cuales son mapeados de regreso por el NAT a la dirección IP privada de origen y los puertos de los endpoints del SIP que están detrás de este.

Ejemplo:

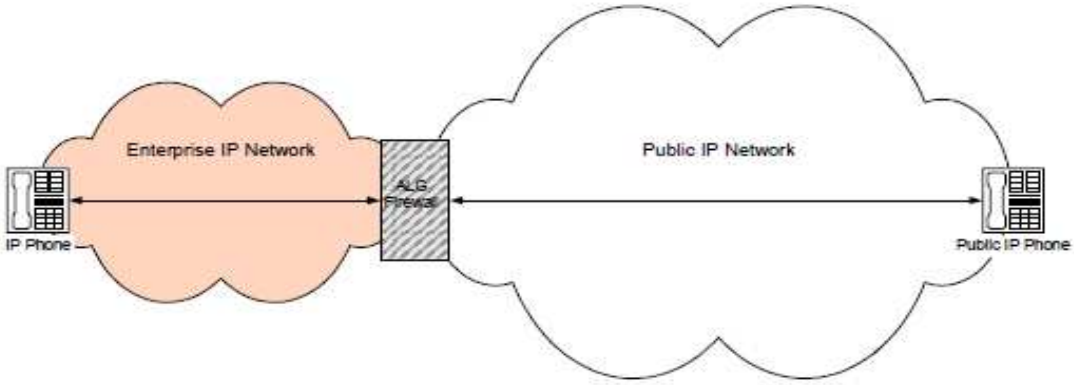


Figura 13. Protocol Aware Firewall

De acuerdo a la Fig. 13, se muestra el establecimiento de un SIP, que consiste en la conexión de una red interna de una empresa con una Red Pública de fuera, vía protocolo – aware ALG Firewall.

ALG propone una solución a considerar en los siguientes pasos:

- Descubrimiento del NAT: Se configura el nombre del Host del servidor web, para lo cual se envía al DNS del servidor una consulta para resolver el nombre del host del servidor web a una dirección IP (vía DHCP).
- El DNS del servidor responde con la dirección IP del servidor web.
- El cliente SIP (Enterprise IP Network) establece una conexión con el servidor web (Public IP Network) y envía una respuesta HTTP.
- El servidor web responde con la dirección IP del NAT
- El cliente SIP envía una respuesta INVITE destinada al SIP del proxy.
- El SIP del proxy reenvía el INVITE al otro cliente.
- Se establece respectivamente los ACK para permitir el mapeo de la información.
- Establecimiento total de la comunicación (VoIP).

En el sistema, cuando se implementa los esquemas de seguridad, se tiene un inconveniente, que ocurre cuando los mensajes del protocolo son encriptados y ALG no es una capa de aplicación fiable en posesión de necesidad de claves y algoritmos.

Muchos de los Firewalls desarrollados en las redes de hoy no son multimedia protocol – aware, los cuales deben ser actualizados. En la actualidad, las redes con dispositivos NAT y/o Firewalls son usualmente desarrollados a lo largo de la ruta transversal de los stream multimedia. De allí, que para asegurar, cada Firewall necesita ser un protocol – aware ALG. Sin embargo el protocolo ALG no es aplicable en ambientes SOHO, donde los dispositivos simples NATs son ampliamente usados.

En el mercado de la tecnología, los vendedores y desarrolladores de ALG permiten desarrollar y agregar tres funcionalidades adicionales, como la seguridad, estabilidad y cuestiones de mantenimiento. De allí que hay numerosas técnicas y soluciones para problemas de NAT transversal en escenarios multimedia típicamente para conexiones de aplicaciones de redes de cliente – cliente en el Internet involucrando hosts conectados en redes privadas, especialmente en desarrollo de aplicaciones Peer to Peer y VoIP (por ejemplo para aplicaciones P2P es BitTorrent) y sistemas con la presencia de pares de NAT homogéneos y heterogéneos.

Hay muchos casos resueltos de NAT, pero no todos son aplicables y reusables para otras aplicaciones, sin embargo, el método utilizado en Skype basado en romper conexiones intermedias para registrar comunicaciones pares y puede usarse en otras aplicaciones P2P. Posibles aplicaciones para resolver NAT como el UDP Hole Punching que permite a dos clientes establecer una sesión UDP P2P directa.

4.3.14 MIDDLEBOX COMMUNICATION (MIDCOM)

Middlebox Communications – Midcom es un concepto emergente que hace que los dispositivos de Firewalls y NAT sean más controlables a través de terceras partes.

La idea de Midcom es permitir la tercera parte en cuanto a aplicaciones confiables para tomar decisiones políticas de nombres de entidades middle en cuanto a aplicaciones de políticas de transporte. Estas aplicaciones confiables podrían comunicar sus necesidades de los dispositivos en el "middle" usando el nuevo protocolo definido por Midcom. Las terceras partes ayudan a los dispositivos Firewalls o NATs a operar sin tener que recurrir a incrustar aplicaciones inteligentes. Esto requiere que los dispositivos NATs continúen proporcionando servicios de seguridad mientras restan protocolos agnósticos a nivel de aplicación.

Las comunicaciones Middlebox enfocan soluciones de problemas de comunicaciones encriptadas. Desafortunadamente, los esquemas propuestos por esta tecnología, especialmente en ambientes NATs. Middlebox toma el rendimiento de las direcciones de las empresas de redes, cuando un servidor del protocolo IP multimedia como un proxy SIP o un gatekeeper estándar sea desarrollado a como de lugar.

Middlebox consta con un protocolo agente que es un protocolo agnóstico, el cual se ejecuta en los Firewalls. Así, el desarrollo de Firewalls que soporta un protocolo Midcom teóricamente permite para una infraestructura común que soporte todos los protocolos de aplicaciones incluyendo varios Multimedia en protocolos IP.

La solución adecuada sería que las empresas manejen sus propios Firewalls. Así, que para la seguridad, se propone que los proxys SIP o gatekeeper estándar es usualmente localizado detrás del Firewall y el protocolo de control puede así dinámicamente proveer información de configuración como listas de acceso.

Teóricamente, Midcom es indicado para ISP, porque un ISP podría usar un protocolo Midcom para controlar un Firewall o NAT desde el exterior de una Red Privada. Prácticamente, esto es poco probable por razones de seguridad. Además, en la práctica, los usuarios usan dos servicios proveedores diferentes: uno como proveedor de transporte y el otro como servicio proveedor multimedia o de conferencia.

5. CONCLUSIONES Y OBSERVACIONES

En primera instancia, el supuesto agotamiento de los rangos de direcciones IPs utilizables en Internet ha obligado a utilizar direcciones IP privadas dentro de las redes de las empresas y usuarios domésticos. Por lo que un equipo IP para ser alcanzado en Internet debe utilizar una IP pública para sus comunicaciones con el propósito de enmascarar la red interna en una o varias IPs públicas.

Hace hincapié a la invención de NAT, en la detención del agotamiento de las direcciones IP válidas, porque permite que varios hosts dentro de una red privada, tengan acceso a Internet con sólo usar unas pocas direcciones IP válidas. Esta es una gran ventaja porque le dio un respiro a IPv4 para que no colapse rápido y dio tiempo para la creación de una nueva versión de IP (IPv6) que solucione el problema de agotamiento de direcciones.

NAT no solamente constituyen una forma de traducción, sino que al igual que los Firewalls son las principales barreras a la adopción generalizada de la tecnología Internet extremo – extremo como VoIP, aportando de cierta seguridad, porque los hosts de las redes externas no conocen las direcciones verdaderas de los hosts que se encuentran dentro de una red privada. NAT hace que sea difícil poder realizar un ataque desde hosts externos o simplemente conseguir información, lo cual se torna complejo atravesar esos obstáculos y es por eso surge técnicas como STUN, TURN, ICE y otras mencionadas en el documento escrito que proporcionan una excelente metodología para abordar este tema.

De acuerdo al análisis realizado, la funcionalidad de STUN y TURN representan protocolos livianos que permiten a las aplicaciones funcionar detrás de entornos NAT y determinar las direcciones IP públicas con las propiedades de asignación de puertos y reglas de filtrado asociados con conexiones TCP a través de NAT.

Cuando se considera ICE, se está estimando una forma de NAT Transversal para comunicaciones Peer to Peer para facilitar las comunicaciones de dos dispositivos SIP con la capacidad de mantener una sesión multimedia salvando todas las dificultades que el NAT pueda poner de por medio. De las tecnologías estipuladas en este trabajo, el ICE es una metodología muy compleja y su implementación real requiere considerable conocimiento y experiencia para hacerlo bien.

Consideraciones a tomar:

TURN es una extensión de STUN.

VIP es un método que solo se centra en aplicaciones específicas autónomas, como: Skipe y BitTorrent.

El proceso ANTS emplea servidores STUN, transmisión de datos y nodos de señalización para informar los servicios de los recursos de conexión disponibles.

Multiple Subscriber Videoconferencing System incluye un switch instalado para videoconferencias como un punto de acceso a redes IP y suscriptores registrados para recibir y ser aplicados en múltiples llamadas de videoconferencia

5.1 Trabajos Futuros

En la actualidad la existencia de Redes IP, compromete cada día a garantizar las comunicaciones. Sin embargo, el estableciendo de métodos confiables para impugnar el acceso a Redes Públicas o Externas, resulta muchas veces obsoleto y/o complejo dependiendo de cada servicio o aplicación, por lo que muchas empresas han visto la necesidad de implementar mecanismos que cooperen con la extracción de información como es el caso de NAT.

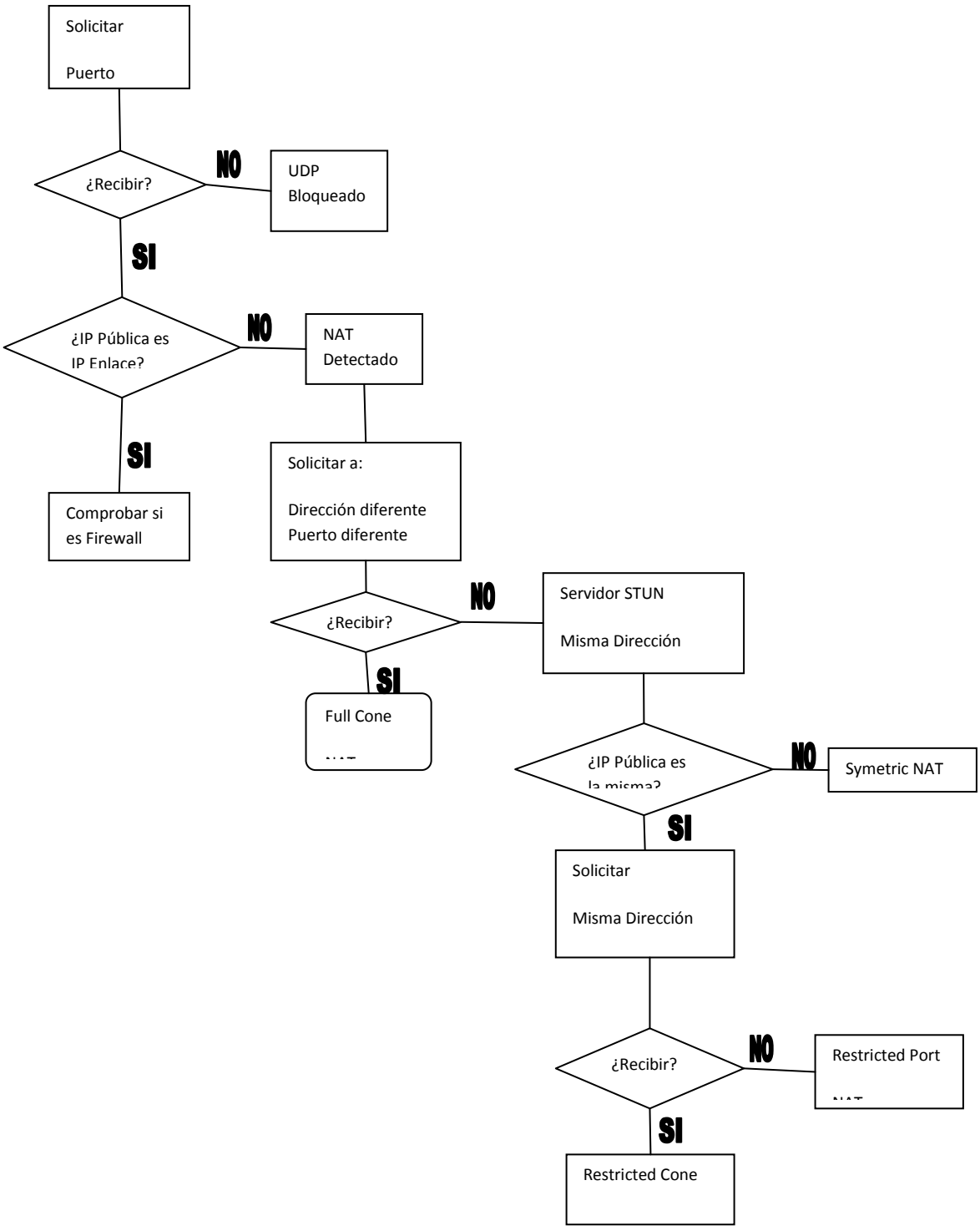
Queda para futuras investigaciones nuevos métodos y tecnologías a experimentar con la finalidad de acaparar la mayoría de casos, Pero las soluciones de NAT, no siempre son adecuados para todas las adversidades que se presentan, especialmente para proveedores del servicio en el establecimiento de un sistema real en Next Generation Networks, no obstante, van a seguir siendo utilizadas las existente y desarrollando nuevas soluciones NAT hasta que se implemente en su totalidad el uso de IPv6, que se prevé aproximadamente hasta el 2017.

Para finalizar, surge la necesidad de estudiar e investigar por parte de las empresas los problemas de NAT, a causa de los costos relacionados a las soluciones para atravesar NAT en una red extremo – extremo para los modelos de servicio mencionados, que por lo general son muy elevados dependiendo de la cantidad de tráfico que se gestione.

6. ANEXOS

6.1 ANEXO1.

ALGORITMO STUN

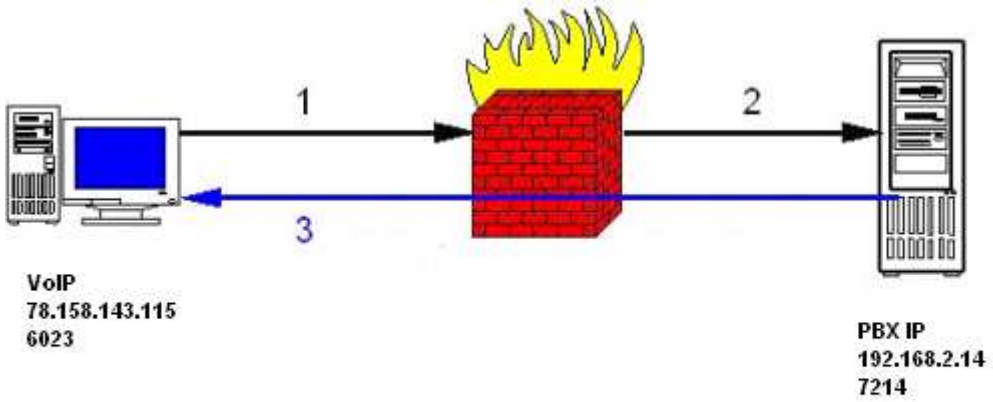


6.2 ANEXO 2.

EJEMPLO STUN

Este ejemplo está basado en el dominio voipproducts.org.

A continuación se muestra la captura de un mensaje SIP Register. Un terminal de VoIP basado en SIP, está instalado detrás de un router con NAT, intenta registrar la extensión 101 en una PBX IP que está fuera de la red local.



Mensaje cuando no se emplea el protocolo STUN:

```
REGISTER sip:voipproducts.org SIP/2.0
Via: SIP/2.0/UDP 192.168.2.14:7214;branch=z9hG4bK-d8754z;rport
Max-Forwards: 70
Contact: : <sip:101@192.168.2.14:7214;rinstance=0639bae5043c66ac>
To: “account1? <sip:101@voipproducts.org>
From: “account1?<sip:101@voipproducts.org>;tag=0a75d76e
Call-ID: OTcxMDU5MGNhNTAxNzgzYjZkODVkY2I3MmE3NDhlNzQ.
CSeq: 1 REGISTER
Expires: 3600
Content-Length: 0
```

78.158.143.115 y puerto 6023 solicita que la centralita remota intente establecer una conexión enviando mensajes SIP a la dirección IP 192.168.2.14 y puerto 7214. Evidentemente, dado que es una dirección privada de otra red, el mensaje no es enrutable y lo más probable es que el router lo pierda. Al perder el paquete no se puede establecer la conexión.

Cuando funciona con la resolución STUN:

Si un teléfono VoIP tiene habilitada la resolución con STUN y se especifica un servidor STUN, el teléfono VoIP envía a servidor STUN una solicitud de resolver la resolución y espera la contestación del servidor. A continuación se muestra los mensajes.

```
Message Type: Binding Response(0×0101)
Message Length: 0×0044
Message Transaction ID: E753D76EA857A24DA38A229F7576E18E
```

Este apartado señala el: Tipo de Mensaje, Longitud del Mensaje y un Identificador único que se emplea en cada seción STUN de binding/response.

```
Attribute: MAPPED-ADDRESS
Attribute Type: MAPPED-ADDRESS(0×0001)
Attribute Length: 8
Protocol Family: IPv4 (0×0001)
Port: 6023
IP: 78.158.143.115 (78.158.143.115)
```

MAPPED ADDRESS indica el origen de la solicitud IP.

```
Attribute: SOURCE-ADDRESS
Attribute Type: SOURCE-ADDRESS(0×0004)
Attribute Length: 8
Protocol Family: IPv4 (0×0001)
Port: 3478
IP: 10.252.131.113 (10.252.131.113)
```

SOURCE ADDRESS se emplea para indicar si se emplean configuraciones NAT dobles. En el ejemplo se ve que se emplean configuraciones NAT dobles, puesto que la dirección IP del teléfono es 192.168.2.14, la IP pública desde la que se recibió el Binding es 78.158.143.115 y la dirección IP desde la que se contactó la última vez al servidor STUN era 10.252.131.113.

```
Attribute: CHANGED-ADDRESS
Attribute Type: CHANGED-ADDRESS(0×0005)
Attribute Length: 8
Protocol Family: IPv4 (0×0001)
Port: 3479
IP: 75.101.138.128 (75.101.138.128)
```

CHANGED ADDRESS indica la dirección IP y el puerto desde el que habría que haber enviado la respuesta.

Mensaje cuando no se emplea el protocolo STUN:

```
REGISTER sip:voipproducts.org SIP/2.0
Via: SIP/2.0/UDP 192.168.2.14:7214;branch=z9hG4bK-d8754z;rport
Max-Forwards: 70
Contact: <sip:101@78.158.143.115:8676;rinstance=c82d2f5b1918e5cf>
To: “account1?<sip:101@voipproducts.org.com>
From: “account1?<sip:101@voipproducts.org>;tag=484b4e36
Call-ID: YWI3Y2I3ODIzOWIxYWI5NDQwMzA5ZTYxMTAzOTM4Y2I.
CSeq: 1 REGISTER
Expires: 3600
Content-Length: 0
```

El cliente de VoIP está a la escucha en la dirección IP interna (192.168.2.14) y en el mismo puerto (7214).

En el campo “Contact” del mensaje SIP de registro, el teléfono VoIP sustituye su dirección IP (192.168.1.14) por la dirección IP externa (78.158.143.115) y el puerto externo (8676) que lo ha encontrado gracias a una resolución STUN que hizo antes de registrarse con la PBX.

“La resolución STUN permite que la PBX IP pueda establecer una conexión con el teléfono VoIP enviando respuestas SIP a la dirección 78.158.143.115 en el puerto 8676 que está mapeado por el NAT a la dirección 192.168.2.14 puerto 7214”.

La mayoría de los protocolos que se utilizan en llamadas de VoIP basadas en SIP emplean UDP como protocolo de transporte, que es un protocolo "connectionless", de ahí que STUN tenga un papel muy importante para que las entidades SIP que está detrás de NATs puedan establecer una llamada de VoIP.

7. BIBLIOGRAFIA

[1] RFC 1930, http://tools.ietf.org/html/rfc1930

[2] RFC 1166, http://www.rfc-editor.org/rfc/rfc1166.txt

[3] RFC 791, http://www.ietf.org/rfc/rfc791.txt

[4] RFC 2460, http://www.ietf.org/rfc/rfc2460.txt

[5] RFC 2893, http://www.ietf.org/rfc/rfc2893.txt

[6] RFC 3053, http://www.faqs.org/rfcs/rfc3053.html

[7] RFC 163, http://www.ietf.org/rfc/rfc163.txt

[8] RFC 4966, http://www.ietf.org/rfc/rfc4966.txt

[9]Connect to the M6Bone Network, Monday April 5th, 2004. http://www.m6bone.net/article.php3%3Fid_article=37.html

[10] Creación de una Isla IPv6 y Conexión al 6Bone, Horacio J. Peña. http://www.uninet.edu/6fevu/text/isla6bone.html

[11] RFC 2765, http://tools.ietf.org/html/rfc2765

[12] RFC 2766, http://www.ietf.org/rfc/rfc2766.txt

[13] RFC 1928, http://www.ietf.org/rfc/rfc1928.txt

[14] RFC 3142, http://tools.ietf.org/html/rfc3142

[15] RFC 2767, http://www.ietf.org/rfc/rfc2767.txt

[16]RFC 1918, http://tools.ietf.org/html/rfc1918

[17] RFC 3027, http://tools.ietf.org/html/rfc3027

[18] J. Rosenberg. Session traversal utilities for NAT (STUN). RFC 5389. Internet Engineering Task Force. October 2008. http://www.ietf.org/rfc/rfc5389.txt [January 2010]. 24

[19] J. Rosenberg. Traversal using relays around NAT (TURN): Relay extensions to session traversal utilities for NAT (STUN), draft-ietf-behaveturn.

[20] Traversal Using Relay NAT (TURN). http://www.jdrosen.net/papers/draft-rosenberg-midcom-turn-07.txt

[21] UPnP-Forum. Internet gateway device (IGD) standardized device control protocol. November 2001. http://www.upnp.org [January 2010]. 25

[22] http://131.159.15.247/pubs/globecom09-draft.pdf, 3

[23] Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for the Session Initiation Protocol (SIP). http://www.jdrosen.net/papers/draft-rosenberg-sipping-ice-00.html

[24] Xugang Wang and Qianni Deng, VIP, A P2P Communication Platform for NAT Traversal, Grid computer Center – Department of Computer Science, Shanghai Jiao Tong University, China. http://www.springerlink.com/index/325u163386607p15.pdf

[25] http://www.jabber.org/

[26] https://tools.ietf.org/html/draft-rosenberg-sip-entfw-02

[27] J. Rosenberg, J.Weinberger, and H.Schulzrinne. NAT friendly SIP , Internet Engineering Task Force Internet-draft. Work in progress, expires February 2002. http://www.softarmor.com/wgdb/docs/ draft-rosenberg-sip-entfw-02.txt. 29

[28] Francisco José Blázquez Sánchez, Diseño y Desarrrollo de un Marco de Pruebas y Detección de NATs, Universidad Carlos III, Madrid 2009. http://e-archivo.uc3m.es/bitstream/10016/9826/2/PFC_Francisco_Jose_Blazquez.pdf. 88-112

[29] Irena Trajkovska, A Research Platform for Hybrid Models Between Cloud Computing and Open Source Paradigms like P2P Streaming and Voluntary Computing with QoS cost functions, Universidad Politécnica de Madrid, Madrid 2010, 15-30.

[30] Integración de Redes. http://www.scribd.com/doc/9566149/IPv6.

[31] Una Panorámica de los Mecanismos de Transición, Javier Sedano, David Fernández, Universidad Politécnica de Madrid, http://www.6sos.org/pdf/panoramica_de_los_mecanismos_de_transicion_a_ipv6.pdf, 2004.

[32]Herramientas de Transición a IPv6. http://dspace.ups.edu.ec/bitstream/123456789/205/3/Capitulo%202.pdf

[33]Bump in the Stack. http://www.networkdictionary.com/Networking/Bump-in-Stack.php

[34]Bump in the API. http://www.networkdictionary.com/Networking/Bump-in-API.php

[35] BEHAVE WG. July 2009. http://tools.ietf.org/html/draft-ietf-behave-turn-16 [January 2010]. 25