www.DarFe.es

"Charlas sobre Ciberseguridad"

(módulo: cursos On-Line Ciberseguridad ***moodle.darFe.es****)*

TEMA 6

Ciberseguridad: Cómo son las entrañas de esta gran red mundial

(Jueves 31 de agosto de 2017)

Índice

1. INTRODUCCIÓN

Esta es la sexta de las charlas de este ciclo, en la cuál desarrollaremos brevemente los conceptos de fondo que hacen que esta red esté integrada como una sola máquina que une todo el mundo.

2. OBJETIVO

Comprender el fondo y las raíces de Internet para poder tener un punto de partida sólido en nuestros esfuerzos en Ciberseguridad.

3. TEMARIO Y FECHAS DE TODO EL CICLO 2017

A continuación se presentan la totalidad de las charlas que conforman este ciclo durante el año 2017.

Temario y fechas

Nº	Tema de la charla	Fecha
1	**Presentación, conceptos y situación de Ciberseguridad. *¿De quién nos defendemos?***	**Jueves 30 de marzo**
2	**Estrategias de Ciberseguridad en grandes redes (*Seguir y perseguir - proteger y proceder*)**	**Jueves 27 de abril**
3	**Ciberdefensa en profundidad y en altura (*la conquista de las cumbres*)**	**Jueves 25 de mayo**
4	**Ciberseguridad: La importancia de los procesos.**	**Jueves 29 de junio**
5	**Ciberseguridad: Plataformas / infraestructuras de Seguridad en Red**	**Jueves 27 de Julio**
6	**Ciberseguridad: Cómo son las entrañas de esta gran red mundial**	**Jueves 31 de agosto**
7	**Ciberseguridad: empleo de SOC y NOC**	**Jueves 28 de setiembre**
8	**Ciberseguridad: la importancia de saber gestionar "Logs"**	**Jueves 26 de octubre**

4. PRESENTACIÓN DEL TEMA DE HOY

Ciberseguridad: Cómo son las entrañas de esta gran red mundial (Jueves 31 de agosto)

En este Webinar, no dedicaremos tiempo a historia de Internet o aspectos conocidos de su evolución, sino a la descripción técnica que nos hace posible hoy en día poder transmitir información por todo el mundo.

Conocemos los diferentes tipos de acceso e infraestructuras básicas que nos permiten conectarnos a la red e inclusive parte de estas zonas, plataformas e infraestructuras que poseen las operadoras nacionales que en definitiva son las que llegan a través de la red fija o móvil hasta cada uno de nosotros, clientes finales. Avancemos ahora más en profundidad sobre los detalles de estas conexiones.

Si comenzamos a analizar esta red de forma jerárquica desde arriba hacia abajo, lo primero que nos encontramos son los grandes "**Carriers**" del mundo, es decir los que interconectan continentes y países de forma bastante piramidal. Existen tres niveles de ellos, conocidos como Tier 1, Tier 2 y Tier 3.

Esta charla profundizará sobre el funcionamiento de estos niveles superiores de Internet que son los que transportan los grandes volúmenes de datos y sus ancho de banda son inimaginables. El conocimiento de sus entrañas es lo que posiciona a cualquier atacante en un nivel superior en cuanto a volúmenes de tráfico y conectividad de extremo a extremo, por lo tanto si lo que deseamos desde el punto de vista de "ciberdefensa" es poder adoptar medidas contra estas acciones delictivas, necesitamos también conocer en detalle el fondo de esta red.

5. RESUMEN TEMAS DE LOS MESES ANTERIORES.

Hemos ido avanzando en conceptos , definiciones, ideas, opiniones de empresas líderes del mercado, analizando niveles de intrusos, predicciones para este año: Organizaciones mafiosas, análisis internacional de grandes empresas, "Resiliencia". Presentamos dos estrategias que nos ofrece la **RFC 1244**: *Proteger y Proceder - Seguir y Perseguir.* Nuestra propuesta fue, invitaros a que seáis

"audaces" y preparéis vuestras infraestructuras paso a paso para enfrentar la segunda de ellas, dejando de lado el viejo concepto estático de la defensa, para poder plantear vuestra seguridad por medio del concepto militar de "**Acción Retardante**" y avanzamos sobre esta operación.

Continuamos nuestro ciclo, haciendo una analogía entre el "**combate de montaña**" y cómo podemos pensar en alturas de nuestras redes y un análisis del reglamento militar.

Quedó la reflexión sobre las alturas dominantes.

- Planos de altura (*Niveles TCP/IP*).
- Planos de Segmentación (*redes de Gestión y de Servicio*).

En la cuarta charla nos centramos en los procesos que creemos fundamentales en nuestras infraestructuras:

- Entrada en producción
- Gestión de cambios
- Gestión de accesos
- Configuraciones e inventario
- Gestión de Backup
- Gestión de Incidencias
- Supervisión y Monitorización
- Gestión de Logs
- Gestión de actualizaciones

En la quinta hablamos de diferentes plataformas / infraestructuras de seguridad que debemos considerar para avanzar en la protección de nuestras empresas.

6. DEBATE SOBRE TAREAS PARA EL HOGAR

Antes de avanzar sobre el tema de hoy, retomemos lo que os invité a tratar durante todo este mes:

1. ¿Profundicé con SNORT?, ¿Como funciona su motor?, ¿pude implementas local rules?
2. ¿Necesito implantar sistemas AntiDDoS.
3. ¿Hice pruebas de IPS con respuestas automáticas?
4. Realizar pruebas de túneles SSH y el empleo de redirección de puertos.
5. ¿Pude instalar una máquina de salto?
6. ¿Qué opinión me merece el empleo de IEEE-802.1ae?

7. PLANTEO INICIAL

En el día de hoy desarrollaremos cuatro conceptos básicos sobre el corazón de nuestras redes:

- **Tubos**
- **Carriers**
- **Protocolo BGP**
- **Sistema DNS**

Por supuesto que para que todo Internet funcione, existen miles de conceptos, infraestructuras, protocolos, regulaciones, empresas, organizaciones, etc. Que también participan en el día a día de esta red, pero para concentrar la charla de hoy en aspectos fundamentales del tema lo haremos específicamente en estos tres que acabamos de presentar.

8. TUBOS

El periodista de tecnología **Andrew Blum** acaba de publicar un libro que intenta comprender la realidad física de Internet. "***Tubos, un viaje hacía el centro de Internet***"

El título del libro de Blum se refiere a un comentario de un senador estadounidense, llamado **Ted Stevens**. Hablando en el Senado el 28 de abril del 2006 respecto a una legislación sobre el negocio de proveedores de Internet, Stevens dijo, "*Internet no es algo que simplemente montas sobre otra cosa. No es un camión. Es una serie de tubos*." Este comentario fue motivo de críticas y risas en su momento.

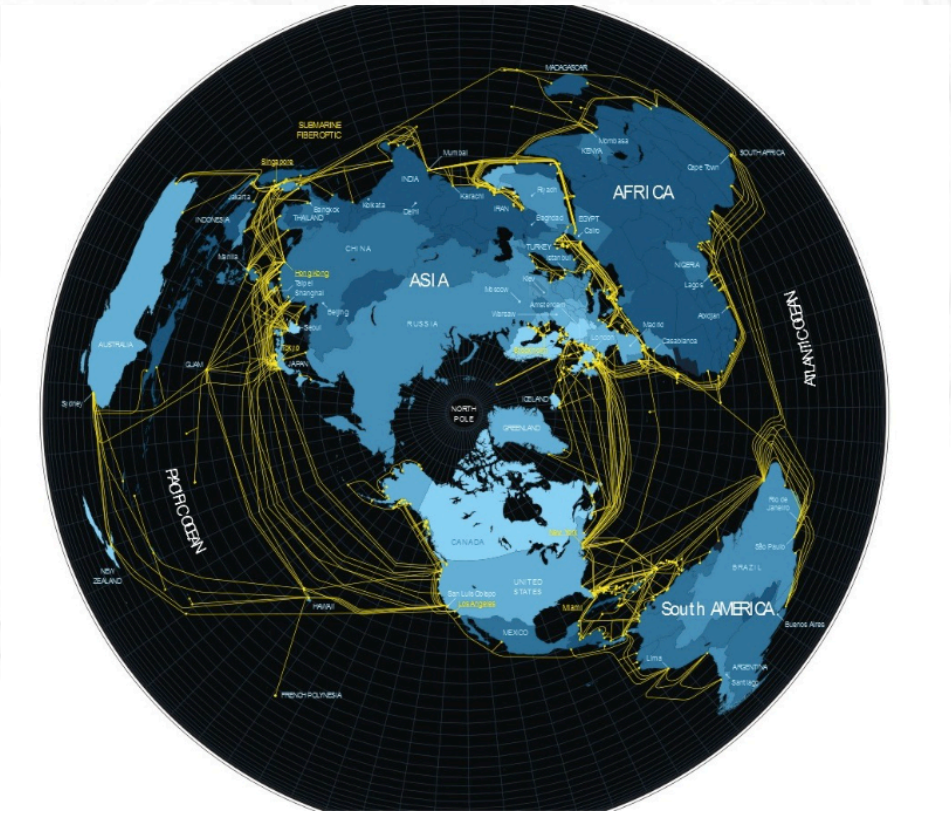
Comenta Blum:

> "*He confirmado, con mis propios ojos, que Internet es muchas cosas en muchos lugares. Pero una cosa que sí es, en todos los lugares donde existe, es una serie de tubos. Hay tubos debajo del mar que conectan Londres con Nueva York. Tubos que conectan Google con Facebook. Hay edificios llenos de tubos, y cientos de miles de caminos y vías de trenes que tienen tubos corriendo a sus lados. Todo lo que haces en línea viaja dentro de un tubo. Dentro de esos tubos, en general, hay fibras de vidrio.*

Y dentro de esas fibras, luz. Y, codificado dentro de esa luz, estamos –cada vez más– nosotros."

"*Una de las cosas que me gustó mucho de los administradores de grandes redes sobre los que escribí es que son diferentes de los típicos técnicos de soporte informático. En parte es porque hay una cierta diplomacia necesaria en lo que hacen. No sólo tienen que administrar su propio sistema, sino que también tienen que conectar sus redes a otras redes. Entonces siempre están negociando entre ellos; siempre tienen que tener en cuenta las necesidades de las otras redes además de las de ellos mismos. Eso los lleva a ser muy empáticos.*

La segunda cosa que me llamó la atención es que ellos tienen una imaginación bien geográfica y específica. Tienen que tener en cuenta cómo está conectado el mundo real para poder armar redes eficientes".



Estos tubos interconectan a nivel físico todos los extremos del planeta, estos "tubos" para establecer las conexiones podemos clasificarlos en tres categorías:

- Fibras ópticas.

- Cables de cobre
- Enlaces de radio

Esto es concretamente lo que denominamos "Medio físico" y es el nivel inferior de nuestro modelo de capas. Los extremos de cada uno de estos medios físicos, se conectan a dispositivos.

Estos dispositivos básicamente los podemos clasificar en dos categorías:

- Conmutadores o Switchs: operan a nivel 2 (*enlace*) del modelo de capas.
- Routers: operan a nivel 3 (*red*) del modelo de capas.

Los "tubos" llegan a una boca física de un router o switch, se conectan al mismo y a partir de allí ingresan o parten los "paquetes" de datos encapsulados en el protocolo que corresponda.

Como cualquier sistema de entrega y recepción, es necesario basarse en algún tipo de "Direccionamiento", el cual para el caso de Internet es el protocolo IP, en la actualidad sigue siendo la versión 4 del mismo, pero ya se está implantando la nueva versión 6, que está instalada y funcionando en gran parte de esta arquitectura mundial, si bien no podemos pensarla como que está en "producción" aún.

Todo este esquema de direccionamiento IP se encuentra asignado y regulado a lo largo de nuestro planeta por **IANA** (Internet Assigned Numbers Authority)

REGISTRY	AREA COVERED
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

(*Imagen tomada de* [*http://iana.org*](http://iana.org))

IANA tiene delegado sus rangos de asignación IP por regiones geográficas, tal cual podemos ver en la imagen anterior. Estas regiones son denominadas **RIR** (Regional Internet Registry).

Otra de las responsabilidades de asignación de IANA es la que respecta a los Sistemas Autónomos (**AS**: Autonomous Systems), los cuáles se tratan de conjuntos de redes IP y routers que se encuentran bajo el

control de una misma entidad (*en ocasiones varias*) y que poseen una política de encaminamiento similar a Internet.

El concepto de Sistema Autónomo es fundamental para el control de Internet, pues los grandes routers de esta red, sólo conocen de AS.

Este tema es el que presentamos en los puntos siguientes.

9. Carriers

Los grandes puntos de interconexión que tratamos en los párrafos anteriores, son gobernados por lo que podemos llamar "**Carriers**". Se trata de grandes corporaciones, que unen el corazón de esta gran red.

Si comenzamos a analizar esta red de forma jerárquica desde arriba hacia abajo, lo primero que nos encontramos son los grandes "Carriers" del mundo, es decir los que interconectan continentes y países de forma bastante piramidal. Existen tres niveles de ellos, conocidos como Tier 1, Tier 2 y Tier 3.

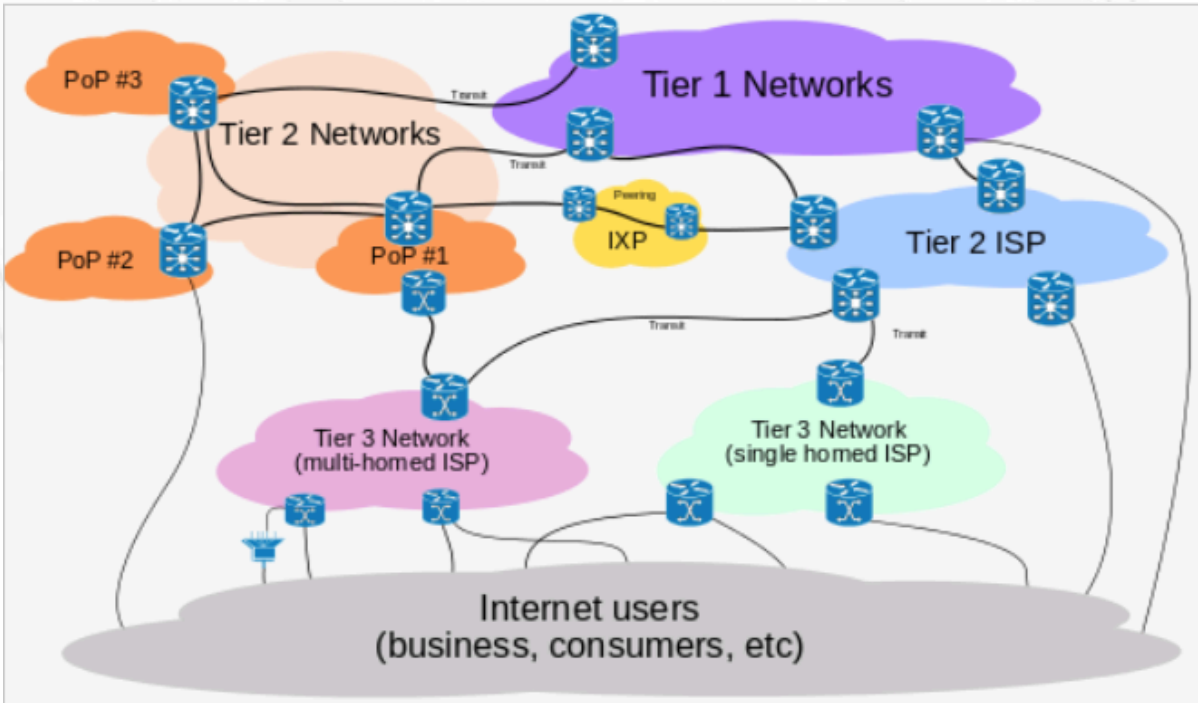


Imagen 1.12 (Tiers de Internet) (Imagen tomada de Wikipedia)

Los **Tier 1** son los grandes operadores globales que tienen tendidos de fibra óptica al menos a nivel continental. Desde la red de un Tier 1 se accede a cualquier punto de Internet, pues todas las redes de Tier 1

deben estar conectadas entre sí. Son backbone, core, núcleo ó troncal de Internet. Si bien se puede llegar a discutir la frontera entre algún Tier 1 específico, los que podemos considerar sin lugar a dudas como Tier 1 son:

Nombre	Sede	Nº as (asN)
Cogent anteriormente PSINet	Estados Unidos	174
Level 3 Communications (Ex Level 3 y Global Crossing)	Estados Unidos	3356 / 3549 / 1
XO Communications	Estados Unidos	2828
AT&T	Estados Unidos	7018
Verizon Business (anteriormente UUnet)	Estados Unidos	701 / 702 / 703
CenturyLink (anteriormente Qwest and Savvis)	Estados Unidos	209 / 3561
Sprint	Estados unidos	1239
Zayo Group anteriormente AboveNet	Estados Unidos	6461
GTT (anteriormente Tinet)	Estados Unidos	3257
NTT Communications (anteriormente Verio)	Japón	2914
Teliasonera International Carrier	Suecia - Finlandia	1299
Tata Communications (adquirió Teleglobe)	India	6453
Deutsche Telekom (Hoy: International Carrier Sales & Solutions)	Alemania	3320
Seabone (Telecom Italia Sparkle)	Italia	6762
Telefónica	España	12956

Independientemente de su magnitud, también deben reunir algunas características como son:

- Deben tener acceso a las tablas completas de routing a través de las relaciones que poseen con sus **peering** (otros Tiers).
- Deben ser propietarios de fibras ópticas transoceánicas y enlaces internacionales.
- Deben poseer redundancia de rutas.

El dato más representativo y actualizado del peso y actividad de cada uno de ellos se puede obtener a través de **CAIDA** (Center for Applied Internet Data Analysis) en:

http://as-rank.caida.org

Un ejemplo cercano de Tier 1 lo tenemos con Telefónica, a través de su empresa **TIWS** (Telefónica International Whole Sales) o actualmente con su nuevo nombre TBS (Telefónica Bussiness Solutions), desde su página Web podemos apreciar el mapa que se presenta a continuación donde se presentan todas los vínculos físicos que controla este Tier 1.

Imagen 1.13 (Red Internacional del Grupo Telefónica) (Imagen tomada de la web: http://www.internationalservices.telefonica.com)

Las diferentes operadoras de telefonía e Internet de cada país, enrutan su tráfico de clientes hacia el resto del mundo a través de estos carriers. Para esta tarea tenemos básicamente dos escenarios:

- Interconexión con su "Carrier" (Salida Internacional): En este caso se trata de routers del ISP, que físicamente están conectados a routers de un "Tier 1 o Tier2" y entregan su tráfico para que ellos lo enruten a través de Internet. Este tipo de enlaces suelen ser redundantes y en general hacia al menos dos Carriers diferentes par garantizar su disponibilidad.

- Punto de Intercambio (**IXP**: Internet eXchange Point) o también denominado o Punto Neutro: Se debe considerar que el tráfico de Internet, tiene un alto porcentaje que se mantiene dentro de las fronteras de cada país (consultas a Web nacionales, correos locales, etc..), este tipo de tráfico no tiene sentido que sea enrutado fuera de estas fronteras pues sobrecargaría las troncales de la red. Para estos casos en muchos países (no todos) se han creado estos IXP, que en definitiva son salas con "Racks" de comunicaciones (básicamente switchs de alta

capacidad) donde se interconectan los grandes carriers de ese país. Al organizarse las rutas BGP, es natural que este tipo de enlaces ofrezcan mayor ancho de banda que si siguieran otros caminos, por lo tanto a la hora de generarse las tablas de ruteo, el "peso" que tienen estos caminos supera cualquier otro, debido a ello se generan rutas locales preferenciales que encaminan el tráfico nacional, sin la necesidad de salir de ese país.

El propósito principal de un punto neutro es permitir que las redes se interconecten directamente, a través de la infraestructura, en lugar de hacerlo a través de una o más redes de terceros. Las ventajas de la interconexión directa son numerosas, pero las razones principales son el costo, la latencia y el ancho de banda.

El tráfico que pasa a través de la infraestructura no suele ser facturado por cualquiera de las partes, a diferencia del tráfico hacia el proveedor de conectividad de un Internet Service Provider (**ISP**).

La técnica y la logística de negocios de intercambio de tráfico entre los Internet Service Provider se rige por los acuerdos de interconexión mutua (**peering**). En virtud de dichos acuerdos, el tráfico a menudo se intercambia sin compensación. Cuando un punto neutro incurre en costos de operación, por lo general éstos son compartidos entre todos sus participantes.

10. Protocolo BGP

Siguiendo con la secuencia de estos párrafos, corresponde ahora tratar el tema de Sistemas Autónomos. Ampliando los conceptos anteriores, se define como "un grupo de redes IP que poseen una política de rutas propia e independiente". Esta definición hace referencia a la característica fundamental de un Sistema Autónomo: realiza su propia gestión del tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet. A cada uno de ellos, y es el que lo identifica de manera única a sus redes dentro de Internet.

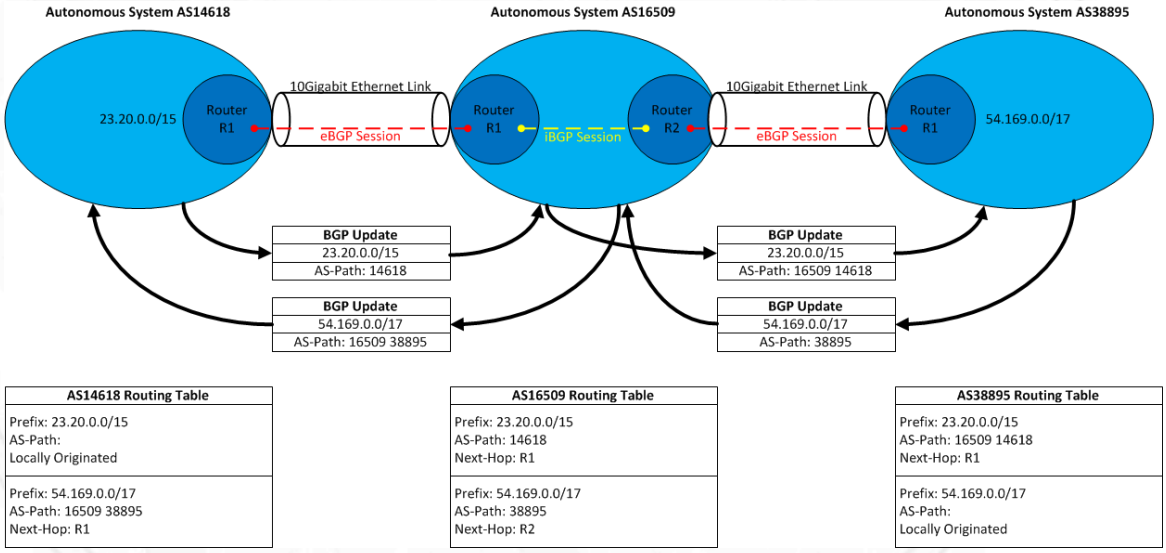
Hasta el año 2007 los números de sistemas autónomos estaban definidos por un número entero de 16 bits lo que permitía un número máximo de 65536 asignaciones de sistemas autónomos. Debido a la demanda, se hizo necesario aumentar la posibilidad La **RFC 4893** introduce los sistemas autónomos de 32 bits, que IANA ha comenzado a asignar. Estos números de 32 bits se escriben como un par de enteros en el formato x.y, donde x e y son números de 16 bits. La representación textual de Números de sistemas autónomos está

definido en la **RFC 5396**.

Los números de Sistemas Autónomos son asignados en bloques por la Internet Assigned Numbers Authority (**IANA**) a Registros Regionales de Internet (**RIRs**).

Los números de sistemas autónomos asignados por IANA pueden se encontrados en el sitio web de IANA: *http://iana.org*

El protocolo **BGP** (Border Gateway Protocol), es el responsable de enrutar todos los paquetes de Internet a lo largo del mundo. Este protocolo responde a un esquema de direccionamiento dinámico, es decir que sus rutas se van modificando frecuentemente sobre la base de diferentes métricas, que en definitiva son parámetros lógicos que permiten decidir por cuál interfaz debe sacar un determinado router cada uno de los paquetes que le llegan a él. Estas rutas se van creando sobre la base de la información que comparten los dispositivos vecinos (neighbor) que conforman esa comunidad BGP. A continuación presentamos una imagen que representa este funcionamiento:



(Imagen tomada de: https://www.awsarchitectureblog.com/2014/12/internet-routing.html)

11. Sistema DNS (Domain Name System)

El sistema **DNS** es el responsable de asociar las direcciones IP con los Nombres que emplea Internet. Esta actividad se lleva a cabo por un sistema estrictamente jerárquico cuya raíz (**root**), son exactamente 13 Sites (*donde cada una de ellas por supuesto está compuesta por más*

de un servidor con redundancia y balanceo de carga). Esta jerarquía como concepto de máximo nivel emplea el nombre de la forma **FQDN** (Fully Qualified Domain Name o Nombre de dominio completo) que se obtiene a partir del árbol, construyendo el dominio desde abajo hasta arriba, incluido el punto final y como máximo tiene 256 caracteres.

Como mencionamos, actualmente existen estos 13 servidores raíz, con los nombres de la forma **letra.root-servers.net**, donde letra va desde la **A** a la **M**. A continuación presentamos la plantilla que está en Wikipedia con el detalle de cada uno de ellos:

Letra	Direc. IPv4	Direc. IPv6	Nro. AS	Nombre antiguo	Operador	Ubicación #sitios (global/local)	Soft ware
A	198.41.0.4	2001:503:ba3e::2:30	AS26415	ns.internic.net	Verisign	distribuido (anycast) 4/0	BIND
B	192.228.79.201	2001:478:65::53	AS4	ns1.isi.edu	USC-ISI	Marina Del Rey, California, U.S. 1/0	BIND
C	192.33.4.12	2001:500:2::c	AS2149	c.psi.net	Cogent Communications	distribuido (anycast) 8/0	BIND
D	199.7.91.13	2001:500:2d::d	AS27	terp.umd.edu	Universidad de Maryland	College Park, Maryland, U.S. 1/0	BIND
E	192.203.230.10	2001:500:a8::e	AS297	ns.nasa.gov	NASA	Mountain View, California, U.S. 1/11	BIND
F	192.5.5.241	2001:500:2f::f	AS3557	ns.isc.org	Internet Systems Consortium	distribuido (anycast) 4/51	BIND 9
G	192.112.36.4	2001:500:12::d0d	AS5927	ns.nic.ddn.mil	Defense Information Systems Agency	distribuido (anycast) 6/0	BIND
H	128.63.2.53	2001:500:1::803f:235	AS13	aos.arl.army.mil	U.S. Army Research Lab	Aberdeen Proving Ground, Maryland, U.S. 2/0	NSD
I	192.36.148.17	2001:7fe::53	AS29216	nic.nordu.net	Netnod (antes Autonómica)	distribuido (anycast) 41/0	BIND
J	192.58.128.30	2001:503:c27::2:30	AS26415		Verisign	distribuido (anycast) 62/13	BIND
K	193.0.14.129	2001:7fd::1	AS25152		RIPE NCC	distribuido (anycast) 5/12	NSD
L	199.7.83.42	2001:500:3::42	AS20144		ICANN	distribuido (anycast) 130/0	NSD
M	202.12.27.33	2001:dc3::35	AS7500		Proyecto WIDE	distribuido (anycast) 4/1	BIND

Estos dispositivos, fueron, son y serán blanco de todo tipo de ataques, pues sin ellos sería prácticamente imposible navegar por Internet, y quizás tampoco por la red de cualquier gran empresa.

La historia de estos dispositivos, podríamos presentarla como que nace de la mano del desarrollo Open Source "**Bind**", que aún mantiene una posición respetable (*Como podemos ver en el cuadro anterior, lo emplean TODOS los root*), si bien hay que admitir que la competencia privada ha dedicado un esfuerzo admirable y hoy en día está ofreciendo productos de la forma de "Appliance" con los que es difícil competir desde el mero software, lo que sí es cierto es que casi todos ellos tienen parte del motor de Bind. El detrimento innegable de Bind es que es un hecho que su administración sigue siendo muy "estricta" en cuanto al empleo de línea de comandos y muy poca gente conoce al detalle sus pormenores, causa por la cual es muy raro encontrarlo actualizado y bien configurado.

Seguridad en **DNSs** y **DNSSec** (Domain Name System Security Extensions)

La organización jerárquica del Sistema de Nombres de Dominio y su trabajo clave en Internet , como ya mencionamos, lo posicionan como uno de los mayores blancos de ataque.

La funcionalidad del sistema DNS es resolver nombres ← → direcciones IP. (*sin esto es imposible navegar*).

Desde su nacimiento en los años 80 hasta hoy, sus mayores debilidades (*y continúan siéndolo*) son los engaños sobre esta asociación, pues son su única función. Hoy también presentan problemas con los llamados "ataques de amplificación" que han sido objeto hace pocos años-

Esta infraestructura inexorablemente debe entrar en contacto con cualquier usuario de Internet dejando el puerto 53 (TCP y UDP) abierto. Su única protección pasa por:

- Bastionar robustamente cada host (hardening) de esta infraestructura.
- Mantener siempre actualizados sus versiones de SSOO y aplicaciones.
- Monitorizar su actividad y configuración permanentemente.
- Colocar las barreras en los elementos que no necesariamente estén visibles.
- asegurar la integridad de sus registros de información (y este es el punto clave).

El diseño original del Domain Name System (DNS) no incluía la seguridad, sino que fue diseñado para ser un sistema distribuido escalable. Las Extensiones de seguridad para el Sistema de Nombres de Dominio (DNSSec) intentan aumentar la seguridad, y al mismo tiempo mantener la compatibilidad con lo más antiguo.

La **RFC 3833** es la primera que intenta documentar algunas amenazas conocidas en el DNS y cómo DNSSec puede responder a las mismas.

Luego de este RFC y desde principios del 2000 empezó a presentarse este conjunto de especificaciones que conforman **DNSSec**, pero recién en 2008, se consolidó con la aparición de la **RFC 5155** "Hashed Authenticated Denial of Existence" conocida como DNSSec3.

También se deben considerar las especificaciones llamadas DNSSec-bis, que describen el actual protocolo DNSSec con más detalle. Ellas son **RFC 4033**, **RFC 4034** y **RFC 4035**.

El registro DNSKEY correcto se autentica a través de una cadena de confianza, que comienza en un conjunto de claves públicas de la zona raíz del DNS, que es la tercera parte de confianza.

El punto clave de toda esta propuesta pasa por la implementación de "firmas" de zonas a través del empleo de certificados digitales.

Con esta estrategia, se asegura la "Integridad" de las zonas de todos los servidores y a su vez las respuestas que se ofrecen a las solicitudes, solucionando con ello el problema más crítico de este servicio.

Servidores de agujero negro.

La **RFC 1918** reserva tres rangos de direcciones de red para su uso en redes privadas en IPv4:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Este tráfico debe ser filtrado por todo ISP en su conexión hacia Internet, pero a pesar de ello, no es raro que este tipo de tráfico se filtre y aparezca de todos modos.

Para hacer frente a este problema, **IANA** ha puesto en marcha inicialmente tres servidores DNS especiales llamados "**servidores de agujeros negros**". En sus inicios los servidores de agujeros negros fueron los siguientes:

- Blackhole-1.iana.org

- Blackhole-2.iana.org
- prisoner.iana.org

Estos servidores están configurados para responder a cualquier consulta con una "dirección inexistente" como respuesta. Esto ayuda a reducir los tiempos de espera ya que la respuesta (negativa) se da de manera inmediata y por lo tanto no se requiere que expire. Además, la respuesta devuelta es también permitida se ser guardada en caché de los servidores DNS recursivos. Esto es especialmente útil debido a una segunda búsqueda para la misma dirección realizada por el mismo nodo, probablemente sería respondida desde la caché local en lugar de consultar a los servidores autorizados de nuevo. Esto ayuda a reducir significativamente la carga de red. Según IANA, los servidores de agujeros negros reciben miles de consultas por segundo.

En la actualidad funciona el proyecto **AS112** que se trata de un grupo de operadores de servidores de nombres de voluntarios que se unieron en un sistema autónomo. Ellos operan instancias de los servidores de nombres con anycast que responden la búsqueda DNS inversa para direcciones de red privada y de enlace local que hayan sido enviadas a la Internet pública. Estas consultas son ambiguas por su naturaleza y no se pueden responder correctamente. Pero las respuestas negativas se proporcionan de todos modos para reducir la carga sobre la la infraestructura DNS pública.

12. TAREAS PARA EL HOGAR (deberes).

Una vez más en esta charla os propongo llevarnos a casa algunas actividades o líneas de reflexión para que comencemos el mes que viene con orto breve debate sobre los mismos.

Os dejo las siguientes "**tareas para el hogar"**:

1. ¿Cómo llevas los conceptos de medio físico?, ¿tienes claro los tipos de cables, fibras y emisiones de radio que existen?
2. Identifica en tu País, quiénes son tu Tier 1, 2 y 3.
3. ¿Empleas BGP en alguno de tus routers?, en ese caso ¿Empleas autenticación de neighborhood?
4. Explora la Web: http://he.net/3d-map/ y analiza sus contenidos.

5. ¿Quiénes son tus DNSs de jerarquía superior?
6. ¿Has avanzado sobre DNSec en tus redes?, ¿Qué conclusiones o comentarios merece?

Nos vemos dentro de un mes con las tareas hechas (*no quiero suspender a nadie….*). Muchas gracias por todas vuestra atención e interés.

Un afectuoso saludo.

Madrid, 31 de agosto de 2017.

Alejandro Corletti Estrada

acorletti@darFe.es