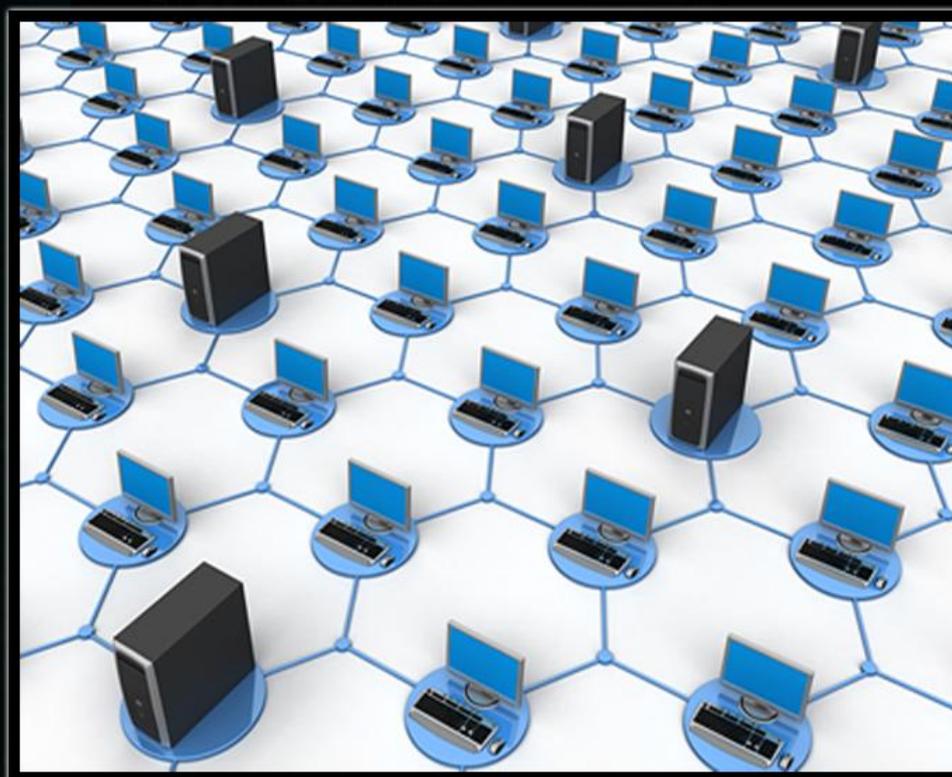


UNDERCODE

TALLER DE REDES



TEMAS

COMPONENTES DE UNA RED
TARJETAS DE RED
SWITCH
ROUTERS
FUNCIONAMIENTO DE UNA RED
PROTOCOLOS
IP PUBLICA / PRIVADA
Y MUCHO MÁS...!

TUTORES

CLOUDSWX
GABRIELA

INTRODUCCIÓN

Cuando comenzamos esta saga de talleres decíamos: "El siguiente texto está dirigido a personas que recién están comenzando a dar sus primeros pasos en el mundo de las redes y la informática, por tanto nuestro propósito es explicarles de forma sencilla cómo es que funciona toda la magia detrás de las luces que parpadean y los botones de "conectar". Está dirigido a nuestra comunidad Underc0de, a sus underc0deanos que son hermanos hijos de otras madres y a todo aquel que le pueda sacar algún provecho."

Saludos, nuevamente hermanos, espero les haya gustado la primera parte del [taller de redes](#) que esta publicada en esta misma sección (por si no lo encuentran en la sección, el enlace esta agregado en el *keyword* "taller de redes" de este párrafo). Después de haberles saludado, que les parece si encendemos los motores y nos embarcamos en el episodio numero 2 de este extraño taller de redes.

1. COMPOSICIÓN MOLECULAR DE UNA RED INFORMÁTICA

El título suena un poco fuera de contexto ¿no? ¿Cómo es eso de la composición molecular de una red? ¿Acaso es un ser vivo? Pues visto desde mi óptica, una red informática es todo un ser viviente, es un ecosistema, un universo que fluye dentro de un cierto caos ordenado, pero dentro de ese caos existen órganos, componentes que hacen posible el funcionamiento de una red, así ¿qué les parece si los explicamos?

1.1. COMPONENTES DE UNA RED

Sé que algunos, quizás están esperando el clásico sermón técnico sobre los dispositivos de una red, pero los que ya se leyeron el primer taller saben bien que aquí pasamos de esas cosas y más bien explicamos de una forma divertida que haga una idea clara en las mentes sobre lo que deseamos explicar, así que aquí vamos.

1.1.2. TARJETAS DE RED

Tu computadora es un aparato magnífico, es un templo de cálculos, códigos, funciones y cosas chulas que puedes hacer (usar Paint, jugar Solitario o al Busca Minas); pero si no puedes conectarte a la red se convierte en algo así como una prisión de la que no puedes escapar, una cárcel que te aísla del resto del universo, tienes tanta información para compartir, tanta información para buscar, pero tu sistema operativo no puede hacerlo por sí solo, necesitas algo que te conecte a la red, algo por donde enviar y recibir esos "1" y "0" de los que hablamos en la primera entrega, y este componente mágico que nos libera de la prisión es "la tarjeta de red". Existen de varios tipos y formas, pero para no liarla mucho que les parece si las definimos en:

a) Tarjetas Ethernet

Esas que tienen un extraño agujero cuadrado por donde conectamos el mágico cable que nos libera.



b) Tarjetas Inalámbricas

Estas son la magia en su más alta expresión, nos conectan al universo sin cables y de forma invisible, (conectarse al mundo nunca fue más sencillo).



Ahora bien, **cada tarjeta de red** tiene un nombre, un valor único, una dirección física conocida como **Dirección MAC** formada por 16 caracteres que suele verse más o menos así: **AB:CD:EF:01:23:45**

Las direcciones MAC tienen diferentes usos, mas adelante veremos uno de ellos cuando estemos explicando los protocolos.

1.1.3. MEDIOS

Para lograr transmitir los "1" y los "0" se necesita de un medio, es decir un algo físico por donde se pueda hacer fluir los bits; para hacer una analogía piensen en un

flujo de agua que necesita llegar a una casa, es necesario una tubería que haga llegar el líquido a su destino. Pues del mismo modo, en las redes se necesitan medios que lleven los bits a la siguiente parada. En una red cableada el medio sería "el cable ethernet", en una red inalámbrica el medio sería... A ver, ¿quién adivina? ... Espero que todos hayan dicho: "el aire" pues sí, en una red inalámbrica el medio es el aire, a través del que se transmiten ondas de radio que tanto el destino como el origen puedan entenderse, esta parte la explicaremos en las entregas venideras, así que tranquilos.

1.1.4 SWITCH

Aquí comienza lo complicado ¿no pensarían que todo sería chistes y lindas historias? (risa malévol). Resulta que lo más normal es que varias computadoras se conecten a la red (obvio, por ello es una red de computadoras), pues cuando varias computadoras se conectan a la misma red cableada necesitan -por así decirle- alguien que ordene la forma en que acceden al medio (¿recuerdan?); es decir, varias computadoras comparten un mismo medio y necesitan alguien que controle quien usa el medio; así que podríamos definir a los **switches** como dispositivos que controlan y permiten el acceso al medio, y aquí el más listo levanta la mano y pregunta:

¿Es decir que en una red inalámbrica también hay switches? La respuesta es "no", no existen los switches como aparatos físicos, pero existen métodos para controlar el acceso al medio. Si se quedan con nosotros en las próximas entregas prometo explicarlo, por ahora vamos a caminar para luego correr.



[Los switches se valen de las direcciones MAC para identificar los equipos conectados a él. Una dirección MAC es un valor único asignado por el fabricante de las tarjetas o dispositivos de red]

1.1.5 ROUTERS

Espero que todos recuerden al señor "Rutenio", pues imaginen que en una red local (esas que tenemos en nuestras casas) podemos comunicar nuestras portátiles, nuestros celulares, nuestros televisores y compartir información entre todos usando solamente un "switch" que va a controlar nuestro acceso al "medio" -hasta aquí todo perfecto-. Ahora, si venimos leyendo desde la tarjeta de red, hemos visto como nuestra libertad va creciendo cada vez más, pues aquí es donde daremos el gran salto. Si tuviésemos la necesidad de comunicarnos con "otra" red necesitaríamos a un **router**. Un router es la puerta de salida hacia el mundo, creo que me animo a contarles una historia para explicarlo.

"En mi país las bodegas de provisiones y alimentos tienen un nombre muy peculiar, se les dice "colmados", y éstos tienen una facilidad muy importante y es que tienen servicio de entrega a domicilio. Si llamas por teléfono y pides algo, te lo envían a tu casa, lo cual es muy cómodo. Consecuencia de ello, los empleados que hacen las entregas conocen casi todas las calles y los números de edificios, pero cuando alguien pide algo en una dirección que nadie conoce, el indicado es Javier, un muchacho que conoce no solo las direcciones cercanas, sino también las más lejanas y es así como todo paquete que no tenga una dirección local es pasado a Javier para su correcta entrega."

El *router* debe tener una dirección IP a la cual enviarle los paquetes que vayan a otras redes, se le conoce también como:

"Default Gateway"

"Puerta de enlace"



Vamos a ver... Si están en Windows, vayan a su botón de inicio y escriban "cmd" (sin las comillas), presionen ENTER y tendrán esa ventana negra y abismal que usamos los hackers para meternos en todas partes. Ahora les daré un comando que

cambiará el mundo: escriban "ipconfig" y presionen ENTER entre toda la información que verán busquen las palabras por las que se conoce normalmente al *router*...

...

....

.....

¿Ya?

....

.....

¡Bien! ahora identifiquen la dirección IP que tiene asignada...

....

.....

....

.....

.....

¡¡¡Bien!!! ¡¡¡Muy bien!!! Recuerden la porque la usaremos más adelante.

Una red puede estar compuesta por muchos más elementos, con diferentes funciones, pero vamos de a poquito para que al final todos entendamos de qué va el asunto. Cabe aclarar que en muchas ocasiones la compañía que nos brinda el servicio de internet (ISP) nos instala un dispositivo que hace de *router* y de *switch* a la vez, con lo cual es poco probable que tengamos un *switch* particular instalado en nuestras casas.

2. ¿CÓMO ES EL FUNCIONAMIENTO DE NUESTRA RED?

Muy bien hermanos, llegados hasta aquí es hora de explicar los mecanismos lógicos que hacen que nuestra red funcione de la forma que lo hace. También tendremos un poco de práctica, porque a ver ¿qué es un taller sin practicas? Tranquilos, que no haremos nada del otro mundo, solo cosas básicas, así que sin más preámbulo vamos a ello.

2.1 PROTOCOLOS BÁSICOS DE REDES

La verdad estaba tratando de buscar un sinónimo a eso de "protocolos", que puede sonar complicado pero no lo es, más abajo la Bruja pone una analogía, así que yo voy a hablar de algunos tipos de protocolos.

2.1.1 ARP (ADDRESS RESOLUTION PROTOCOL)

Cuando queremos enviar una carta a otro país simplemente la enviamos al servicio postal y allá el señor Rutenio (¿lo recuerdan?) se encarga de poner la correspondencia en el camino adecuado para su destino. Pero quiero que se representen la siguiente imagen mental: llegan al salón de clases en su primer día; por lo tanto, no conocen los nombres de ninguno de sus compañeros, pese a que en el pizarrón están escritos los nombres de cada uno de ellos todavía es imposible saber cómo se llama cada cual. De repente, en la pizarra notan un nombre muy curioso: un tal "Alvarus Black Díaz Drake", recorren el salón de lado a lado pero no saben quién es; aún así necesitan comunicarse con él de forma privada para preguntarle por el origen de su extraño nombre. Una carta bastaría, pero ¿a quién? Así que se arman de valor y preguntan en voz alta:

"¿!!Quién es Alvarus Black Diaz Drake!!?"

A lo que Black se pone de pie y dice: "Yo soy"

Entonces de forma discreta preparan la carta y se la entregan.

FIN

Los detalles de la respuesta a la carta no nos interesan en este momento, lo que importa es lo siguiente:

En una red local es necesario saber "la dirección MAC y la dirección IP" para enviar un paquete a otro dispositivo en la misma red; lo normal es que el nodo emisor sepa de antemano la dirección IP a la que desea enviar datos, pero si es "el primer día de clases" no sabrá la dirección MAC del destinatario; así que el equipo envía un mensaje *broadcast* (que es lo mismo que decir en voz alta en un salón de clases) preguntando:

¿Quién tiene la dirección IP XXX.XXX.XXX.XXX ? ["¿!!Quién es Alvarus Black Díaz Drake!!?"]

Y el nodo que tenga esa dirección IP responderá con su dirección MAC.

ARP se vale de mensajes para cumplir su cometido, estos pueden ser de pregunta (**ARP REQUEST**) o de respuesta (**ARP RESPONSE**).

*Los mensajes **REQUEST** son *broadcast*, lo que significa que se envían a toda la red, recuérdelo bien, un mensaje *broadcast* es enviado a todos los nodos de una red (mas adelante lo usaremos para explicar más cosas).

*Los mensajes **RESPONSE** son *unicast*, lo que significa que solamente se envían a un único nodo en la red, comúnmente al que preguntó en voz alta. Es decir, que se pregunta a todos, pero sólo uno responde.

2.1.2. DHCP (DYNAMIC HOST CONTROL PROTOCOL)

Estoy seguro de que más de uno ha visto estas siglas, como también estoy seguro de que quizás a más de uno les tocó ponerle la dirección IP a su equipo alguna vez (si nunca lo han hecho -tranquilos- no se pierden de nada). Colocar las direcciones IP a 1 o 2 equipos no es nada del otro mundo, pero se imaginan tener que ponerle la dirección manualmente a cada dispositivo en nuestra red ¿cada vez que nos conectamos? Qué tal una breve historia para ilustrarlo:

Carlos se levanta por las mañanas y se conecta a la red para leer las noticias desde su *tablet*, pero antes de conectarse debe asignarle la dirección IP a su equipo, así como configurar la dirección de la puerta de enlace y demás cosas. Al finalizar se ducha y se va al trabajo, cuando llega a su estación de trabajo debe conectarse a la red para poder trabajar, pero debe configurar todo en su estación de trabajo, dirección IP, puertas de enlaces, etc... Al medio día sale a la cafetería a tomarse un café y decide conectarse desde allí con su tableta a la red, pero debe borrar la configuración que usa en su casa y cambiarla por los valores de la cafetería.

¿Se imaginan una vida así?

Muchos de ustedes estarán pensando que eso es imposible, y estoy de acuerdo con ustedes, debería existir un mecanismo que haga estas cosas de forma automática por nosotros... Un momento... ¡Claro que existe! Se llama DHCP.

En el mundo del *networking* existen dos formas para asignar direcciones IP:

- a) Manual o estática
- b) Automática o dinámica

DHCP es el protocolo que se encarga de asignar direcciones IP, puertas de enlaces y más cosas para que podamos conectarnos siempre de forma automática sin tener que cargar con el problema de Carlos.

Ahora tendríamos que hablar de NAT. Qué tal si dejamos que Gabriela (AKA "La bruja") nos ilustre un poco, le cedo el cursor a la Bruja...

¡Hola Chic@s!

Ante el irresistible llamado de Cl0ud, Gabriela reportándose :D (más conocida como "la Bruja") por lo que raudamente pilló el cursor... y directo al teclado.

Me parece bueno, recordar algunas cosas: La dirección IP es una identificación informática, formada por un grupo de 4 números decimales (separados por puntos), por ejemplo:

10.10.10.10

200.200.200.200

Esto permite identificar redes y dispositivos en el gran universo de internet, las siglas significan *Internet Protocol*.

3. ¿QUÉ ES UN PROTOCOLO?

[El Brujo (Cl0ud) habla de distintos tipos de protocolos, pero vamos a ver que son como concepto].

Para entender qué es un Protocolo, podemos hacer una analogía con la vida real, por ejemplo, cuando nos invitan a comer cumplimos una serie de normas:

- I. Nos lavamos las manos.
- II. Nos sentamos a la mesa.
- III. Esperamos que todos los comensales estén servidos.
- IV. Pegamos un ojo al chico que nos gusta.
- V. Comenzamos a comer.

Es decir, son ciertas pautas, reglas de orden, que vamos siguiendo para el intercambio gastronómico.

Igual sucede con el Protocolo de Direcciones de Internet. Éste deriva su denominación porque es usado en redes que utilizan un estándar, un conjunto de normas, acuerdos pre-establecidos, para que pueda procesarse la comunicación entre los dispositivos (de una red privada o en la propia internet).

Estas reglas aseguran que, por ejemplo, todas las máquinas de una red puedan comunicarse (hablar, entenderse) bajo un mismo "código", sin importar qué tan distintas sean.

Ahora bien, cuando nos conectamos a internet, lo hacemos a través de un proveedor de internet (ISP = *Internet Service Provider*), quien nos asigna dirección IP globalmente única; pero si nos preguntamos:

4. ¿DE DÓNDE SACAN LOS ISP ESAS DIRECCIONES QUE NOS ASIGNAN?

Pues antes de responder a la pregunta anterior, tenemos que saber que en estos asuntos del mundo de las redes e internet existen ciertas autoridades que son las que llegan a acuerdos y disponen pautas, entre ellas hay dos personajes muy importantes que pasamos a presentaros:

La señora **IANA** [*] (*Internet Assigned Numbers Authority*): Toda ella una autoridad (y con mucho carácter para imponer sus convenciones) encargada, entre otras cosas, de otorgar direcciones IP a los ISP de todo el mundo.

Los señores **IETF** (*Internet Engineering Task Force*): Este es un grupo invisible para la mayoría de los usuarios, pero son estos quienes definen las tecnologías, ya sea porque marcan el inicio de una nueva tecnología y anunciar el desuso de otra.

[*] Actualmente la IANA (Autoridad para Asignación de Números de Internet, o en inglés: *Internet Assigned Numbers Authority*) es operada por la Corporación para la Asignación de Números y Nombres en Internet (ICANN, *Internet Corporation for Assigned Names and Numbers*).

Así que entre todas estas autoridades se dispuso las direcciones se dividieran en dos grupos: **las IP públicas y las IP privadas**, en función de la red a que pertenezcan. Es decir, si es para estar en casa o para salir de "marcha" a internet.

Esta separación entre **IP públicas e IP privadas**, tiene una explicación: Cuando se creó TCP/IP la cantidad de cosas conectadas a la red era mucho menor y nunca se pensó que internet llegaría a ser lo que es hoy día. Entonces el crecimiento exponencial de la demanda de conexiones a Internet -sumado que el número de direcciones IP v.4 es limitado - deriva en que se está llegando a un agotamiento de las direcciones disponibles.

En consecuencia, se reservaron algunos rangos (que veremos más adelante) para ser usados solamente en redes privadas, por ejemplo: en nuestra casa; sin importar si se repite la identidad numérica dado que no "salen" a internet.

4.2. IP PÚBLICA

Como la dirección de una casa que puede ser vista por todos, la IP pública es visible para todo Internet, de ahí que sea pública. Es posible que si nunca habéis pegado de cerca a la informática, no estéis muy familiarizados con ver la vuestra.

¿Qué os parece si vemos cómo hacerlo?

Hay varias formas de ver nuestra IP pública, pero un método simple es seguir los siguientes pasos para saberla:

a.- Abrid el navegador.

b.- Navegad hasta <https://www.whatismyip.com/es/>

c.- ¡Listo! Ahí tenéis vuestra dirección IP pública, única e irrepetible (al menos de forma temporal ya que ésta va cambiando, pero eso lo explicaremos más adelante).

4.3. IP PRIVADAS

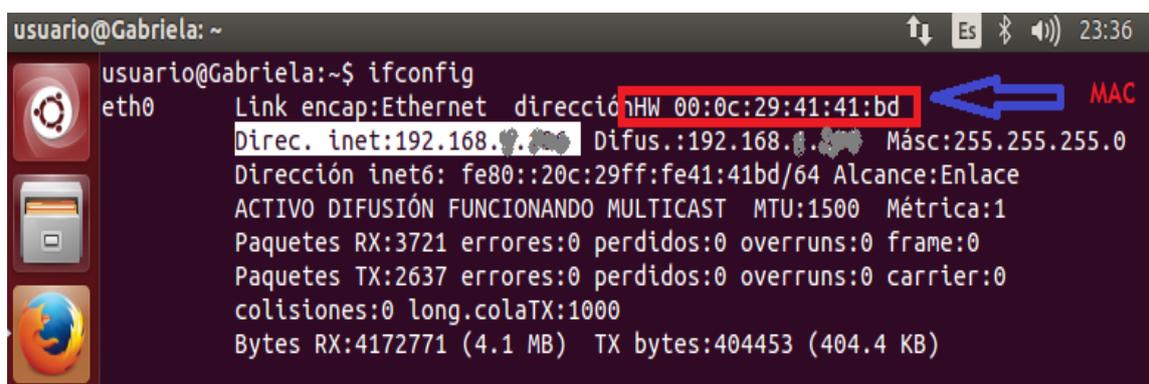
Éstas son las IP de andar por casa, identifican los dispositivos u ordenadores dentro de una red doméstica o privada (intranet).

Se dice que ofrecen mayor seguridad que una dirección IP pública ya que prácticamente nadie podría acceder a una red local desde internet.

Al ser identificadores que corresponden a una intranet, pueden repetirse en diferentes entornos locales sin que haya ningún conflicto dado que quedan "aisladas" de las redes públicas; y más aún, las podemos usar para establecer una red privada aunque no tengamos conexión a internet.

Dentro del grupo de direcciones privadas su uso es libre y gratuito (pues sí, increíblemente no pagamos por su utilización, de momento. (Al tiempo, que todo llegará :D).

Por cierto, Cl0ud les comentó como pueden ver su IP privada en Windows, os dejo como pueden encontrarla en Linux, en mi caso Ubuntu y la MAC en la interfaz eth0 . Alcanza con abrir la terminal y tipear **ifconfig**:

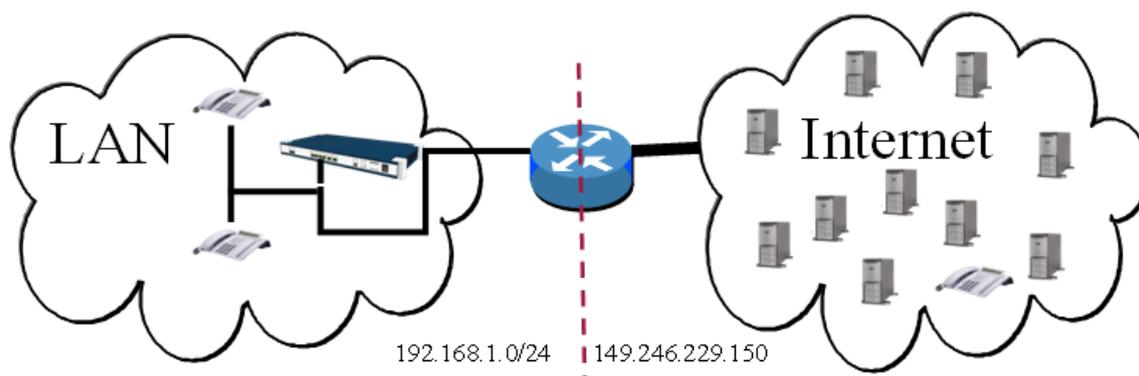


```
usuario@Gabriela: ~  
usuario@Gabriela:~$ ifconfig  
eth0      Link encap:Ethernet  direcciónHW 00:0c:29:41:41:bd ← MAC  
Direc. inet:192.168.1.100  Difus.:192.168.1.100  Másc:255.255.255.0  
Dirección inet6: fe80::20c:29ff:fe41:41bd/64  Alcance:Enlace  
ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1  
Paquetes RX:3721 errores:0 perdidos:0 overruns:0 frame:0  
Paquetes TX:2637 errores:0 perdidos:0 overruns:0 carrier:0  
colisiones:0 long.colaTX:1000  
Bytes RX:4172771 (4.1 MB)  TX bytes:404453 (404.4 KB)
```

5. LLEGAMOS A NAT... *Network Address Translation* (Traducción de Direcciones de Red)

Como las IP privadas no se enrutan a internet, es decir no permiten el paso de paquetes que se envíen o provengan de internet; **en principio** tendríamos que pensar que estamos aislados (O_O) sin posibilidad de navegar.

Sin embargo, para nuestra salvación \o/, el *router* hará de frontera entre los dos entornos de red, utilizando una técnica especial llamada **NAT** que opera como puente entre ambas *networkings*.



En la escuela nos pusieron el siguiente ejemplo: NAT, es algo así como si fuera un individuo de doble nacionalidad que se pasea desde nuestro país a un Estado vecino. Cuando necesitamos algo del exterior se lo pedimos a NAT, éste cruza la frontera, hace las compras en el extranjero y regresa a nosotros con los paquetes de fuera.

Técnicamente, NAT es un mecanismo implementado en el protocolo TCP/IP, por el cual se realiza el servicio de traducción de las direcciones locales, convirtiéndolas en direcciones públicas antes de enviar o recibir paquetes del exterior.

5.1. ¿POR QUÉ SURGE NAT?

NAT fue desarrollado con el fin de ofrecer una solución temporal al agotamiento de las direcciones IP únicas. ¡NAT es un economizador! del uso de las IP públicas. Si NAT no existiera, y dentro de nuestra red local tenemos 9999 ordenadores cada una con su IP privada, necesitaríamos que para salir a internet se nos asignaran 9999 IPs públicas, esto no es posible de acuerdo a la disponibilidad de direcciones externas.

Es en este escenario que aparece NAT, y con él solo necesitaremos una IP pública para que toda nuestra red (los 9999 ordenadores) tenga acceso a internet, pues lo que en realidad hace es “cambiar” la dirección de origen del paquete (IP interna) traduciéndola a una IP externa.

Por tanto, NAT permite a los dispositivos de cualquier red local conectarse a servicios con direcciones públicas de la red global; y de este modo, todo el tráfico que entre o salga de la red interna debe pasar por el *router* habilitado para NAT. En otras palabras podemos decir que es el “enlace” entre el ámbito privado (por ejemplo, la red local de una empresa) y el espacio público, como lo es la red de internet.

Estos conceptos de NAT son generales, en talleres futuros veremos los tipos de NAT, cuyo uso depende de los diferentes escenarios.

Nos leemos en el próximo taller