Nuestras brújulas son los DNS, ¡siempre!

Escrito el miércoles 12 de junio de 2019

Actualizado el martes 22 de octubre de 2018

Tenemos tiempo que no escribimos por acá, hemos estado ocupados con lo de la Reconversión Monetaria y haciendo otros trabajos donde, además, hemos aprendido mucho (recordemos siempre nuestro "mantra": «*Solo se que no se nada*»).

Esta entrada será muy sencilla, a nivel de principiante (ea, sin intención de connotación peyorativa, para nada, ojo) pero si tienen conocimiento básico sobre el Sistema de Nombres de Dominio recomendamos que hagan clic hacia este artículo para ampliar conocimientos.

Antecedentes

Que serán breves: el Internet como lo conocemos proviene del ARPANET y ya para entonces se hizo patente que se necesitaba un método práctico para recordar (y manejar) las direcciones IP de cada servidor web. Pensemos que cada dirección IP es como un número de teléfono: es la mejor analogía con el mundo real (de hecho el cableado, infraestructura, las conexiones conmutadas, etc. realmente fueron inspiradas por las redes telefónicas ya adaptadas al mundo digitalizado de ceros y unos al punto que en la actualidad los teléfonos corren sobre Internet, "***a grosso modo"***).

El Sistema de Nombres de Dominio (DNS, por sus siglas en inglés, "*Domain Name System*") se encarga precisamente de eso: a un nombre de dominio que le preguntemos nos retribuye la dirección IP del servidor web encargado de la página web correspondiente (si el servidor lo cambian de dirección, pues el DNS se actualiza al cabo de pocas horas). Obviamente que en los tiempos actuales esto se ha vuelto mucho más complejo: existen los *balanceadores de carga* y las *redes de distribución de contenido* **pero esencialmente sigue funcionando de la misma manera, a grandes rasgos.**

Protocolo de Configuración Dinámica de Anfitrión

Al igual como sucede con los teléfonos, tanto móviles como fijos, **para poder marcar un número primero debemos tener nuestro propio número**, y ese es el trabajo del Protocolo de configuración dinámica de Anfitrión (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP).

Para facilitar las cosas nuestro Proveedor de Servicios de Internet (ISP, por la sigla en inglés de "*Internet Service Provider*"), es decir, la empresa o ente que nos conecta a Internet, dispone de uno o varios servidores dedicados a esto. Una vez que nos dan las credenciales procedemos a conectarnos por nuestro módem (del tipo que sea, generalmente ADSL en estos tiempos) nos darán una dirección IP por medio de este protocolo. Junto a ello también nos darán las direcciones IP de los servidores DNS para que hagamos las consultas de los dominios que necesitamos -o queremos- visitar ***(entiéndase que estaremos "navegando por Internet")***. *Todo esto sucede de manera transparente a nosotros los usuarios, es decir, se hace de manera automática y sin nuestra ayuda ni intervención.*

Los problemas comienzan cuando nuestro proveedor de Internet sufre una caída de su servidores DNS... o simplemente necesitamos unos servidores DNS que nos protejan de que vayamos a sitios "obscuros" de la red... ***Para todo eso está escrita esta entrada y ojalá les sea útil.***

> Si no están seguros con lo que hacen, o están ayudando a un amigo o familiar **DETÉNGANSE AHORA**. Cambiar los valores de los DNS los pueden dejar "incomunicados" *y tendrán que pagarle a una persona que realmente sepa del asunto*. Pero si son del tipo de persona que les gusta "arremangarse" la camisa ***y no tienen miedo de meterse en sus propios equipos (porque son suyos y para eso los compraron, para usarlos de la manera que mejor les de la gana) pues este artículo está dedicado a ustedes.*** En todo caso la responsabilidad última, al igual que la de utilizar el software libre, **recae siempre sobre sus hombros, única y exclusivamente** (por Twitter @ks7000 podrán consultarnos pero no es obligación alguna que los ayudemos, con que tengan impreso esta página y seguir las instrucciones será más que suficiente para enmendar cualquier error).

Bienvenidos al siglo XXI

Hasta acá todo es válido si estuviéramos en el siglo 20 pero va a ser que no... En nuestras casas ahora tenemos cantidad de dispositivos conectados, *incluso a nuestros vecinos si no tuvimos la precaución de colocar una contraseña a nuestro enrutador inalámbrico.*

Como las direcciones IP versión 4 son bastante escasas y solo nos asignan una sola a nuestro módem, inventaron las redes privadas que llevan otro tipo de numeración distinto **precisamente**

con nuestro propio servidor DHCP ¿dónde está localizado? ¡Pues en nuestro propio enrutador inalámbrico corre como servicio!

Actualmente, con la miniaturización, tenemos enrutadores que también funcionan como módem pero los conceptos siguen siendo lo mismos. *Generalmente se utiliza una red clase C que comienza por 192.168.X.X donde X toma valor desde cero hasta 254* (ambos valores NO se utilizan) por lo que podemos tener cientos e incluso miles de direcciones privadas para nuestros dispositivos los cuales deberán saber cuál es la *puerta predeterminada* (enrutador) para de allí sea cambiada la dirección IP de nuestro paquete por la **dirección IP pública que nos asigno nuestro ISP.**

Elementos de hardware de red

Estimamos conveniente dejar por acá los conceptos relacionados con los aparatos que conectan nuestros equipos:

- De lo que es un concentrador *("hub", en inglés).*
- De lo que es un *conmutador* ("*switch*")
- De lo que es un *enrutador* ("*router*").

Conexión a nuestro enrutador

Nuestro enrutador tendrá pues, ***muy probablemente la dirección privada local 192.168.0.1 ó 192.168.1.1***, y cuando lo instalaron o lo instalamos lo primero que debimos haber hecho es haber cambiado la contraseña que viene de fábrica (cualquier *hacker* o *cracker* conoce el truco de, por medio del modelo del enrutador, tratar de ingresar con la contraseña que viene de fábrica).

Una vez que tengamos dichas credenciales podremos ingresar y comenzar a realizar nuestras personalizaciones. Lo que verán será algo ***MUY PARECIDO*** *a lo que tengan en sus hogares u oficinas.* Lo primero que observaremos será el ESTADO de nuestro enrutador: la dirección IP que nos haya asignado nuestro ISP (acá hemos ocultado valores para proteger nuestra privacidad, hay mucho *cracker* suelto por ahí). Nótese las direcciones de los servidores DNS de nuestro proveedor PRINCIPAL la empresa CANTV y nótese que estamos, a la vez, conectado a una puerta principal predeterminada cuyo último valor es 1, se estila (pero no es obligatorio) que las compuertas predeterminadas (las que conducen a Internet) tengan ese valor particular.

El hecho que acá tengamos esos DNS asignados **no necesariamente quiere decir que serán los valores que tendrán nuestros dispositivos conectados localmente.** Debemos buscar un apartado que diga DHCP:

Realmente acá es que estableceremos los valores de nuestra red, los que asignaremos a nuestros aparatos cuando se conecten a nuestro enrutador, en este caso usamos la nomenclatura 192.168.1.X

Actualizado el miércoles 12 de junio de 2019

> Norton DNS es un servicio que despareció del esquema de negocios de esa compañía; recientemente están disponibles los nuevos DNS públicos de la empresa **Cloudflare**, los cuales estamos evaluando: 1.1.1.1 y 1.0.0.1

~~Ahora bien esos valores de DNS que recomendamos corresponde a la empresa Norton (con su producto "Norton ConnectSafe"), la misma que años atrás fue muy famosa por su antivirus (en el siglo pasado el sr. Norton hizo dinero a raudales con su programa para recuperar archivos borrados, pero esa es otra historia). Una vez hallamos colocado SOLAMENTE ESOS VALORES (no tocar lo demás) podremos guardar *y generalmente es necesario reiniciar el enrutador, el aparato nos preguntará si deseamos hacerlo de una vez.* Tardará más o menos un minuto mientras desconecta todos los dispositivos, se reconecta a Internet (puede ser posible que nuestro ISP nos asigne otra dirección IP **pero no tiene absolutamente nada que ver con nuestro cambio**) y reconecte todos los dispositivos con los nuevos DNS.~~

~~Ya conectados hacemos una prueba y veremos algo como lo anterior: ya no dependemos de los DNS de nuestro ISP y a la vez estamos protegidos contra las páginas tanto de violencia como porno y **tampoco podremos acceder a las páginas maliciosas conocidas.**~~

Cambiando los DNS en Ubuntu 16

Ahora vamos a ver a nivel de nuestras máquinas, que bien pueden ignorar los valores que nos "asigna" nuestro enrutador, y podremos colocar los otros DNS que recomendamos (si no nos importa perder un poco de nuestra privacidad): los de Google. En Ubuntu 16 vamos a "Inicio" y luego escogemos "Configuración del sistema":

Seleccionamos "Red" y allí podremos cambiar los siguientes valores:

Procedemos a realizar la modificación:

Si escribimos mal el formato de las direcciones DNS el botón de "Guardar" se deshabilitará, debemos separar por puntos y con comas, tal como está en la figura. Inmediatamente los valores serán tomados.

Cambiando los DNS en Windows 7

Para la plataforma Windows traemos unas imágenes tomadas de una máquina virtual que tenemos, el procedimiento es muy parecido en la diferentes versiones, primero vamos al "Panel de Control" y seleccionamos "Redes y recursos compartidos" haciendo clic :

Hacemos clic en "Conexión de área local":

Hacemos clic en "Propiedades":

Tranquilo, tranquilas, **ya vamos a terminar**, hacemos clic en "Protocolo de Internet versión 4" y clic en "Propiedades":

Estos valores que ven pertenecen a **OpenDNS** lo cual probablemente no nos diga nada ni signifique algo conocido, pero aclaramos que pertenecen a la poderosa empresa **Cisco System** la cual produce y fabrica las compuertas que mueven a Internet... Osea nuestros ISP compran los aparatos, la mayoría, de esa marca. Incluso llegaron a vender enrutadores para uso doméstico, pero fueron pocos modelos.

El tema de la privacidad

Obviamente que estamos en manos de alguno de estas empresas: nuestro propio IPS, Google, Norton o Cisco (hay muchos otros) y se da el caso que dichas empresas llevan cuenta y estadística sobre nuestros hábitos de navegación, ***esa información vale dinero, ellos como consultores de informática son capaces de medir el mercado ¿cuál banco recibe más visitas? ¿De cuáles países? Ellos se lucran de ello.*** Así las cosas pues preferimos contar al menos con una retribución y Norton "nos protege" en gran parte pero veamos otro aspecto.

El tema de la seguridad: la evasión

Evidentemente que cada usuario con su ordenador o teléfono celular puede asignarse sus propios DNS (incluso colocarse su propia dirección IP local, pero eso será tema para otra entrada), la solución a ello *sería bloquear las direcciones IP de la mayoría de DNS "abiertos" para obligarlos así a utilizar los DNS de Norton.*

Otra estrategia más fácil para los usuarios es instalar el navegador Opera el cual hemos comprobado que tiene sus propios DNS (pero no nos hemos dado a la tarea de averiguar cuáles). Contra esto por ahora no tenemos solución pero eventualmente la hallaremos.

Un poco más allá

Si no disponemos de un enrutador podremos habilitar una computadora vieja con dos tarjetas de red, una para el módem y otra para un *concentrador* o "switch", un aparato que viene a ser como una regleta para conectar más dispositivos cableados (claro está , obviamente no tendremos "wifi"). dicho aparato es mucho más barato y una computadora vieja que funcione la formateamos e instalamos Lubuntu y habilitamos para que pase las conexiones de la red de área local hacia el módem y de allí al Internet (es más fácil decirlo que hacerlo).

Con esta configuración también podremos tener nuestro propio DNS (aparte del servidor DHCP) y no estaremos limitados al *firmware* del enrutador. De esta manera nuestra imaginación no tendrá límites, incluso podremos colocar un enrutador WIFI en "modo puente" para que esté a continuación de nuestro servidor GNU/Linux pero que no ofrezca ningún servicio sino que pase los paquetes sin más (esto es posible por la definición de las siete capas de red, modelo OSI).

Conclusión

Impriman estas instrucciones para que las puedan consultar si "caen fuera de línea" ¡Esperamos que pueda proteger sus equipos!

Fuentes consultadas

En idioma castellano

- «¿Cómo crear un punto de acceso WiFi en Ubuntu 18.04 LTS?»
- «*Root Server*: Los principales DNS del mundo» por DavidOchoBits.

En idioma francés:

- «Comment fonctionne Internet ?»

En idioma inglés:

- «Web Architecture 101» by Jonathan Fulton.
- «Half a Billion IoT Devices Vulnerable to DNS Rebinding Attacks» by Catalin Cimpanu.