1 – Nombre, describa algunas formas de transmisión de Datos en IoT

Algunos modelos para desplegar y hacer funcionar IoT son:

a) Dispositivo a dispositivo

La comunicación de dispositivo a dispositivo representa dos o más dispositivos que se conectan directamente y se comunican entre sí.

Este modelo se usa comúnmente en los sistemas de automatización del hogar para transferir pequeños paquetes de datos de información entre dispositivos a una velocidad de datos relativamente baja.

Algunos ejemplos son:

- WiFi

Normalmente la conectividad WiFi es la opción obvia elegida por los desarrolladores dada la omnipresencia de WiFi en entornos domésticos y comerciales: existe en la actualidad una extensa infraestructura ya instalada que transfiere datos con rapidez y permite manejar grandes cantidades de datos. Actualmente, el standard WiFi más habitual utilizado en los hogares y en muchas empresas es muy adecuado para la transferencia de archivos, pero que consume demasiada potencia para desarrollar aplicaciones IoT.

- Estándar: Basado en 802.11n
- Frecuencia: 2,4GHz y 5GHz
- Alcance: Aproximadamente 50m

- Velocidad de transferencia: hasta 600 Mbps, pero lo habitual es 150-200Mbps, en función del canal de frecuencia utilizado y del número de antenas (el standard 802.11-ac ofrece desde 500Mbps hasta 1Gbps)

- Bluetooth

Bluetooth es una de las tecnologías de transmisión de datos de corto alcance más establecidas, muy importante en el ámbito de la electrónica de consumo.

El nuevo Bluetooth de baja energía, también conocido como Bluetooth LE o Bluetooth Smart, es otro protocolo importante para desarrollar aplicaciones IoT. Se caracteriza por ofrecer un alcance similar al de la tecnología Bluetooth normal, pero con un consumo de energía significativamente reducido.

- Estándar: Bluetooth 4.2

- Frecuencia: 2,4GHz (ISM)

- Alcance: 50-150m (Smart/LE)

- Velocidad de transferencia: 1Mbps (Smart/LE)

- ZigBee

ZigBee es una tecnología inalámbrica más centrada en aplicaciones domóticas e industriales.

ZigBee/RF4CE tiene algunas ventajas significativas como el bajo consumo en sistemas complejos, seguridad superior, robustez, alta escalabilidad y capacidad para soportar un gran número de nodos. Por lo que es una

tecnología bien posicionada para marcar el camino del control wireless y las redes de sensores en aplicaciones IoT y M2M.

- Estándar: ZigBee 3.0 basado en IEEE 802.15.4
- Frecuencia: 2.4GHz
- Alcance: 10-100m
- Velocidad de transferencia: 250kbps
- Red de telefonía móvil

Cualquier aplicación IoT que necesite funcionar en grandes áreas puede beneficiarse de las ventajas de la comunicación móvil GSM/3G/4G. La red de telefonía móvil es capaz de enviar grandes cantidades de datos, especialmente a través de 4G, aunque el consumo de energía y el coste económico de la conexión podrían ser demasiado altos para muchas aplicaciones.

Sin embargo, puede ser ideal para proyectos que integren sensores y que no requieran un ancho de banda muy grande para enviar datos por Internet.

- Estándares: GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G)
- Frecuencias: 900 / 1800 / 1900 / 2100
- Alcance: hasta 35km para GSM; hasta 200km para HSPA
- Velocidad de transferencia (descarga habitual): 35-170kps (GPRS), 120-384kbps (EDGE), 384Kbps-2Mbps (UMTS), 600kbps-10Mbps (HSPA), 3-10Mbps (LTE)

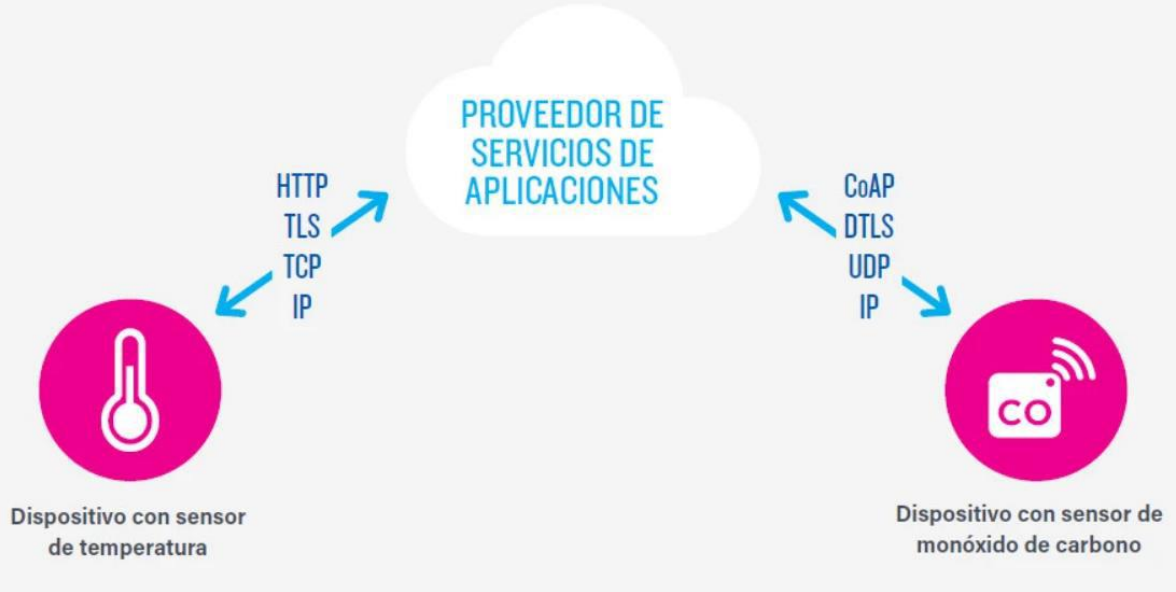
b) Dispositivo a Nube

La comunicación de dispositivo a nube implica un dispositivo de IoT que se conecta directamente a un servicio en la nube para intercambiar datos y controlar el tráfico de mensajes.

Un caso de uso para Dispositivo-a-Nube basado en redes celulares son las etiquetas inteligentes que rastrea al perro o gato de la casa mientras el usuario no está.

FIGURA 2

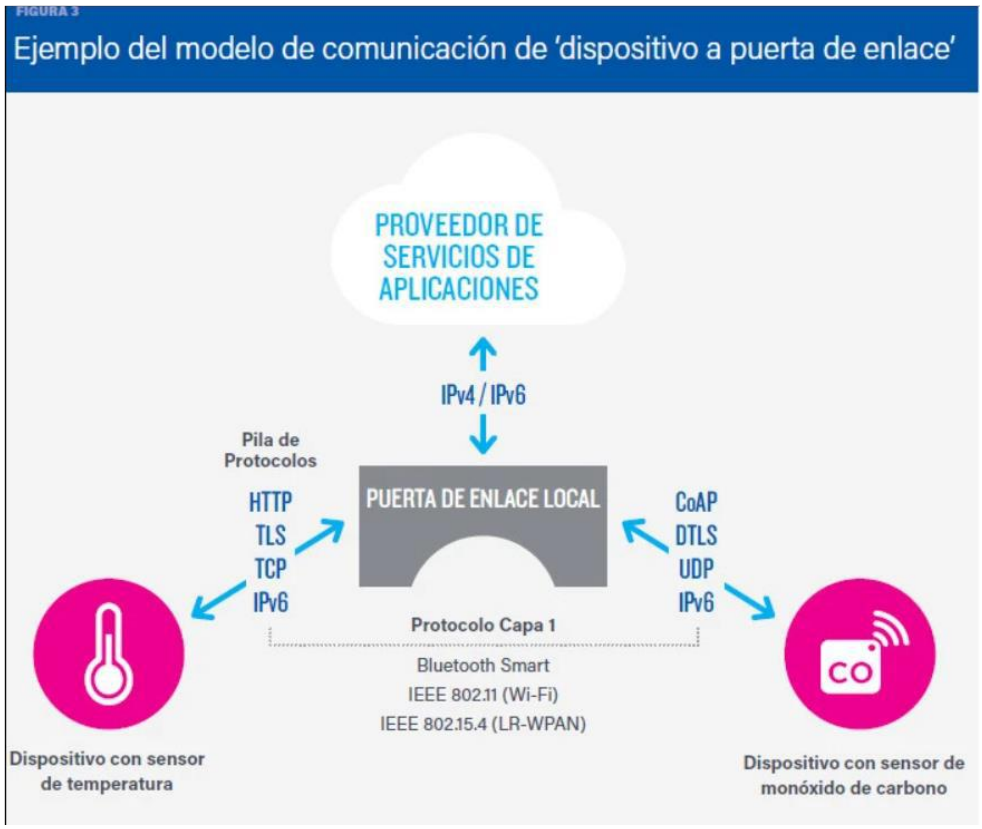
Diagrama del modelo de comunicación dispositivo a la nube



c) Dispositivo a Puerta de Enlace

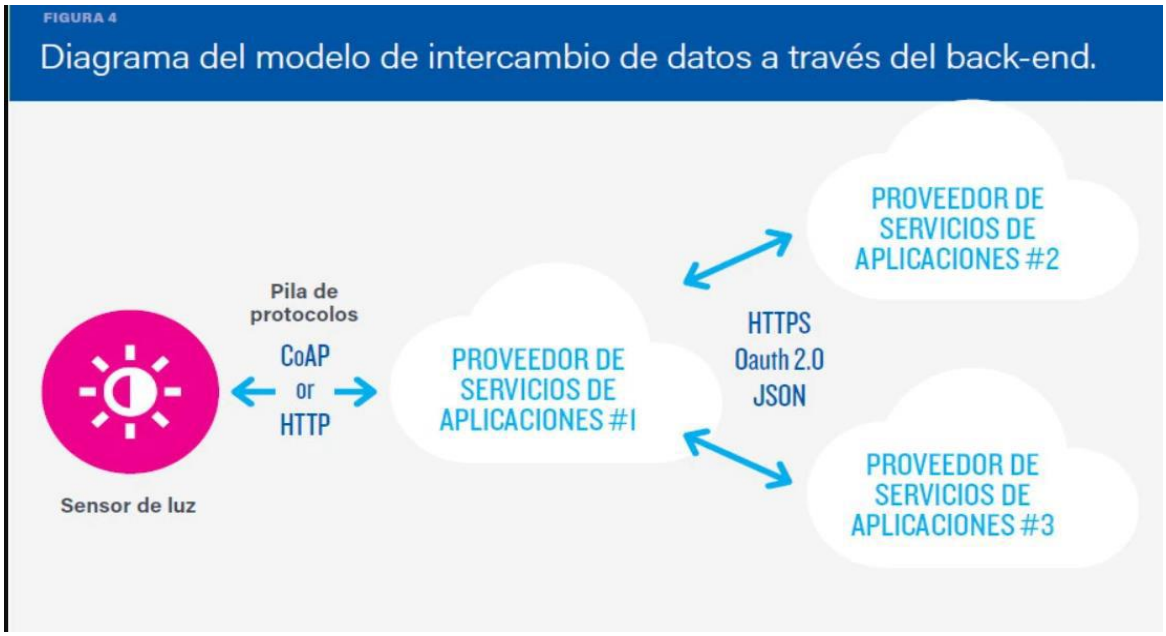
En el modelo de dispositivo a puerta de enlace, los dispositivos se conectan básicamente a un dispositivo intermediario para acceder a un servicio en la nube. Si la puerta de enlace es un teléfono inteligente, este software podría

adoptar la forma de una aplicación que se empareja con el dispositivo de IoT y se comunica con un servicio en la nube.



d) Back End Data Sharing

Back-End Data-Sharing extiende esencialmente el modelo de comunicación de dispositivo a nube para que terceros autorizados puedan acceder a los dispositivos y los datos del sensor. Bajo este modelo, los usuarios pueden exportar y analizar datos de objetos inteligentes desde un servicio en la nube en combinación con datos de otras fuentes y enviarlos a otros servicios para su agregación y análisis.



Ventajas de las comunicaciones Wireless:

· Escalable: Las redes inalámbricas no requieren ninguna instalación de hardware. Típicamente involucran configuraciones y pueden estar listos y funcionando en poco tiempo. También se pueden ampliar muy fácilmente sin tener en cuenta las obstrucciones de la instalación.

· Bajo coste: Debido al avance en la tecnología inalámbrica, así como al número de fabricantes, el coste de la tecnología inalámbrica ha ido disminuyendo en los últimos años.

Desventajas de las comunicaciones Wireless:

· Interferencia: Los dispositivos electrónicos en las proximidades de las redes inalámbricas pueden interferir fácilmente y pueden causar pérdidas en la conexión o reducir la calidad de la misma.

• Velocidad más lenta: Las redes inalámbricas son susceptibles a una mayor latencia e interferencia de señal lo que afecta a la velocidad y consistencia de los datos.

Otra forma de transmitir datos en el IoT es mediante conexiones alámbricas o cableadas, se pueden conectar mediante cables Ethernet o USB.

· ETHERNET: es una tecnología de red cableada que utiliza cables de cobre para transmitir datos.

· USB (Universal Serial Bus): dentro del mundo IoT, se utilizan para conectar sensores, actuadores y demás dispositivos a un sistema central o a una unidad de procesamiento.

· Fibra Óptica: ideal para aplicaciones que requieran alta velocidad.

Ventajas de los dispositivos conectados con redes alámbricas (wired):

· Fiabilidad: Las conexiones Ethernet existen desde hace mucho más tiempo que la tecnología Wi-Fi, lo que la hace mucho más fiable. Son menos propensos a las conexiones caídas y son más confiables sin necesidad de depuración constante.

· Velocidad: Las conexiones por cable se ven menos afectadas por factores locales como paredes, suelos, armarios, longitud de la habitación, interferencias de otros dispositivos electrónicos, etc. Esto permite que la conectividad por cable sea mucho más rápida que la inalámbrica. Las transmisiones de datos por cable no son sensibles a las distancias y la colocación de los dispositivos no tiene ningún efecto adverso en el rendimiento de la conexión.

· Seguridad: Las conexiones por cable suelen estar alojadas detrás del cortafuegos de su red de área local (LAN) y, por lo tanto, permiten un control completo del sistema de comunicaciones. Esto significa que no hay datos de transmisión que puedan ser pirateados.

Desventajas:

· Coste: Las conexiones por cable son más caras que las inalámbricas debido al costo del alambre, los costos de mano de obra para la instalación. En el caso de un cable dañado, los costes de reparación o sustitución son también muy elevados en comparación con las redes inalámbricas de mantenimiento relativamente bajo.

· Movilidad: Las redes cableadas tendrían que estar enterradas en paredes, suelos y techos para llegar a los sensores que necesitan conectarse a ellas. Dado que los sensores son pequeños y pueden colocarse en cualquier lugar de una instalación, a veces sería físicamente imposible alcanzarlos.

· Escalabilidad: La construcción y extensión de redes cableadas requiere planificación y presupuesto para su construcción. Los sistemas alámbricos necesitan que el hardware sea adquirido, instalado y configurado antes de que pueda ser completamente operativo. La escalabilidad sería un problema no sólo para que las redes funcionen rápidamente, sino también para la planificación y los costes.

2– ¿Cómo se aplica la amplitud modulada (AM) en sistemas IoT? ¿Dónde se usa? Ejemplifique.

La amplitud modulada (AM) es una técnica de modulación utilizada en la transmisión de señales de radio en la que se varía la amplitud de la señal

portadora de alta frecuencia de acuerdo con la información de la señal de baja frecuencia que se desea transmitir.

En los sistemas de IoT (Internet de las cosas), la AM se puede utilizar para transmitir señales de sensores y otros dispositivos conectados a través de redes inalámbricas de largo alcance como LoRaWAN y Sigfox. En este caso, los sensores o dispositivos IoT emiten una señal de baja frecuencia que se modula en amplitud en una señal de alta frecuencia para su transmisión a través de la red inalámbrica.

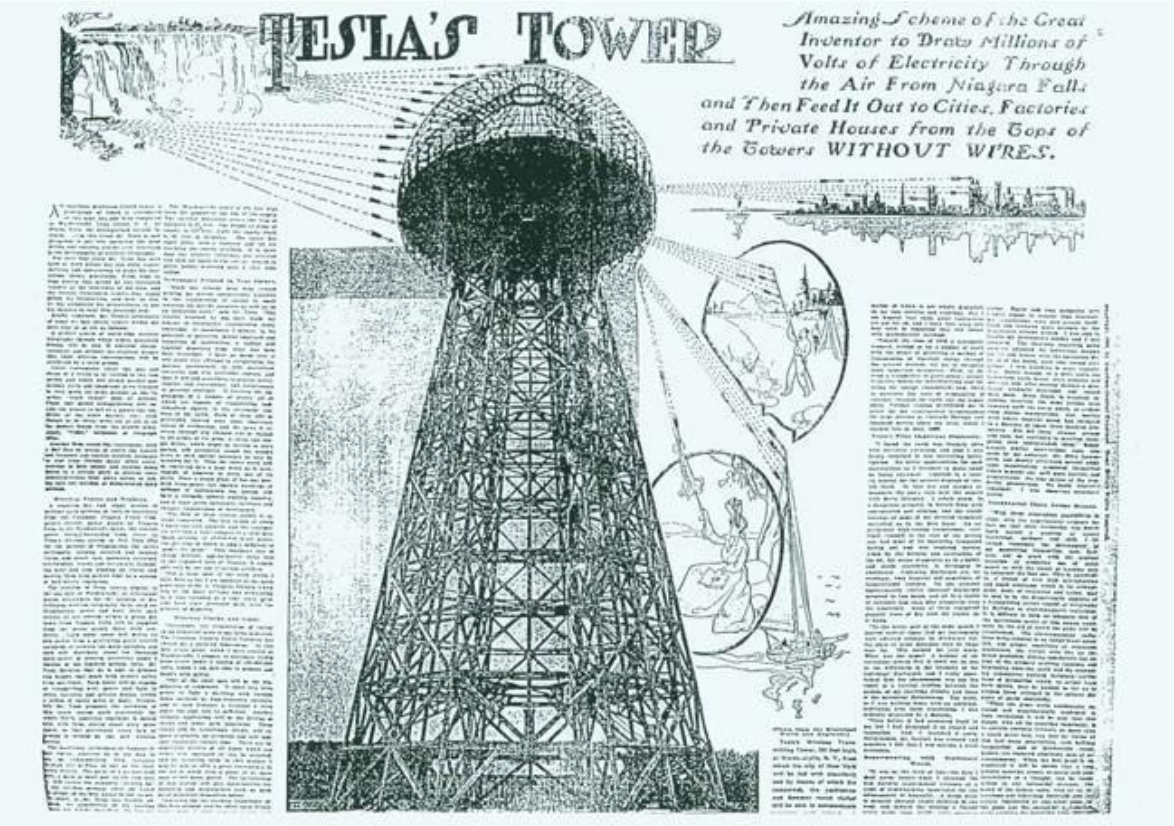
Por ejemplo, en la agricultura de precisión, los sensores IoT se utilizan para medir la humedad del suelo, la temperatura y otros parámetros importantes para el crecimiento de los cultivos. Estos sensores pueden estar equipados con dispositivos de modulación AM que les permiten enviar señales a un concentrador o una estación base que se comunica con una red LoRaWAN. La señal modulada se transmite a través de la red inalámbrica y se puede recibir en una estación central de datos para su procesamiento y análisis.

En resumen, la AM es una técnica de modulación utilizada en sistemas IoT para transmitir señales de baja frecuencia de dispositivos conectados a través de redes inalámbricas de largo alcance. Se puede utilizar en una variedad de aplicaciones, incluyendo agricultura de precisión, monitoreo ambiental y seguimiento de activos.

3– ¿Cómo se aplica la Frecuencia Modulada (FM) en sistemas IoT?. ¿Dónde se usa?. Ejemplifique.

RFEH es una forma de técnica de transferencia de energía inalámbrica en la que las señales de radio Frecuencia (RF) recibidas se convierten en

electricidad. También conocido como barrido de energía de RF. El dispositivo de recolección de energía de RF puede proporcionar energía para dispositivos no conectados. Hay dos casos de uso: la captación de la señal RF para alimentar el propio de-modulador y receptor de la señal para utilizarla como la antigua radio de galena o los actuales Tags de RFID. O capturar la energía de RF para alimentar un circuito con otro propósito como el de leer un sensor de temperatura.



Su historia es larga

Allá por el año 1901 se empezó a construir una torre Wardenclyffe. Fué diseñada e ideada por el inventor Nikola Tesla con la intención de suministrar energía libre de forma inalámbrica. Y es ahora, 120 años después. Que otras torres, esta vez en forma de antenas van a lograr su sueño.

Esta técnica no ha empezado de la mano del movimiento Maker actual, sino de los ingenieros que diseñaron las Radios de Galena. Eran dispositivos de recepción de emisiones de radio de Amplitud Modulada (AM) y Onda Media y que no necesitaban alimentación eléctrica ya que la tomaban a través de la antena. La señal se sintonizaba con una bobina y se rectificaba gracias a la propiedad de un cristal semiconductor de sulfuro de plomo, que es el mineral de galio de donde viene su nombre.

Cómo se aplica la Frecuencia Modulada (FM) en sistemas IoT.

La frecuencia modulada en IOT permite transmitir información a través de una onda portadora variando su frecuencia. En aplicaciones analógicas, la frecuencia instantánea de la señal modulada es proporcional al valor instantáneo de la señal moduladora. Se puede enviar datos digitales por el desplazamiento de la onda de frecuencia entre un conjunto de valores discretos, modulación conocida como modulación por desplazamiento de frecuencia.

Dentro de los avances más importantes que se presentan en las comunicaciones, uno de los más importantes es, sin duda, la mejora de un sistema de transmisión y recepción en características como la relación señal–ruido, pues permite una mayor seguridad en las mismas. Es así como el paso de modulación de amplitud (AM), a la modulación de frecuencia (FM) establece un importante avance no solo en el mejoramiento que presenta la relación señal ruido, sino también en la mayor resistencia al efecto del desvanecimiento y a la interferencia, tan comunes en AM.

La modulación de frecuencia también se utiliza en las frecuencias de audio para sintetizar sonido. Esta técnica, conocida como síntesis FM, fue popularizada en los inicios de los sintetizadores digitales y se convirtió en una

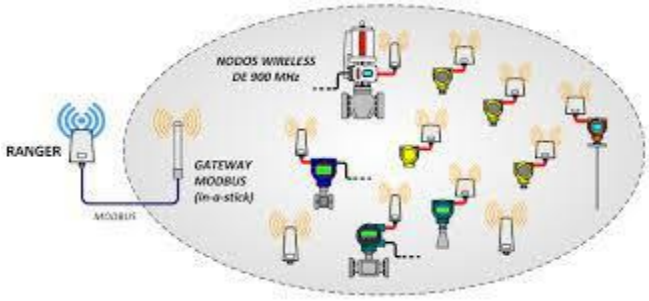
característica estándar para varias generaciones de tarjetas de sonido de computadoras personales.

Donde se utilizan estos dispositivos?

Estos dispositivos inteligentes son utilizados en la fabricación, el comercio minorista, el sector de la salud y otras empresas para generar eficiencias empresariales.

Ejemplos de dispositivos:

Módulo de radio LoRa de ultra largo alcance: RF1276



4– ¿Cómo se aplica la Cuadratura de Amplitud (QAM) en sistemas IoT?. ¿Dónde se usa? Ejemplifique.

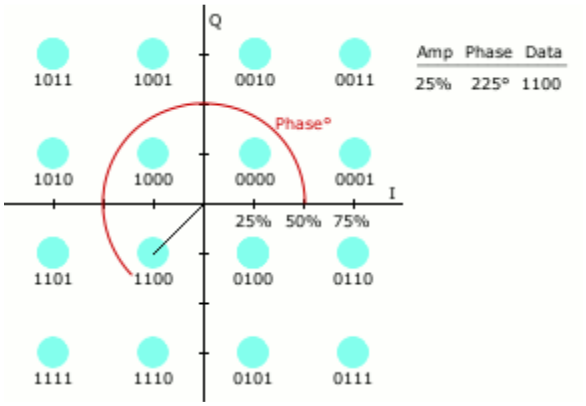
Modulación QAM

La señal modulada en QAM está compuesta por la suma lineal de dos señales previamente moduladas.

Modulación de amplitud en cuadratura QAM (Quadrature Amplitude Modulation) consiste en modular por desplazamiento en amplitud (ASK) de

forma independiente, dos señales portadoras que tienen la misma frecuencia pero que están desfasadas entre sí 90º.

La señal modulada QAM es el resultado de sumar ambas señales ASK. Estas pueden operar por el mismo canal sin interferencia mutua porque sus portadoras al tener tal desfase, se dice que están en cuadratura. Estas dos ondas generalmente son señales sinusoidales en la cual una onda es la portadora y la otra es la señal de datos.



Ecuación Matemática

Las amplitudes de las dos señales moduladas en ASK (a y b),toman de forma independiente los valores discretos an y bn correspondientes al total de los “N” estados de la señal moduladora codificada en banda base multinivel N= n x m.

Las amplitudes de las dos señales moduladas en ASK (a y b), toman de forma independiente los valores discretos an y bn correspondientes al total de los “N” estados de la señal moduladora codificada en banda base multinivel N= n x m. Una modulación QAM se puede reducir a la modulación simultanea de amplitud ASKn,m y fase PSKn,m de una única portadora, pero solo

cuando los estados de amplitud An,m y de fase Hn,m que esta dispone, mantienen con las amplitudes de las portadoras originales an y bn.

Ventajas.

- Mayor inmunidad al Ruido.
- Menor consumo de energía eléctrica.
- Menor costo.
- Mayor capacidad para acarrear grandes cantidades de información respecto a los métodos de modulación analógica.
- Proveen transmisiones de mejor calidad.
- Compatibilidad con servicios digitales de datos.
- Mayor seguridad en la transmisión de información.

Inmunidad al ruido.

La inmunidad que tiene la señal modulada en cuanto a las perturbaciones y al Ruido de la línea, es mayor cuanto más separados estén los puntos del diagrama de estados. Se trata, pues, de buscar una "constelación" de puntos, en analogía con la astronomía, con unas coordenadas de amplitud y fase que hagan máxima la separación entre ellos.

El 2019 marco el lanzamiento del estándar inalámbrico 802.11ax, mejor conocido como Wi-Fi 6. Esta tecnología aporta mayor velocidad que su antecesor, sino una mejor experiencia de usuario en múltiples sentidos, ante la proliferación de dispositivos móviles y del IoT.

Lo primero y básico es que el Wi-Fi 6 no es un nuevo medio para conectarse a Internet como fibra, sino que es un estándar actualizado que los dispositivos de Wi-Fi, especialmente los enrutadores, pueden aprovechar para transmitir señales Wi-Fi de manera más eficiente.

Se están implementando los enrutadores Wi-Fi 6 de marcas como Cisco, Netgear, Asus y TP-Link. El Samsung Galaxy S10, por su parte, fue el primer teléfono compatible con Wi-Fi 6, y otros dispositivos se les seguirán sumando.

En la Argentina, la Secretaría de Innovación Pública estableció un marco regulatorio para comenzar a comercializar la red Wi-Fi 6 y Wi-Fi 6E en el país.

El Wi-Fi 6 utiliza las mismas bandas que el Wi-Fi tradicional, pero el Wi-Fi 6E utiliza una nueva banda de frecuencias en el rango de 5925 MHz a 7125 MHz.

Se publicó la Resolución 102/2020 en el Boletín Oficial para reglamentar el uso de esta banda ancha. Según la resolución, atribuirían la banda de frecuencias de 5925 a 6425 MHz a "los servicios de la tecnología de la información y las comunicaciones (TIC) de tipo fijo y móvil para uso privado"

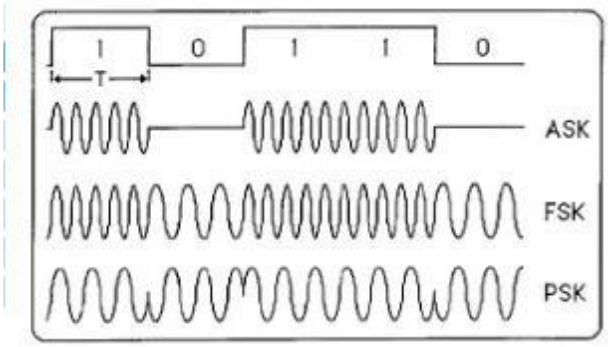
Esta tecnología tiene mayor cobertura y mejor rendimiento en zonas con más usuarios conectados que el Wi-Fi tradicional por su modulación 1024-QAM. Este tipo de modulación conocida como "amplitud en cuadratura" aguanta altas demandas. Cuanto más QAM tenga tu router, más códigos binarios se transmiten por la red.

Según la subsecretaría, mejorará el rendimiento de "aplicaciones que demandan un mayor ancho de banda, como la transmisión de video de alta definición".

5) ¿Cómo se aplica las Modulaciones Digitales ASK, FSK, PSK en sistemas IoT?. ¿Dónde se usa? Ejemplifique.

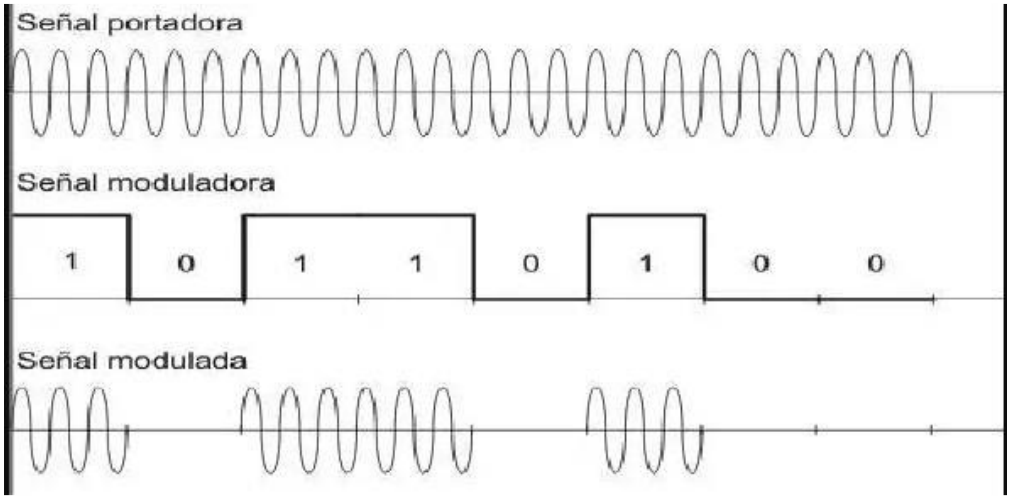
Para los sistemas digitales de comunicación que emplean canales pasa banda, resulta ventajoso modular una portadora analógica con la corriente

digital de datos antes de la transmisión. Las tres formas básicas de la modulación digital correspondiente a la AM, FM y PM se conocen como conmutación de desplazamiento de amplitud (ASK Amplitude- shift keying) Conmutación de desplazamiento de frecuencia (FSK Frecuency- Shift keying) y conmutación por desplazamiento de fase (PSK Phase-shift Keying). Esta práctica abarca las técnicas de modulación digital.



ASK (Modulación por desplazamiento de amplitud)

En el conmutador de desplazamiento de amplitud, la amplitud de una señal portadora de alta frecuencia se alterna entre dos valores en respuesta a un código PCM. En el caso binario, la elección habitual es el conmutador de encendido-apagado, la onda de amplitud resultante consiste en pulsos de RF, llamado marcas, que representa el binario 1, y espacios que representan al binario 0.



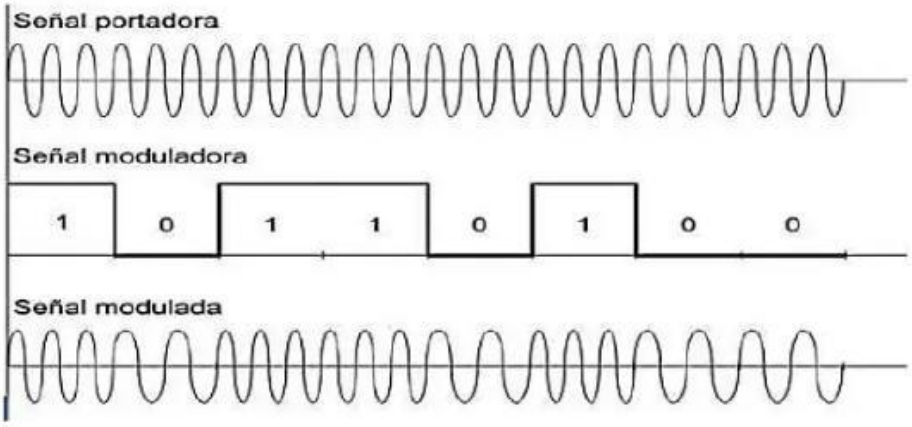
La modulación en ASK no es otra cosa que una variante de la modulación en AM que se adapta perfectamente a las condiciones de los sistemas digitales, además de que les permite trabajar sobre una sola frecuencia de transmisión en vez de tener que lidiar con pulsos cuadrados que contienen componentes en todas las frecuencias del espectro.

Su recuperación también resulta ser más sencilla, dado que sólo depende de sincronizar la frecuencia de las señales sinusoidales que sirven de portadoras y regeneradoras dependiendo si se hallan en el modulador o el demodulador.

El ASK por sí sólo, a pesar de todas estas consideraciones, no es uno de los métodos más utilizados debido a que para cada frecuencia es necesario realizar un circuito independiente, además de que sólo puede transmitirse un solo bit al mismo tiempo en una determinada frecuencia. Otro de los inconvenientes es que los múltiplos de una frecuencia fundamental son inutilizables y que este tipo de sistemas son susceptibles al ruido.

FSK (Modulación desplazamiento de frecuencia)

Este es un tipo de modulación de frecuencia cuya señal modulante es un flujo de pulsos binarios que varía entre valores predeterminados. En los sistemas demodulación por salto de frecuencia. La señal moduladora hace variar la frecuencia de la portadora, de modo que la señal modulada resultante codifica la información asociándola a valores de frecuencia diferentes.



La frecuencia instantánea de la señal portadora se alterna entre dos o más valores en respuesta al código PCM. La onda FSK puede considerarse compuesta por dos ondas ASK de diferentes frecuencias portadoras.

La señal moduladora solo varía entre dos valores de tensión discretos formando un tren de pulsos donde uno representa un "1" o "marca" y el otro representa el "0" o "espacio". Generalmente estas 2 frecuencias de la señal corresponden a desplazamientos de igual magnitud pero en sentidos opuestos de la frecuencia de la señal portadora.

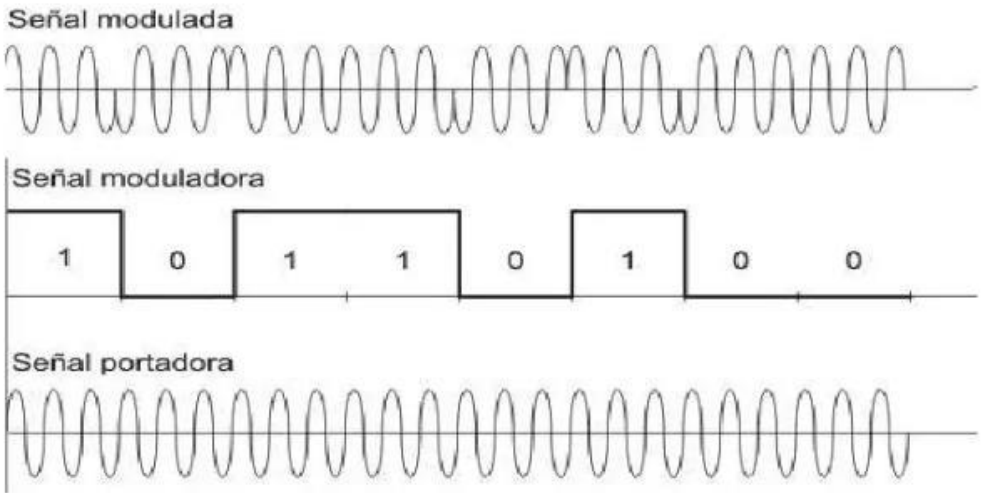
Las ventajas de FSK sobre ASK se hacen notables cuando el índice de modulaciones grande debido a que se aumenta la protección contra el ruido y las interferencias, obteniendo un comportamiento más eficiente respecto a ASK, puesto que en este caso la pequeña modulación de amplitud mencionada en el caso de FSK de banda angosta, se hace despreciable.

PSK (Modulación por desplazamiento de fase)

Esta es una forma de modulación angular que consiste en hacer variar la fase de la portadora entre un número determinado de valores discretos. La diferencia con la modulación de fase convencional (PM) es que mientras en ésta la variación de fase es continua, en función de la señal moduladora, en la PSK la señal moduladora es una señal digital y, por tanto, con un número de estados limitado.

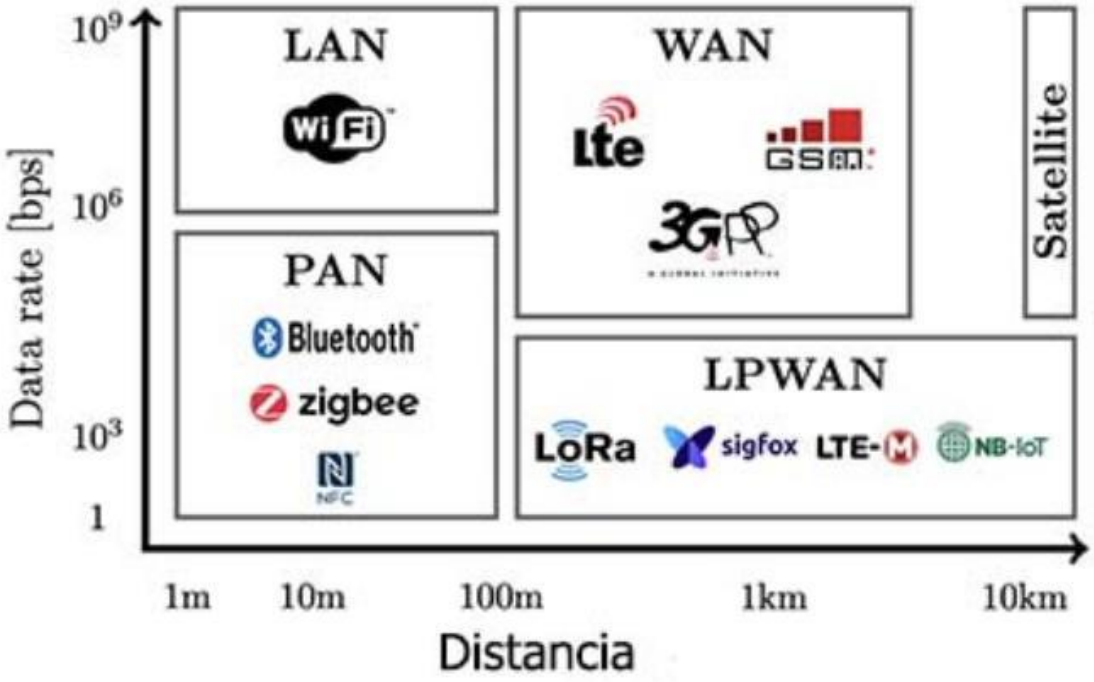
Con la transmisión de desplazamiento de fase binaria son posibles dos fases de salida para una sola frecuencia de la portadora, una fase de salida representa el “1”lógico y la otra un “0” lógico, conforme la señal digital de entrada cambia de estado, la fase de la portadora de salida se desplaza entre dos ángulos que están 180° fuera de fase (otro nombre para esta modulación es transmisión inversa de fase PRK).

La modulación PSK se caracteriza porque la fase de la señal portadora representa cada símbolo de información de la señal moduladora, con un valor angular que el modulador elige entre un conjunto discreto de 2 valores posibles. Un modulador PSK representa directamente la información mediante el valor absoluto de la fase de la señal modulada, valor que el demodulador obtiene al comparar la fase de ésta con la fase de la portadora sin modular



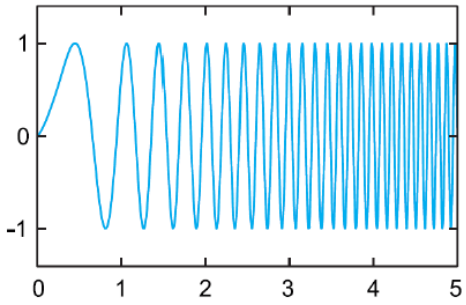
Aplicaciones

- La modulación por desplazamiento de frecuencia y la modulación por desplazamiento de amplitud se utilizan típicamente a velocidades de hasta 1.200 bps en líneas de calidad telefónica.
- La modulación por desplazamiento de fase es usada en: LAN inalámbrica, RFID (Transmisores pasivos), bluetooth 2.0, televisión en alta definición y la televisión satelital.
- En ASK transmisiones con fibra óptica, ya que es muy fácil "encender" y "apagar" el haz de luz; además la fibra soporta las desventajas de los métodos de modulación de amplitud ya que posee poca atenuación.
- La modulación por desplazamiento de amplitud se solía usar en transmisión de datos en código morse.
- Transmisión por Cable transoceánico.



Protocolos usuales en internet de las cosas.

Modulación de LoRa



LoRa Chirp Spread Spectrum illustration.

Debemos conocer un poco sobre la modulación de LoRa cuando deseamos trabajar con esta tecnología, para así entender cómo funciona la misma y comprender su potencial.

En los sistemas de espectro ensanchado de secuencia directa (DSSS), la fase de la portadora cambia de acuerdo con una secuencia de códigos, logrado al multiplicar la señal de data con un código de ensanchamiento.

Este código es una secuencia de pulsos *chips*. Esta secuencia se produce a una velocidad de datos mucho más rápida que la señal de datos, ensanchando así el ancho de banda de la señal original.

Es importante tener claro que el término *chip* se utiliza para distinguir los bits codificados más cortos de los bits sin codificar más largos de la señal de información.

En el receptor, la data se recupera al multiplicar la señal recibida por una réplica de la secuencia de código generada localmente, lo que descomprime efectivamente la señal ensanchada a su original ancho de banda sin ensanchamiento.

El DSSS es ampliamente usado en aplicaciones de comunicación de datos. Pero no está diseñado para dispositivos de bajo costo y poco consumo de energía.

La modulación de LoRa aborda todos los problemas asociados con los sistemas de DSSS, en términos de bajo consumo y añadiendo robustez a las técnicas tradicionales de espectro ensanchado.

La gran diferencia que tiene la modulación LoRa, respecto a la modulación tradicional de espectro ensanchado, es que una vez la señal de data es llevada a una velocidad de datos más alta (mediante la secuencia de *chip*) es modulada en una señal *Chirp* que varía continuamente en la frecuencia, por eso la modulación LoRa recibe el nombre de CSS.

6) ¿Qué es el Protocolo HTTP?, ¿Cuáles son sus características? Ejemplifique.

HTTP (Hypertext Transfer Protocol), en español: Protocolo de Transferencia de Hipertexto, es el protocolo por excelencia de transferencia para el hipertexto. Por lo tanto, es el enlace de normas para transportar archivos de texto, imágenes, gráficas, sonido, video y otros tipos de archivos multimedia que pueden ser consumidos en la World Wide Web. Es un protocolo de comunicación entre aplicaciones basado en el intercambio de texto. El protocolo HTTP es el que impulsa todo internet. Los navegadores web utilizan este protocolo para solicitar páginas web a los servidores. El servidor devuelve todos los datos necesarios en código HTML para que puedan mostrarse en el navegador.

Cómo Funciona El Protocolo HTTP

Así como los humanos nos comunicamos a través del lenguaje, las computadoras se pueden comunicar a través de HTTP gracias al modelo de TCP/IP.

Las reglas principales de HTTP se suelen definir por los *headers*, que se dividen en dos grupos: los *headers* de petición y los headers de respuesta:

Header request (petición)

Suelen estar definidos por el método de petición, hacia donde se hará el *request*, y la información que enviará la petición.

Header response (respuesta)

Suele estar definido principalmente por la respuesta del servidor y también por las características de la respuesta.

Características del protocolo HTTP

Las características principales del protocolo HTTP son:

1. Conexión única

Desde la versión 2.0 de HTTP, este usa una conexión única para generar múltiples solicitudes y respuestas en paralelo, lo cual a la hora de procesar las solicitudes genera una eficiencia mayor en la respuesta.

2. Elimina la información redundante

Al eliminar la información redundante se busca evitar el envío de datos repetidos durante una misma conexión, así se consigue un menor consumo de recursos y, por lo tanto, se obtiene una menor latencia.

3. Tiene multiplexación

Al ser un protocolo multiplexado, puede enviar y recibir varios mensajes al mismo tiempo, optimizando la comunicación. Esta característica mejora considerablemente la velocidad de carga.

4. Es un protocolo binario

HTTP trabaja mediante tramas y al ser un protocolo binario facilita encontrar el comienzo y el final de cada *frame,* lo cual al ser un protocolo de texto podría llegar a ser complicado de identificar. Adicionalmente, los protocolos binarios son más simples, por lo que tienden a ser menos propensos a errores.

5. Servicio *server push*

Este servicio de HTTP se basa en estimaciones con las que el servir es capaz de enviar información al usuario antes de que esta sea solicitada para conseguir que la información esté disponible de forma inmediata.

6. Compresión de cabeceras

En versiones anteriores, dados los requerimientos de las solicitudes, las cabeceras tenían un tamaño considerable, lo cual aumentaba el tiempo para obtener respuestas. A partir de la versión 2.0 las cabeceras empezaron a ser comprimidas para mejorar la eficiencia en la respuesta haciendo uso de un algoritmo simple y poco flexible llamdo HPACK.

7. Priorización de flujos

Un mensaje HTTP se puede dividir en múltiples fragmentos al ir desde el cliente hasta el servidor o viceversa y el orden en que lleguen a su destino es fundamental, es por eso que a cada flujo de le puede asignar un peso que va desde 1 hasta 256 y una dependencia. Haciendo uso de las prioridades y dependencias el protocolo crea un árbol de prioridades para los mensajes y solicitudes.

7) Qué es el Protocolo HTTPS?, ¿Cuáles son sus características? Ejemplifique

En la actualidad, la seguridad y privacidad al navegar por los sitios web, se estima como una prioridad para todos los internautas. Gracias a dicha

necesidad global, surgió el reconocido protocolo HTTPS o “Protocolo seguro de transferencia de hipertexto” que proporciona un completo cifrado y autenticado a los usuarios de la red.

En vista de su notable potencia, muchas personas desean conocer, verdaderamente, para que sirve este protocolo y cuáles son sus principales características. Por lo que, en este post, especificaremos dicha información y, adicionalmente, mencionaremos cuáles son sus mejoras y limitaciones, como funciona y por qué garantiza la mayor seguridad posible en la red.

Si bien es cierto, HTTPS hace referencia a un protocolo de aplicación que está destinado a la transferencia segura de datos de hipertexto y se basa en el protocolo HTTP, pero es la versión segura de este. Así, consiste en un protocolo que ofrece la posibilidad de establecer una conexión fiable entre el cliente y el servidor con el objetivo de evitar cualquier intercepción por parte de personas no autorizadas.

En tal sentido, el Protocolo Seguro para la Transferencia de Hipertexto opera como un tipo de conexión que sirve para encriptar los datos de los usuarios. Gracias a esto, las personas que navegan en la red podrán obtener un intercambio de datos completamente encriptado, en vista de que el servidor estará autenticado.

En cuanto a su funcionamiento, básicamente, cuando un usuario confirma una entrada de URL en la barra de direcciones con la tecla Enter o, en su defecto, hace clic en un enlace; el navegador establece una conexión de forma automática. A continuación, con el uso del protocolo HTTPS, el servidor presenta un certificado que lo autentica como un proveedor confiable. Después, el usuario podrá verificar dicha autenticidad y con ello,

enviará una clave de sesión que solo será leída por el servidor; sin la intercepción de un tercero.

Dado su funcionamiento, la principal particularidad del famoso protocolo HTTPS, radica en que se ocupa de crear un canal seguro sobre una red insegura, básicamente. Con ello, logra proporcionar una protección contra diferentes tipos de ataques o amenazas, para garantizar que el servidor sea verificado y resulte de confianza.

Por su parte, de forma técnica, el Protocolo Seguro para la Transferencia de Hipertexto, contempla las siguientes características de sumo interés:

- Emplea un cifrado basado en la seguridad de textos SSL/TLS con el objetivo de crear un canal encriptado pertinente para el tráfico de información sensible. Considerando que, el nivel de cifrado dependerá del servidor remoto y el navegador usado.

- Por suerte, su utilización no requiere ninguna instalación de software adicional. Como consecuencia, puede ser empleado por cualquier usuario y sin restricción alguna. Lo cual, inspira confianza en los clientes potenciales, debido a la autenticación que realiza con un certificado.

- El protocolo HTTPS también se caracteriza por mostrar una óptima integración con los principales navegadores web, tales como: Google Chrome, Mozilla Firefox, Opera, Safari e Internet Explorer.

- Generalmente, este protocolo de seguridad se distingue a partir de un icono de candado que se encuentra en la parte derecha de la barra de direcciones. De esa forma, permite identificar páginas web confiables. Considerando que, además, también incluye el término “https” al inicio de la dirección URL.

- El contenido que se transmite con conexiones HTTPS, no puede ser almacenado en caché. Esto, para algunas personas puede ser ventajoso y para otras, un punto en contra.

- Para poder preparar un servidor web, en términos de configuración, para que admita conexiones HTTPS; el administrador tendrá que crear un certificado de clave pública para el servidor web.

- Un protocolo HTTPS puede ser vulnerado cuando se aplica a contenido estático de publicación disponible.

- En caso de que un infiltrado o una persona no confiable logre capturar los datos trasmitidos a partir del protocolo HTTPS, igualmente no podrá descifrar la información en cuestión porque está totalmente encriptada.

El antiguo HTTP consiste en un protocolo que permite realizar una petición de datos y recursos, por lo que se considera la base de cualquier intercambio de datos en la web. Sin embargo, a lo largo del tiempo, ha sido señalado como un protocolo muy fácil de violentar porque simplifica, para todas aquellas personas infiltradas, la captura de datos que se están transmitiendo.

Como consecuencia, se creó el protocolo HTTPS con el objetivo de cambiar la funcionalidad del protocolo HTTP y proporcionar una mayor seguridad.

Puesto que, el Protocolo Seguro para la Transferencia de Hipertexto hace uso de un cifrado en el que los infiltrados no logran descifrar la información, aun y cuando puedan capturar la transmisión de la misma. Pues, se mantiene encriptado en su totalidad. Por lo tanto, la principal diferencia entre el protocolo HTTP y HTTPS, radica en la seguridad que proporcionan. Tomando

en cuenta que, este último emplea la misma tecnología que el antiguo HTTP, pero incluye encriptación SSL.

Sumado a ello, se observan las siguientes distinciones:

- En el protocolo HTTP las direcciones URL inician con “http://”. Mientras que, en el HTTPS, dichos enlaces empiezan con “https://”.

- Generalmente, el protocolo HTTP usa el puerto 80, por omisión. En cambio, los HTTPS utilizan el puerto 443.

- A diferencia del HTTP que está sujeto a ataques man-in-the-middle y eavesdropping, por lo que permiten que las personas malintencionadas adquieran acceso a cuentas de un sitio web, bancos e información confidencial; el HTTPS se encuentra diseñado para soportar y resistir dichos ataques, por lo que resulta más seguro.

- Regularmente, el HTTP opera en la capa más alta del Modelo OSI. Sin embargo, el protocolo HTTPS opera en una subcapa más baja para garantizar el cifrado de un mensaje HTTP previo a la trasmisión y descifrar los datos, una vez recibidos.

Los datos enviados a través de un protocolo HTTPS están asegurados gracias a un protocolo conocido como “Transport Layer Security” o “TLS” que, por defecto, proporciona tres capas de protección primordiales y así, determina el funcionamiento del protocolo HTTPS mejorado.

Dichas capas de protección de red, son las siguientes:

Cifrado

Por lo general, siempre que un equipo emite un mensaje desde el navegador web hacia el servidor web, existe la posibilidad de que la información sea capturada por alguien que está tratando de interceptar el canal de comunicación, con el fin de espiar todo el tráfico.

No obstante, el protocolo HTTPS se encarga de cifrar los datos de intercambios y los mantiene seguros ante miradas indiscretas. Gracias a esto, mientras el usuario esté navegando en un sitio web, ninguna otra persona podrá espiar sus movimientos ni realizar un seguimiento de sus actividades con el objetivo de usurpar su información confidencial. Más bien, la comunicación con el servidor web se hará efectiva de forma segura a partir de un cifrado de punto a punto.

Integridad

Así como existen riesgos de seguridad con los que se puedan perder los datos, también es posible que el mensaje transmitido desde el navegador web hasta el servidor sea capturado con el fin de cambiar la información que hay en él. Por lo que, una vez modificado, se enviará al destinatario y así, afectará la integridad del emisor.

Pero, por suerte, el protocolo HTTPS se ocupa de garantizar la integridad de los datos para que no puedan ser dañados ni modificados durante el proceso de transferencia, independientemente de que haya sido intencional o no. Esto significa que, bajo cualquier circunstancia, el mensaje llegará al receptor exactamente como se envió, sin riesgos a reducir su integridad.

Autenticación

El protocolo HTTPS también provee un gran nivel de autenticación, de forma que, logra proteger a los usuarios en contra de diferentes ataques. De tal

modo, construye la confianza de las personas al suministrar páginas web que sean completamente auténticas.

Lo cual, ha sido verificado previamente, conociendo la identidad de quien ha enviado el mensaje por medio del uso de una firma digital. Por su parte, cabe acotar que, esta ventaja la consigue por medio de los certificados SSL, con los que se puede afirmar que estás conectado al lugar correcto. Tomando en cuenta que, por defecto, un certificado SSL es el encargado de mostrar que el navegador web es válido y que ha sido presentado por una autoridad de certificación legal.

Limitaciones

A pesar de que el protocolo HTTPS mejorado presenta numerosos beneficios a los usuarios, lo cierto es que también tiene algunos puntos en contra que vale la pena tomar en cuenta.

Por consiguiente, a continuación, nombramos cuales son las principales limitaciones o desventajas del HTTPS:

- Por defecto, el nivel de protección depende de la exactitud de la implementación del navegador web y los algoritmos de cifrado soportados. Por lo que, al no ser independientemente, podría presentar ciertas brechas en términos de privacidad.

- A partir de las conexiones HTTPS, es imposible almacenar el contenido en memoria caché. Lo cual, resulta desfavorable para diversos usuarios.

- Se ha evidenciado que, el protocolo HTTPS exhibe vulnerabilidad una vez se aplica a contenido estático de publicación disponible. Lo cual, facilita acciones no fidedignas por parte de usuarios no confiables que buscan tener

acceso al texto plano y al texto cifrado. Esto, sirve para un ataque criptográfico.

- Otro punto débil radica en un menor rendimiento, como resultado del empleo del cifrado SSL. Puesto que, por naturaleza, el servidor tendrá que hacer numerosos cálculos y con ello, incrementa el tiempo de espera para dar respuesta.

- Desafortunadamente, los hosts virtuales no funcionan con el protocolo HTTPS. Pues, los servidores SSL solamente logran presentar un certificado, de manera estricta, para una combinación de Puerto/IP en particular.

- Los cargos adicionales por certificados pueden ser distintamente altos y, aparte, revela costes crecientes debido al aumento del tráfico. Por ende, las tarifas pueden llegar a ser muy altas en sitios web nuevos y pequeños, más que todo.

Seguridad

A pesar de que el protocolo HTTPS garantiza el cifrado en la transmisión de datos, en realidad no es tan seguro como parece. Pues, con las diferentes amenazas que operan en la red actualmente, el símbolo de seguridad de dicho protocolo no logra garantizar que una página web esté protegida en su totalidad. Considerando que, en este momento, los sitios maliciosos utilizan cada vez más HTTPS (sobre todo, los de phishing). Esto se debe a que, una conexión segura no es equivalente a un sitio seguro.

En otras palabras, se destaca que, a pesar de que el protocolo HTTPS cifra la información que es transmitida entre el sitio y tú, no tiene nada que ver con la seguridad del sitio web en concreto. Puesto que, un sitio malicioso podrá conseguir un certificado de este tipo sin problemas y cifrar todo el tráfico que

se produce entre la página y tú para que no existan fisgones de por medio. No obstante, aunque aseguren que nadie más puede espiar los datos que suministras, tu contraseña e información confidencial estará en manos de dichos sitios.

Por lo tanto, podrá ser usurpada desde allí. Es decir, desde una web falsa o insegura. Como conclusión, la presencia del candado correspondiente al protocolo HTTPS, simplemente indica el uso de un certificado que garantiza un tráfico seguro y libre de las miradas de terceros. Sin embargo, dicho protocolo no emite avisos en torno a la inseguridad que contenga un sitio HTTPS malicioso que puede estar manipulado por estafadores online.

8 – ¿Qué son los estándares Web HTML y CSS? ¿Y cuáles son sus características?

En primer lugar, definiremos lo que son los ***estándares web***. son todas aquellas especificaciones y protocolos que describen el comportamiento de la World Wide Web. Estos estándares se caracterizan por ser abiertos, es decir, no estar cubiertos por patentes o licencias de uso, y otorgan una interoperabilidad entre los sitios web y las diferentes herramientas para interactuar con ellos, como navegadores web, software de desarrollo de páginas, lectores especializados, entre otros.

Ahora mencionaremos 2 de los más populares:

HTML (HyperText Markup Language – Lenguaje de marcada de hipertexto): es un estándar a cargo de la W3C que sirve de referencia del software que conecta con la elaboración de páginas web en sus diferentes versiones,

define una estructura básica y un código (código HTML) para la definición del contenido presente en una página web.

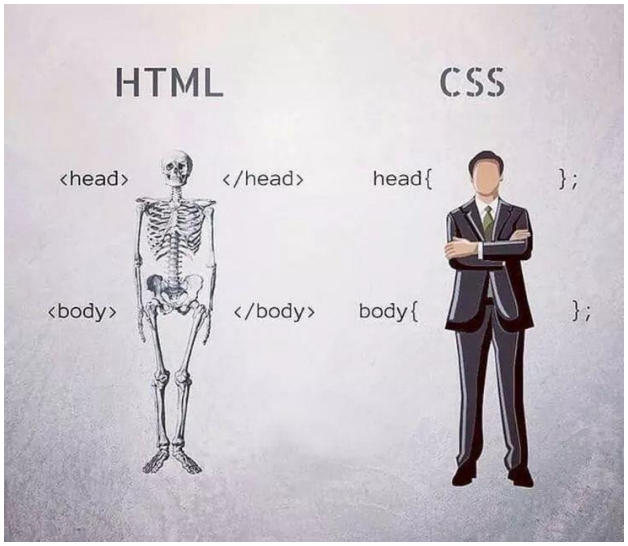
Características de HTML:

- De fácil uso y entendimiento.
- Permite describir hipertextos.
- Multiplataforma.
- Permite la visualización de páginas web aunque no se posea conexión a Internet (se debe haber descargado la información de la página previamente).
- Se constituye de una etiqueta inicial, un bloque de texto y una etiqueta final.
- Es lenguaje estático.
- Etiquetas limitadas.

CSS (Cascading Style Sheets – Hojas de estilo en cascada): es un lenguaje de diseño gráfico usado para definir y crear la presentación visual de una página web escrita en HTML. Está diseñado principalmente para marcar la separación entre el contenido del documento y la presentación del mismo.

Características del CSS:

- Lenguaje sencillo y de muy fácil compresión.
- Optimiza la edición, facilitando así la accesibilidad y promoviendo la creatividad de los desarrolladores.
- Prioriza la limpieza del código.
- Multiplataforma.


HTML
CSS
<head>
</head>
head{
};
<body>
</body>
body{
};