



INTRODUCCIÓN AL INTERNET DE LAS COSAS

CONTENIDO

Introducción.....	4
¿Qué es el internet de las cosas?.....	4
¿Cómo funciona el IOT?.....	4
IoT en la industria.....	6
IoT en agricultura.....	6
IoT en medicina.....	7
IoT en ciudades inteligentes	7
Tecnologías	8
Conceptos de redes LAN.....	8
Importancia del uso de la red LAN.....	8
Protocolo TCP/ IP	9
Protocolo IP.....	12
Capa de Transporte.....	13
Protocolo DHCP.....	13
Funcionamiento y mensajes de intercambio.....	14
Arquitecturas de comunicación IoT.....	15
Protocolo Zigbee.....	17
Aplicaciones de Zigbee.....	17
Automatización del hogar.....	17
Automatización industrial.....	19
Otros usos	19
Protocolo Bluetooth.....	20
Formato de paquetes Bluetooth.....	22
Redes Wi-Fi.....	23
Modo de funcionamiento.....	27
Modo ad hoc.....	28

INTRODUCCIÓN AL INTERNET DE LAS COSAS

Modo infraestructura.....	28
Seguridad.....	29
Plataformas de hardware.....	32
Bluetooth.....	32
Como funciona el Bluetooth.....	32
Usos del Bluetooth.....	33
Wi-Fi.....	33
¿Cómo funciona la tecnología Wi-Fi?.....	34
¿Qué es un punto de acceso inalámbrico?.....	34
¿Qué es un router inalámbrico?.....	34
¿Qué es una zona Wi-Fi portátil?.....	35
Otras plataformas hardware.....	35
Netduino.....	35
.Net Gadgear.....	36
Raspberry PI.....	36
Plataformas de Software.....	37
Node-Red.....	37
Edición de flujo en el navegador.....	37
Arduino IDE.....	39
Como funciona	40
Visualización de datos en la red e inteligencia artificial.....	42
Importancia	43

INTRODUCCIÓN

Se puede explicar de varias maneras, y desde varios puntos de vista, pero la forma más común de describirlo es como un ecosistema de tecnologías que monitorizan el estado de objetos físicos, capturando datos significativos, y comunicando esta información a aplicaciones software a través de redes IP. Estos datos se pueden comunicar al fabricante, al usuario y/o a otros dispositivos conectados a la red. Los conceptos recurrentes en todas las definiciones del Internet de las cosas incluyen los objetos inteligentes (Smart Objects), comunicaciones máquina a máquina (M2M, machine to machine), tecnologías RF y un hub central de información.

Desde que se acuñó por primera vez el término (en 1999, Kevin Ashton), la definición del IoT ha evolucionado a lo largo de los años. Al inicio se usaba para describir las limitaciones de la relación entre internet, los ordenadores, y el mundo físico. Ashton describía cómo casi todos los datos disponibles en internet eran originados por un humano. Con nuevas tecnologías emergentes y más al alcance, Ashton creía que la información acerca de cosas necesitaba que no fuera dependiente de una interacción manual; podía ser un proceso automatizado.

¿Qué es el internet de las cosas?

El Internet de las cosas (IoT) es el proceso que permite conectar elementos físicos cotidianos al Internet: desde objetos domésticos comunes, como las bombillas de luz, hasta recursos para la atención de la salud, como los dispositivos médicos; también abarca prendas y accesorios personales inteligentes e incluso los sistemas de las ciudades inteligentes.

¿Cómo funciona el IOT?

El término IoT hace referencia a todos los sistemas de dispositivos físicos que reciben y transfieren datos a través de redes inalámbricas con intervención

INTRODUCCIÓN AL INTERNET DE LAS COSAS

humana mínima, lo cual es posible gracias a la integración de dispositivos informáticos en todo tipo de objetos.

Por ejemplo, un termostato *inteligente* (es decir, que utiliza el *IoT*) recibe datos de la ubicación de su automóvil inteligente mientras conduce para ajustar la temperatura de su casa antes de que llegue. Todo esto se logra sin su intervención e incluso ofrece un mejor resultado que si lo hiciera de forma manual.

Un sistema de IoT tradicional, como el hogar inteligente descrito anteriormente, funciona enviando, recibiendo y analizando datos de forma permanente en un ciclo de retroalimentación. Según el tipo de tecnología de IoT, las personas o los sistemas de inteligencia artificial y aprendizaje automático (IA/ML) pueden analizar estos datos casi de inmediato o durante un cierto tiempo.

Los dispositivos de IoT están potenciados para ser nuestros ojos y oídos cuando no podemos estar allí físicamente. Equipados con sensores, los dispositivos capturan los datos que podríamos ver, oír o percibir. Luego comparten los datos según lo indicado y los analizamos para que nos ayuden a fundamentar y automatizar nuestras acciones o decisiones posteriores. Hay cuatro etapas clave en este proceso:

1. . Capturar los datos. A través de sensores, los dispositivos de IoT capturan datos de sus entornos. Esto podría ser tan simple como la temperatura o tan complejo como un feed de video en tiempo real.
2. . Compartir los datos. Usando las conexiones de red disponibles, los dispositivos de IoT hacen que estos datos sean accesibles a través de una nube pública o privada, según se indique
3. . Procesar los datos. En este punto, el software se programa para que haga algo en base a esos datos –como encender un ventilador o enviar una advertencia–.
4. .Actuar según los datos. Se analizan los datos acumulados de todos los dispositivos de una red de IoT. Esto brinda información estratégica poderosa para fundamentar acciones y decisiones de negocio confiables.

IoT en la industria

El mantenimiento preventivo es una de los campos industriales donde el Internet de las Cosas más se aplica; tradicionalmente, el mantenimiento de maquinaria y equipamiento industrial se realiza a partir de inspecciones periódicas y segmentadas, lo que puede provocar fallas y descomposturas imprevistas; el uso de sensores de IoT conectados a máquinas y equipo permite, en tiempo real, monitorear las condiciones generales de su funcionamiento: temperatura, niveles de combustibles y lubricantes, compresión, calidad de las piezas, etc., enviando datos a un centro de control que los procesa y con la ayuda de Machine Learning alerta posibles irregularidades, anticipándose a ellas.

Otra función altamente beneficiosa de IoT en la industria es el sector de los almacenes inteligentes, que a través de sensores registran en tiempo real el estado de los productos almacenados en bodegas, asegurando la preservación de su calidad; con ayuda de la robótica, un almacén inteligente puede funcionar de manera eficiente y automatizada, ahorrando costos y aumentando la productividad.

IoT en agricultura

Esta tecnología está revolucionando el sector agrícola por medio de sensores que miden en tiempo real las condiciones de los cultivos, antes y después de ser sembrados, reconociendo la calidad del suelo, su humedad, bioquímica, contenido de nutrientes, así como las condiciones atmosféricas del plantío; estos datos permiten elaborar una estrategia de cultivo integral que prevé situaciones irregulares e indica cómo efectuar el riego de agua y qué tipo de fertilizantes utilizar.

IoT en medicina

Por medio de wearables –un emblemático dispositivo de la dinastía IoT– y otros gadgets, es posible conectar el estado de salud de una persona enferma o no con médicos, centros de salud o parientes, quienes pueden detectar en tiempo real

INTRODUCCIÓN AL INTERNET DE LAS COSAS

las irregularidades y actuar en consecuencia o prever un síntoma que se avizora en el futuro gracias a los datos recabados de la presión arterial del paciente, nivel de glucosa, temperatura, entre otros.

IoT en ciudades inteligentes

Una de las prioridades de muchas ciudades del mundo es volverse inteligentes y conectarse entre sí; la base de ello es la tecnología IoT que busca optimizar el funcionamiento complejo de una urbe, dinamizarlo, volverlo más seguro e intentar resolver problemas como la vialidad, el transporte y la contaminación, que no fueron previstos a tiempo.

Existe todo un abanico de aplicaciones de IoT para el sector urbano; uno de ellos son los semáforos inteligentes que operan a partir del registro de datos reales del tránsito vehicular (en lugar de patrones estandarizados), otro es el uso del teléfono celular para detectar un lugar donde estacionar un vehículo; de igual modo, es posible rastrear en tiempo real, con GPS, cualquier tipo de vehículos – personales, empresariales, de servicios públicos–, así como el empleo de navegadores digitales que señalan las rutas más viables y fluidas.

TECNOLOGÍAS

Conceptos de redes LAN

Las redes de área local (Local Area Network) son un conjunto de dispositivos electrónicos conectados entre sí que comparten una línea de comunicación común

www.inadet.com.mx

INTRODUCCIÓN AL INTERNET DE LAS COSAS

o un enlace inalámbrico con un servidor. La conexión LAN abarca dispositivos y periféricos conectados a un servidor dentro de un área relativamente pequeña, como una oficina, sucursal o edificio. Este tipo de red fue desarrollado para transmitir cantidades de datos grandes en poco tiempo.

Los dispositivos conectados con este tipo de enlace, comparten herramientas y recursos como la misma conexión a Internet, impresoras, escáneres, cámaras, discos duros (u otro dispositivo de almacenamiento), programas que permiten intercambiar archivos, mensajes, realizar llamadas por IP o sesiones de video.

Importancia del uso de la red LAN

Como especialistas en consultoría de redes domésticas e industriales, sabemos que este sistema permite poder compartir datos y recursos; de ahí que se puede decir que, para las grandes empresas, este tipo de conexiones les permiten realizar sus actividades a nivel local e internacional.

La red LAN se basa en la conexión de varios dispositivos pequeños llamados nodos para poder acceder a los datos y recursos que tienen esos dispositivos entre sí. Se pueden controlar los datos de impresión, datos de disco duro y discos de almacenamiento externo que se sitúan de manera remota.

Sin embargo, la red LAN tiene también cosas en contra, debido a que el rango al que pertenece la ubicación donde estemos puede ser pequeño. Además, la distancia al nodo principal va a tener mucha relación con la calidad de servicio y velocidad que tenga nuestro dispositivo.

También es importante comentar que el número de nodos que se pueden conectar a una sola *Local Area Network* es limitado. Cuantos más nodos se carguen a la red, mayor necesidad de recursos necesitará la computadora y más complicado se hará realizar una conexión.

INTRODUCCIÓN AL INTERNET DE LAS COSAS

Este tipo de redes son de uso común y cotidiano en negocios, empresas y hogares, pudiendo presentar una topología de red distinta de acuerdo a las necesidades específicas de la red, tales como:

- **Red en bus.** En la que un mismo cable (o *backbone*) conecta a las computadoras y permite la transmisión de datos en línea recta, haciéndola sencilla pero susceptible a daños del cable o a la interrupción del tráfico.
- **Red en estrella.** En la que todos los computadores se conectan a un servidor central que administra los recursos de la red y los asigna según se le solicite.
- **Red en anillo.** En la que todos los computadores están conectados con sus vecinos mediante una transmisión unidireccional, que interrumpe la red de haber un fallo en algún nivel de la misma.
- **Red mixta.** Combina dos o más modelos de los anteriores.

Protocolo TCP/ IP

Los protocolos son conjuntos de normas para formatos de mensaje y procedimientos que permiten a las máquinas y los programas de aplicación intercambiar información. Cada máquina implicada en la comunicación debe seguir estas normas para que el sistema principal de recepción pueda interpretar el mensaje. El conjunto de protocolos TCP/IP puede interpretarse en términos de capas (o niveles).

Capa

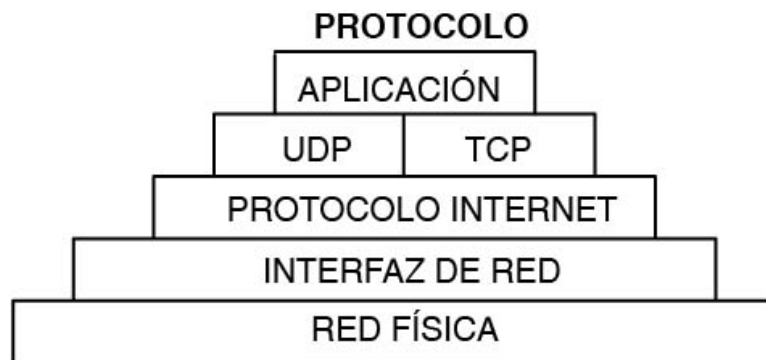
Capa de aplicación

Capa de transporte

Capa de red

Capa de interfaz de red

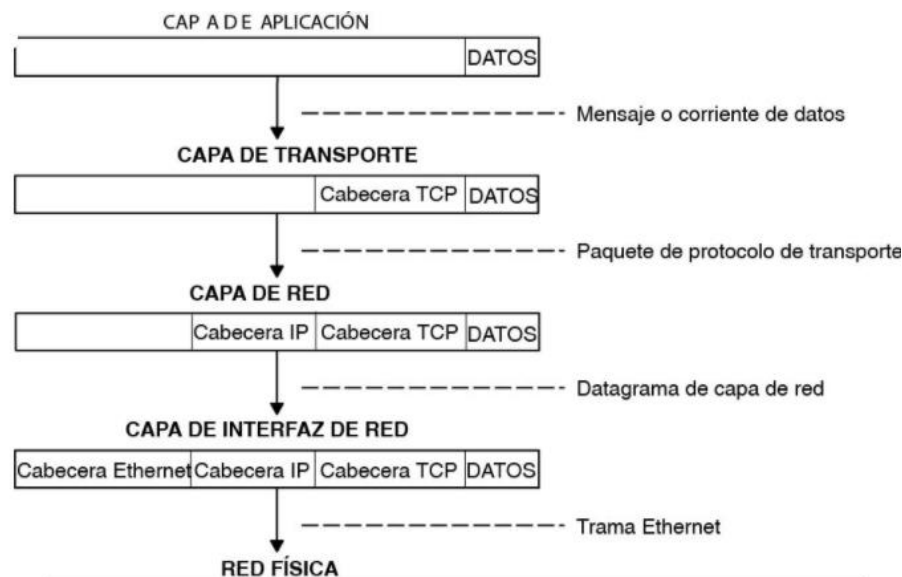
Hardware



INTRODUCCIÓN AL INTERNET DE LAS COSAS

TCP/IP define cuidadosamente cómo se mueve la información desde el remitente hasta el destinatario. En primer lugar, los programas de aplicación envían mensajes o corrientes de datos a uno de los protocolos de la capa de transporte de Internet, UDP (User Datagram Protocol) o TCP (Transmission Control Protocol). Estos protocolos reciben los datos de la aplicación, los dividen en partes más pequeñas llamadas *paquetes*, añaden una dirección de destino y, a continuación, pasan los paquetes a la siguiente capa de protocolo, la capa de red de Internet.

La capa de red de Internet pone el paquete en un datagrama de IP (Internet Protocol), pone la cabecera y la cola de datagrama, decide dónde enviar el datagrama (directamente a un destino o a una pasarela) y pasa el datagrama a la capa de interfaz de red. La capa de interfaz de red acepta los datagramas IP y los transmite como *tramas* a través de un hardware de red específico, por ejemplo, redes Ethernet o de Red en anillo.



Esta figura muestra el flujo de información de las capas de protocolo TCP/IP del remitente al host. Las tramas recibidas por un sistema principal pasan a través de las capas de protocolo en sentido inverso. Cada capa quita la información de cabecera correspondiente, hasta que los datos regresan a la capa de aplicación.

INTRODUCCIÓN AL INTERNET DE LAS COSAS

El TCP/IP fue diseñado para ser compatible con cualquier sistema operativo, hardware o software.

A continuación, muestra los datos que fluyen en ambas direcciones a través de las capas TCP/IP.

- **Protocolo Internet (IP) versión 6:** Internet Protocol (IP) versión 6 (IPv6 o IPng) es la siguiente generación de IP y se ha diseñado para ser un paso de desarrollo de IP versión 4 (IPv4).
- **Rastreo de paquetes:** El rastreo de paquetes es el proceso mediante el cual puede verificar la vía de acceso a través de las capas hasta el destino.
- **Cabeceras de paquete de interfaz de red:** En la capa de Interfaz de red, se adjuntan cabeceras de paquete a los datos de salida.
- **Protocolos a nivel de red Internet:** Los protocolos a nivel de red Internet manejan las comunicaciones de máquina a máquina.
- **Protocolos a nivel de transporte de Internet:** Los protocolos de nivel de transporte TCP/IP permiten a los programas de aplicación comunicarse con otros programas de aplicación.
- **Protocolos a nivel de aplicación de Internet:** TCP/IP implementa protocolos de Internet de nivel superior en el nivel de programa de aplicación.
- **Números asignados:** Por compatibilidad con el entorno de red general, se asignan números conocidos públicamente para las versiones, las redes, los puertos, los protocolos y las opciones de protocolo de Internet. Adicionalmente, también se asignan nombres conocidos públicamente a máquinas, redes, sistemas operativos, protocolos, servicios y terminales.

Protocolo IP

El protocolo IP y sus protocolos de enrutamiento asociados son posiblemente la parte más significativa del conjunto TCP/IP. El protocolo IP se encarga de:

- **Direcciones IP:** Las convenciones de direcciones IP forman parte del protocolo IP. Cómo diseñar un esquema de direcciones IPv4 introduce las

INTRODUCCIÓN AL INTERNET DE LAS COSAS

direcciones IPv4 y Descripción general de las direcciones IPv6 las direcciones IPv6.

- **Comunicaciones de host a host**: El protocolo IP determina la ruta que debe utilizar un paquete, basándose en la dirección IP del sistema receptor.
- **Formato de paquetes**: El protocolo IP agrupa paquetes en unidades conocidas como datagramas. Puede ver una descripción completa de los datagramas en Capa de Internet: preparación de los paquetes para la entrega.
- **Fragmentación**: Si un paquete es demasiado grande para su transmisión a través del medio de red, el protocolo IP del sistema de envío divide el paquete en fragmentos de menor tamaño. A continuación, el protocolo IP del sistema receptor reconstruye los fragmentos y crea el paquete original.

Capa de transporte

La capa de transporte TCP/IP garantiza que los paquetes lleguen en secuencia y sin errores, al intercambiar la confirmación de la recepción de los datos y retransmitir los paquetes perdidos. Este tipo de comunicación se conoce como transmisión de punto a punto.

Protocolo DHCP

El Protocolo de configuración dinámica de host (DHCP) es un protocolo cliente/servidor que proporciona automáticamente un host de protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada. Las RFC 2131 y 2132 definen DHCP como un estándar de Internet Engineering Task Force (IETF) basado en el Protocolo de arranque (BOOTP), un protocolo con el que DHCP comparte muchos detalles de implementación. DHCP permite a los hosts obtener la información de configuración de TCP/IP necesaria de un servidor DHCP.

Cuando tenemos un servidor DHCP en funcionamiento, todas las direcciones IP que ha proporcionado a diferentes clientes se guardan en un listado donde se relaciona la IP que se le ha proporcionado (dirección lógica) y la dirección MAC

www.inadec.com.mx

INTRODUCCIÓN AL INTERNET DE LAS COSAS

(dirección física de la tarjeta de red). Gracias a este listado, el servidor DHCP se asegura de no proporcionar a dos equipos diferentes la misma dirección IP, lo que ocasiona un caos en la red local. A medida que el servidor va asignando direcciones IP, también tiene en cuenta cuándo pasa un determinado tiempo y caducan, quedando libres para que otro cliente pueda obtener esta misma dirección IP. El servidor DHCP sabrá en todo momento quién ha estado en posesión de una dirección IP, cuánto tiempo ha estado, y cuándo se ha asignado a otro cliente.

El protocolo DHCP incluye varias formas de asignación de direcciones IP, dependiendo de la configuración que realicemos y el escenario, podremos usar una forma de asignación u otra:

- **Manual o estática:** el servidor DHCP nos permitirá configurar un listado de parejas IP-MAC con el objetivo de que siempre se le proporcione a un cliente una determinada dirección IP, y que esta dirección no cambie nunca.
- **Automática:** el servidor DHCP se encarga de proporcionar una dirección IP al cliente que realiza la solicitud, y estará disponible para este cliente hasta que la libere. Existen routers que internamente están configurados para proporcionar direcciones IP privadas de forma secuencial, sin embargo, hay firmwares que están diseñados para proporcionar una dirección IP específica dentro del rango y que no es secuencial, en base a un algoritmo interno y la dirección MAC que se haya conectado.
- **Dinámica:** este método permite reutilización dinámica de las direcciones IP.

Funcionamiento y mensajes de intercambio

La comunicación entre el servidor DHCP y los clientes DHCP que tengamos conectados en la red se realiza a través del protocolo UDP, un protocolo que ya conocemos de otros artículos y que es un protocolo no orientado a conexión. En el caso del servidor DHCP usamos el protocolo UDP puerto 67, en el caso de los clientes usamos el protocolo UDP en el puerto 68. Si tenemos un firewall bloqueando estos puertos, ya sea en el servidor o en el cliente, deberemos revisarlo y añadir una regla

INTRODUCCIÓN AL INTERNET DE LAS COSAS

de aceptar para origen y/o destino estos puertos, de lo contrario el servicio no funcionará, y no podremos obtener las direcciones IP automáticamente.

ARQUITECTURAS DE COMUNICACIÓN IOT

La arquitectura del sistema IoT suele describirse como un proceso de cuatro etapas en el que los datos fluyen desde los sensores conectados a las "cosas" a través de una red y, finalmente, a un centro de datos corporativo o a la nube para su procesamiento, análisis y almacenamiento.

En la Internet de las cosas, una "cosa" puede ser una máquina, un edificio o incluso una persona. Los procesos de la arquitectura de la IO también envían datos en la otra dirección en forma de instrucciones o comandos que indican a un actuador o a otro dispositivo conectado físicamente que realice alguna acción para controlar un proceso físico. Un actuador puede hacer algo tan sencillo como encender una luz o tan importante como detener una línea de montaje si se detecta un fallo inminente.

- **Fase 1: Sensores y Actuadores**

El proceso comienza con los sensores y actuadores, los dispositivos conectados que supervisan (en el caso de los sensores) o controlan (en el caso de los actuadores) alguna "cosa" o proceso físico. Los sensores captan datos sobre el estado de un proceso o una condición ambiental, como la temperatura, la humedad, la composición química, los niveles de fluido en un depósito, el flujo de fluido en una tubería o la velocidad de una línea de montaje, entre otros.

www.inadet.com.mx

INTRODUCCIÓN AL INTERNET DE LAS COSAS

En algunos casos, un sensor puede detectar una condición o evento que requiere una respuesta casi inmediata para que un actuador pueda realizar acciones de corrección en tiempo real.

- **Fase 2: Pasarelas de Internet y sistemas de adquisición de datos**

Un sistema de adquisición de datos (DAS) recoge los datos brutos de los sensores y los convierte de formato analógico a digital. A continuación, el DAS agrega y formatea los datos antes de enviarlos a través de una pasarela de Internet mediante WAN inalámbrica (como Wi-Fi o celular) o WAN cableada para la siguiente fase de procesamiento.

En este punto, el volumen de datos es máximo. Las cantidades pueden ser enormes, especialmente, por ejemplo, en una fábrica donde cientos de sensores pueden estar recogiendo datos simultáneamente. Por eso, los datos también se filtran y se comprimen hasta alcanzar un tamaño óptimo para su transmisión.

- **Fase 3: Preprocesamiento: Análisis en la frontera**

Una vez que los datos del IoT han sido digitalizados y agregados, necesitarán ser procesados para reducir aún más el volumen de datos antes de que vayan al centro de datos o a la nube. El dispositivo de borde puede realizar algunos análisis como parte del preprocesamiento. El aprendizaje automático puede ser muy útil en esta fase para proporcionar información al sistema y mejorar el proceso de forma continua, sin esperar a que las instrucciones lleguen desde el centro de datos corporativo o la nube. El procesamiento de este tipo suele tener lugar en un dispositivo situado cerca de donde residen los sensores.

- **Fase 4: Análisis en profundidad en la nube o en el centro de datos**

En la fase 4 del proceso, se pueden utilizar potentes sistemas informáticos para analizar, gestionar y almacenar los datos de forma segura. Esto suele tener lugar en el centro de datos corporativo o en la nube, donde se pueden combinar los datos de múltiples sitios/sensores de campo para proporcionar una imagen más amplia del sistema global de IoT y ofrecer información procesable tanto a los responsables de TI como a los de la empresa. Una empresa puede tener operaciones en

INTRODUCCIÓN AL INTERNET DE LAS COSAS

diferentes zonas geográficas y los datos del IoT pueden analizarse para identificar tendencias y patrones clave, o para detectar anomalías.

A este nivel, se pueden utilizar aplicaciones específicas del sector y/o de la empresa para realizar análisis en profundidad y aplicar reglas de negocio para determinar si es necesario tomar medidas. Los datos entrantes pueden indicar cambios deseables en la configuración de los dispositivos u otras formas de optimizar el proceso, formando un bucle que facilita la mejora constante. La fase 4 también incluye el almacenamiento en un almacén de datos, tanto para el registro como para el análisis posterior.

Protocolo Zigbee

ZigBee es un estándar que define un conjunto de protocolos para el armado de redes inalámbricas de corta distancia y baja velocidad de datos. Opera en las bandas de 868 MHz, 915 MHz y 2.4 GHz y puede transferir datos hasta 250Kbps.

La idea de usar una conexión inalámbrica para controlar sensores y adquirir datos tiene muchos años. Existen numerosas soluciones propietarias usadas en domótica, pero el gran inconveniente que tienen es la incompatibilidad entre sensores, controles y equipos de procesamiento de datos que obliga a hacer pasarelas (gateways) para interconectar dispositivos de diferentes marcas.

El estándar ZigBee fue diseñado con las siguientes especificaciones:

- Ultra bajo consumo que permita usar equipos a batería
- Bajo costo de dispositivos y de instalación y mantenimiento de ellos.
- Alcance corto (típico menor a 50 metros).
- Optimizado para ciclo efectivo de transmisión menor a 0.1 %
- Velocidad de transmisión menor que 250 kbps. Típica: menor que 20 kbps

Existen muchos estándares que se pueden usar en redes de corto alcance tales como el 802.11 y Bluetooth. Cada uno de estos está desarrollado para una clase de aplicación determinada. ZigBee es el estándar más aceptado hoy para usar en redes de sensores y actuadores que deban operar a batería.

Aplicaciones de Zigbee

Automatización en el hogar

Es una de las aplicaciones más usadas de ZigBee ya que es muy fácil la instalación de dispositivos y la modificación de posición de los mismos. Los usos típicos son:

- Seguridad: Sensores de movimiento, de rotura de cristales, apertura de puertas y ventanas. A pesar de su baja velocidad también se usa para transmitir imágenes de cámara de seguridad de baja calidad.
- Lectura de instrumentos de servicios: Los medidores de consumo de agua, gas y energía eléctrica deben leerse en forma regular a efecto de facturar los servicios. Es posible crear una red tipo malla para que la información de los medidores llegue directamente a la empresa de servicio. También los medidores ZigBee podrían comunicarse con los artefactos dentro de la casa. Por ejemplo, ante un pico de consumo eléctrico se podría desconectar algún equipo de alto consumo. ZigBee ayuda a la creación de medidores inteligentes.
- Sistema de riego automático: El uso de un medidor de humedad de suelo permite mejorar la eficiencia del consumo de agua. Se puede distribuir una red de sensores de humedad en un parque de modo que solo se riegue las zonas secas y controlar el tiempo de regado. Una red inalámbrica de sensores facilita enormemente la instalación y el mantenimiento.
- Control de iluminación: Para poder controlar el encendido de una lámpara se necesita un cableado a una llave interruptora en una caja de una pared. ZigBee simplifica la instalación de nuevas lámparas o controles en lugares donde no está la cañería para pasar un cable.

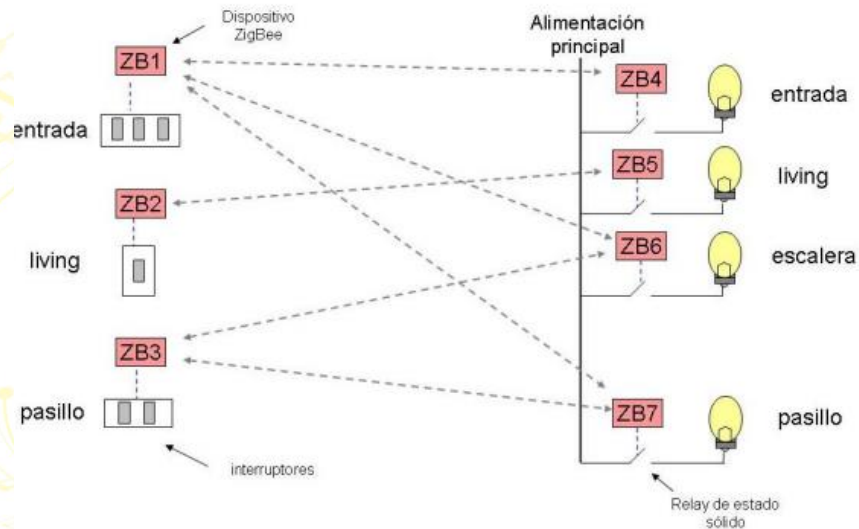


Figura 2: Control de luces en una casa usando ZigBee

- **Controles remotos:** Tradicionalmente los controles remotos de TV, DVD y equipos de audio usan tecnología óptica infrarroja cuya limitación más importante es que solo funciona a muy poca distancia y sin obstáculos. No puede, por ejemplo, penetrar una pared. Además, la comunicación es unidireccional. Como ZigBee usa radiofrecuencia, desaparecen estas limitaciones. Por ejemplo, alguien puede desde otra habitación manejar el equipo de audio y recibir en un display del control remoto, datos de la canción que está escuchando.

Automatización industrial

Para identificar piezas es necesario agregar alguna marca que dé alguna información. Actualmente se usan etiquetas de códigos de barra e identificadores de radiofrecuencia de tipo pasivo (passive RFID: Radio Frequency Identification). Estas, son marcas (tags) formadas por un circuito integrado de memoria que cuando se acercan a un campo electromagnético de determinada frecuencia, se pueden leer y grabar. El inconveniente mayor es que solo trabajan a pocos centímetros del lector. Usando ZigBee es posible construir marcas activas (active RFID) que se lean a mayor distancia y además usarse para brindar información indirecta sobre su localización usando tres o más nodos ZigBee de ubicación conocida.

Otros usos

En hospitales: para el control de pacientes, y medidores y alarma en terapia intensiva. En hoteles: para controlar el acceso a las habitaciones. En monitoreo ambiental: en aplicaciones de redes de sensores como temperatura, humedad, presión, redes de protección de incendio, etc.

Protocolo Bluetooth

Uno de los principales objetivos de la tecnología bluetooth es conseguir que aplicaciones de diferentes fabricantes mantengan una comunicación fluida. Para conseguirlo, receptor y transmisor deben ejecutarse sobre la misma pila de protocolos.

La pila está constituida por dos clases de protocolos. Una primera clase llamada de protocolos específicos que implementa los protocolos propios de Bluetooth. Y una segunda clase formada por el conjunto de protocolos adoptados de otras especificaciones. Esta división en clases en el diseño de la pila de protocolos de Bluetooth permite aprovechar un conjunto muy amplio de ventajas de ambas. Por un lado, al implementar protocolos específicos de Bluetooth permite utilizar los beneficios que aporta la adopción de la tecnología Bluetooth.

Radio Bluetooth (RF)

Bluetooth fue diseñado para operar en un entorno de radio frecuencia ruidoso (LANs, mandos, hornos microondas), y para ello utiliza un esquema de reconocimiento rápido y saltos de frecuencia para garantizar la robustez del enlace. Este sistema opera en la banda de frecuencia de 2.4 GHz, libre para ISM (Industrial, Científica, Medica) más exactamente comenzando en 2.402 GHz y acabando en 2.4835 GHz

La distancia nominal del enlace está comprendida entre 10 cm. y 10 m, pero se puede aumentar a más de 100 m elevando la potencia de transmisión Otro

INTRODUCCIÓN AL INTERNET DE LAS COSAS

aspecto importante es el consumo cuyos valores en los estados más habituales son 300uA (máx.), 30uA (standby), -50uA (hold/park).

- Características de la modulación

La modulación que emplea Bluetooth es GFSK (Gaussian Frequency Shift Keying) con un producto ancho de banda por tiempo $BT=0.5$. Este tipo de modulación permite un bajo coste. La desviación mínima no ha de ser menor de 115 KHz.

-Características del dispositivo receptor

El aspecto más importante en el dispositivo receptor es el nivel de sensibilidad. Para poder medir una tasa de error de bit, el equipo receptor envía de vuelta la información decodificada. Para una tasa de error o BER (Bit Error Rate) del 0.1% se define el nivel de sensibilidad de un receptor Bluetooth mayor o igual a -70dBm.

Banda Base (Base Band)

Baseband, es la capa física del diseño de Bluetooth. Esta define los canales físicos y los enlaces, aparte de otros servicios tales como información de conexión, errores de conexión, selección de canales y seguridad. Un canal Bluetooth, está representado por una secuencia de saltos pseudo aleatorios a través de los 79 o 23 RF

más
Bluetooth
mismo
una

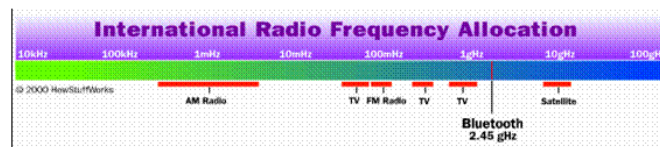
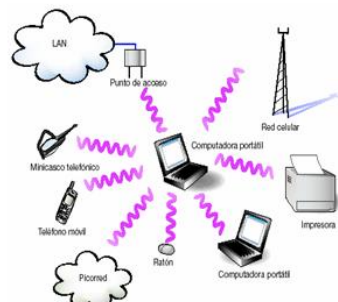


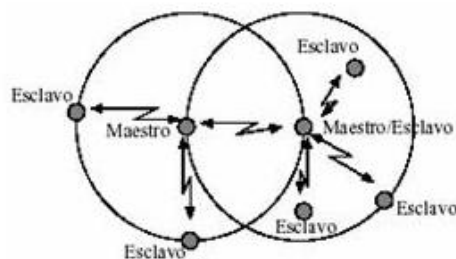
Figura 2. Locación de Radiofrecuencia



www.inadet.com.mx

canales. Dos o
dispositivos
que usan el
canal forman
picored.

La topología Bluetooth permite la interconexión de varias piconets formando una scatternet. Aunque no existe sincronización entre piconets, un dispositivo puede pertenecer a varias de ellas haciendo uso de la multiplexación por división del tiempo (TDD), aunque el dispositivo solo está activo en una piconet a la vez.



Formato de paquetes Bluetooth

En Bluetooth todos los datos que se envían a través del canal son fragmentados y enviados en paquetes. Además, la información se encuentra protegida mediante códigos detectores y/o correctores de errores. En cada ranura solo se puede enviar un paquete. El receptor los recibirá y los procesará empezando por el bit menos significativo.

Los paquetes se pueden clasificar en diferentes tipos atendiendo al número de slots (ranuras) que ocupan y dependiendo de si los enlaces son síncronos o asíncronos:

INTRODUCCIÓN AL INTERNET DE LAS COSAS

- Enlaces asíncronos: La tasa de transmisión máxima que se consigue se sitúa alrededor de 723 kbps. El campo de datos es de longitud variable. Hay tres tipos de paquetes según quepan en 1, 3 o 5 slots.
- Enlaces síncronos: El campo de datos de usuario es fijo. Este tipo de enlaces soporta full-duplex con unas tasas de transmisión mucho menores que en el caso de los enlaces asíncronos, alrededor de 64 kbps en los dos sentidos. Sólo hay paquetes que caben en 1 slot.

Los paquetes que ocupan 3 o 5 slots, son denominados multislots. Estos no utilizan saltos de frecuencia. Se envían por la misma frecuencia durante todos los slots que ocupe el paquete. Una vez finalizada la transmisión del paquete se cambia la frecuencia.

Composición del paquete: Código de acceso (72 bits): . Es usado para sincronización, identificación y compensación. Todos los paquetes comunes que son enviados sobre el canal de lapiconet están precedidos del mismo código de acceso al canal.

Redes Wi-Fi

Las redes inalámbricas son aquellas que posibilitan la interconexión de dos o más equipos entre sí sin que intervengan cables, constituyendo así un eficaz medio para la transmisión de cualquier tipo de datos. Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas en lugar de cableado estándar.

Dependiendo del tamaño de la red o de la cobertura que proporciona, se pueden clasificar en los diferentes tipos:

- **WPAN** (*Wireless Personal Area Network*)

Una red inalámbrica de área personal, incluye redes inalámbricas de corto alcance que abarcan un área de algunas decenas de metros. Este tipo de red se

www.inadet.com.mx

INTRODUCCIÓN AL INTERNET DE LAS COSAS

usa generalmente para conectar dispositivos periféricos. Destacan principalmente tecnologías como Bluetooth (IEEE 802.15.1), Zigbee (IEEE 802.15.4) o HomeRF.

- **WLAN** (*Wireless Local Area Network*)

En las redes de área local, se pueden encontrar tecnologías inalámbricas basadas en HiperLAN como HiperLAN2 o tecnologías basadas en WiFi, que siguen el estándar IEEE 802.11x.

- **WMAN** (*Wireless Metropolitan Area Network*)

Las WMAN se basan en el estándar IEEE 802.16x o WiMax, así como en LMDS (*Local Multipoint Distribution Service*).

- **WWAN** (*Wireless Wide Area Network*)

Las redes inalámbricas de área extensa tienen el alcance más amplio de todas las redes inalámbricas. En estas redes encontramos tecnologías como UMTS (*Universal Mobile Telecommunications System*), utilizada con los teléfonos móviles de tercera generación (3G) y la tecnología digital para móviles GPRS (*General Packet Radio Service*).

El comité IEEE 802.11 es el encargado de desarrollar los estándares para las redes de área local inalámbricas. Este estándar, se basa en el mismo marco de estándares que Ethernet, garantizando un excelente nivel de interoperatividad y asegurando una implantación sencilla de las funciones y dispositivos de interconexión Ethernet/WLAN.

La conexión de redes inalámbricas se restringe a las dos primeras capas del modelo TCP/IP, es decir, el nivel físico y el nivel de enlace, los cuales se explicarán a detalle a continuación. Si, además, los elementos de la red soportan enrutamiento o enmascaramiento NAT.

Los tres puntos siguientes, afectan a la capa física.

- **Número de canal**

www.inadet.com.mx

INTRODUCCIÓN AL INTERNET DE LAS COSAS

El número de canal identifica el rango de frecuencias de trabajo. Para redes IEEE 802.11b se usan los canales 1, 7 y 13 en Europa para asegurar suficiente separación de frecuencias y evitar conflictos. Para redes 802.11a no hay riesgo de que los canales se solapen, sólo hay que asegurarse que los nodos cercanos estén operando en canales diferentes. Algunos dispositivos definen automáticamente el canal basado en la frecuencia ociosa escaneando el espectro.

- **Potencia de transmisión**

A mayor potencia de transmisión, el punto de acceso tendrá un mayor rango de cobertura, sin embargo, debe evitarse usar más potencia de la necesaria pues aumenta la probabilidad de interferir con otros usuarios. Para muchos países el máximo límite legal es 100 mW, mientras en otros el límite es de 1 W.

- **Velocidad de transmisión**

La tasa de transmisión empleada dependerá del estándar del dispositivo, así para 801.11b el límite superior estará en los 11 Mbps, y para 802.11a y 802.11b en 54 Mbps. En la mayoría de dispositivos, es seleccionable una tasa inferior al límite del estándar.

Los siguientes tres puntos siguientes afectan a la capa de enlace.

- **Modos de operación o funcionamiento**

El estándar 802.11 define dos modos operativos, el modo de infraestructura en el que los clientes de tecnología inalámbrica se conectan a un punto de acceso y el modo ad-hoc en el que los clientes se conectan entre sí sin ningún punto de acceso.

- **SSID (*Service Set Identifier*)**

El SSID es el nombre de la LAN inalámbrica. Se trata de una cadena de texto sensible a mayúsculas y minúsculas, que acepta hasta 32 caracteres alfanuméricos y es usada durante el proceso de asociación a una red inalámbrica.

INTRODUCCIÓN AL INTERNET DE LAS COSAS

El SSID de un dispositivo se difunde por defecto en las tramas beacon para anunciar su presencia. Esto significa que cualquiera con un adaptador inalámbrico puede ver su red en términos de su SSID. Muchos dispositivos ofrecen la posibilidad de desactivar la difusión del SSID para ocultar la red al público. Este hecho puede mejorar la seguridad de la red inalámbrica.

- **Control de acceso al medio**

Un dispositivo envía tramas beacon periódicamente para difundir su presencia y la información de la red a las estaciones clientes en su radio de cobertura. Las estaciones pueden obtener lista de los dispositivos disponibles buscando estas tramas continuamente en todos canales 802.11. El intervalo de beacon, es la cantidad de tiempo entre la transmisión de tramas beacon de un punto de acceso, su valor por defecto es generalmente 10 ms.

RTS/CTS (*Request-To-Send / Clear-To-Send*) es el método usado por las redes inalámbricas del estándar IEEE 802.11 acceder al medio y reducir colisiones. RTS/CTS introduce mecanismos para evitar colisiones mediante el método CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), lo que hace al método de acceso más robusto; pero incrementa el tráfico en la red. Cuando un nodo desea enviar datos, envía una trama RTS, el punto de acceso (AP) la recibe y responde con una trama CTS si el medio está libre. Cuando el nodo recibe el CTS, este comienza a enviar sus datos. Todos los nodos deben ser capaces de escuchar al punto de acceso, la trama CTS alcanzará a todos los nodos conectados a él. La trama CTS incluye un valor del tiempo que los otros nodos deberán esperar para enviar otras tramas RTS.

En esta capa además se llevan a cabo las técnicas de filtrado MAC de acceso al medio, cifrado WEP o WPA y restricciones de acceso por autenticación que se verán en el punto de seguridad.

Protocolo	Descripción
802.11	Primer estándar que permite un ancho de banda de 1 a 2 Mbps. Trabaja a 2,4 GHz
802.11a	Llamado también WiFi5. Tasa de 54 Mbps. Trabaja entorno a 5 GHz, frecuencia menos saturada que 2,4.
802.11b	Conocido como WiFi. El más utilizado actualmente. Las mismas interferencias que para 802.11 ya que trabaja a 2,4 GHz. Tasa de 11 Mbps.
802.11c	Es una versión modificada del estándar 802.1d, que permite combinar el 802.1d con dispositivos compatibles 802.11 en el nivel de enlace de datos.
802.11d	Este estándar es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11e	Define los requisitos de ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo. Está destinado a mejorar la calidad del servicio en el nivel de la capa de enlace de datos.
802.11f	Su objetivo es lograr la interoperabilidad de puntos de acceso (AP) dentro de una red WLAN multiproveedor. El estándar define el registro de puntos de acceso dentro de una red y el intercambio de información entre ellos cuando un usuario se traslada desde un punto de acceso a otro.
802.11g	Ofrece un ancho de banda de 54 Mbps en el rango de frecuencia de 2,4 GHz. Es compatible con el estándar 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
802.11h	El objetivo es que 802.11 cumpla los reglamentos europeos para redes WLAN a 5 GHz. Los reglamentos europeos para la banda de 5 GHz requieren que los productos tengan control de la potencia de transmisión y selección de frecuencia dinámica.
802.11i	Aprobada en Julio 2004, se implementa en WPA2. Destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el protocolo de encriptación AES.
802.11n	Se basa en la tecnología MIMO. Trabaja en la frecuencia de 2,4 y 5 GHz. Soportará tasas superiores a los 100Mbps.
802.11s	Redes Mesh o malladas.

Modos de funcionamiento

El estándar 802.11 define dos modos operativos, el modo de infraestructura en el que los clientes de tecnología inalámbrica se conectan a un punto de acceso y el modo ad-hoc en el que los clientes se conectan entre sí sin ningún punto de acceso

www.inadet.com.mx

INTRODUCCIÓN AL INTERNET DE LAS COSAS

Modo ad hoc

En redes IEEE 802.11, el modo ad hoc se denota como Conjunto de Servicios Básicos Independientes (*IBSS, Independent Basic Service Set*). El modo ad hoc, también conocido como punto a punto, es un método para que clientes inalámbricos puedan establecer una comunicación directa entre sí, no siendo necesario involucrar un punto de acceso central. Todos los nodos de una red ad hoc se pueden comunicar directamente con otros clientes. Cada cliente inalámbrico en una red ad hoc debería configurar su adaptador inalámbrico en modo ad hoc y usar los mismos SSID y número de canal de la red. Este tipo de redes normalmente está formado por un pequeño grupo de dispositivos dispuestos cerca unos de otros, siendo su rendimiento menor a medida que el número de nodos crece.

Configuración	Nodo 1	Nodo 2
Modo	Ad hoc	
SSID	El mismo	
Canal	El mismo	
IP	IP _A (normalmente fija)	IP _B (normalmente fija)

En una red ad hoc, el rango del BSS está determinado por el rango de cada estación, por lo que, si dos estaciones de la red están fuera de rango la una de la otra, no podrán comunicarse aun cuando puedan ver otras estaciones. A diferencia del modo infraestructura, el modo ad hoc no tiene un sistema de distribución que pueda enviar tramas de datos desde una estación a la otra.

Modo infraestructura

En el modo de infraestructura (*BSS, Basic Service Set*), cada estación se conecta a un punto de acceso a través de un enlace inalámbrico. La configuración formada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura se llama conjunto de servicio básico o BSS. Estos forman una célula y se

INTRODUCCIÓN AL INTERNET DE LAS COSAS

identifica a través de un BSSID, que corresponde con la dirección MAC del punto de acceso.

Es posible vincular varios puntos de acceso juntos para formar un conjunto de servicio extendido o ESS (*Extended Service Set*). El sistema de distribución también puede ser una red conectada, un cable entre dos puntos de acceso o incluso una red inalámbrica. El ESSID, a menudo es abreviado por SSID, que no es más que el nombre de la red. A continuación, se muestra la configuración típica del modo infraestructura.

Configuración	Punto de Acceso	Usuarios
Modo	Infraestructura	
SSID	Debe definir un SSID	Conectar al SSID
Canal	Debe definir canal	Descubrir el canal
IP	Normalmente servidor DHCP	Asignado por DHCP

Los puntos de acceso se comunican entre sí con el fin de intercambiar información sobre las estaciones, así cuando un usuario se mueve desde un BSS a otro dentro de un ESS, el adaptador inalámbrico de su equipo puede cambiarse de punto de acceso dependiendo la calidad de la señal que reciba o la saturación del nodo, permitiendo al cliente inalámbrico moverse de forma transparente de un punto de acceso a otro. Esta característica es conocida como itinerancia.

Normalmente, en una configuración típica como se muestra en la Figura 8, uno de los AP se conecta a una red cableada con acceso a Internet, por el que fluirá todo el tráfico que requiera una estación o red no alcanzable por los AP.

Seguridad.

Este punto es fundamental, ya que las redes inalámbricas usan ondas de radio y son más susceptibles de ser interceptadas, es decir, no brindan la protección y privacidad de un cable, por lo que se hace casi indispensable proveer de mecanismos de seguridad a nivel de enlace que garanticen la integridad y

INTRODUCCIÓN AL INTERNET DE LAS COSAS

confiabilidad de los datos, en definitiva, se busca asegurar que la información transmitida entre los puntos de acceso y los clientes no sea revelada a personas no autorizadas. En este punto, también se tratarán los mecanismos de autenticación y control de acceso, como medida de seguridad diseñada para establecer la validez de una transmisión.

A continuación, se explica brevemente en qué consisten los principales mecanismos que intentan o ayudan a garantizar la privacidad, integridad y confidencialidad de la transmisión.

- **Mecanismo de seguridad WEP (*Wired Equivalent Privacy*)** obsoleto

La confidencialidad en redes inalámbricas ha sido asociada tradicionalmente con el término WEP, que forma parte del estándar IEEE 802.11 original, de 1999. Su propósito fue brindar un nivel de seguridad comparable al de las redes alambradas tradicionales. Se trata de un mecanismo basado en el algoritmo de cifrado RC4, y que utiliza el algoritmo de chequeo de integridad CRC (*Chequeo de Redundancia Cíclica*). Un mal diseño del protocolo provocó que al poco tiempo de ser publicado quedara obsoleto. Actualmente existen varios ataques y programas para quebrar el WEP tales como Aircrack, Wepcrack, Kismet o Aircrack-ng. Algunos de los ataques se basan en la limitación numérica de los vectores de inicialización del algoritmo de cifrado RC4, o la presencia de la llamada “debilidad IV” en un datagrama. Este mecanismo no es recomendado para garantizar la seguridad de una red.

- **WPA y WPA2**

En 2003 se propone el Acceso Protegido a redes WiFi o WPA y luego queda certificado como parte del estándar IEEE 802.11i, con el nombre de WPA2 en 2004.

WPA y WPA2 pueden trabajar con y sin un servidor de distribución de llaves. Si no se usa un servidor de llaves, todas las estaciones de la red usan una llave de tipo PSK (*Pre-Shared-Key*), en caso contrario se usa habitualmente un servidor IEEE 802.1x.

www.inadet.com.mx

INTRODUCCIÓN AL INTERNET DE LAS COSAS

- **Filtrado MAC**

Es un mecanismo que realizan los puntos de acceso que permite únicamente acceder a la red a aquellos dispositivos cuya dirección física MAC sea una de las especificadas. El mecanismo se puede utilizar como control adicional; pero es fácilmente vulnerable aplicando un clonado de la MAC a suplantar.

- **Detener la difusión de la SSID como medida de seguridad**

Se pueden configurar los puntos de accesos para que no difundan periódicamente las llamadas *Tramas Baliza* o *Beacon Frames*, con la información del SSID. Evitar esta publicación implica que los clientes de la red inalámbrica necesitan saber de manera previa que SSID deben asociar con un punto de acceso; pero no impedirá que una persona interesada encuentre la SSID de la red mediante captura de tráfico. Este sistema debe considerarse tan solo como una precaución adicional más que una medida de seguridad.

- **Protocolo 802.11x**

Este protocolo ofrece un marco para autenticar y controlar el acceso a los puntos de accesos. Sirve como soporte para implementaciones de seguridad sobre servidores de autenticación. El funcionamiento se puede ver en la Figura 9 y es básicamente el siguiente, el cliente envía una petición al servidor de autenticación a través del AP, quien comprueba el certificado o el nombre de usuario y contraseña utilizando esquemas de autenticación como EAP encargados de la negociación. Si es aceptado, el servidor autorizará el acceso al sistema y el AP permite el acceso asignando los recursos de red.

PLATAFORMAS DE HARDWARE

Una plataforma de hardware puede referirse a la arquitectura del ordenador o la arquitectura del procesador. Por ejemplo, los CPUs x86 y x86-64 constituyen una de las más comunes las arquitecturas de computadoras en uso en los

INTRODUCCIÓN AL INTERNET DE LAS COSAS

ordenadores de propósito general. Estas máquinas suelen ejecutar una versión de Microsoft Windows, aunque también se puede ejecutar otros sistemas operativos, tales como Linux, OpenBSD, NetBSD, Mac OS X y FreeBSD.

Una arquitectura ARM es común en los teléfonos inteligentes y Tablet PC, que corren Android, iOS y otros sistemas operativos móviles.

Bluetooth

El Bluetooth es un protocolo de comunicaciones que sirve para la transmisión inalámbrica de datos (fotos, música, contactos...) y voz entre diferentes dispositivos que se hallan a corta distancia, dentro de un radio de alcance que, generalmente, es de diez metros. Por ejemplo, gracias a esta tecnología, podemos vincular nuestro smartphone con una impresora para imprimir nuestras fotos preferidas sin necesidad de cables.

El uso del Bluetooth se ha asociado a los teléfonos móviles, ya que éstos fueron de los primeros dispositivos en incorporar el protocolo. Sin embargo, esta tecnología inalámbrica se encuentra presente, hoy en día, en smartphones, tablets, portátiles, ratones, teclados, impresoras, auriculares, televisores, cámaras digitales, reproductores MP3 o videoconsolas.

Como funciona el Bluetooth

La tecnología Bluetooth transmite inalámbricamente datos y voz a través de ondas de radio que operan en la banda ISM (no comercial) de los 2,4 GHz. Para ello, hace uso de las Redes Inalámbricas de Área Personal (WPAN, por sus siglas en inglés). Al realizarse la transferencia por radiofrecuencia, los dispositivos no tienen la obligación de hallarse alineados.

Por otro lado, sin embargo, los equipos deben encontrarse dentro de un radio de alcance, que suele ser corto, aunque pueda variar en función del aparato. Así, se clasifican de la siguiente manera:

- Dispositivos de Clase 1. Tienen una potencia máxima permitida de 100 mW y, por tanto, un alcance de 100 metros.

INTRODUCCIÓN AL INTERNET DE LAS COSAS

- Dispositivos de Clase 2. Se caracterizan por tener un radio de alcance de entre 5 y 10 metros, dado que su potencia máxima permitida es de 2,5 mW. Estos son los más habituales.
- Dispositivos de Clase 3. Cuentan con una potencia máxima de 1 mW y un alcance de, tan sólo, un metro.

Usos del bluetooth

Las posibilidades que ofrece la tecnología Bluetooth son numerosas e interesantes, en especial gracias a su fácil transmisión de, por ejemplo, fotos o canciones sin la necesidad de cables. A continuación, algunas de sus aplicaciones más frecuentes:

- Transmisión de archivos, contactos, etc. entre diferentes usuarios con Bluetooth, o entre distintos dispositivos de un mismo usuario.
- Conexión inalámbrica entre productos y accesorios tecnológicos. Este es el caso de las videoconsolas que incorporan Bluetooth, las cuales pueden hacer uso de mandos sin cables conectados a ellas por el protocolo, o de los sistemas de audio y su vinculación inalámbrica con los altavoces.
- Acceso a contenidos específicos en áreas públicas.
- Conexión inalámbrica entre un dispositivo e Internet.

Wi-Fi

Wifi es una tecnología de red inalámbrica a través de la cual los dispositivos, como computadoras (portátiles y de escritorio), dispositivos móviles (teléfonos inteligentes y accesorios) y otros equipos (impresoras y videocámaras), pueden interactuar con Internet. Permite que estos dispositivos, entre tantos otros, intercambien información entre sí y establezcan, de esta manera, una red.

La conectividad a Internet se logra a través de un router inalámbrico. Cuando accede a wifi, se conecta a un router inalámbrico que permite que los dispositivos que admiten wifi interactúen con Internet.

¿Cómo funciona la tecnología Wi-Fi?

www.inadet.com.mx

INTRODUCCIÓN AL INTERNET DE LAS COSAS

Desde el punto de vista técnico, el estándar IEEE 802.11 define los protocolos que permiten la comunicación con los dispositivos inalámbricos actuales que admiten wifi, incluidos routers y puntos de acceso inalámbrico. Los puntos de acceso inalámbrico son compatibles con diferentes estándares IEEE.

Cada estándar es una modificación que recibe aprobación después de cierto tiempo. Los estándares funcionan con diversas frecuencias, proporcionan distintos anchos de banda y admiten distintas cantidades de canales.

¿Qué es un punto de acceso inalámbrico?

Un punto de acceso inalámbrico permite que los dispositivos inalámbricos se conecten a la red inalámbrica. Disponer de una red inalámbrica facilita la conexión de dispositivos nuevos y les brinda soporte flexible a los trabajadores móviles.

El funcionamiento de un punto de acceso inalámbrico en relación con una red es similar al funcionamiento de un amplificador en relación con un equipo de música estéreo. Un punto de acceso toma el ancho de banda proveniente de un router y lo extiende para que muchos dispositivos puedan conectarse a la red desde distancias más lejanas. Sin embargo, un punto de acceso inalámbrico no se limita a extender la red Wi-Fi. También puede brindar datos valiosos sobre los dispositivos conectados a la red, proporcionar seguridad proactiva y responder a muchos otros fines prácticos.

¿Qué es un router inalámbrico?

Los routers inalámbricos suelen encontrarse en los hogares. Se trata de los dispositivos de hardware que los proveedores de servicios de Internet utilizan para conectarse a su red de Internet por cable o xDSL. A veces el router inalámbrico se denomina dispositivo de red de área local inalámbrica (WLAN). Una red inalámbrica también se denomina red wifi.

Un router inalámbrico combina las funciones de red de un router y un punto de acceso inalámbrico

¿Qué es una zona Wi-Fi portátil?

INTRODUCCIÓN AL INTERNET DE LAS COSAS

Una zona Wi-Fi portátil es una zona de cobertura móvil obtenida a través de un proveedor de telefonía celular. Se trata de un pequeño dispositivo que emplea torres de red celular que transmiten señales de ancho de banda 3G o 4G de alta velocidad. Diversos dispositivos, como iPads y laptops, pueden luego conectarse de manera inalámbrica con el dispositivo, que, a la vez, se conecta sin inconvenientes a Internet donde sea que esté. De un modo similar a lo que sucede con el teléfono celular, el costo mensual de la zona de cobertura portátil se basa en el plan de uso de datos que seleccione. El acceso a Internet a través de una zona Wi-Fi portátil es más confiable que el acceso a través de zonas Wi-Fi públicas estáticas.

Otras plataformas hardware

Netduino



Esta es la plataforma de Microsoft para programación de microcontroladores, la cual fue desarrollada por Secret Lab LLC, basándose en la idea de Arduino.

Básicamente tomaron un procesador de Atmel (el mismo fabricante que los procesadores de Arduino) de 32 bits y 48 MHz y desarrollaron una placa compatible con Arduino junto con el .NET Micro Framework, que es, ni más ni menos, una versión muy reducida del framework de .NET que todos conocemos. Esta idea permite acercar a los desarrolladores de .NET (que no somos pocos) al mundo de la programación de microcontroladores utilizando una placa compatible con todos los sensores y dispositivos que ya existen para Arduino.

INTRODUCCIÓN AL INTERNET DE LAS COSAS

Placa	Procesador	Velocidad	Voltaje	ROM	RAM	Puertos digitales	con PWM	Entradas analógicas	Otros puertos	Tamaño
Netduino										
netduino	Atmel SAM7X	48 MHz	7.5 V	128 kB	60 kB	14	4	6		71 mm × 53.3 mm
netduino plus 2	STMicro STM32F4	168 MHz	7.5 V	384 kB	100+ kB	14	6	6	I2c Micro SD Ethernet	71 mm × 53.3 mm
netduino go	STMicro STM32F4	168 MHz	7.5 V	384 kB	100+ kB				8 puertos gbus	68.6 mm × 53.3 mm

.NET Gadgeteer

Esta plataforma, que fue lanzada en 2011, está basada en la idea de poder conectar de forma muy sencilla distintos dispositivos a nuestra placa base, sin necesidad de pensar en resistencias, consumo de los componentes ni nada por estilo, o sea, más o menos como un “lego para desarrolladores”. Al momento esta plataforma posee muchos dispositivos en el mercado: display, cámaras, interfaces de red, lectores/grabadores de tarjetas, joysticks, bluetooth, etc.



Raspberry Pi

Esta placa fue creada por la “Fundación Raspberry Pi” del Reino Unido para estimular la enseñanza de las ciencias de la computación en las escuelas. Su salida a la venta fue a principios de este año, 2012, con un total de 10.000 placas fabricadas en China y Taiwan. Esta placa se diferencia en mucho a las anteriores, para empezar ya viene con puertos HDMI, RCA (para conectarlo a una TV) y USB (al que se le puede conectar un teclado o mouse), GPU compatible con OpenGL ES 2.0 y OpenVG que puede decodificar video con calidad blue-ray (H.264/MPEG-4 AVC) a 40MBits/s y soporta resoluciones desde 640 × 350 hasta 1920 × 1200, procesador ARM1176JZFS de 700 MHz, audio, slot para tarjetas SD / MMC / SDIO y, lo que hace la mayor diferencia, viene con Linux, más específicamente con Raspbian, una versión derivada de Debian, aunque le podemos instalar la distribución que queramos, inclusive Android.

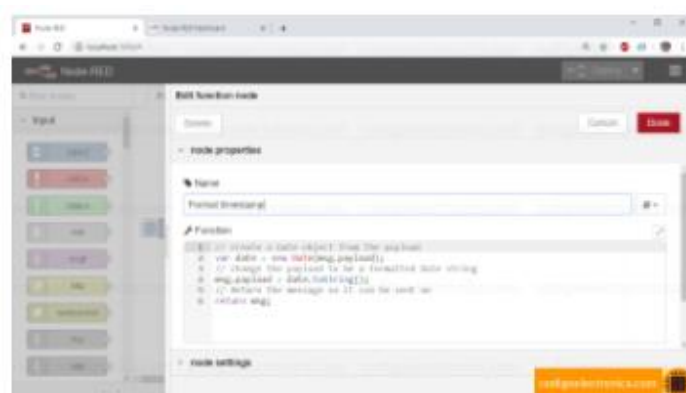
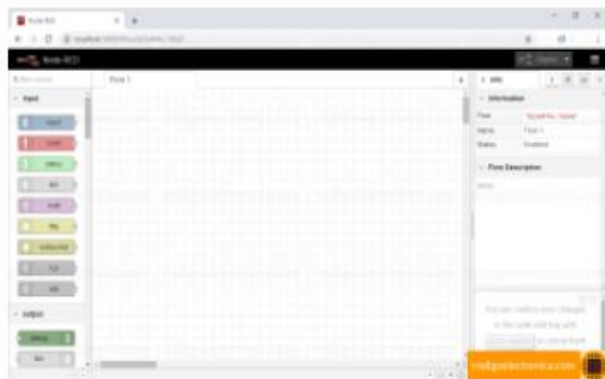
PLATAFORMAS DE SOFTWARE

Node -Red

Es una herramienta de programación que permite conectar entre sí dispositivos hardware, APIs y servicios en-linea en formas completamente nuevas e interesantes. Proporciona un editor basado en navegador que facilita la conexión de flujos mediante la amplia gama de nodos en la paleta que se pueden implementar en su tiempo de ejecución con un solo clic.

Edición de flujo en el navegador

Node-RED proporciona un editor de flujo que es usado en el navegador, el cual facilita la conexión y creación de los flujos mediante el amplio rango de nodos en la paleta. Los flujos se pueden implementar en tiempo de ejecución con un solo clic.

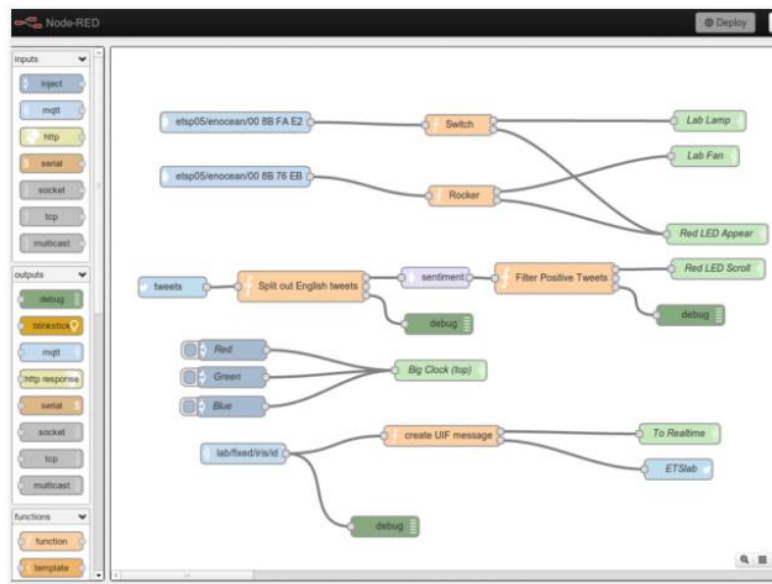


Node red está basado en nodejs, el cual permite un tiempo de ejecución y una carga liviana, aprovechando al máximo su modelo sin bloqueo controlado por eventos. Esto lo hace ideal para ejecutarse en hardware de bajo costo y pocos recursos, como Raspberry Pi, así como en la nube.

Con más de 225,000 módulos en el repositorio de paquetes de Node, es fácil extender el rango de nodos de paleta para agregar nuevas capacidades.

La estructura mínima son los nodos. Estos se arrastran a través de la interfaz gráfica y nos permiten hacer una tarea concreta. Recibir una llamada HTTP, un mensaje MQTT o la activación de un pulsador.

Todos estos nodos se organizan en flujos o flows que agrupan nodos que se conectan entre ellos. Todo de una forma visual, sin apenas tener que programar.



Node-RED es un motor de flujos con enfoque IoT, que permite definir gráficamente flujos de servicios, a través de protocolos estándares como REST, MQTT, Websocket, AMQP... además de ofrecer integración con apis de terceros.

La facilidad de desarrollo de nuevos nodos, así como la portabilidad de los flujos, confieren a Node-RED un marcado enfoque social. Gran parte de su éxito se fundamenta en que los nodos y flujos desarrollados por una persona u organización, pueden ser aprovechados por otras. En este sentido, en el sitio oficial de Node-RED encontramos una sección de contribuciones de terceros, con más de 1000 nodos y flujos subidos por la comunidad y listos para utilizar.

INTRODUCCIÓN AL INTERNET DE LAS COSAS

IDE – entorno de desarrollo integrado, llamado IDE (sigla en inglés de integrated development environment), es un programa informático compuesto por un conjunto de herramientas de programación. Puede dedicarse en exclusiva a un solo lenguaje de programación o bien puede utilizarse para varios.

Un IDE es un entorno de programación que ha sido empaquetado como un programa de aplicación; es decir, que consiste en un editor de código, un compilador, un depurador y un constructor de interfaz gráfica (GUI). Además en el caso de Arduino incorpora las herramientas para cargar el programa ya compilado en la memoria flash del hardware.

El IDE de Arduino va a ser la herramienta de trabajo con Arduino y habrá que conocer su funcionamiento.

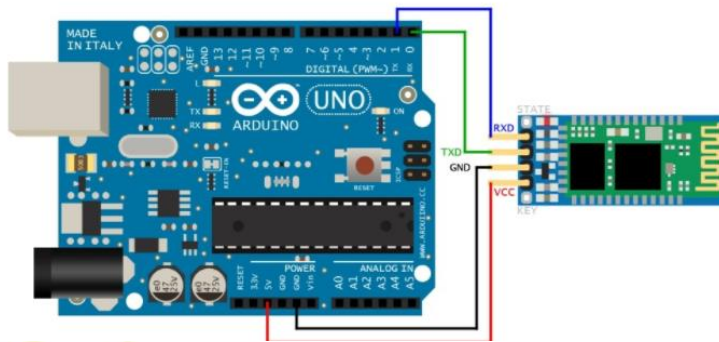
Los programas de Arduino están compuestos por un solo fichero con extensión “ino”, aunque es posible organizarlo en varios ficheros. El fichero principal siempre debe estar en una carpeta con el mismo nombre que el fichero.

Anteriormente a la versión 1.x de Arduino se usaba la extensión “pde”. Cuando se pasó a la versión 1.x hubo grandes cambios, que deben tenerse en cuenta si se usa el código antiguo.

El software libre son los programas informáticos cuyo código es accesible por cualquiera para que quien quiera pueda utilizarlo y modificarlo. Arduino ofrece la plataforma Arduino IDE (Entorno de Desarrollo Integrado), que es un entorno de programación con el que cualquiera puede crear aplicaciones para las placas Arduino, de manera que se les puede dar todo tipo de utilidades.

INTRODUCCIÓN AL INTERNET DE LAS COSAS

Es una placa con todos los elementos necesarios para conectar periféricos a las entradas y salidas de un microcontrolador, y que puede ser programada tanto en Windows como macOS y GNU/Linux. Un proyecto que promueve la filosofía 'learning by doing', que viene a querer decir que la mejor manera de aprender es cacharreando.



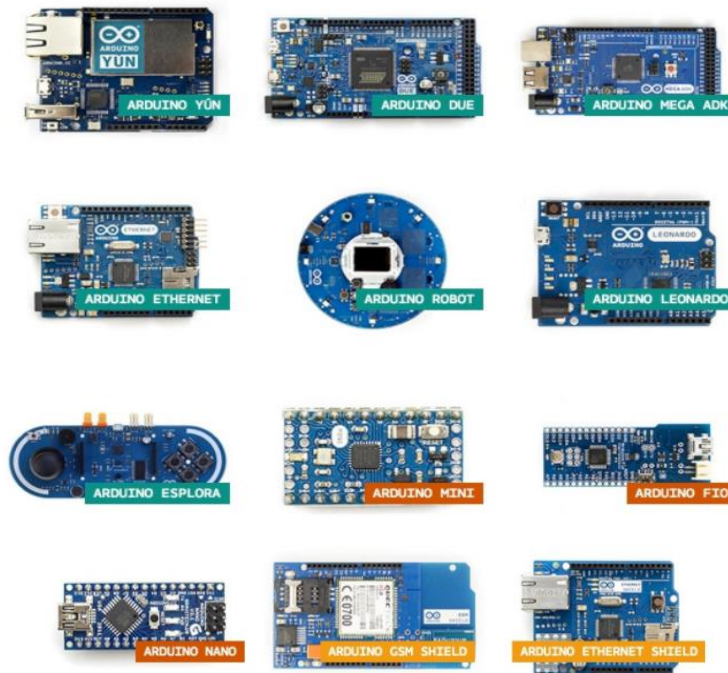
Como funciona

El Arduino es una placa basada en un microcontrolador ATMEL. Los microcontroladores son circuitos integrados en los que se pueden grabar instrucciones, las cuales las escribes con el lenguaje de programación que puedes utilizar en el entorno Arduino IDE. Estas instrucciones permiten crear programas que interactúan con los circuitos de la placa.

El microcontrolador de Arduino posee lo que se llama una interfaz de entrada, que es una conexión en la que podemos conectar en la placa diferentes tipos de periféricos. La información de estos periféricos que conectes se trasladará al microcontrolador, el cual se encargará de procesar los datos que le lleguen a través de ellos.

El tipo de periféricos que puedas utilizar para enviar datos al microcontrolador depende en gran medida de qué uso le estés pensando dar. Pueden ser cámaras para obtener imágenes, teclados para introducir datos, o diferentes tipos de sensores.

También cuenta con una interfaz de salida, que es la que se encarga de llevar la información que se ha procesado en el Arduino a otros periféricos. Estos periféricos pueden ser pantallas o altavoces en los que reproducir los datos procesados, pero también pueden ser otras placas o controladores.



Arduino es un proyecto y no un modelo concreto de placa, lo que quiere decir que compartiendo su diseño básico te puedes encontrar con diferentes tipos de placas. Las hay de varias formas, tamaños y colores para a las necesidades del proyecto en el que estés trabajando, las hay sencillas o con características mejoradas, Arduinos orientados al Internet de las Cosas o la impresión 3D y, por supuesto, dependiendo de estas características te encontrarás con todo tipo de precios.



VISUALIZACIÓN DE DATOS EN LA RED E INTELIGENCIA ARTIFICIAL

La visualización de datos es la práctica de traducir información en un contexto visual, como un mapa o gráfico, para facilitar que el cerebro humano comprenda y extraiga información útil. El objetivo principal de la visualización de datos es facilitar la identificación de patrones, tendencias y valores atípicos en grandes conjuntos de datos. El término a menudo se usa indistintamente con otros, incluidos gráficos de información, visualización de información y gráficos estadísticos.

La visualización de datos es uno de los pasos del proceso de ciencia de datos, que establece que una vez que los datos se han recopilado, procesado y modelado, deben visualizarse para obtener conclusiones. La visualización de datos también es un elemento de la disciplina más amplia de la arquitectura de presentación de datos (DPA), que tiene como objetivo identificar, localizar, manipular, formatear y entregar datos de la manera más eficiente posible.

Puede ser utilizado por los maestros para mostrar los resultados de las pruebas de los estudiantes, por científicos informáticos que exploran los avances en inteligencia artificial (IA) o por ejecutivos que buscan compartir información con las partes interesadas. También juega un papel importante en proyectos de big data. A medida que las empresas acumulaban colecciones masivas de datos durante los primeros años de la tendencia de los grandes datos, necesitaban una forma de obtener una visión general de sus datos de manera rápida y fácil. Las herramientas de visualización eran un ajuste natural.

Es fundamental para el análisis avanzado por razones similares. Cuando un científico de datos escribe algoritmos avanzados de análisis predictivo o aprendizaje automático (*machine learning* o ML), se vuelve importante visualizar los resultados para monitorear los resultados y garantizar que los modelos funcionen según lo previsto. Esto se debe a que las visualizaciones de algoritmos complejos son generalmente más fáciles de interpretar que las salidas numéricas.

Importancia

La visualización de datos proporciona una forma rápida y efectiva de comunicar información de manera universal utilizando información visual. La práctica también puede ayudar a las empresas a identificar qué factores afectan el comportamiento del cliente; determinar áreas que necesitan ser mejoradas o que necesitan más atención; hacer que los datos sean más memorables para las partes interesadas; entender cuándo y dónde colocar productos específicos; y predecir los volúmenes de ventas.

Otros beneficios de la visualización de datos incluyen:

- La capacidad de absorber información rápidamente, mejorar los conocimientos y tomar decisiones más rápidas.
- Una mayor comprensión de los próximos pasos que deben tomarse para mejorar la organización.
- Una capacidad mejorada para mantener el interés de la audiencia con información que puedan entender.
- Una distribución fácil de información que aumenta la oportunidad de compartir ideas con todos los involucrados.
- Eliminar la necesidad de científicos de datos ya que los datos son más accesibles y comprensibles.
- Una mayor capacidad para actuar sobre los resultados rápidamente y, por lo tanto, lograr el éxito con mayor velocidad y menos errores.