Universidad de Costa Rica.

Escuela de Ciencias de la Computación

Sigla y curso:	CI-0121 Redes de Comunicación de Datos	**Grupo:**	01
Título:			
Fecha de realización:		**Fecha de entrega:**	
Profesor:		**Asistente:**	
Estudiante:	Ramírez Umaña Daniel Ricardo		_____/100
Estudiante:	Vílchez Ulloa Rodrigo		_____/100
Estudiante:	Villalobos Mora Oscar		_____/100
Estudiante:	Sequeira Bonilla Josué		_____/100

Introducción:

Con el crecimiento de las redes interconectadas a nivel global y surgieron nuevas necesidades, con lo que fue necesario establecer un protocolo para poder evitar conflictos, además para agilizar este proceso. Es así como surge el protocolo DHCP.

Para facilitar la búsqueda de sitios en Internet se necesita una forma inequívoca para identificar dónde se ubican los recursos buscados, pero aprender dirección IPv4 o IPv6 puede resultar tedioso para los humanos. Es por ello que se utiliza un sistema de nombres de dominio para facilitar a los usuarios acceder a la información contenida en servidores web por ejemplo.

Objetivos:

- Ilustrar cómo se puede identificar de forma única a un dispositivo que esté conectado a una red, desde nivel local como global en caso de Internet.
- Introducir el concepto de DHCP, la razón por la que este surge.
- Enlistar algunos de los ataques conocidos y vulnerabilidades a la IP conocidas y formas conocidas de mitigarlas.
- Describir el rol de los diferentes servidores DNS en una consulta donde el cliente solicita una dirección IP a través de un nombre de dominio.

- Reconocer que hay autoridades a nivel mundial y en Costa Rica que administran nombres de dominio y sus respectivas direcciones IP.
- Nombrar los tipos de registro en el servicio DNS.
- Dar a conocer los niveles en los nombres de dominio.
- Identificar que hay formas de aumentar la seguridad en el servicio DNS con la encriptación del DNSsec, así como su funcionamiento.

Desarrollo:

1. ¿Qué es un protocolo de red de internet?

Se le conoce como protocolo de comunicaciones al conjunto de reglas que se deben seguir dos o más elementos que quieran comunicarse entre ellas. En informática se tiene la familia de protocolos de internet, que son los protocolos con los que se transmiten datos entre computadoras a través de la internet. Para que los protocolos de comunicación funcionen de manera adecuada todas las partes involucradas deben estar acordadas en sintaxis, semántica y sincronización.

Uno de los acuerdos son los paquetes de información y su formato. Los paquetes son los bloques en los que se divide la información para transmitir de manera simple. Los paquetes son análogos a las tramas de niveles inferiores a la capa de red y al igual que ellas los paquetes están compuestos de una cabecera, el área de datos y la cola que a diferencia de las tramas, esta parte comúnmente incluye código de detección de errores. Los paquetes de capa de red son tomados del área de datos de la trama.

El formato de los paquetes de la capa de red tienen un formato de campos de acuerdo con el protocolo IP. Entre sus campos están: la versión de IP que utiliza, el tamaño de la cabecera, tipo de servicio a dar, longitud del paquete, identificación de éste, controles de fragmentación, tiempo de vida, protocolo a nivel de transporte, y otras opciones. La parte que interesa en esta investigación son las direcciones de origen y destino. 32 bits de cada una que corresponden a direcciones IP.

1.1. ¿Qué es una dirección IP?

La dirección IP son los números que identifican la interfaz de red de un dispositivo conectado a internet. La IP puede cambiar debido a cambios en la red o porque el dispositivos encargado de asignar las direcciones decida asignar otra IP. Los dispositivos que se usan comúnmente como teléfonos inteligentes, computadoras personales, y otros de índole personal suelen cambiar su dirección IP constantemente.

Para poder acceder a los sitios de internet estos se almacenan en un servidor, para poder acceder a ellos de manera remota este servidor debe estar conectado a internet, por lo tanto debe tener una IP asignada. Sin embargo estos sitios no pueden estar cambiando constantemente de dirección pues eso complicaría a niveles casi imposibles el acceso al sitio; por su naturaleza tienen una dirección IP fija.

Los dispositivos se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, para las personas no es sencillo recordar siquiera una dirección, por lo tanto existen nombres de dominio correspondientes a estas direcciones.

2. ¿Qué es el protocolo DHCP?

El protocolo de configuración dinámica de host por sus siglas en inglés es un protocolo de tipo Cliente-Servidor, donde hay dos partes involucradas: los proveedores del recurso o servicio, siendo estos los servidores y los que realizan la solicitud, los clientes.

Este protocolo tiene la capacidad de asignar direcciones IP de manera dinámica mediante un servidor DHCP, de esta forma los clientes que reciben esta asignación de dirección pueden comunicarse con otras redes. El servidor tiene una lista de direcciones IP y asigna aquellas que están libres

2.1. ¿Cómo asigna las direcciones IP?

A diferencia del protocolo BOOTP que le antecedió con la cual la asignación de direcciones IP debían ser configuradas manualmente, esta puede tanto asignar direcciones IP de forma automática como manual, pero es en especial su asignación automática lo que se convierte en un factor positivo dado el auge de las redes.

DHCP basa las asignaciones de dirección de IP en el modelo Cliente-Servidor (el terminal que quiere conectarse solicita la configuración IP a un servidor DHCP, el cual recurre a una base de datos que contiene los parámetros de red asignable).

2.1.1. Asignación automática:

Paso 1: El cliente DHCP envía un paquete **DHCPDISCOVER** a la dirección 255.255.255.255 desde la dirección 0.0.0.0. (a esto se le conoce como broadcast o difusión amplia). El cliente establece conexión con todos los integrantes de la red para localizar servidores DHCP disponibles e informar la petición.

Paso 2: En el puerto 67 aquellos servidores que hayan escuchado la petición responden la solicitud con un archivo **DHCPOFFER** con:

- La dirección IP libre.
- La dirección MAC del cliente.
- La máscara de la subred.
- La dirección IP y el ID del servidor.

Paso 3: Con el DHCPREQUEST el cliente DHCP escoge un paquete y se contacta con el servidor que haya sido escogido (todos los demás servidores también son notificados de que un servidor ha sido escogido).

Paso 4: Para concluir, el servidor le confirma al cliente los parámetros TCP/IP junto con el paquete **DHCPACK**. El DHCP guarda los datos recibidos localmente y se conecta con la red.

Alternativamente si el servidor durante el proceso ya había asignado la dirección a otro cliente o si ya no contaba con más direcciones para ofrecer devuelve un **DHCPACK(**DHCP not acknowledged o «no reconocido»**)**.

2.1.2. Asignación manual:

2.1.2.1. Ejemplo en Linux:

Para habilitar DHCP con Linux se utiliza el comando “sudo apt install isc-dhcp-server”

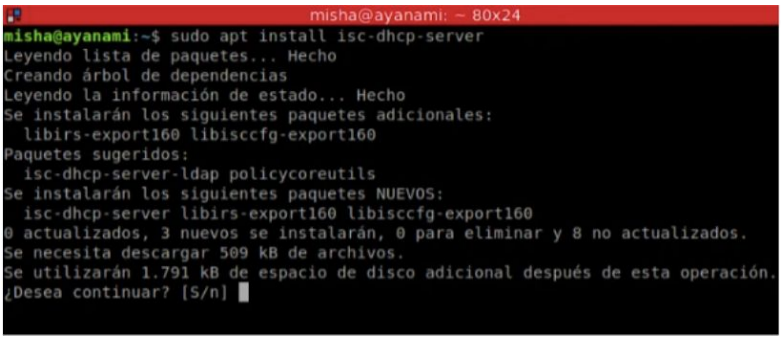


Figura 1: Habilitar DHCP con Linux

Posteriormente se configura el DHCP con “sudo nano /etc/dhcp/dhcpd.conf”

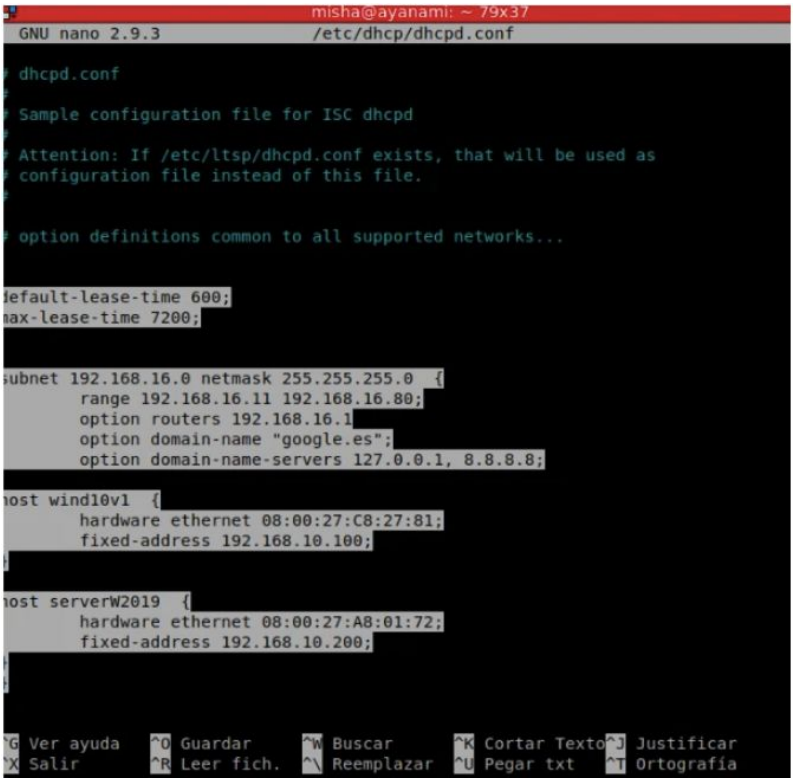
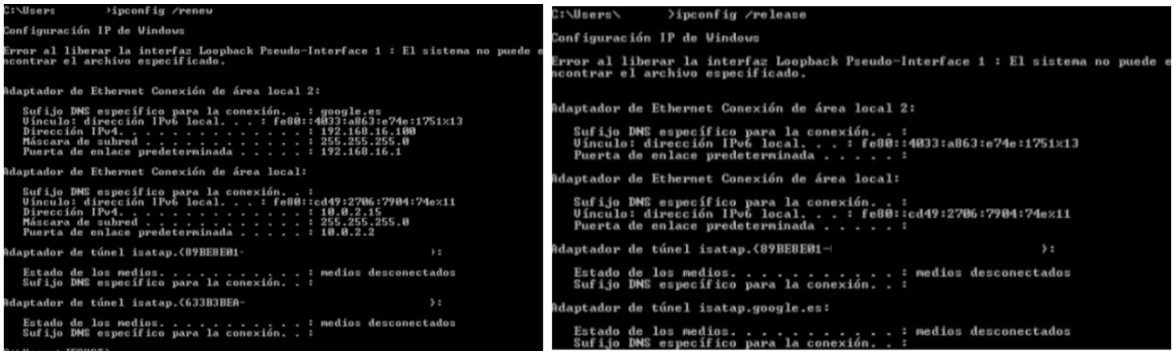


Figura 2: Configurar DHCP en Linux

Finalmente se procede a liberar la configuración Ip y solicitar una nueva configuración con los comandos “Ipconfig /release” y “Ipconfig /renew” respectivamente.



Figuras 3 y 4: Libera la configuración Ip y solicitar una nueva configuración con Linux

2.1.2.2. Ejemplo en Windows 10:

Para Activar y configurar DHCP con Windows 10 es necesario abrir el panel de control desde el menú inicial o con **[Windows]+[X]**

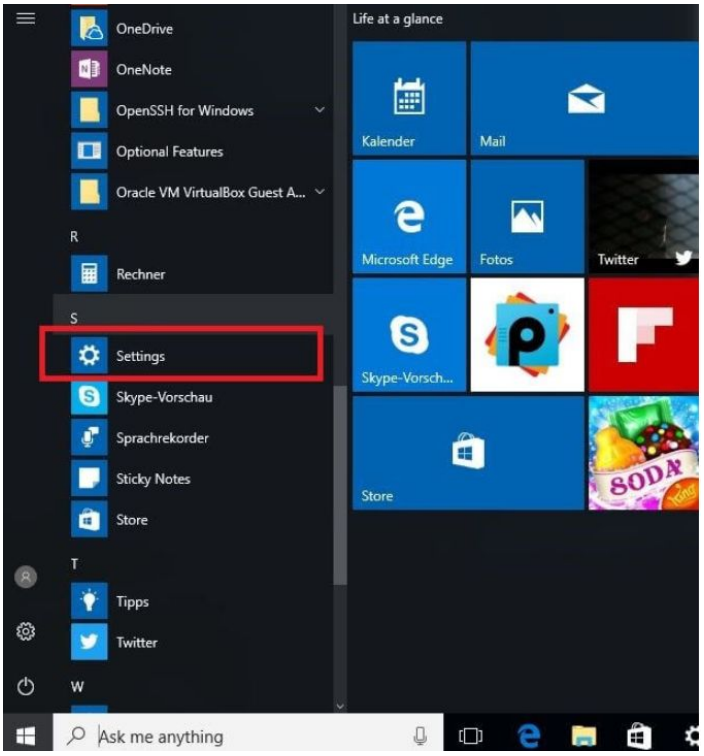


Figura 5: Paso 1 para activar y configurar DHCP con Windows 10

Ahora se hace clic en "Redes e Internet" y posteriormente clic en "Cambiar la configuración del adaptador"

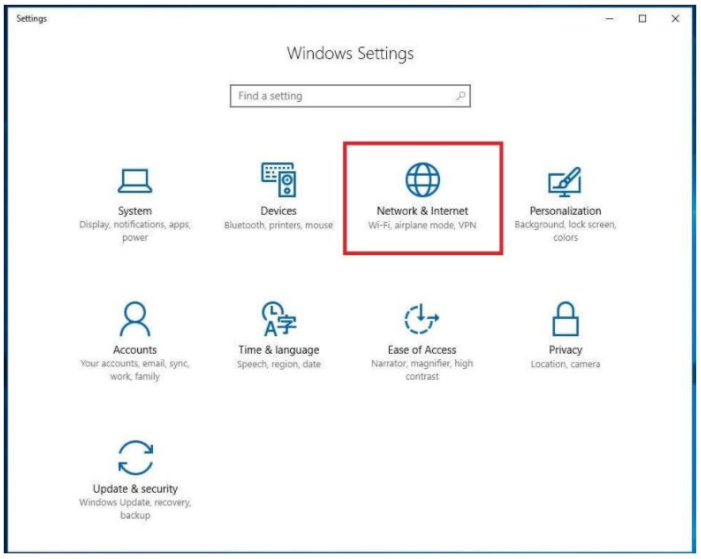


Figura 6: Paso 2 para activar y configurar DHCP con Windows 10

Ahora se hace clic derecho en la conexión LAN y selecciona "Propiedades" en el menú desplegable.

En el listado de protocolos y servicios activados y desactivados marcar la versión del protocolo que corresponda y abrir la ventana de propiedades.

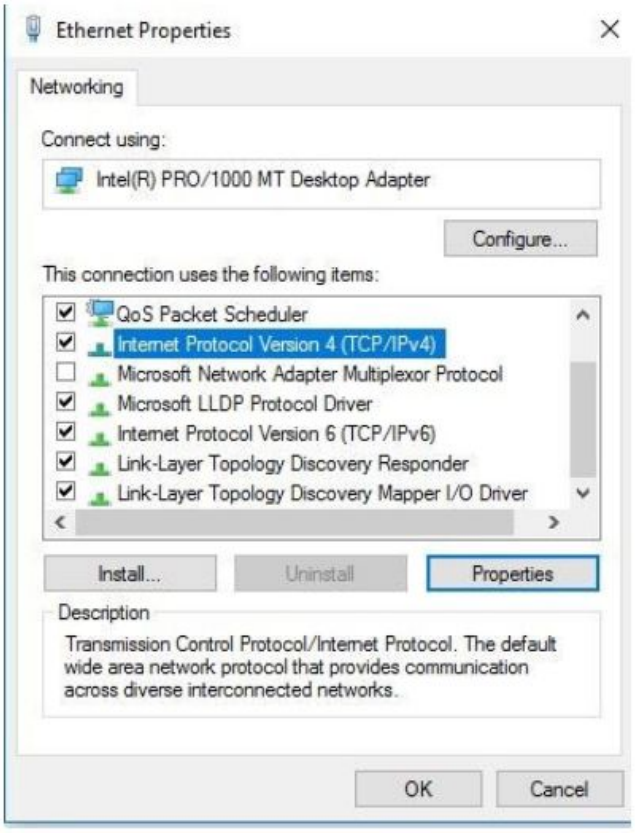
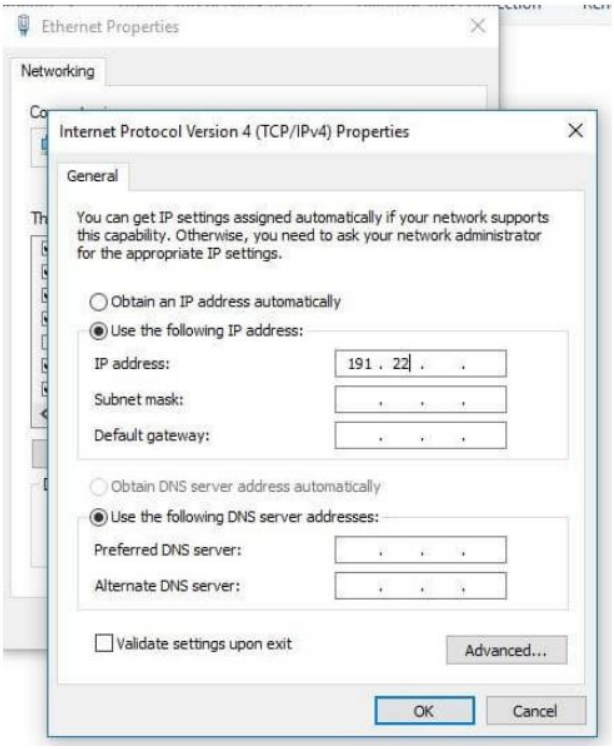


Figura 7: Paso 3 para activar y configurar DHCP con Windows 10

Por defecto está definida la obtención automática de dirección IP y si no lo estuviera se activa marcando esta opción. También se puede escoger la asignación estática, para lo cual se introducen los parámetros de red manualmente.



Para desactivar DHCP en Windows 10 hay que abrir la interfaz del servidor DHCP y llevar a cabo los ajustes correspondientes.

2.2. Vulnerabilidades y ataques a la DHCP y alternativas para mitigarlas:

2.2.1. DHCP Starvation Attack:

Este ataque ocurre cuando un atacante envía constantemente solicitudes falsificadas DHCP utilizando diferentes **direcciones MAC** en el campo **chaddr** a un servidor DHCP.

Los dos métodos a continuación podrían prevenir tales ataques:

- Para prevenir ataques que utilizan paquetes encapsulados DHCP con diferentes direcciones de origen MAC:
- Para prevenir ataques que utilizan paquetes encapsulados DHCP con una misma dirección de origen MAC:
    - Habilitar la verificación de dirección MAC en el servidor DHCP.
    - El servidor DHCP comparará el campo chaddr de alguna de las solicitudes DHCP con la dirección MAC de origen en el encabezado del frame.
    - Si son iguales el servidor DHCP verifica esta solicitud como legal y la procesa.
    - Si son distintas el servidor descarta la solicitud DHCP.
        - Para esto ingrese al visor del sistema (system-view).

- Entre al visor de interface (interface / interface-type / interface-number).
- Habilite la verificación de la dirección MAC (dhcp server check mac-address) ya que esta por defecto está deshabilitada.

2.2.2. DHCP Poisoning Attack:

Un ataque de Man-In-The-Middle (MITM) se logra cuando un atacante envenena la caché ARP de dos dispositivos con la dirección MAC (48 bits) de su NIC (Tarjeta de Interfaz de Red) Ethernet. Una vez que el caché ARP ha sido envenenado con éxito, cada uno de los dispositivos víctimas envía todos sus paquetes al atacante cuando se comunica con el otro dispositivo. Esto coloca al atacante en el centro de la ruta de comunicación entre los dos dispositivos víctimas; de ahí el nombre de ataque "hombre en el medio" (MITM). Permite al atacante vigilar fácilmente todas las comunicaciones entre los dispositivos víctimas.

2.2.3. DHCP Snooping Attack:

Las característica de DHCP snooping (fisgar DHCP) de los switches Cisco y Juniper pueden ayudar a mitigar el tipo de ataque DHCP spoofing, que consiste en configurar un servidor DHCP para capturar tráfico (una especie de man in the middle) y poder responder a las peticiones de DHCP.

Con el mecanismo DHCP snooping, los puertos están configurados en 2 estados de confianza o no confianza. Si un puerto está configurado como de confianza, puede recibir respuestas DHCP (los servidores DHCP legítimos están en interfaces de confianza) mientras que el resto de servidores/ordenadores (puertos de acceso) estarán en los de no confianza y si una falsa respuesta de (servidor) DHCP del atacante intenta ingresar a un puerto que no es de confianza, el puerto se desactivará.

Para evitar esto hay que configurar todos los puertos para los diferentes estados de confiable (trusted) o no confiable (untrusted). Si un puerto no está configurado para ser un puerto confiable, por defecto se considera un puerto no confiable.

2.2.4. DHCP Spoofing Attack:

La suplantación de DHCP ocurre cuando un atacante intenta responder a las solicitudes de DHCP y trata de listarse a sí mismo como la puerta de enlace predeterminada (gateway) o el servidor DNS, por lo tanto, inicia un ataque man in the middle attack. Con esto puede interceptar el tráfico de los usuarios antes de reenviarlo a la puerta de enlace real o realizar DoS inundando el servidor DHCP real con solicitudes para bloquear los recursos de la dirección IP.

Una forma de controlarlo es viendo quién puede enviar respuestas DHCP en la red con la característica de DHCP snooping.

2.2.5. DHCP Act Inject

Este ataque es producido cuando por medio de inyección de código script se mandan consultas que le permiten al atacante ya sea tener acceso a la dirección IP o en su efecto a la modificación de este.

2.2.6. DHCPig:

Aunque esta serie trata de la explotación de la capa 2, cubriendo el DHCP, que tradicionalmente se describe como un protocolo de capa 7, ya que implica comunicaciones UDP entre un cliente y un servidor y no proporciona directamente un servicio a las capas superiores, como lo haría, por ejemplo, un protocolo de enrutamiento.

2.2.7. Special situation DoS attack:

En este tipo de ataque se solicitan direcciones IP repetidamente al servidor DHCP para obtener todo el pool de direcciones disponibles, el atacante puede lograrlo haciendo que parezcan solicitudes DHCP hechas desde diferentes direcciones MAC. El atacante puede lograr esto haciendo que las solicitudes de DHCP parezcan provenir de diferentes direcciones MAC.

Para resolver este ataque DoS, se puede limitar el número de mensajes que se pueden pasar a la interfaz por segundo, de esta forma se logra hacer más lento o prevenir completamente

2.2.8. DHCP Rogue Server:

2.3. Parámetros que puede asignar al cliente con ayuda de la base de datos:

2.3.1. Dirección IP única: se puede asignar una dirección IP que no cambie, principalmente usada en IPs de un sitio web.

2.3.2. Máscara de subred: combinación de bits que delimita el ámbito de red. Indica a los dispositivos qué parte de la dirección IP es el número de la red, subred y host.

2.3.3. Puerta de enlace estándar: nodo que sirve como enlace entre dos redes, conecta y dirige el tráfico.

2.3.4. Servidores DNS: software para servidores que recurre a la base de datos DNS para responder a peticiones de nombres de dominio.

2.3.5. Configuración proxy por WPAD (Web Proxy Auto-Discovery Protocol): método usado por los clientes de servidores proxy para localizar el identificador de un archivo de configuración.

2.4. BOOTP vs. DHCP. ¿Por qué hoy en día ya no se usan los protocolos de arranque?

Siendo el DHCP en realidad una extensión del protocolo BOOTP desarrollado para conectar al Boot Server aquellos dispositivos como terminales y estaciones de trabajo sin disco duro, se convirtió en el protocolo estándar para la gestión de IP en redes gracias a las diferentes optimizaciones, pasando así el protocolo BOOTP a solo tener un valor histórico. Dado al crecimiento de las redes y al uso de dispositivos móviles la falta de automatización del proceso de configuración empezó a convertirse en un gran problema.

	BOOTP	**DHCP**
Configuración de direcciones IP	Requiere la configuración manual de las tablas de direcciones.	Soporta tanto la asignación automática y la obtención automática de direcciones IP como la configuración manual.
Direcciones IP temporales	No es posible.	Posible durante un periodo de tiempo limitado.
Soporte para dispositivos móviles	No es posible.	Soporta la movilidad de los clientes de red.
Índice de errores	Elevado debido a la configuración manual.	Prácticamente inmune a los errores gracias a la configuración automática de los componentes de red.
Requisitos del sistema	Ninguno.	Requiere disco duro para almacenar y reenviar la información.

3. ¿Qué es el protocolo DNS?

El servicio DNS (Domain Name Service o Servicio de Nombres de Dominio) es un servicio de Internet que traduce direcciones por nombre como www.unizar.es a direcciones IP utilizadas por la máquinas por ejemplo www.example.com en 192.0.2.1 y viceversa, de dirección IP a nombre (Unizar, s.f.). Se le conoce como resolución DNS y es para utilizar nombres fácilmente legibles y memorizables por las personas (Instituto Nacional de Tecnologías de la Comunicación - INTECO , s.f.).

3.1. Espacios de nombres de primer, segundo y tercer nivel

Los dominios de primer nivel se clasifican en dos categorías: por países (ccTLD – country code Top Level Domains) y genéricos (gTLD – generic Top Level Domains).

Los dominios de países o dominios geográficos (ccTLD): Son los que están asignados a sitios creados para un país en particular. Hay una clave o código para cada país, con la que se identifica fácilmente a qué país pertenece el dominio. Normalmente su extensión es de dos letras, por ejemplo: **.mx** México, **.ca** Canadá, **.es** España, **.au** Australia, **.co** Colombia, **.us** Estados Unidos… (GenuinoCloud, 2016)

Figura 1: Country Code Top Level Domain

Los dominios genéricos gTLD son muy conocidos, de acuerdo con el fin del sitio se elige la extensión. Por ejemplo:

- .com Negocios con fines de lucro
- .edu Organizaciones educativas
- .net Organizaciones en Internet
- .info Sitios brindan información
- .org Organizaciones sin fines de lucro
- .gob Instituciones gubernamentales

Hay dominios que tienen restricciones y para poder registrarlos se debe cumplir con ciertos requisitos. En el caso de ".gob", sólo puede ser usado por Gobierno Federal, Estatal y Municipal (instituciones relacionadas con gobierno). Para poder solicitar el uso de este dominio, se debe seguir una serie de pasos: Un escrito firmado por el responsable de la institución para la autorización del dominio de Internet, facilitar los datos que el proveedor

solicite, copia de identificación oficial del representante legal que firma (GenuinoCloud, 2016).

New top level domains (nTDL): Antes no había mucha variedad en cuanto a los TLD disponibles. Sin embargo, todo esto cambió cuando la Corporación Internacional para la Asignación de Nombres y Números (ICANN) lanzó su programa Nuevo dominio genérico de nivel superior (gTLD). Este programa fue diseñado para aumentar la cantidad de opciones de TLD y pidió a los usuarios de Internet que envíen solicitudes para nuevas adiciones. La ICANN finalmente recibió 1.930 sugerencias antes de que se alcanzara el plazo establecido. El proceso comenzó alrededor de 2005, pero ICANN no comenzó a lanzar los nuevos TLD hasta 2013. Desde entonces, se han aprobado más de mil solicitudes. (A2 Hosting, 2020)

Por ejemplo, muchas personas han debatido el efecto que el uso de TLD poco comunes puede tener en la optimización de motores de búsqueda de un sitio. Google ha asegurado a los usuarios que el TLD de un sitio no tiene ningún impacto en las clasificaciones de búsqueda. (A2 Hosting, 2020)

Por otro lado, el uso de un TLD moderno en su sitio web puede resultar beneficioso por razones como:

- Estos dominios a menudo pueden ser más baratos de comprar que las opciones más tradicionales.
- El uso de un TLD que sea relevante para el nicho o la audiencia de su sitio puede ayudarlo a fortalecer su marca.
- Un TLD inusual también puede ayudar a que su sitio se destaque en un mercado abarrotado.

Sin embargo, los nuevos TLD no están exentos de posibles inconvenientes. Quizás una de las mayores preocupaciones en torno a su uso es la credibilidad. Por ejemplo, una encuesta realizada por Varn encontró que los usuarios generalmente confiaban más en .com y .co.uk que en las nuevas opciones de TLD. (A2 Hosting, 2020)

La gente está acostumbrada a ver .com y .net después de todo, y a menudo espera que las empresas establecidas tengan este tipo de extensiones. Eso no significa que deba limitarse a los TLD más corrientes, pero sí significa que querrá pensar detenidamente sobre su elección. (A2 Hosting, 2020)

Ejemplos de este dominio son: .new, .app, .download, .vip, .online, .tech, .space, .tech, .cada, .academy, .xyz, entre muchos otros (Don Dominio, s.f.)

Dominios de Segundo Nivel: Son dominios que se encuentran una jerarquía más abajo del dominio de primer nivel o Top Level Domain, su extensión está formada por dos partes. Por ejemplo:

.com.mx Negocios con fines de lucro en México
.com.es Negocios con fines de lucro en España
.org.mx Organizaciones sin fines de lucro en México
.edu.mx Instituciones educativas en México (GenuinoCloud, 2016)

Dominio de tercer nivel: Muchas veces se le considera como la parte que se agrega a la izquierda del dominio, puede ser tomado en cuenta como el subdominio o como la parte "www" que se le agrega al inicio. Algunos se utilizan para balancear la carga de sitios con mucho tráfico. Como www1.minegocio.com o www2.midominio.com.mx. Otro ejemplo de dominio de tercer nivel al que se le podría considerar subdominio es: finanzas.minegocio.com. Estos subdominios se asignan con frecuencia para identificar departamentos de una organización o empresa (GenuinoCloud, 2016)

Subdominios: Son dominios formados por una palabra antes del dominio principal. Normalmente esta palabra da una idea general sobre el enfoque del sitio o describir cierta sección dentro del sitio u organización. (GenuinoCloud, 2016)

3.2. ICANN (Internet Corporation for Assigned Names and Numbers)

La Corporación de Asignación de Nombres y Números de Internet, o ICANN, es una organización sin fines de lucro con sede en California reconocida por la mayoría de las principales organizaciones gubernamentales. ICANN es responsable de gran parte del trabajo técnico y de políticas para Internet. Están involucrados en una amplia gama de proyectos, pero son directamente responsables del proceso de nTLD (name.com, s.f.)

3.3. Tipos de Servidores DNS

Los servidores DNS entran dentro de cuatro categorías:

Solucionadores recursivos (recursos de DNS): La consulta DNS llega primero a este servidor que funciona como intermediario entre un cliente y un servidor de nombres DNS. Cuando recibe la consulta DNS de un cliente web, el solucionador recursivo responderá con datos almacenados en caché o enviará una consulta a un servidor de nombres raíz, seguido de otra solicitud a un servidor de nombres de dominio de primer nivel y después a un servidor de

nombres autoritativo, después de recibir una respuesta de este último que contiene la dirección IP solicitada, el solucionador recursivo responde al cliente. (Cloudflare, s.f.)

El solucionador recursivo almacena en caché la información recibida de los servidores de nombres autoritativos, de esta forma si otro cliente solicita la dirección IP de un nombre de dominio ya almacenado en caché, el solucionador ya no necesita hacer todas las peticiones a los servidores de nombres sino que envía el registro almacenado localmente. (Cloudflare)

Un solucionador recursivo puede ser ofrecido por el proveedor de internet (ISP), el 8.8.8.8 de Google, 1.1.1.1 de Cloudflare y hay otros. (Cloudflare, s.f.)

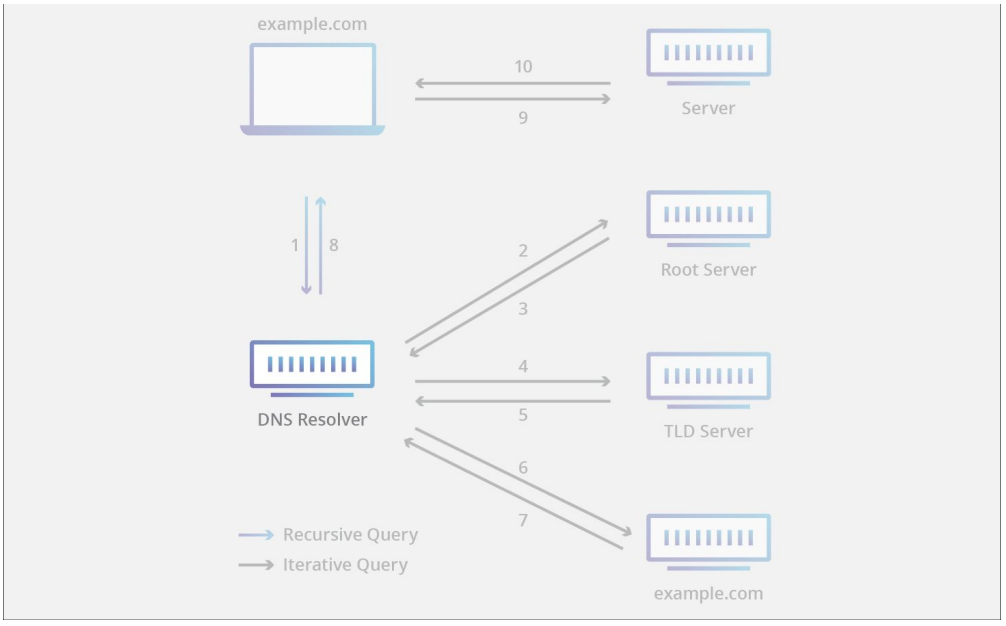


Figura 2: DNS resolver

Servidores de nombres raíz: Los 13 servidores de nombres raíz y sus copias son conocidos por todos los solucionadores recursivos y a ellos le hacen la primera consulta al buscar un registro DNS. Un servidor raíz acepta la consulta de un solucionador recursivo que incluye un nombre de dominio y le responde dirigiéndolo a un servidor de nombres de primer nivel según la extensión del dominio por el que se consulta como .com, .net, .org... (Cloudflare, s.f.)

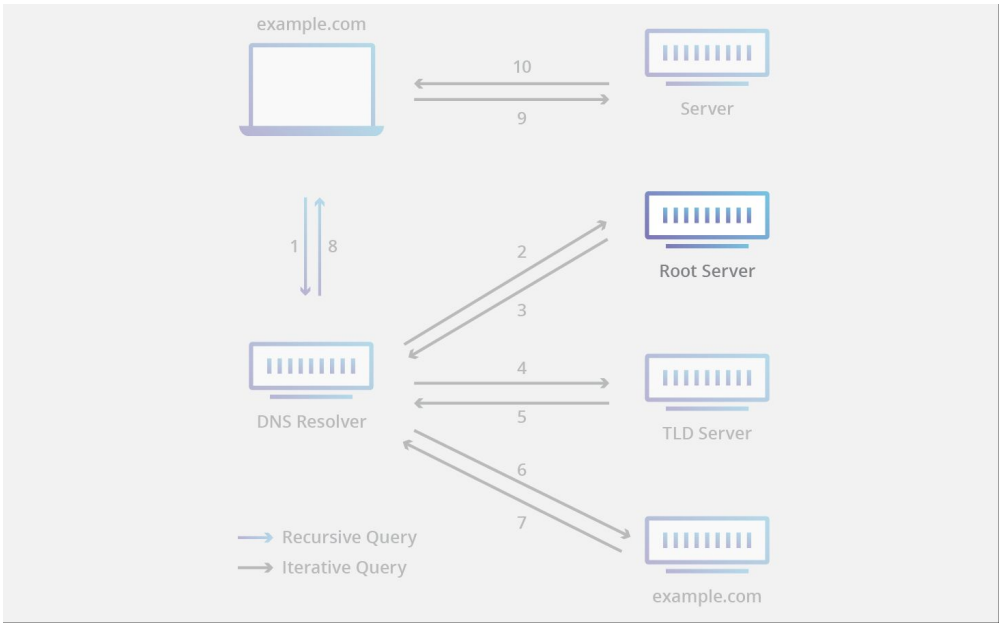


Figura 3: Servidor de nombres raíz

Servidores de nombres de primer nivel: Este servidor mantiene información para todos los nombres de dominio que comparten una extensión de dominio común por ejemplo .com, .net, u otro que venga tras el último punto de la url. (Cloudflare, s.f.)

Por ejemplo un servidor de nombres de primer nivel ".com" tiene información de todos los sitios web ".com". Si un usuario consulta por la página "www.google.com", el solucionador recursivo después de consultar a un servidor raíz, envía una petición a un servidor de nombres de primer nivel ".com" que respondería "señalando" al servidor de nombres autoritativo que tiene la dirección IP de www.google.com (Cloudflare, s.f.).

Los servidores de primer nivel tiene 2 divisiones principales:

- ***Dominios de primer nivel genéricos:*** No son específicos de países, algunos de los dominios de nivel superior genéricos más conocidos son .com, .org, .net, .edu, y .gov.
- ***Dominios de primer nivel de código de país:*** Incluyen todos los dominios que sean específicos de un país o estado. Por ejemplo: .uk, .us, .ru y .jp (Cloudflare, s.f)

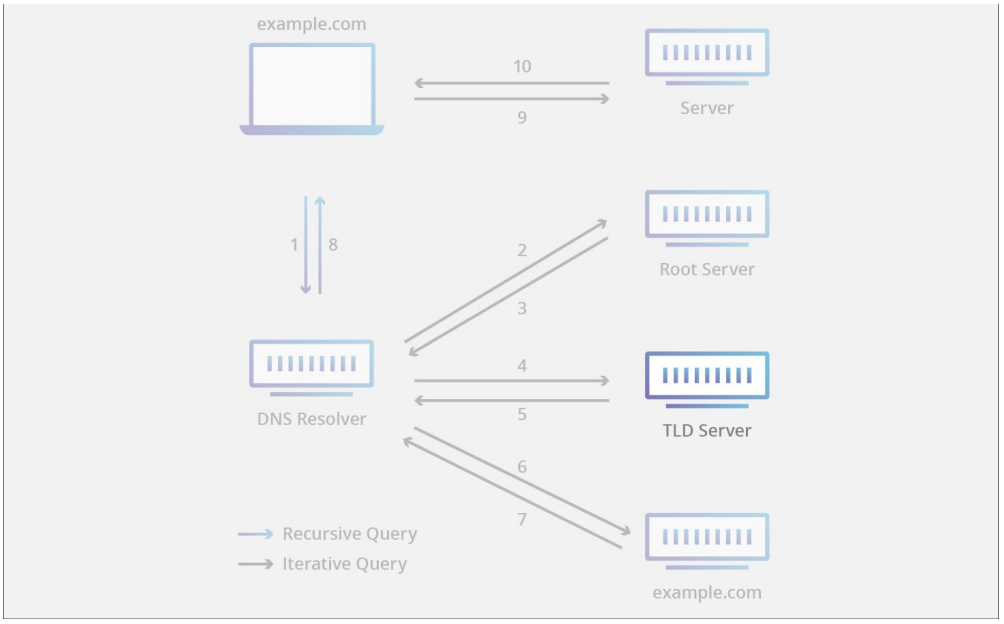


Figura 4: Servidor de nombres de primer nivel

Servidores de nombres autoritativos: Guarda información completa de un espacio de dominio o de varios, de los cuales es responsable. La respuesta del servidor de nombres de primer nivel redireccionará hasta llegar a un servidor de nombres autoritativo (generalmente el último en el recorrido de búsqueda de la dirección IP). Este servidor guarda información específica para el nombre de dominio al que sirve como google.com. (Cloudflare, s.f)

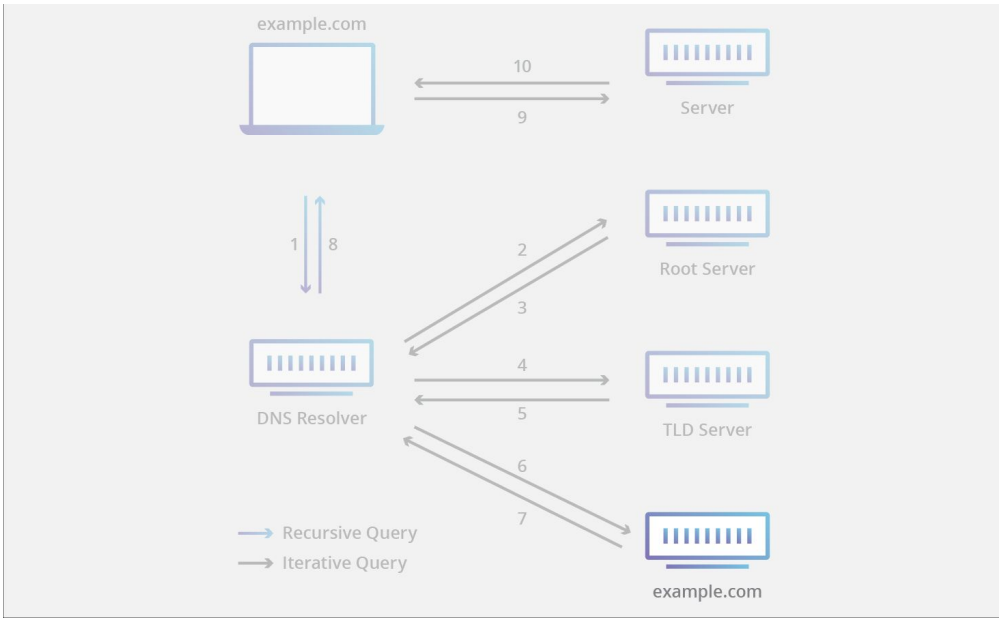


Figura 5: Servidor de nombre autoritativo

3.4. Componentes (Elementos integrantes del DNS)

Espacio de nombres de dominios: Es una estructura de árbol jerárquica donde cada nodo tiene 0 o más registros con información del dominio RR (Resource Records). El nodo raíz está en lo más alto y de él salen ramas que forman lo que se conoce como zonas, esto nodos también pueden tener más dominios o nodos, que asimismo se pueden dividir en subdominios (bajando en la jerarquía). (INTECO , s.f.).

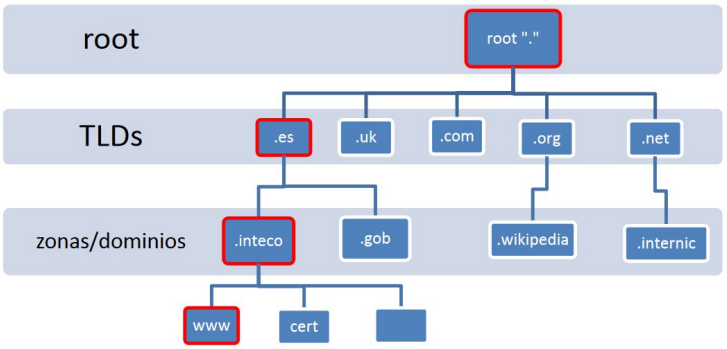


Figura 6: Espacio de nombres de dominios

Servidores de Nombres: Son servidores que están encargados de mantener y proporcionar información del espacio de nombres o dominios. (INTECO , s.f.).

Resolvers: Son servidores caché o programas cliente que se encargan de hacer las consultas necesarias para obtener la información solicitada por el cliente. (INTECO , s.f.).

3.5. Nombres de Dominio y Jerarquía

Los nombres de dominio suelen ser representados mediante una topología de árbol, donde en su nivel más bajo sus diferentes nodos se utilizan como etiquetas de los medios. El nombre del dominio consta de una concatenación de las etiquetas de un camino. Estas etiquetas son de tipo alfanuméricas con un límite de 63 caracteres de longitud y cada una separada por un punto, de hecho se incluye también un punto al final, pero suele omitirse. Un ejemplo sería www.ejemplo.com.

Un nombre de dominio en total no debe exceder los 255 caracteres y se escribe siempre de derecha a izquierda, el punto final que suele omitirse es quien separa la etiqueta raíz del resto de la jerarquía. Este primer nivel se le conoce como TLD o Dominio de Nivel Superior. Todos los dominios deben estar registrados bajo un TLD, ya sea .com, .org, .net, etc. Luego del TLD se encuentra el dominio, que viene siendo el nombre con el que se lo conoce al sitio. Y por último se encuentra la etiqueta host. En nuestro ejemplo www.ejemplo.com *www* es el host, *ejemplo* es el dominio y *com* el TLD.

Cada dominio o subdominio tiene una o más zonas de autoridad que publican la información acerca del dominio y los servicios de cualquier dominio incluido. La jerarquía de las zonas de autoridad coincide con la jerarquía de los dominios. Al inicio de esa jerarquía se encuentran

los servidores raíz: los servidores que responden cuando se busca resolver un dominio de primer y segundo nivel. (Gonzáles, 2014)

3.6. Registros DNS (RR: Resource Records)

Hay varios tipos de registros, identificando un tipo de información. Esta información es formateada para transmitirla en un registro de 6 campos en mensajes DNS.. En la siguiente tabla se muestran los 6 posibles campos en un mensaje DNS. (INTECO , s.f.)

Tabla 1

Formato de registro. Resource Record (RR)

Campo	Descripción	Longitud (bytes)
NAME	Nombre del dominio al que pertenece el registro	Cadena variable
TYPE	Código del tipo de registro	2 bytes
CLASS	Código de clase del registro	2 bytes
TTL	Tiempo en segundos durante el cual el registro es cacheado	4 bytes
RDLENGTH	Indica la longitud en bytes del campo RDATA	4 bytes
RDATA	Cadena de longitud variable que describe el registro de acuerdo al tipo y clase del mismo	Cadena variable

El campo TYPE identifica con un código de qué tipo de registro se trata. Hay una gran cantidad de estos tipos definidos para cubrir otras tantas funcionalidades. Algunos de los tipos más comunes se muestran en la siguiente tabla:

Tabla 2

Valores más habituales campo TYPE

TIPO (valor campo TYPE)	Función
A = *Address* – (Dirección)	Traduce (resuelve) nombres de recursos a direcciones IPv4
AAAA = *Address* – (Dirección)	Traduce (resuelve) nombres de recursos a direcciones IPv6
CNAME = *Canonical Name* – (Nombre Canónico)	Crear nombres adicionales, o alias, para el recurso
NS = *Name Server* – (Servidor de Nombres)	Indica qué servidor(es) almacenan la información del dominio consultado
MX = *Mail Exchange* (Registro de Intercambio de Correo)	Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio. Tiene un balanceo de carga y prioridad para el uso de uno o más servicios de correo.
PTR = *Pointer* – (Puntero)	Inverso del registro A, traduciendo IPs en nombres de dominio.
SOA = *Start of authority* – (Autoridad de la zona)	Indica el servidor DNS primario de la zona, responsable del mantenimiento de la información de la misma.
HINFO = *Host INFOrmation* – (Información del recurso)	Descripción de la CPU y sistema operativo que almacena la información de un dominio. Suele ocultarse.
TXT = TeXT - (Información textual)	Permite a los dominios proporcionar datos adicionales.
LOC = LOCalización	Permite indicar las coordenadas geográficas del dominio.
SRV = SeRVicios -	Información sobre los servicios que ofrecidos
SPF = *Sender Policy Framework* -	Ayuda a combatir el Spam. En este registro se especifica cual o cuales hosts están autorizados a enviar correo desde el dominio dado. El servidor que recibe, consulta el SPF para comparar la IP desde la cual le llega. Su uso se pretende abandonar a favor de registro TXT[3].
ANY = Todos	Para solicitar todos los registros disponibles

3.7. NIC Costa Rica

La organización sin fines de lucro NIC Costa Rica es independiente de la Academia Nacional de Ciencias que se encarga de proveer nombres de dominio .cr y sus subcategorías (.co.cr, .fi.cr, .or.cr, .sa.cr, .ed.cr, ac.cr y .go.cr). Su administración y asignación de nombres bajo .cr se rige por las normas de ICANN (Internet Corporation for Assigned Names and Numbers) e IANA (Internet Assigned Numbers Authority). (NIC, s.f.)

NIC Costa Rica desarrolla proyectos tanto a nivel nacional como internacional. Entre sus principales objetivos están promover la venta de sus dominios. Así como facilitar y promover el desarrollo de Internet mediante la participación activa en los diferentes sectores del país y el aporte de tecnologías innovadoras (NIC, s.f.).

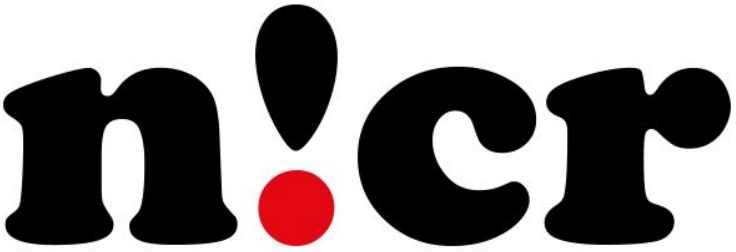


Figura 7: NIC Costa Rica logo

4. ¿Qué es el DNSsec?

Las extensiones de seguridad de DNS (DNSSEC) son un conjunto de estándares del Grupo de trabajo de ingeniería de internet (IETF) creados para abordar vulnerabilidades en el Sistema de nombres de dominio (DNS) y protegerlo contra las amenazas en línea.

Básicamente, DNSsec agrega autenticación o una capa al DNS para hacer que el sistema sea más seguro, pues cuando este fue diseñado, la seguridad no era un problema relevante por el uso que se le daba al internet. Esto porque pueden haber consecuencias, dadas por un uso malicioso, de la capacidad del DNS para cambiar el mapeo name-to-address (proceso que se da para encontrar la dirección IP de una computadora al utilizar su nombre de host). DNSsec permite comprobar la autenticidad de los datos. (2010, Oracle)

4.1. Funcionamiento

Se basa en una criptografía de una llave pública donde cada zona DNS tiene un par de claves que puede ser tanto pública como privada. Su funcionamiento se basa en que, toda información que sea enviada por un servidor DNS está firmada con la clave privada de la zona que envía la información, para que el que la reciba pueda verificar su identidad. En general, DNSsec ofrece los siguientes servicios: una prueba de dónde se originaron los datos, que en general se verifica que los datos que van a ser retornados hayan sido aprobados por el dueño de la zona; una distribución de claves públicas, que es útil para almacenar y recuperar claves públicas de manera segura; y el último, provee una autenticación de solicitudes y transacciones, que es para defender de algunos posibles ataques. Estas firmas aseguran al cliente que los datos recibidos son originados en la fuente que se especificó y que no han sido modificados maliciosamente en el camino, además de que garantiza si un nombre de dominio no existe, lo que aumenta la fiabilidad en la red.

Su relación con el proceso que realiza DNS es que, cuando se solicita la dirección IP de un sitio particular a un servidor de nombres recursivo y el servidor solicita este registro, la clave asociada a esa zona también se solicita, lo que permite verificar que el registro de esa dirección sea igual al registro en el servidor de nombres autoritativos. El usuario puede acceder al sitio en cuestión si el servidor de nombres recursivo determina que nada fue modificado durante la transmisión, este proceso se conoce como validación.

¿En qué ocasiones es útil DNSsec?

- Cuando se intentan hacer ataques de suplantación donde en ocasiones se intenta redirigir al usuario al sitio fraudulento donde se puede comprometer la información del usuario.
- Ofrece protección ante los ataques de interceptación del tráfico.

Es necesario recalcar que, cuando se quiera firmar una zona con DNSsec, se necesita mayor uso de recursos del CPU y del disco para realizar la consulta, por lo que si el tráfico del servidor es alto, puede afectar la manera en que se distribuyen los recursos y el uso de estos.

4.2. Cambios del DNSsec al DNS

Se verifica de manera segura que los datos e información que hayan sido recibidos realmente provenga de la zona donde se cree que se originaron. También permite asegurar que la información y los datos transmitidos no hayan sido modificados en el camino desde que haya sido firmada por el dueño de la zona con la clave privada.

4.3. Tipos de registros asociados al DNSsec

El primero es un registro KEY que almacena la llave pública de una zona, usuario o host, el protocolo usado para la transmisión y otros bits. El segundo tipo de registro es el registro SIG. Otros tipos de registros ofrecidos por DNSsec son: DS, NSEC-NSEC3, CDNSKEY-CDS.

Conclusiones:

Si bien existen formas de mitigar ataques a la DHCP, estas no son infalibles, por lo que es necesario evitar lo más posible poner el riesgo el sistema tomando la mayor cantidad de medidas necesarias posibles.

Es necesario llevar a cabo una correcta identificación de dispositivos en la comunicación dentro de toda una red, por ello se utilizan protocolos que funcionan como estándares para realizar dichas comunicaciones de forma exitosa.

El servicio de nombres de dominio (DNS) facilita al usuario humano solicitar recursos de un sitio web ya que es más fácil y significativo dar direcciones por nombres que por direcciones IP. Para que los usuarios utilicen tecnología, debe ser fácil de usar.

Se necesita llegar a un consenso y orden al definir nombres de dominio, por ello las organizaciones que lo administran como NIC en Costa Rica que se rige bajo ICANN (una rama del IANN) a nivel mundial, cumplen con este objetivo.

De igual forma como este es un servicio en Internet, está abierto al mundo y por lo tanto está expuesto a ataques. Por ello es necesario emplear mecanismos de seguridad para evitar incidentes que afecten a los usuarios o recursos, aquí es donde cobra gran importancia el DNSsec.

Bibliografía:

A2 Hosting. (2020, 25 agosto). Understanding the New Top Level Domains (TLDs). Recuperado 20 de septiembre de 2020, de https://www.a2hosting.com/blog/new-top-level-domains/

Acerca de NIC | NIC Costa Rica. (s. f.). NIC. Recuperado 16 de septiembre de 2020, de https://www.nic.cr/acerca-de-nic/

Cloudflare. (s. f.). Ilustración de solucionador recursivo. [Figura]. Recuperado de https://www.cloudflare.com/es-es/learning/dns/dns-server-types/

Cloudflare. (s. f.). Ilustración de servidor de nombres raíz. [Figura]. Recuperado de https://www.cloudflare.com/es-es/learning/dns/dns-server-types/

Cloudflare. (s. f.). Ilustración de servidor de nombres de primer nivel. [Figura]. Recuperado de https://www.cloudflare.com/es-es/learning/dns/dns-server-types/

Cloudflare. (s. f.). Ilustración de servidor de nombre autoritativo. [Figura]. Recuperado de https://www.cloudflare.com/es-es/learning/dns/dns-server-types/

Cloudflare. (s. f.). Ilustración de árbol jerárquico de espacio de nombres. [Figura]. Recuperado de https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/guia_de_seguridad_en_servicios_dns.pdf

Configuring DHCP starvation attack protection. (2020). Configuring DHCP starvation attack protection. https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3942_l3-ip-svcs_cg/content/483572327.htm

Don Dominio. (s. f.). Registro de dominios al mejor precio. Recuperado 20 de septiembre de 2020, de https://www.dondominio.com/products/domains/

GenuinoCloud. (2016). Ilustración de ccTLD. [Figura]. Recuperado de https://genuinocloud.com/wp-content/uploads/2016/02/dominios-geograficos.png

GenuinoCloud. (2016). ¿Qué es un dominio de primer nivel? Recuperado 21 de septiembre de 2020, de https://genuinocloud.com/blog/que-es-un-dominio-de-primer-nivel/

González, G. (2014, 25 abril). *Cómo funcionan los DNS*. Hipertextual. https://hipertextual.com/archivo/2014/04/como-funcionan-dns/

ICANN. (2020). DNSSEC – What Is It and Why Is It Important? Recuperado de https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

INCIBE. (2019, 11 junio). DNSSEC, asegurando la integridad y autenticidad de tu dominio web. Recuperado de https://www.incibe.es/protege-tu-empresa/blog/dnssec-asegurando-integridad-y-autenticidad-tu-dominio-web

INTECO (Instituto Nacional de Tecnologías de la Comunicación), INCIBE (Instituto Nacional de Ciberseguridad), López, A. L. P., & Fírvida, D. (s.f.). *Guía de seguridad en Servicios DNS*. https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/guia_de_seguridad_en_servicios_dns.pdf

Name.com. (s. f.). Domain extensions list | gTLDs, ccTLDs, nTLDs, and legacy domains. Recuperado 20 de septiembre de 2020, de https://www.name.com/domains

NIC Costa Rica. (s. f.). Ilustración de logo NIC Costa Rica. [Figura]. Recuperado de https://www.nic.cr/accion.

Oracle. (2010). Name-to-Address Resolution (System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)). Recuperado de https://docs.oracle.com/cd/E19683-01/806-4077/ad1intro-37915/index.html

Rouse, M. (2017, 20 octubre). DNSSEC, extensiones de seguridad de DNS. Recuperado de https://searchdatacenter.techtarget.com/es/definicion/DNSSEC-extensiones-de-seguridad-de-DNS

Servicio DNS - Descripción. (s. f.). Universidad Zaragoza. Recuperado 3 de septiembre de 2020, de https://sicuz.unizar.es/comunicaciones/dns/servicio-dns-descripci%C3%B3n

Tipos de servidor DNS. (s. f.). Cloudflare. Recuperado 3 de septiembre de 2020, de https://www.cloudflare.com/es-es/learning/dns/dns-server-types/

V. (s. f). Funcionamiento de las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC) - Verisign. Recuperado de https://www.verisign.com/es_LA/domain-names/dnssec/how-dnssec-works/index.xhtml