Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

PROPUESTA DE DISEÑO DE UNA INTERFAZ DE ADQUISICIÓN DE DATOS PARA MEDIDORES ELÉCTRICOS POR MEDIO DEL PROTOCOLO TCP/IP

Francisco José García Rodas
Asesorado por la Inga. Ingrid Rodríguez de Loukota

Guatemala, agosto de 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

PROPUESTA DE DISEÑO DE UNA INTERFAZ DE ADQUISICIÓN DE DATOS PARA MEDIDORES ELÉCTRICOS POR MEDIO DEL PROTOCOLO TCP/IP

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

FRANCISCO JOSÉ GARCÍA RODAS
ASESORADO POR LA INGA. INGRID RODRÍGUEZ DE LOUKOTA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, AGOSTO DE 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Raúl Eduardo Ticún Córdova
VOCAL V	Br. Henry Fernando Duarte García
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Alfredo Enrique Beber Aceituno (a.i.)
EXAMINADORA	Inga. Ingrid Salomé Rodríguez de Loukota
EXAMINADOR	Ing. Carlos Eduardo Guzman Salazar
EXAMINADOR	Ing. Marvin Marino Hernández Fernandez
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

PROPUESTA DE DISEÑO DE UNA INTERFAZ DE ADQUISICIÓN DE DATOS PARA MEDIDORES ELÉCTRICOS POR MEDIO DEL PROTOCOLO TCP/IP

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 12 de marzo de 2015.

Francisco José García Rodas

Guatemala 4 de abril de 2016

Ingeniero
Carlos Eduardo Guzmán Salazar
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Estimado Ingeniero Guzmán.

Me permito dar aprobación al trabajo de graduación titular: ¨**Propuesta de diseño de una interfaz de adquisición de datos para medidores eléctricos por medio del protocolo TCP/IP**¨, del señor Francisco José García Rodas, por considerar que cumple con los requisitos establecidos.

Por tanto, el autor de este trabajo de graduación y, yo, como su asesora, nos hacemos responsables por el contenido y conclusiones del mismo.

Sin otro particular, me es grato saludarle.

Atentamente,

Inga. Ingrid Rodríguez de Loukota
Colegiada 5,356
Asesora

Ingrid Rodríguez de Loukota
Ingeniera en Electrónica
colegiado 5356

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 30. 2016.
Guatemala, 28 de ABRIL 2016.

Señor Director
Ing. Francisco Javier González López
Director Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: PROPUESTA DE DISEÑO DE UNA INTERFAZ DE ADQUISICIÓN DE DATOS PARA MEDIDORES ELÉCTRICOS POR MEDIO DEL PROTOCOLO TCP/IP , del estudiante Francisco José García Rodas que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Área Electrónica

sro

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 30. 2016.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto bueno del Coordinador de Área, al trabajo de Graduación del estudiante; FRANCISCO JOSÉ GARCÍA RODAS Titulado: PROPUESTA DE DISEÑO DE UNA INTERFAZ DE ADQUISICIÓN DE DATOS PARA MEDIDORES ELÉCTRICOS POR MEDIO DEL PROTOCOLO TCP/IP, procede a la autorización del mismo.

Ing. Francisco Javier González López

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 30 DE MAYO 2016.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 383.2016

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **PROPUESTA DE DISEÑO DE UNA INTERFAZ DE ADQUISICIÓN DE DATOS PARA MEDIDORES ELÉCTRICOS POR MEDIO DEL PROTOCOLO TCP/IP,** presentado por el estudiante universitario: **Francisco José García Rodas,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Pedro Antonio Aguilar Polanco
Decano

Guatemala, agosto de 2016

/gdech

ACTO QUE DEDICO A:

Dios	Por darme la familia que tengo, y permitirme cumplir este objetivo.
Mis padres	Ana, Aníbal por apoyarme en mis estudios y brindarme consejos cuando lo he necesitado.
Mis hermanos	Fernando, Evila por estar presente en mi vida y por compartir las distintas etapas que hemos vivido juntos.
Mis Abuelos	Por apoyarme en las distintas etapas por las que he pasado, por estar presentes en la culminación de los logros alcanzados.
Mis tíos	Por ser parte de mi vida, y por los consejos que me han brindado.
Primos	Por ser parte importante de mi vida.
Compañeros Universitarios	Por compartir las diversas etapas de nuestra vida universitaria y por la amistad que me han brindado.

AGRADECIMIENTOS A:

Sociedad Guatemalteca	Por el pago de mis estudios de educación superior.
La Universidad de San Carlos de Guatemala	Por permitirme estudiar y darme una profesión con la que puedo desenvolverme en el mercado laboral.
Facultad de Ingeniería	Por otorgarme los conocimientos necesarios para culminar el pensum de Ingeniería Electrónica.
Catedráticos Universitarios	Por compartir sus conocimientos de manera desinteresada
Asesor de Tesis	A la Ingeniera Ingrid Rodríguez de Loukota por asesorarme en este proyecto de graduación, y por los conocimientos que compartió con mi persona.
Compañeros de Trabajo	Por compartir sus vivencias laborales y brindarme consejos.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
Bits	Bits
Bps	Bits por segundo
Byte	Byte
Hz	Hertz (ciclos por segundo)
mA	Miliamperio
Ohm	Ohm
V	Voltio
W	Watts

GLOSARIO

ACK	Acuse de recibo.
AES	Esquema de cifrados por bloques.
AMM	Administrador del Mercado Mayorista.
ARP	Protocolo de resolución de direcciones.
CDMA	Multiplexación por división de código.
DES	Algoritmo de cifrado.
Ethernet	Estándar de transmisión de datos para redes.
FTP	Protocolo para transferencia de archivos.
Hardware	Todas las partes físicas de un sistema informático.
ICMP	Protocolo de Mensajes de Control de Internet.
IPSEC	Protocolo de internet seguro.
LAN	Red de área local.
MD5	Algoritmo de resumen del mensaje 5.

OSI	Modelo de interconexión de sistemas abiertos.
RARP	Protocolo de resolución de direcciones inverso.
Raspberry Pi	Interfaz de sistema embebido.
RSA	Sistema criptográfico de clave pública.
SHA	Algoritmo de Hash seguro
SMTP	Protocolo para transferencia simple de correo**.**
Software	Programa, soporte lógico.
SSL	Protocolo de cifrado de paquetes a través de la red.
TCP	Protocolo de control de transmisión.
TDMA	Acceso múltiple por división de tiempo.
Telnet	Protocolo para acceso remoto a otro dispositivo.
UDP	Protocolo de intercambio de datagramas.
VPN	Red privada virtual.
WAN	Red de área amplia o extensa.

RESUMEN

Esta solución contempla el diseño de una interfaz de adquisición de datos de un medidor eléctrico para cumplir con la norma de medición comercial del Administrador del Mercado Mayorista (AMM). La solución está sustentada en el protocolo de comunicación TCP/IP debido a que este contempla todas las capas por las cuales un paquete de datos es manipulado, desde una capa avanzada hasta una muy inferior en la que la información contenida es transformada a valores de voltaje y corriente.

El protocolo de comunicación TCP/IP ofrece dos formas de enviar paquetes en una red de comunicación, el primero es de una forma segura, transporte TCP, para lo que se utiliza un sistema de control en el cual se establece una secuencia de números por cada paquete transmitido de forma consecutiva que sirve para determinar si la transmisión ha sido exitosa o se debe repetir alguno de los paquetes en caso de que la secuencia no se cumpla.

Existe un método adicional, transporte UDP, para enviar paquetes, el cual no garantiza una forma segura, pero es funcional para transmisión de vídeo o voz, debido a que la pérdida de paquetes no representa un daño total en la reconstrucción de la información recibida, sin embargo, este método es mucho más rápido en comparación con el anterior.

Para el diseño de esta solución se contempla utilizar la red celular como medio de transmisión, la cual interactúa con el protocolo TCP para establecer las capas por las que un paquete de información debe ser transformado hasta poder enviar la información de forma inalámbrica por el espectro

electromagnético a una antena de telefonía celular, mediante la interacción con los elementos que convergen en una red móvil serán transmitidos.

OBJETIVOS

General

Ofrecer una alternativa de comunicación para medidores eléctricos de forma remota utilizando muy poca infraestructura física y, con ello, facilitar el cumplimiento de la Norma de Coordinación Comercial No. 14.8, del Administrador del Mercado Mayorista.

Específicos

1. Implementar un sistema de interrogación remota que utilice la red celular 3G con la finalidad de reducir costos de infraestructura.

2. Utilizar el protocolo de comunicación TCP/IP para garantizar una conexión efectiva y minimizar errores en la transmisión de datos.

3. Desarrollar un sistema de control, para supervisar constantemente la conectividad con la interfaz de adquisición de datos, para evitar interrupciones con la comunicación remota.

4. Hacer uso de los criterios adecuados en el diseño de la interfaz, por medio de los de sistemas embebidos, con el propósito de reducir la utilización de dispositivos externos.

INTRODUCCIÓN

Este proyecto de graduación consiste en diseñar una interfaz de adquisición que permita acceder en tiempo real a un medidor eléctrico por medio de una dirección IP. Para esta solución se presenta dos tipos de diseño, el primero contempla el uso de una IP pública y el segundo el uso de una IP privada, esto se logra con la utilización de la red celular como medio de transporte. Se busca establecer una comunicación a distancia manteniendo una tasa de comunicación continua para poder interactuar con el medidor de distintas formas (lecturas de consumo, parámetros de configuración, sincronización de tiempo, pruebas de comunicación, chequeo de operación y mantenimientos).

Con el diseño de la interfaz de comunicación se pretende ofrecer una alternativa cuya inversión económica en infraestructura sea mínima, debido a que, como parte del medio para la conectividad a una red WAN, se utilizará una tarjeta SIM con cobertura de tecnología 3G, la cual direccionará el tráfico de datos a una red WAN o LAN, dependiendo de la necesidad de establecer una comunicación bidireccional, y la interfaz a su vez tendrá asociada una dirección IP estática, la cual puede ser pública o privada.

Debido a que la cantidad de tráfico que maneja el medidor eléctrico está compuesta por datos de consumo que se integran cada 15 minutos según el normativo del AMM y parámetros propios de configuración del medidor. Estos paquetes de datos representan una cantidad de bytes bastante pequeña, es por esta razón que se puede utilizar, de forma eficiente, la tasa de subida que

ofrece la red de tecnología 3G, aunque puede generar algunos retardos debido a la cobertura que se tenga en algunas locaciones remotas.

Para un diseño eficiente del funcionamiento de la interfaz de adquisición de datos se tiene contemplado la utilización de una Raspberry Pi, debido a que es una computadora con un sistema operativo basado en Linux, el cual permite interactuar con hardware y software de forma rápida. Además, cuenta con pines de conectividad para diferentes protocolos de comunicación, los cuales serán útiles para interactuar con el medidor eléctrico y con un dispositivo módem serial encargado de establecer la comunicación con la tarjeta SIM de tecnología celular.

1. PROTOCOLO DE COMUNICACIÓN TCP/IP

TCP/IP es un conjunto de protocolos, cuya sigla significa protocolo de control de transmisión/protocolo de internet y se pronuncia "T-C-P-I-P". Proviene de los nombres de dos protocolos importantes del conjunto de protocolos, es decir, del protocolo TCP y del protocolo IP.

En algunos aspectos, TCP/IP representa todas las reglas de comunicación para internet y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para enrutar paquetes de datos. Debido a que el conjunto de protocolos TCP/IP originalmente se creó con fines militares, está diseñado para cumplir con una cierta cantidad de criterios, entre ellos:

- Dividir mensajes en paquetes
- Usar un sistema de direcciones
- Enrutar datos por la red
- Detectar errores en las transmisiones de datos

El conocimiento del conjunto de protocolos TCP/IP no es esencial para un simple usuario, de la misma manera que un espectador no necesita saber cómo funciona su red audiovisual o de televisión. Sin embargo, para las personas que desean administrar o brindar soporte técnico a una red TCP/IP, su conocimiento es fundamental.

Para aplicar el modelo TCP/IP en cualquier equipo, independientemente del sistema operativo, el sistema de protocolos TCP/IP se ha dividido en diversos módulos.

Cada uno de estos realiza una tarea específica. Además, estos módulos realizan sus tareas uno después del otro en un orden específico, es decir que existe un sistema estratificado. Esta es la razón por la cual se habla de modelo de capas.

El término capa se utiliza para reflejar el hecho de que los datos que viajan por la red atraviesan distintos niveles de protocolos. Por lo tanto, cada capa procesa sucesivamente los datos (paquetes de información) que circulan por la red, les agrega un elemento de información (llamado encabezado) y los envía a la capa siguiente.

El modelo TCP/IP es muy similar al modelo OSI (modelo de 7 capas) que fue desarrollado por la Organización Internacional para la Estandarización (ISO) para estandarizar las comunicaciones entre equipos.

1.1. Modelo OSI

OSI significa interconexión de sistemas abiertos. Este modelo fue establecido por ISO para implementar un estándar de comunicación entre equipos de una red, es decir, las reglas que administran la comunicación entre equipos.

De hecho, cuando surgieron las redes, cada fabricante contaba con su propio sistema (se trata de un sistema patentado), por lo que coexistían

diversas redes incompatibles. Por esta razón fue necesario establecer un estándar.

La función del modelo OSI es estandarizar la comunicación entre equipos para que diferentes fabricantes puedan desarrollar productos (software o hardware) compatibles (siempre y cuando sigan estrictamente el modelo OSI).

El modelo OSI es un modelo que comprende 7 capas, mientras que el modelo TCP/IP tiene solo 4. En realidad, el modelo TCP/IP se desarrolló casi a la par que el modelo OSI, es por ello que está influenciado por este pero no sigue todas las especificaciones del modelo OSI.

Las capas del modelo OSI son las siguientes:

- La capa física define la manera en la que los datos se convierten físicamente en señales digitales en los medios de comunicación (pulsos eléctricos, modulación de luz, otros).
- La capa de enlace de datos define la interfaz con la tarjeta de red y cómo se comparte el medio de transmisión.
- La capa de red permite administrar las direcciones y el enrutamiento de datos, es decir, su ruta a través de la red.
- La capa de transporte se encarga del transporte de datos, su división en paquetes y la administración de potenciales errores de transmisión.
- La capa de sesión define el inicio y la finalización de las sesiones de comunicación entre los equipos de la red.
- La capa de presentación define el formato de los datos que maneja la capa de aplicación (su representación, su compresión y cifrado) independientemente del sistema.

- La capa de aplicación le brinda aplicaciones a la interfaz. Por lo tanto, es el nivel más cercano a los usuarios, administrado directamente por el software.

1.2. Modelo TCP/IP

Está influenciado por el modelo OSI, también utiliza el enfoque modular (utiliza módulos o capas), pero solo contiene cuatro:

- Capa de acceso a la red: especifica la forma en la que los datos deben enrutarse, sea cual sea el tipo de red utilizado.
- Capa de internet: es responsable de proporcionar el paquete de datos (datagrama).
- Capa de transporte: brinda los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión.
- Capa de aplicación: incorpora aplicaciones de red estándar (Telnet, SMTP, FTP y otros).

1.2.1. Encapsulación de datos

Durante una transmisión, los datos cruzan cada una de las capas en el nivel del equipo remitente. En cada capa se le agrega información al paquete de datos. Esto se llama encabezado, es decir, una recopilación de información que garantiza la transmisión. En el nivel del equipo receptor, cuando se atraviesa cada capa, el encabezado se lee y después se elimina. Entonces, cuando se recibe, el mensaje se encuentra en su estado original.

En cada nivel, el paquete de datos cambia su aspecto porque se le agrega un encabezado. Por lo tanto, las designaciones cambian según las capas:

- El paquete de datos se denomina mensaje en el nivel de la capa de aplicación.
- El mensaje después se encapsula en forma de segmento en la capa de transporte.
- Una vez que se encapsula el segmento, en la capa de internet toma el nombre de datagrama.
- Finalmente, se habla de trama en el nivel de capa de acceso a la red.

1.2.2. Capa de acceso a la red

Es la primera capa en TCP/IP, ofrece la capacidad de acceder a cualquier red física y brinda los recursos que se deben implementar para transmitir datos a través de la red.

Por lo tanto, la capa de acceso a la red contiene especificaciones relacionadas con la transmisión de datos por una red física, cuando es una red de área local (red en anillo, Ethernet, FDDI), conectada mediante línea telefónica u otro tipo de conexión a una red. Trata los siguientes conceptos:

- Enrutamiento de datos por la conexión
- Coordinación de la transmisión de datos (sincronización)
- Formato de datos
- Conversión de señal (análoga/digital)
- Detección de errores a su llegada

Afortunadamente, todas estas especificaciones son invisibles al ojo del usuario, ya que en realidad es el sistema operativo el que realiza estas tareas, mientras los *drivers* de hardware permiten la conexión a la red (por ejemplo, el *driver* de la tarjeta de red).

1.2.3. Capa de internet

Es la capa más importante (si bien todas son importantes a su manera), ya que es la que define los datagramas y administra las nociones de direcciones IP. Permite el enrutamiento de datagramas (paquetes de datos) a equipos remotos junto con la administración de su división y ensamblaje cuando se reciben. La capa de internet contiene 5 protocolos:

- Protocolo IP
- Protocolo ARP
- Protocolo ICMP
- Protocolo RARP
- Protocolo IGMP

Los primeros tres protocolos son los más importantes para esta capa.

1.2.4. Capa de transporte

Los protocolos de las capas anteriores permiten enviar información de un equipo a otro. La capa de transporte permite que las aplicaciones que se ejecutan en equipos remotos puedan comunicarse, el problema es identificar estas aplicaciones. De hecho, según el equipo y su sistema operativo, la aplicación puede ser un programa, una tarea, un proceso, entre otros.

Además, el nombre de la aplicación puede variar de sistema en sistema, es por ello que se ha implementado un sistema de numeración para poder asociar un tipo de aplicación con un tipo de datos. Estos identificadores se denominan puertos.

La capa de transporte contiene dos protocolos que permiten que dos aplicaciones puedan intercambiar datos independientemente del tipo de red (es decir, independientemente de las capas inferiores). Estos dos protocolos son los siguientes:

- TCP, un protocolo orientado a conexión que brinda detección de errores.
- UDP, un protocolo no orientado a conexión en el que la detección de errores es obsoleta.

1.2.5. Capa de aplicación

Se encuentra en la parte superior de las capas del protocolo TCP/IP, contiene las aplicaciones de red que permiten la comunicación mediante las capas inferiores. Por lo tanto, el software en esta capa se comunica mediante uno o dos protocolos de la capa inferior (la capa de transporte), es decir, TCP o UDP.

Existen diferentes tipos de aplicaciones para esta capa, pero la mayoría son servicios de red o aplicaciones brindadas al usuario para proporcionar la interfaz con el sistema operativo. Se pueden clasificar según los servicios que brindan:

- Servicios de administración de archivos e impresión (transferencia)
- Servicios de conexión a la red
- Servicios de conexión remota
- Diversas utilidades de internet

1.3. Tráfico TCP

TCP (que significa protocolo de control de transmisión) es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo o van hacia él (es decir, el protocolo IP).

Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que se sepa con anticipación que el protocolo es TCP). TCP es un protocolo orientado a conexión, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

1.3.1. Características del protocolo TCP

Las principales características que permite el protocolo TCP son las siguientes:

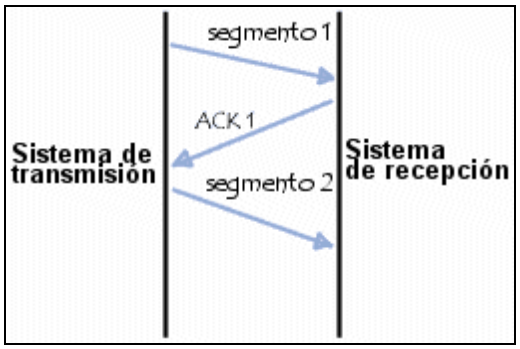
- Colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.
- Monitoreo del flujo de los datos y así evitar la saturación de la red.
- Los datos se forman en segmentos de longitud variada para entregarlos al protocolo IP.
- Multiplexar los datos, que la información que viene de diferentes fuentes (por ejemplo, aplicaciones) en la misma línea pueda circular simultáneamente.
- Comenzar y finalizar la comunicación amablemente.

1.3.2. Confiabilidad de las transferencias

El protocolo TCP permite garantizar la transferencia de datos confiable, a pesar de que usa el protocolo IP que no incluye ningún monitoreo de la entrega de datagramas. De hecho, el protocolo TCP tiene un sistema de acuse de recibo que permite al cliente y al servidor garantizar la recepción mutua de datos.

Cuando se emite un segmento, se lo vincula a un número de secuencia. Con la recepción de un segmento de datos, la máquina receptora devolverá un segmento de datos donde el indicador ACK esté fijado en 1 (para poder indicar que es un acuse de recibo) acompañado por un número de acuse de recibo que equivale al número de secuencia anterior.

Figura 1. **Sistema de transmisión, recepción**



Fuente: *Confiabilidad de las transferencias*. http://es.ccm.net/contents/281-protocolo-tcp**.** Consulta: 20 de febrero de 2015.

Además, usando un temporizador que comienza con la recepción del segmento en el nivel de la máquina originadora, el segmento se reenvía cuando

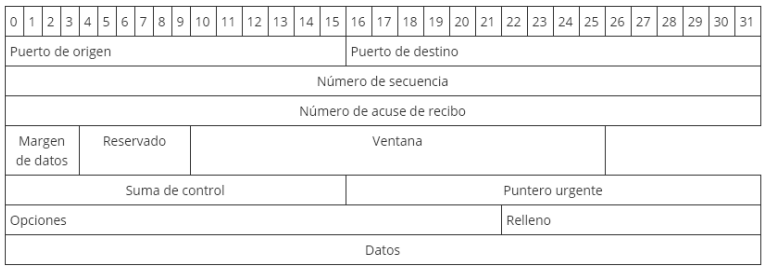
ha transcurrido el tiempo permitido, ya que en este caso la máquina originadora considera que el segmento está perdido.

Sin embargo, si el segmento no está perdido y llega al destino, la máquina receptora lo sabrá, gracias al número de secuencia, que es un duplicado, y solo retendrá el último segmento que llegó al destino.

1.3.3. Formato de los datos en TCP

Un segmento TCP está formado de la siguiente manera:

Figura 2. **Trama de datos TCP**



Fuente: *Formato de los datos en TCP*. http://es.ccm.net/contents/281-protocolo-tcp. Consulta: 21 de febrero de 2015.

El significado de los diferentes campos es:

- Puerto de origen (16 bits): puerto relacionado con la aplicación en curso en la máquina origen
- Puerto de destino (16 bits): puerto relacionado con la aplicación en curso en la máquina destino
- Número de secuencia (32 bits): cuando el indicador SYN está fijado en 0, el número de secuencia es el de la primera palabra del segmento actual.

Cuando SYN está fijado en 1, el número de secuencia es igual al número de secuencia inicial utilizado para sincronizar los números de secuencia (ISN).

- Número de acuse de recibo (32 bits): el número de acuse de recibo, también llamado número de descargo, se relaciona con el número (secuencia) del último segmento esperado y no el número del último segmento recibido.
- Margen de datos (4 bits): esto permite ubicar el inicio de los datos en el paquete. Aquí, el margen es fundamental porque el campo opción es de tamaño variable.
- Reservado (6 bits): un campo que actualmente no está en uso, pero se proporciona para el uso futuro.
- Indicadores (6x1 bit): los indicadores representan información adicional:
    - URG: si este indicador está fijado en 1, el paquete se debe procesar en forma urgente.
    - ACK: si este indicador está fijado en 1, el paquete es un acuse de recibo.
    - PSH (PUSH): si este indicador está fijado en 1, el paquete opera de acuerdo con el método PUSH.
    - RST: si este indicador está fijado en 1, se restablece la conexión.
    - SYN: indica un pedido para establecer una conexión.
    - FIN: si este indicador está fijado en 1, se interrumpe la conexión.
- Ventana (16 bits): campo que permite saber la cantidad de bytes que el receptor desea recibir sin acuse de recibo.
- Suma de control (CRC): la suma de control se realiza tomando la suma del campo de datos del encabezado para poder verificar la integridad del encabezado.
- Puntero urgente (16 bits): indica el número de secuencia después del cual la información se torna urgente.

- Opciones (tamaño variable): diversas opciones.
- Relleno: espacio restante después de que las opciones se rellenan con ceros para tener una longitud que sea múltiplo de 32 bits.

1.4. Tráfico UDP

El protocolo UDP (protocolo de datagrama de usuario) es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Este protocolo es muy simple, ya que no proporciona detección de errores (no es un protocolo orientado a conexión). Por lo tanto, el encabezado del segmento UDP es muy simple.

1.4.1. Formato de los datos en UDP

El formato de los datos en UDP se presenta a continuación.

Figura 3. **Trama de datos UDP**

puerto de origen (16 bits);	puerto de destino (16 bits);
longitud total (16 bits);	suma de comprobación del encabezado (16 bits);
datos (longitud variable).	

Fuente: *Trama de datos UDP*. http://es.ccm.net/contents/284-protocolo-udp. Consulta: 22 de febrero de 2015.

El significado de los diferentes campos es:

- Puerto de origen: es el número de puerto relacionado con la aplicación del remitente del segmento UDP. Este campo representa una dirección de respuesta para el destinatario, por lo tanto, este campo es opcional. Esto significa que, si el puerto de origen no está especificado, los 16 bits de este campo se pondrán en cero. En este caso, el destinatario no podrá responder (lo cual no es estrictamente necesario, en particular para mensajes unidireccionales).
- Puerto de destino: este campo contiene el puerto correspondiente a la aplicación del equipo receptor al que se envía.
- Longitud: este campo especifica la longitud total del segmento, con el encabezado incluido. Sin embargo, el encabezado tiene una longitud de 4 x 16 bits (que es 8 x 8 bits) por lo tanto, la longitud del campo es necesariamente superior o igual a 8 bytes.
- Suma de comprobación: es una suma de comprobación realizada de manera tal que permita controlar la integridad del segmento.

1.5. Túnel VPN

Una red VPN (red privada virtual) es una red privada construida dentro de una infraestructura de red pública, por ejemplo internet. Las empresas pueden usar una red VPN para conectar, de manera segura, oficinas y usuarios remotos por medio de un acceso a internet económico suministrado por un tercero, en lugar de utilizar enlaces WAN dedicados o enlaces de acceso telefónico de larga distancia.

Las organizaciones pueden usar una red VPN para reducir sus costos de ancho de banda de WAN, a la vez que aumentan las velocidades de conexión al usar la conectividad a internet de ancho de banda elevado, tales como DSL, *ethernet* o cable.

Una red VPN proporciona el máximo nivel de seguridad posible a través de seguridad IP cifrada (IPsec) o túneles VPN *secure sockets layer* (SSL) y tecnologías de autenticación. Estas redes protegen los datos que se transmiten por VPN de un acceso no autorizado.

Las empresas pueden aprovechar la infraestructura de internet fácil de aprovisionar de la VPN, para añadir rápidamente nuevos emplazamientos y usuarios. También pueden aumentar enormemente el alcance de la red VPN sin ampliar la infraestructura de forma significativa.

1.5.1. Algoritmos de encriptación

Encriptar significa aplicar un algoritmo de cifrado determinado junto con una clave, a una determinada información que se quiere transmitir confidencialmente. En el cifrado digital se encuentra dos tipos de criptografía: simétrica y asimétrica.

1.5.1.1. Simétricos

El cifrado mediante clave simétrica significa que dos o más usuarios, tienen una única clave secreta, esta clave será la que cifrará y descifrará la información transmitida a través del canal inseguro.

Es decir, la clave secreta la deben tener los dos usuarios. Con dicha clave, el usuario A cifrará la información, la mandará a través del canal inseguro y, a continuación, el usuario B descifrará esa información con la misma clave que ha usado el usuario A.

Para que un algoritmo de clave simétrica sea fiable debe cumplir:

- Una vez que el mensaje es cifrado, no se puede obtener la clave de cifrado/descifrado ni tampoco el texto en claro.
- Si se conoce el texto en claro y el cifrado, se debe tardar más y gastar más dinero en obtener la clave que el posible valor derivado de la información sustraída (texto en claro).

Se debe tener en cuenta que los algoritmos criptográficos son públicos, por lo que su fortaleza debe depender de su complejidad interna y de la longitud de la clave empleada para evitar los ataques de fuerza bruta.

La seguridad en clave simétrica reside en la propia clave secreta, por lo tanto, el principal problema es la distribución de esta clave a los distintos usuarios para cifrar y descifrar la información. La misión del emisor y receptor es mantener la clave en secreto, si cae en manos equivocadas, ya no se podría considerar que la comunicación es segura y se deberia generar una nueva clave.

1.5.1.1.1. DES

Su arquitectura está basada en un sistema monoalfabético, donde un algoritmo de cifrado aplica sucesivas permutaciones y sustituciones al texto en claro. En un primer momento, la información de 64 bits se somete a una permutación inicial, a continuación se somete a una permutación con entrada de 8 bits y otra de sustitución de entrada de 5 bits, todo ello constituido a través de un proceso con 16 etapas de cifrado.

El algoritmo DES usa una clave simétrica de 64 bits, los 56 primeros bits son empleados para el cifrado y los 8 bits restantes se usan para comprobación de errores durante el proceso. La clave efectiva es de 56 bits, por tanto, se tienen 2^{56} combinaciones posibles, por lo que la fuerza bruta se hace casi imposible.

- Ventajas

    - Es uno de los sistemas más empleados y extendidos, por lo tanto, es de los más probados.
    - Implementación sencilla y rápida.

- Inconvenientes

    - No se permite una clave de longitud variable, es decir, no se puede aumentar para tener una mayor seguridad.
    - Es vulnerable al criptoanálisis diferencial (2^{47} posibilidades) siempre que se conozca un número suficiente de textos en claro y cifrados.
    - La longitud de la clave de 56 bits es demasiado corta y, por lo tanto, vulnerable. Actualmente DES ya no es un estándar, debido a que en 1999 fue roto por un ordenador.

1.5.1.1.2. 3DES

Se basa en aplicar el algoritmo DES tres veces, la clave tiene una longitud de 128 bits. Si se cifra el mismo bloque de datos dos veces con dos llaves diferentes (de 64 bits), aumenta el tamaño de la clave. El 3DES parte de una llave de 128 bits, que es divida en dos llaves, A y B.

Al recibir los datos, se aplica el algoritmo DES con la llave A, a continuación, se repite con la llave B y luego otra vez con la llave A.

3DES aumenta de forma significativa la seguridad del sistema de DES, pero requiere más recursos del ordenador. Existe una variante del 3DES, conocida como DES-EDE3, con tres claves diferentes y una longitud de 192 bits, consiguiendo un sistema mucho más robusto.

1.5.1.1.3. AES

Este algoritmo es el más conocido entre los usuarios de *routers*, ya que WPA opera con AES como método de cifrado. Este cifrado puede implementar tanto en sistemas hardware como en software. El sistema criptográfico AES opera con bloques y claves de longitudes variable, hay AES de 128 bits, de 192 bits y de 256 bits.

El resultado intermedio del cifrado constituye una matriz de bytes de cuatro filas por cuatro columnas. A esta matriz se le vuelve a aplicar una serie de bucles de cifrado basado en operaciones matemáticas (sustituciones no lineales de bytes, desplazamiento de filas de la matriz, combinaciones de las columnas mediante multiplicaciones lógicas y sumas XOR con base en claves intermedias).

- Seguridad de AES

AES tiene 10 rondas para llaves de 128 bits, 12 rondas para llaves de 192 bits y 14 rondas para llaves de 256 bits. En 2006, los mejores ataques conocidos fueron las 7 rondas para claves de 128 bits, 8 rondas para llaves de 192 bits y 9 rondas para claves de 256 bits.

Algunos criptógrafos muestran preocupación sobre la seguridad del AES. Ellos creen que el margen entre el número de rondas especificado en el cifrador y los mejores ataques conocidos es muy pequeño. Otra preocupación es la estructura de AES. A diferencia de la mayoría de cifradores de bloques, AES tiene una descripción matemática muy ordenada.

Se debe recordar que AES es usado en los cifrados *wireless* de los *routers* de los hogares como método de cifrado (no clave), ya que en los *routers* se puede usar una clave estática o una dinámica mediante un servidor Radius. AES también es usado por Open SSL y por supuesto en Open VPN (ya que usa las librerías Open SSL).

Los algoritmos de cifrado de bloque como AES separan el mensaje en trozos de tamaño fijo, por ejemplo, de 64 o 128 bits. La forma en que se gestionan estos bloques de mensaje, se denomina modo de cifrado.

1.5.1.2. Asimétricos

La criptografía de clave asimétrica también es conocida como clave pública, emplea dos llaves diferentes en cada uno de los extremos de la comunicación.

Cada usuario tendrá una clave pública y otra privada. La clave privada tendrá que ser protegida y guardada por el propio usuario, será secreta y no la deberá conocer nadie. La clave pública será accesible a todos los usuarios del sistema de comunicación.

Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver en un sentido, pero muy complicado de realizarlo en sentido inverso a menos que se conozca la llave.

Las claves públicas y privadas se generan simultáneamente y están ligadas una a la otra. Esta relación debe ser muy compleja para que resulte muy difícil de obtener una a partir de la otra.

Las parejas de claves tienen funciones diversas y muy importantes, entre las que destacan:

- Cifrar la información
- Asegurar la integridad de los datos transmitidos
- Garantizar la autenticidad del emisor

1.5.1.3. Cifrado con clave asimétrica

Si una persona con una pareja de claves cifra un mensaje con la llave privada, ese mensaje solo podrá ser descifrado con la llave pública asociada. Si se cifra con la pública, se descifra con la privada.

Si se cifra un mensaje con la clave privada, se podrá descifrar con la propia llave privada, se debería usar la pública. La criptografía asimétrica proporciona autenticidad, integridad y no repudio. Para que un algoritmo sea considerado seguro debe cumplir:

- Si se conoce el texto cifrado, debe resultar muy difícil o imposible extraer el texto en claro y la clave privada.

- Si se conoce el texto en claro y el cifrado, debe resultar más costoso obtener la clave privada que el texto en claro.
- Si los datos han sido cifrados con la clave pública, solo debe existir una clave privada capaz de descifrarlo, y viceversa.

La ventaja del cifrado asimétrico sobre el simétrico radica en que la clave pública puede ser conocida por todo el mundo (no así la privada), sin embargo, en el cifrado simétrico deben conocer la misma clave los dos usuarios (y la clave debe hacerse llegar a cada uno de los distintos usuarios por el canal de comunicación).

1.5.1.4. Algoritmos de cifrado de clave asimétrica

Existen dos algoritmos principales, el Diffie-Hellman y RSA.

1.5.1.4.1. Diffie-Hellman

No es un algoritmo asimétrico propiamente dicho, se usa para generar una clave privada simétrica a ambos extremos de un canal de comunicación inseguro. Se emplea para obtener la clave secreta con la que posteriormente se cifra la información, junto con un algoritmo de cifrado simétrico. Su seguridad radica en la dificultad de calcular los logaritmos discretos de números grandes.

El problema de este algoritmo es que no proporciona autenticación, no puede validar la identidad de los usuarios, por lo tanto, si un tercer usuario se pone en medio de la “conversación”, también se le facilitarían las claves y podría establecer comunicaciones con el emisor y el receptor suplantando las identidades.

1.5.1.4.2. RSA

Este algoritmo se basa en la pareja de claves pública y privada de las que ya se ha hablado antes. La seguridad de este algoritmo radica en el problema de la factorización de números enteros.

- Ventajas
    - Resuelve el problema de la distribución de las llaves simétricas (cifrado simétrico).
    - Se puede emplear para ser utilizado en firmas digitales.
- Desventajas
    - La seguridad depende de la eficiencia de los ordenadores.
    - Es más lento que los algoritmos de clave simétrica.
    - La clave privada debe ser cifrada por algún algoritmo simétrico.

1.5.1.5. Algoritmos de autenticación (o hash)

Una función hash es el método para generar claves o llaves que representen de manera casi unívoca a un documento o conjunto de datos. Es una operación matemática que se realiza sobre este conjunto de datos de cualquier longitud y su salida es una huella digital de tamaño fijo e independiente de la dimensión del documento original. El contenido es ilegible.

Es posible que existan huellas digitales iguales para objetos diferentes, porque una función hash, en el caso del SHA-1 tiene 160 bits, y los posibles objetos a resumir no tienen un tamaño límite.

A partir de un hash, o huella digital, no se puede recuperar el conjunto de datos originales. Los más conocidos son el MD5 y el SHA-1. Cifrar una huella digital se conoce como firma digital. Los requisitos que deben cumplir las funciones hash son:

- Imposibilidad de obtener el texto original a partir de la huella digital.
- Imposibilidad de encontrar un conjunto de datos diferentes que tengan la misma huella digital (aunque como se ha visto anteriormente es posible que este requisito no se cumpla).
- Transformar un texto de longitud variable en una huella de tamaño fijo (como el SHA-1 que es de 160 bits).
- Facilidad de empleo e implementación.

1.5.1.5.1. MD5

Es una función hash de 128 bits. Como todas las funciones hash, toma unos determinados tamaños a la entrada y salen con una longitud fija (128 bits).

El algoritmo MD5 no sirve para cifrar un mensaje. La información original no se puede recuperar ya que hay pérdida de datos.

1.5.1.5.2. SHA-1

Es parecido al famoso MD5, pero tiene un bloque de 160 bits en lugar de los 128 bits del MD5. La función de compresión es más compleja que la función de MD5. SHA-1 es más lento que MD5 porque el número de pasos son de 80 (64 en MD5) y porque tiene mayor longitud que MD5 (160 bits contra 128 bits). Lo que convierte a SHA-1 más robusto y seguro, totalmente apto para VPN por ejemplo.

1.5.1.5.3. SHA-2

Las principales diferencias con SHA-1 radican en en su diseño y que los rangos de salida han sido incrementados. Se pueden encontrar SHA-224, SHA-256, SHA-384, y SHA-512.

El más seguro es el que mayor salida de bits tiene, el SHA-512, que tiene 80 rondas (pasos) como el SHA-1, pero se diferencia de este en:

- Tamaño de salida 512 por los 160 de SHA-1.
- Tamaño del bloque, tamaño de la palabra y tamaño interno que es el doble que SHA-1.

Como ocurre con todos los cifrados y hash, cuanto más seguro, más lento su procesamiento y uso, se debe encontrar un equilibrio entre seguridad y velocidad.

1.5.1.6. Protocolo de seguridad IPsec

El IPsec es un conjunto de protocolos para la seguridad de las comunicaciones IP que proporciona encriptación, integridad y autenticación. IPsec ingresa el mensaje necesario para proteger las comunicaciones VPN, pero se basa en algoritmos existentes. Existen dos protocolos de estructura IPsec.

- Encabezado de autenticación (AH): se utiliza cuando no se requiere o no se permite la confidencialidad. AH proporciona la autenticación y la integridad de datos para paquetes IP intercambiados entre dos sistemas.

Verifica que cualquier mensaje intercambiado de R1 a R3 no haya sido modificado en el camino.

- Contenido de seguridad encapsulado (ESP): proporciona confidencialidad y autenticación mediante la encriptación del paquete IP.

2. PROTOCOLO DE COMUNICACIÓN RS-232

Es una de las normas más populares empleadas en la comunicación serie (su inserción en el PC incrementó su popularidad). Fue desarrollada en la década de los 60 para gobernar la interconexión de terminales y módems. Está patrocinada por la EIA (Asociación de Industrias Eléctricas).

2.1. Consideraciones en la comunicación serie

Cuando se transmite información a través de una línea serie es necesario utilizar un sistema de codificación que permita resolver los siguientes problemas:

- Sincronización de bits: el receptor necesita saber dónde comienza y dónde termina cada bit en la señal recibida para efectuar el muestreo de la misma en el centro del intervalo de cada símbolo (bit para señales binarias).
- Sincronización del carácter: la información serie se transmite por definición bit a bit, pero la misma tiene sentido en palabras o bytes.
- Sincronización del mensaje: es necesario conocer el inicio y fin de una cadena de caracteres por parte del receptor para detectar algún error en la comunicación de un mensaje.

2.2. Velocidad de transmisión

Se expresa en bits por segundo o baudios, el baudio es un concepto más general que bit por segundo. El primero queda definido como el número de

estados de la señal por segundo, si solo existen dos estados (que pueden ser representados por un bit, que identifica dos unidades de información), entonces baudio es equivalente a bit por segundo. Baudio y bit por segundo se diferencian cuando es necesario más de un bit para representar más de dos estados de la señal.

La velocidad de transmisión queda limitada por el ancho de banda, potencia de señal y ruido en el conductor de señal. La velocidad de transmisión queda básicamente establecida por el reloj. Su misión es examinar o muestrear continuamente la línea para detectar la presencia o ausencia de los niveles de señal ya predefinidos. El reloj sincroniza además todos los componentes internos.

2.2.1. Líneas o canales de comunicación

Se pueden establecer canales para la comunicación de acuerdo a tres técnicas, siempre tomando al microprocesador o microcontrolador como referencia (transmisor) y al periférico como destino (receptor):

- *Simplex*
- Semiduplex (*half duplex*)
- Totalmente *dúplex* (*Full duplex*)

2.2.2. *Simplex*

En ella la comunicación serie usa una dirección y una línea de comunicación. Siempre existirá un transmisor y un receptor, no ambos. La ventaja de este sistema consiste en que es necesario solo un enlace a dos hilos.

La desventaja radica en que el extremo receptor no tiene ninguna forma de avisar al extremo transmisor sobre su estado y sobre la calidad de la información que se recibe. Esta es la razón por la cual, generalmente, no se utiliza.

2.2.3. Semidúplex

La comunicación serie se establece a través de una sola línea, pero en ambos sentidos. En un momento el transmisor enviará información y en otro recibirá, por lo que no se puede transferir información en ambos sentidos de forma simultánea.

Este modo permite la transmisión, desde el extremo receptor de la información, sobre el estado de dicho receptor y sobre la calidad de la información recibida, por lo que permite así la realización de procedimientos de detección y corrección de errores.

2.2.4. *Full duplex*

Se utilizan dos líneas (una transmisora y otra receptora) y se transfiere información en ambos sentidos. La ventaja de este método es que se puede transmitir y recibir información de manera simultánea.

La mayoría de los dispositivos especializados para la comunicación pueden transferir información tanto en *full duplex* como en *half duplex* (el modo *simplex* es un caso especial dentro de *half duplex*).

2.3. Modos de transmisión

Existen dos modos básicos para realizar la transmisión de datos y son:

- Modo asíncrono
- Modo síncrono

Las transmisiones asíncronas son aquellas en que los bits que constituyen el código de un carácter, se emiten con la ayuda de impulsos suplementarios que permiten mantener en sincronia los dos extremos.

En las transmisiones síncronas los caracteres se transmiten consecutivamente, no existiendo ni bit de inicio ni bit de parada entre los caracteres, estando dividida la corriente de caracteres en bloques, enviándose una secuencia de sincronización al inicio de cada bloque.

2.3.1. Transmisión asíncrona

Cuando se opera en modo asíncrono no existe una línea de reloj común que establezca la duración de un bit y el carácter puede ser enviado en cualquier momento. Esto conlleva a que cada dispositivo tenga su propio reloj y que previamente se ha acordado que ambos dispositivos transmitirán datos a la misma velocidad.

No obstante, en un sistema digital, un reloj es normalmente utilizado para sincronizar la transferencia de datos entre las diferentes partes del sistema. El reloj definirá el inicio y fin de cada unidad de información, así como la velocidad de transmisión. Si no existe reloj común, algún modo debe ser utilizado para sincronizar el mensaje.

En realidad, la frecuencia con la que el reloj muestrea la línea de comunicación es mucho mayor que la cadencia con que llegan los datos. Por ejemplo, si los datos están llegando a una cadencia de 2 400 bps, el reloj examinará la línea unas 19 200 veces por segundo, es decir, ocho veces la cadencia binaria. La gran rapidez con que el reloj muestrea la línea, permite al dispositivo receptor detectar una transmisión de 1 a 0 o de 0 a 1 muy rápidamente y mantener así la mejor sincronización entre los dispositivos emisor y receptor.

El tiempo por bit en una línea en que se transfiere la información a 2 400 bps es de unos 416 microsegundos (1 seg/2 400). Una frecuencia de muestreo de 2400 veces por segundo nos permitirá muestrear el principio o el final del bit.

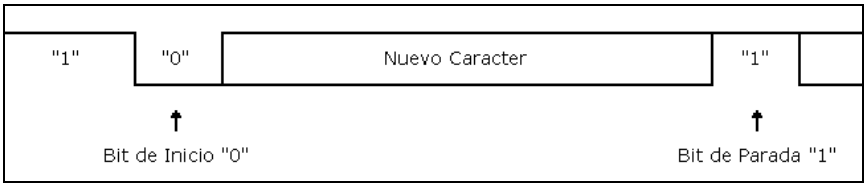
En ambos casos se detectará el bit, sin embargo, no es extraño que la señal cambie ligeramente y permanezca la línea con una duración un poco más larga o más corta de lo normal. Por todo ello, una frecuencia de muestreo lenta no sería capaz de detectar el cambio de estado de la señal a su debido tiempo, dando lugar a que la estación terminal no recibiera los bits correctamente.

2.3.1.1. Bit de inicio y bit de parada

En la transmisión asíncrona, un carácter a transmitir es encuadrado con un indicador de inicio y fin de carácter, de la misma forma que se separa una palabra con una letra mayúscula y un espacio en una oración. La forma estándar de encuadrar un carácter es a través de un bit de inicio y un bit de parada.

Durante el intervalo en que no son transferidos caracteres, el canal debe poseer un "1" lógico. Al bit de parada se le asigna también un "1". Al bit de inicio del carácter a transmitir se le asigna un "0". Por todo lo anterior, un cambio de nivel de "1" a "0" lógico le indicará al receptor que un nuevo carácter será transmitido.

Figura 4. **Transmisión asíncrona**



Fuente: *Transmisión asíncrona*. http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 23 de febrero de 2015.

2.3.1.2. Reglas de transmisión asíncrona

La transmisión asíncrona está definida por la Norma RS232, en la que se profundizará más adelante y que se basa en las siguientes reglas:

- Cuando no se envían datos por la línea, esta se mantiene en estado alto (1).
- Cuando se desea transmitir un carácter, se envía primero un bit de inicio que pone la línea ha estado bajo (0) durante el tiempo de un bit.
- Durante la transmisión, si la línea está a nivel bajo, se envía un 0 y si está a nivel alto se envía un 1.
- A continuación, se envían todos los bits del mensaje a transmitir con los intervalos que marca el reloj de transmisión. Por convenio se transmiten entre 5 y 8 bits.

- Se envía primero el bit menos significativo, siendo el más significativo el último en enviarse.
- A continuación del último bit del mensaje se envía el bit (o los bits) del final que hace que la línea se ponga a 1 por lo menos durante el tiempo mínimo de un bit. Estos bits pueden ser un bit de paridad para detectar errores y el bit o bits de *stop*, que indican el fin de la transmisión de un carácter.

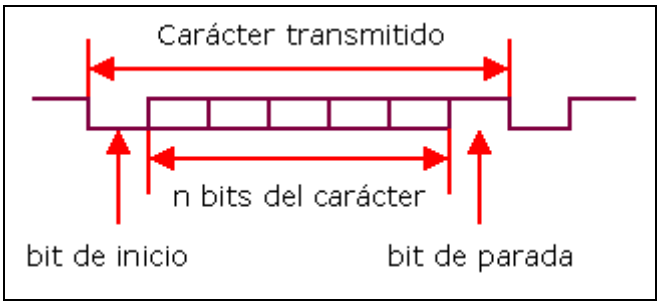
Los datos codificados por esta regla pueden ser recibidos siguiendo los pasos siguientes:

- Esperar la transición 1 a 0 en la señal recibida.
- Activar el reloj con una frecuencia igual a la del transmisor.
- Muestrear la señal recibida al ritmo de ese reloj para formar el mensaje.
- Leer un bit más de la línea y comprobar si es 1 para confirmar que no ha habido error en la sincronización.

2.3.1.3. Velocidad de transmisión

En la transmisión asíncrona, por cada carácter se envía al menos 1 bit de inicio y 1 bit de parada, así como opcionalmente 1 bit de paridad. Esta es la razón de que los baudios no se correspondan con el número de bits de datos que son transmitidos.

Figura 5. **Formato básico de transmisión asíncrona**

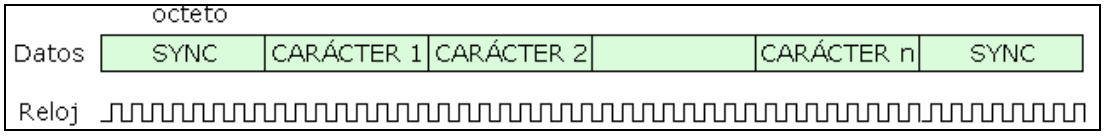


Fuente: *Formato básico de transmisión asíncrona*. http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 23 de febrero de 2015.

2.3.2. Transmisión síncrona

Es un método más eficiente de comunicación, en cuanto a velocidad de transmisión. Esto viene dado porque no existe ningún tipo de información adicional entre los caracteres a ser transmitidos.

Figura 6. **Transmisión sincrónica**



Fuente: *Transmisión sincrónica*. http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 2 de marzo de 2015.

Cuando se transmite de manera síncrona, lo primero que se envía es un octeto de sincronismo ("sync"). El octeto de sincronismo realiza la misma función que el bit de inicio en la transmisión asíncrona, indicando al receptor que va a ser enviado un mensaje. Este carácter, además, utiliza la señal local

de reloj para determinar cuándo y con qué frecuencia será muestreada la señal, es decir, permite sincronizar los relojes de los dispositivos transmisor y receptor.

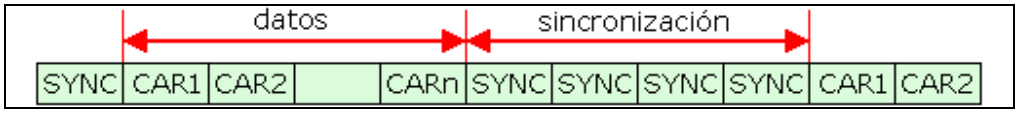
La mayoría de los dispositivos de comunicación llevan a cabo una resincronización contra posibles desviaciones del reloj, cada uno o dos segundos, insertando para ello caracteres del tipo "sync" periódicamente dentro del mensaje.

Los caracteres de sincronismo deben diferenciarse de los datos del usuario para permitir al receptor detectar los caracteres "sync". Por ejemplo, el código ASCII utiliza el octeto 10010110.

Existen ocasiones en que son definidos dos caracteres de sincronismo, esto puede ser necesario si, por cualquier motivo, el carácter "sync" original se desvirtuara, el siguiente permitirá la reinicialización del receptor. En segundo lugar, puede ocurrir que el equipo receptor necesite un tiempo adicional para adaptarse a la señal entrante.

Cuando se transmite de forma síncrona, es necesario mantener el sincronismo entre el transmisor y el receptor cuando no se envían caracteres, para ello son insertados caracteres de sincronismo de manera automática por el dispositivo que realiza la comunicación.

Figura 7. **Inserción automática de caracteres de sincronismo**



Fuente: *Caracteres de sincronismo.* http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 2 de marzo de 2015.

El receptor/transmisor síncrono debe indicar, además, cuándo el sincronismo ha sido logrado por parte del receptor.

2.3.3. Detectar errores en la comunicación

Cuando se escriben o se envían datos, pueden producirse errores, entre otras cosas, por ruidos inducidos en las líneas de transmisión de datos. Por esto es necesario comprobar la integridad de los datos transmitidos mediante algún método que permita determinar si se ha producido un error. En un caso típico, si al transmitirse un mensaje se determina que se ha producido un error, el receptor solicita de nuevo el mensaje al emisor. Se pueden detectar errores de acuerdo a la forma de transmisión:

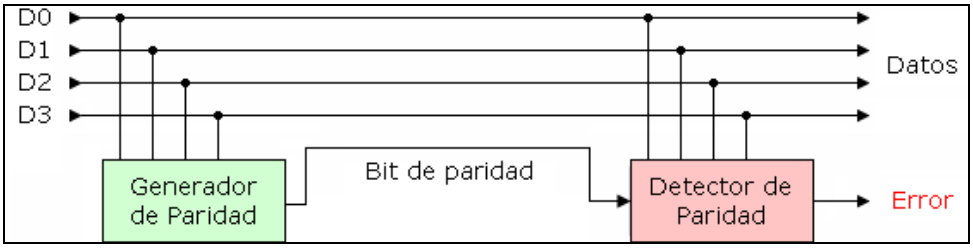
- Transmisión asíncrona
    - Paridad
    - Sobreescritura
    - Error de encuadre (*framing*)
- Transmisión síncrona
    - Paridad
    - Sobreescritura

2.3.3.1. Detectores de paridad

Como un error en una transmisión serie solamente suele afectar a un bit, uno de los métodos más comunes para detectar errores es el control de la

paridad. El control de paridad consiste en añadir un bit, denominado de paridad, a los datos que se envían o escriben.

Figura 8. **Detector de paridad**



Fuente: *Detector de paridad*. http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 3 de marzo de 2015.

La paridad puede ser par o impar.

2.3.3.1.1. Paridad par

El bit de paridad será cero cuando el número de bit "unos" que contienen los datos a transmitir sea un número par, y el bit de paridad será uno cuando los datos que se mandan contienen un número impar de unos.

Tabla I. **Paridad par**

Dato	Paridad
0000 0001	1
0101 0001	1
0101 0101	0
0000 0000	0

Fuente: elaboración propia.

La suma de los bits que son unos, contando datos y bit de paridad dará siempre como resultado un número par de unos.

2.3.3.1.2. Paridad impar

En el sistema de paridad impar, el número de unos (datos + paridad) siempre debe ser impar.

Tabla II. **Paridad impar**

Dato	Paridad
0000 0001	0
0101 0001	0
0101 0101	1
0000 0000	1

Fuente: elaboración propia.

2.3.3.1.3. Método *checksum*

Puede existir el caso en que, por ejemplo, se alteren dos bits en un carácter transmitido y, si se ha implementado la comprobación de paridad, el error no será detectado.

Existen otros métodos de detección de errores, como la comprobación de redundancia cíclica (CRC) y la comprobación de suma (*checksum*). Por su simplicidad, será abordado el método checksum.

El método *checksum* puede ser utilizado tanto en la transmisión síncrona como en la asíncrona. Se basa en la transmisión, al final del mensaje, de un

byte (o bytes) cuyo valor sea el complemento a dos de la suma de todos los caracteres que han sido transmitidos en el mensaje.

El receptor implementará una rutina que suma todos los bytes de datos recibidos y al resultado se le sumará el último byte (que posee la información en complemento a dos de la suma de los caracteres transmitidos) y, si la recepción del mensaje ha sido correcta, el resultado debe ser cero.

2.4. Norma RS232

Como antes se adelantó, la Norma RS232 es una de las más populares que se utilizan en la comunicación serie y es la que se utiliza en las computadoras. Si bien actualmente está ampliamente superada por la transmisión serie a través de USB, de manera que está remitiendo su uso (por ejemplo, ya no se implementa en ordenadores portátiles).

La Norma RS232 está definida tanto para la transmisión síncrona como para la asíncrona, pero cuando se utiliza esta última, solo un conjunto de terminales es utilizado.

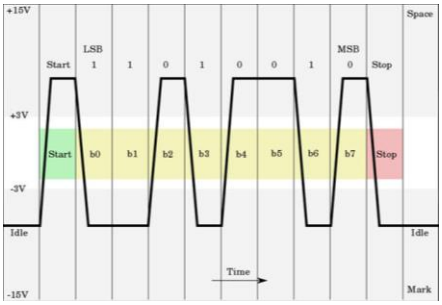
2.4.1. Características eléctricas

Se establece que la longitud máxima del cable no debe ser superior a los 15 metros y la velocidad máxima de transmisión es, en principio, 128,000 bps. Los niveles lógicos no son compatibles TTL, considerando:

- 1 lógico entre -3 y -15 V
- 0 lógico entre +3 y +15 V

Trazado de los niveles de tensión para el carácter ASCII "K" (0x4b) con 1 bit de inicio, 8 de datos y 1 de stop.

Figura 9. **Niveles de tensión transmisión UART**



Fuente: *Niveles de tensión transmisión*. http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 3 de marzo de 2015.

2.4.2. Velocidad

La velocidad está estandarizada según la Norma RS 232C en baudios:

- 75
- 110
- 150
- 300
- 600
- 1200
- 2400
- 4800
- 9600
- 19200

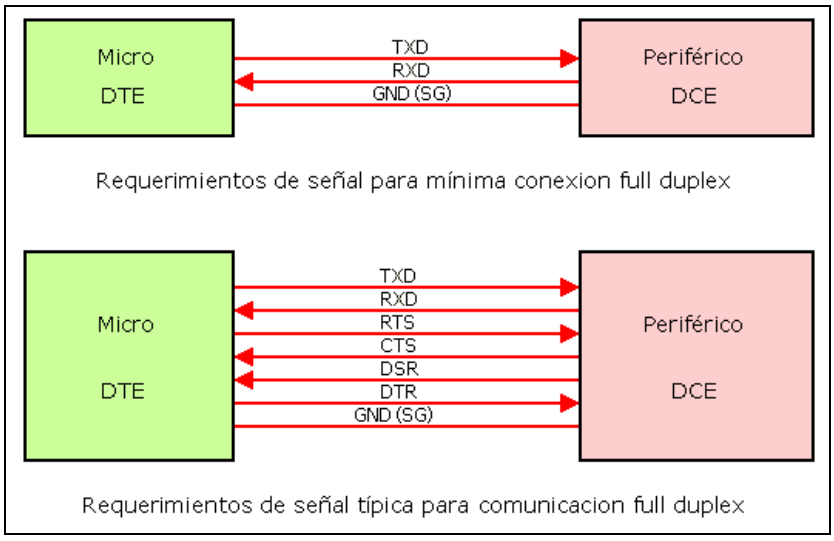
Fuera de la norma:

- 38400
- 57600
- 76800
- 115200

2.4.3. Interfaz TTL-RS232

Para una comunicación *full duplex* desde la UART de un microprocesador o microcontrolador deben conectarse un mínimo número de señales, concretamente TXD y RXD, así como la masa (GND, SG o *signal ground*). Sin embargo, una interfaz típica RS232 requiere al menos 7 señales.

Figura 10. **Comunicación *full duplex***



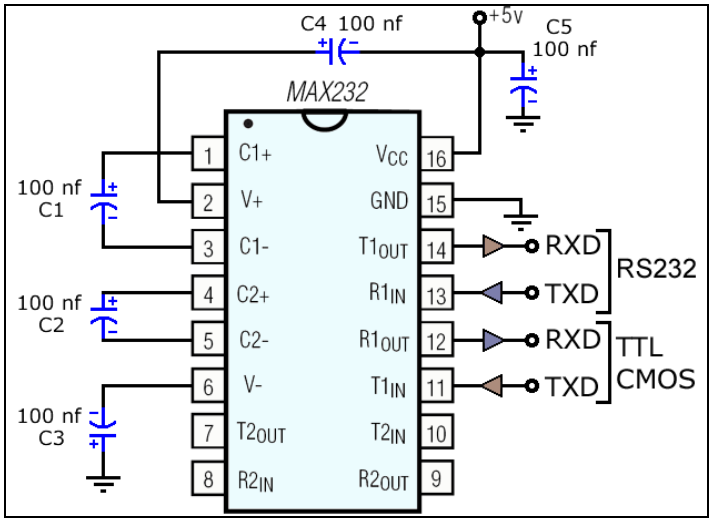
Fuente: *Comunicación full duplex*. http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 4 de marzo de 2015.

Las líneas adicionales se utilizan para la puesta de acuerdo entre el DTE (por ejemplo, un PC) y el DCE (por ejemplo, un ratón).

El terminal para transmitir datos (TXD) es utilizado para transferir datos del DTE al DCE, por lo que debe ser conectado a la línea receptora serie del periférico. De manera idéntica, la línea receptora de datos (RXD) debe ser conectada a la línea transmisora del periférico.

Para convertir TTL a RS232 se pueden usar circuitos típicos de transistores y diodos discretos o los circuitos integrados MC1488 y MC1489, sin embargo, existe un circuito integrado muy popular que permite esta conversión. El MAX232 es un conversor de nivel TTL/RS232, solo es necesario este circuito integrado y 4 condensadores. La interfaz mínima con el MAX232 entre un dispositivo con salida serie TTL o CMOS y el conector RS232 se muestra en la siguiente figura.

Figura 11. **Conexión RS232**

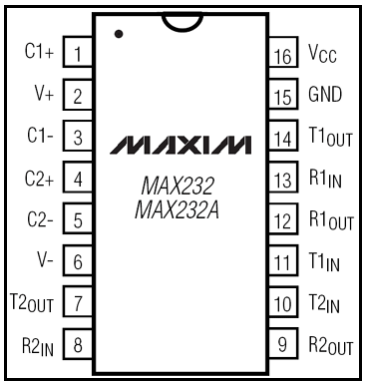


Fuente: *Conexión*. http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 4 de marzo de 2015.

2.4.4. MAX232

Dispone internamente de 4 conversores de niveles TTL al estándar RS232 y viceversa, para comunicación serie como los usados en los ordenadores, el COM1 y el COM2.

Figura 12. **Integrado MAX 232**

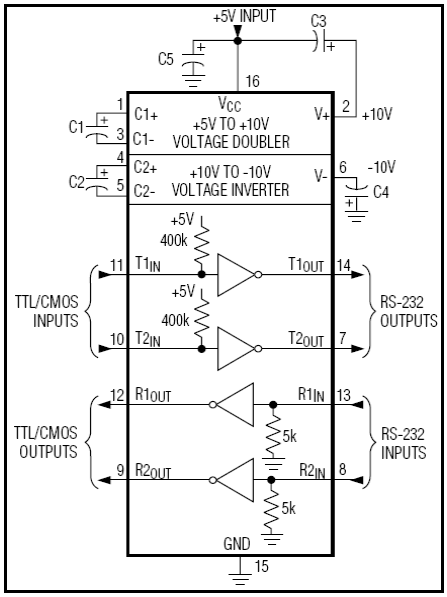


Fuente: *Integrado 232*. http://perso.wanadoo.es/pictob/comserie.htm.
Consulta: 4 de marzo de 2015.

El circuito integrado lleva internamente 2 conversores de nivel de TTL a RS232 y otros 2 de RS232 a TTL, con lo que en total se podrá manejar 4 señales del puerto serie del PC. Por lo general, las más usadas son TXD, RXD, RTS, CTS, estas dos últimas son las usadas para el protocolo handshaking, pero no es imprescindible su uso.

Para que el MAX232 funcione correctamente se deben poner unos condensadores externos, todo esto se observa en la figura 13 en la que solo se han cableado las líneas TXD y RXD que son las más usadas para casi cualquier aplicación.

Figura 13. **Estructura interna IC MAX 232**



Fuente: *Estructura interna IC MAX 232*. http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 4 de marzo de 2015.

En el MAX232 todos los condensadores deben ser de 1 microfaradio para llegar hasta 120 Kbps o de 100 nanofaradios para llegar hasta 64 Kbps. Para el MAX232A, los condensadores han de ser de 100 nanofaradios y se consiguen hasta 200 Kbps. Este integrado es usado para comunicar un microcontrolador o sistema digital con una PC o sistema basado en el estándar RS232.

2.4.4.1. RS232 en el PC

El puerto serie de un ordenador trabaja en modo asincrónico. El puerto serie recibe y envía información fuera del ordenador mediante un determinado software de comunicación o un *driver* del puerto serie. La información se envía al puerto carácter a carácter. Cuando se ha recibido un carácter, el puerto serie envía una señal por medio de una interrupción indicando que el carácter está

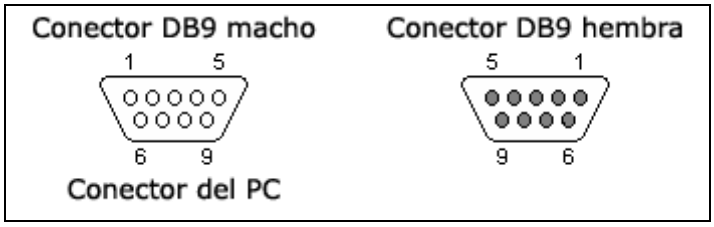
listo. Cuando el ordenador ve la señal, los servicios del puerto serie leen el carácter.

Existen dos tipos de interfaces RS232, puesto que la norma fue diseñada para dos tipos de equipos, el DTE (equipo terminal de datos) y el DCE (equipo de comunicación de datos). Existen entonces dos tipos de interfaz RS232, la DTE (conector macho) y la DCE (conector hembra):

- Interfaz DTE (macho) en la PC
- Interfaz DCE (hembra) en los módems, ratones y otros dispositivos

En una PC se utilizan conectores DB9 macho, de 9 patillas, por los que se conectan los dispositivos al puerto serie. Los conectores hembra que se enchufan tienen una colocación de patillas diferente, de manera que se conectan la patilla 1 del macho con la patilla 1 de la hembra, la patilla 2 con el 2, y así sucesivamente.

Figura 14. **Conectores DB9**



Fuente: *Conectores DB9*. http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 4 de marzo de 2015.

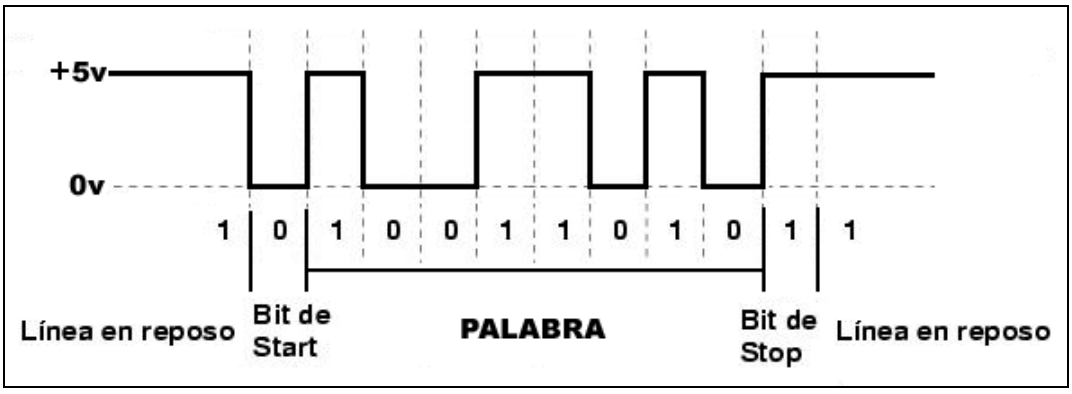
RS232 no admite comunicaciones a más de 15 metros y 20 Kbps (se puede utilizar mayor distancia y velocidad, pero no es el estándar). La

comunicación es efectuada con 25 terminales diferentes, cada uno con su función. RS232 está definida tanto para la comunicación síncrona como asíncrona, pero cuando se utiliza esta última solo se utiliza un conjunto de los 25 terminales.

Normalmente, las comunicaciones serie en el PC tienen los siguientes parámetros: 9 600 baudios, 1 bit de *start*, 8 bits de datos, 1 bit de *stop* y sin paridad.

En la figura 15 se observa un ejemplo de la transmisión en TTL del dato binario 01011001. La línea en reposo está a nivel lógico alto (+5 voltios).

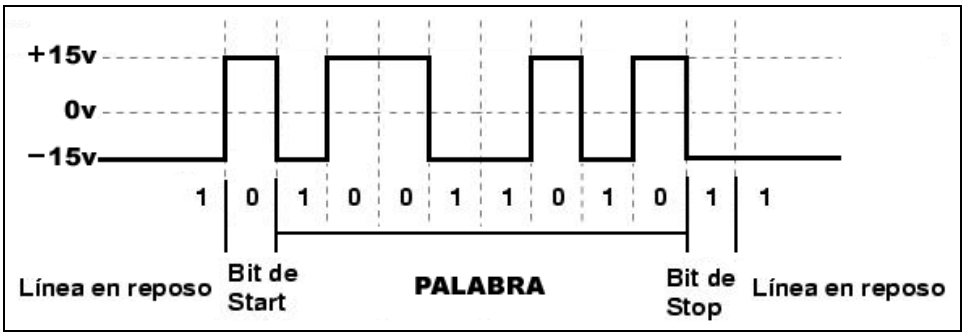
Figura 15. **Transmisión niveles TTL**



Fuente: *Transmisión niveles*. http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 7 de marzo de 2015.

En la figura 16 se observa un ejemplo de la transmisión en RS232 del dato binario 01011001. La línea en reposo está a nivel lógico alto (-15 voltios).

Figura 16. **Transmisión niveles RS232**



Fuente: *Transmisión niveles RS232*. http://perso.wanadoo.es/pictob/comserie.htm. Consulta: 4 de marzo de 2015.

3. SISTEMAS EMBEDIDOS

Un sistema embebido (anglicismo de *embedded*) o empotrado (integrado, incrustado) es un sistema de computación diseñado para realizar una o algunas pocas funciones dedicadas, frecuentemente en un sistema de computación en tiempo real.

Al contrario de lo que ocurre con las computadoras de propósito general (por ejemplo una computadora personal o PC) que están diseñadas para cubrir un amplio rango de necesidades, los sistemas embebidos, se diseñan para cubrir necesidades específicas. En un sistema embebido, la mayoría de los componentes se encuentran incluidos en la placa base (la tarjeta de vídeo, audio, módem, entre otros) y muchas veces los dispositivos resultantes no tienen el aspecto de lo que se suele asociar a una computadora.

Algunos ejemplos de sistemas embebidos podrían ser dispositivos como un taxímetro, un sistema de control de acceso, la electrónica que controla una máquina expendedora o el sistema de control de una fotocopiadora, entre otras múltiples aplicaciones.

Por lo general, los sistemas embebidos se pueden programar directamente en el lenguaje ensamblador del microcontrolador o microprocesador incorporado sobre el mismo, o también, utilizando los compiladores específicos, pueden utilizarse lenguajes como C o C++. En algunos casos, cuando el tiempo de respuesta de la aplicación no es un factor crítico, también pueden usarse lenguajes interpretados como JAVA.

Puesto que los sistemas embebidos se pueden fabricar por decenas de millares o por millones de unidades, una de las principales preocupaciones es reducir los costos. Los sistemas embebidos suelen usar un procesador relativamente pequeño y una memoria pequeña. Los primeros equipos embebidos que se desarrollaron fueron elaborados por IBM en los años 80.

Los programas de sistemas embebidos se enfrentan normalmente a tareas de procesamiento en tiempo real.

3.1. Componentes de un sistema embebido

En la parte central se encuentra el microprocesador, microcontrolador, DSP u otro. Es decir, la CPU o unidad que aporta capacidad de cómputo al sistema, pudiendo incluir memoria interna o externa, un micro con arquitectura específica según requisitos.

La comunicación adquiere gran importancia en los sistemas embebidos. Lo normal es que el sistema pueda comunicarse mediante interfaces estándar de cable o inalámbricas. Así un SI normalmente incorporará puertos de comunicaciones del tipo RS-232, RS-485, SPI, I^2C, CAN, USB, IP, wifi, GSM, GPRS, DSRC, entre otros. El subsistema de presentación suele ser una pantalla gráfica, táctil, LCD, alfanumérico, entre otros.

Se denominan actuadores a los posibles elementos electrónicos que el sistema se encarga de controlar. Puede ser un motor eléctrico, un conmutador tipo relé u otro. El más habitual puede ser una salida de señal PWM para control de la velocidad en motores de corriente continua.

El módulo de E/S analógicas y digitales suele emplearse para digitalizar señales analógicas procedentes de sensores, activar diodos led, reconocer el estado abierto cerrado de un conmutador o pulsador, entre otros.

El módulo de reloj es el encargado de generar las diferentes señales de reloj a partir de un único oscilador principal. El tipo de oscilador es importante por varios aspectos: por la frecuencia necesaria, por la estabilidad necesaria y por el consumo de corriente requerido. El oscilador con mejores características en cuanto a estabilidad y costo es el basado en un resonador de cristal de cuarzo, mientras que los que requieren menor consumo son los RC. Mediante sistemas PLL se obtienen otras frecuencias con la misma estabilidad que el oscilador patrón.

El módulo de energía se encarga de generar las diferentes tensiones y corrientes necesarias para alimentar los diferentes circuitos del SE. Usualmente se trabaja con un rango de posibles tensiones de entrada, que mediante conversores AC/DC o DC/DC, se obtienen las diferentes tensiones necesarias para alimentar los diversos componentes activos del circuito.

Además de los conversores AC/DC y DC/DC, tienen otros módulos típicos, filtros, circuitos integrados supervisores de alimentación, y demás.

El consumo de energía puede ser determinante en el desarrollo de algunos sistemas embebidos que necesariamente se alimentan con baterías, con lo que el tiempo de uso del SE suele ser la duración de la carga de las baterías.

3.1.1. Microprocesadores y sistemas embebidos

Un microprocesador es una implementación en forma de circuito integrado (IC) de la unidad central de proceso (CPU) de una computadora. Frecuentemente se refiere a un microprocesador como simplemente CPU, y la parte de un sistema que contiene al microprocesador se denomina subsistema de CPU. Los microprocesadores varían en consumo de potencia, complejidad y costo. Los hay de unos pocos miles de transistores y con costo inferior a 2 euros (en producción masiva) hasta de más de cinco millones de transistores que cuestan más de 600 euros.

Los subsistemas de entrada/salida y memoria pueden ser combinados con un subsistema de CPU para formar una computadora o sistema embebido completo. Estos subsistemas se interconectan mediante los buses de sistema (formados a su vez por el bus de control, el bus de direcciones y el bus de datos).

El subsistema de entrada acepta datos del exterior para ser procesados, mientras que el subsistema de salida transfiere los resultados hacia el exterior. Lo más habitual es que hayan varios subsistemas de entrada y varios de salida. A estos subsistemas se les reconoce habitualmente como periféricos de E/S.

El subsistema de memoria almacena las instrucciones que controlan el funcionamiento del sistema. Estas instrucciones comprenden el programa que ejecuta el sistema. La memoria también almacena varios tipos de datos: datos de entrada que aún no han sido procesados, resultados intermedios del procesado y resultados finales en espera de salida al exterior.

Es importante darse cuenta de que los subsistemas estructuran a un sistema según funcionalidades. La subdivisión física de un sistema, en términos de circuitos integrados o placas de circuito impreso (PCB) puede y es normalmente diferente. Un solo circuito integrado (IC) puede proporcionar múltiples funciones, como memoria y entrada/salida.

Un microcontrolador (MCU) es un IC que incluye una CPU, memoria y circuitos de E/S. Entre los subsistemas de E/S que incluyen los microcontroladores se encuentran los temporizadores, los convertidores analógicos a digital (ADC) y digital a analógico (DAC), y los canales de comunicaciones serie. Estos subsistemas de E/S se suelen optimizar para aplicaciones específicas (por ejemplo, audio, vídeo, procesos industriales, comunicaciones, entre otros).

Se debe señalar que las líneas reales de distinción entre microprocesador, microcontrolador y microcomputador en un solo chip están difusas, y se denominan en ocasiones de manera indistinta unos y otros.

En general, un SE (sistema electrónico) consiste en un sistema con microprocesador cuyo hardware y software están específicamente diseñados y optimizados para resolver un problema concreto eficientemente. Normalmente un SE interactúa continuamente con el entorno para vigilar o controlar algún proceso mediante una serie de sensores. Su hardware se diseña normalmente a nivel de chips, o de interconexión de PCB, buscando la mínima circuitería y el menor tamaño para una aplicación particular.

Otra alternativa consta del diseño a nivel de PCB consistente en el ensamblado de placas con microprocesadores comerciales que responden normalmente a un estándar como el PC-104 (placas de tamaño concreto que se

interconectan entre sí “apilándolas” unas sobre otras, cada una de ellas con una funcionalidad específica dentro del objetivo global que tenga el SE).

Esta última solución acelera el tiempo de diseño, pero no optimiza ni el tamaño del sistema, ni el número de componentes utilizados, ni el costo unitario. En general, un sistema embebido simple contará con un microprocesador, memoria, unos pocos periféricos de E/S y un programa dedicado a una aplicación concreta almacenado permanentemente en la memoria.

El término embebido o empotrado hace referencia al hecho de que el microcomputador está encerrado o instalado dentro de un sistema mayor y su existencia como microcomputador puede no ser aparente. Un usuario no técnico de un sistema embebido puede no ser consciente de que está usando un sistema computador. En algunos hogares, las personas que no tienen por qué ser usuarias de una computadora personal estándar (PC), utilizan del orden de diez o más sistemas embebidos cada día.

Las microcomputadoras en estos sistemas controlan electrodomésticos como televisores, videos, lavadoras, alarmas, teléfonos inalámbricos, entre otros. Incluso una PC tiene sistemas embebidos en el monitor, impresora, y periféricos en general, adicionales a la CPU de la propia PC. Un automóvil puede tener hasta un centenar de microprocesadores y microcontroladores que controlan cosas como la ignición, transmisión, dirección asistida, frenos antibloqueo (ABS), control de la tracción, entre otros.

Los sistemas embebidos se caracterizan normalmente por la necesidad de dispositivos de E/S especiales. Cuando se opta por diseñar el sistema embebido partiendo de una placa con microcomputador, también es necesario

comprar o diseñar placas de E/S adicionales para cumplir con los requisitos de la aplicación concreta.

Muchos sistemas embebidos son sistemas de tiempo real. Un sistema de tiempo real debe responder, dentro de un intervalo restringido, a eventos externos mediante la ejecución de la tarea asociada con cada evento. Los sistemas de tiempo real se pueden caracterizar como blandos o duros.

Si un sistema de tiempo real blando no cumple con sus restricciones de tiempo, simplemente se degrada el rendimiento del sistema, pero si el sistema es de tiempo real duro y no cumple con sus restricciones de tiempo, el sistema fallará. Este fallo puede tener posiblemente consecuencias catastróficas.

Un sistema embebido complejo puede utilizar un sistema operativo como apoyo para la ejecución de sus programas, sobre todo cuando se requiere la ejecución simultánea de los mismos. Cuando se utiliza un sistema operativo, lo más probable es que se tenga que tratar de un sistema operativo de tiempo real (RTOS), que es un sistema operativo diseñado y optimizado para manejar fuertes restricciones de tiempo asociadas con eventos en aplicaciones de tiempo real. En una aplicación de tiempo real compleja, la utilización de un sistema operativo de tiempo real multitarea puede simplificar el desarrollo del software.

Una PC embebida posee una arquitectura semejante a la de un PC. Brevemente, estos son los elementos básicos:

3.1.1.1. Microprocesador

Es el encargado de realizar las operaciones de cálculo principales del sistema. Ejecuta el código para realizar una determinada tarea y dirige el funcionamiento de los demás elementos que le rodean, a modo de director de una orquesta.

3.1.1.2. Memoria

En esta se encuentra almacenado el código de los programas que el sistema puede ejecutar, así como los datos. Su característica principal es que debe tener un acceso de lectura y escritura lo más rápido posible para que el microprocesador no pierda tiempo en tareas que no son meramente de cálculo. Al ser volátil, el sistema requiere de un soporte donde se almacenen los datos, incluso sin disponer de alimentación o energía.

3.1.1.3. Caché

Memoria más rápida que la principal en la que se almacenan los datos y el código accedido últimamente. Dado que el sistema realiza microtareas, muchas veces repetitivas, la caché ahorra tiempo, ya que no hará falta ir a memoria principal si el dato o la instrucción ya se encuentra en la caché. Dado su alto precio, tiene un tamaño muy inferior (8–512 KB) con respecto a la principal (8–256 MB). En el interior del chip del microprocesador se encuentra una pequeña caché (L1), pero normalmente se tiene una mayor en otro chip de la placa madre (L2).

3.1.1.4. Disco duro

En él la información no es volátil y puede conseguir capacidades muy elevadas. A diferencia de la memoria que es de estado sólido, este suele ser magnético. Pero su excesivo tamaño a veces lo hace inviable para PC embebidas, con lo que se requieren soluciones como unidades de estado sólido. Otro problema que presentan los dispositivos magnéticos, a la hora de integrarlos en sistemas embebidos, es que llevan partes mecánicas móviles, lo que los hace inviables para entornos donde estos estarán expuestos a ciertas condiciones de vibración. Existen en el mercado varias soluciones de esta clase (DiskOnChip, CompactFlash, IDE Flash Drive, entre otros) con capacidades suficientes para la mayoría de sistemas embebidos (desde 2 MB hasta más de 1 GB). El controlador del disco duro de PC estándar cumple con el estándar IDE y es un chip más de la placa madre.

3.1.1.5. Disco flexible

Su función es la de almacenamiento, pero con discos con capacidades mucho más pequeñas y la ventaja de su portabilidad. Normalmente se encontraban en computadora personal estándar, pero no así en una PC embebida. Llevan varios años en total desuso en PC comunes.

3.1.1.6. BIOS-ROM

BIOS (*basic input & output system*, sistema básico de entrada y salida) es el código que es necesario para inicializar la computadora y para poner en comunicación los distintos elementos de la placa madre. La ROM (*read only memory*, memoria de solo lectura no volátil) es un chip donde se encuentra el código BIOS.

3.1.1.7. CMOS-RAM

Es un chip de memoria de lectura y escritura alimentado con una pila donde se almacena el tipo y ubicación de los dispositivos conectados a la placa madre (disco duro, puertos de entrada y salida, entre otros). Además, contiene un reloj en permanente funcionamiento que ofrece al sistema la fecha y la hora.

3.1.1.8. Chipset

Chip que se encarga de controlar las interrupciones dirigidas al microprocesador, el acceso directo a memoria (DMA) y al bus ISA, además de ofrecer temporizadores. Es frecuente encontrar la CMOS-RAM y el reloj de tiempo real en el interior del Chipset.

3.1.1.9. Entradas al sistema

Pueden existir puertos para *mouse*, teclado, vídeo en formato digital, comunicaciones serie o paralelo, entre otros.

3.1.1.10. Salidas del sistema

Puertos de vídeo para monitor o televisión, pantallas de cristal líquido, altavoces, comunicaciones serie o paralelo, entre otros.

3.1.1.11. Ranuras de expansión para tarjetas de tareas específicas

Pueden no venir incorporadas en la placa madre, como pueden ser más puertos de comunicaciones, acceso a red de computadoras vía LAN (*local area*

network, red de área local) o vía red telefónica: básica, RDSI (red digital de servicios integrados), ADSL (*asynchronous digital subscriber loop*, lazo digital asíncrono del abonado), cable módem, entre otros. Un PC estándar suele tener muchas más ranuras de expansión que una PC embebida. Las ranuras de expansión están asociadas a distintos tipos de bus: VESA, ISA, PCI, NLX (ISA + PCI), entre otros.

Existen fabricantes que integran un microprocesador y los elementos controladores de los dispositivos fundamentales de entrada y salida en un mismo chip, pensando en las necesidades de los sistemas embebidos (bajo coste, pequeño tamaño, entradas y salidas específicas). Su capacidad de proceso suele ser inferior a los procesadores de propósito general, pero cumplen con su cometido, ya que los sistemas donde se ubican no requieren tanta potencia. Los principales fabricantes son STMicroelectronics (familia de chips STPC), AMD (familia Geode), Motorola (familia ColdFire) e Intel.

En cuanto a los sistemas operativos necesarios para que un sistema basado en microprocesador pueda funcionar y ejecutar programas suelen ser específicos para los sistemas embebidos. Así, se encuentran sistemas operativos de bajos requisitos de memoria, posibilidad de ejecución de aplicaciones de tiempo real, modulares (inclusión solo de los elementos necesarios del sistema operativo para el sistema embebido concreto), y más.

3.2. Ventajas de un sistema embebido sobre las soluciones industriales tradicionales

Los equipos industriales de medida y control tradicionales están basados en un microprocesador con un sistema operativo privativo o específico para la aplicación correspondiente.

Dicha aplicación se programa en ensamblador para el microprocesador dado o en lenguaje C, realizando llamadas a las funciones básicas de ese sistema operativo que en ciertos casos ni siquiera llega a existir.

Con los modernos sistemas PC embebida basados en microprocesadores i486 o i586, se llega a integrar el mundo del PC compatible con las aplicaciones industriales. Ello implica numerosas ventajas:

- Posibilidad de utilización de sistemas operativos potentes que ya realizan numerosas tareas: comunicaciones por redes de datos, soporte gráfico, concurrencia con lanzamiento de *threads*, entre otros. Estos sistemas operativos pueden ser los mismos que para PC compatibles (Linux, Windows, MS-DOS) con fuertes exigencias en hardware o bien ser una versión reducida de los mismos con características orientadas a los PC embebidos.

- Al utilizar dichos sistemas operativos se pueden encontrar fácilmente herramientas de desarrollo software potentes, así como numerosos programadores que las dominan, dada la extensión mundial de las aplicaciones para PC compatibles.

- Reducción en el precio de los componentes hardware y software debido a la gran cantidad de PC en el mundo.

3.3. Raspberry Pi

Es un computador de placa reducida o (placa única) (SBC) de bajo costo desarrollado en Reino Unido por la Fundación Raspberry Pi, con el objetivo de estimular la enseñanza de ciencias de la computación en las escuelas.

El diseño incluye un System-on-a-chip Broadcom BCM2835, que contiene un procesador central (CPU) ARM1176JZF-S a 700 MHz (el firmware incluye unos modos Turbo para que el usuario pueda hacerle *overclock* de hasta 1 GHz sin perder la garantía) un procesador gráfico (GPU) VideoCore IV, y 512 MB de memoria RAM (aunque originalmente al ser lanzado eran 256 MB).

El diseño no incluye un disco duro ni unidad de estado sólido, ya que usa una tarjeta SD para el almacenamiento permanente; tampoco incluye fuente de alimentación ni carcasa.

A pesar que el Modelo A no tiene un puerto RJ45, se puede conectar a una red usando un adaptador USB-Ethernet suministrado por el usuario. Por otro lado, a ambos modelos se les puede conectar un adaptador wifi por USB, para tener acceso a redes inalámbricas o internet. El sistema cuenta con 256 MB de memoria RAM en su modelo A y con 512 MB de memoria RAM en su modelo B. Como es típico en los ordenadores jóvenes, se pueden usar teclados y ratones con conexión USB compatible con Raspberry Pi.

El Raspberry Pi no viene con reloj en tiempo real, por lo que el sistema operativo debe usar un servidor de hora en red, o pedir al usuario la hora en el momento de arrancar el ordenador de la pared. Sin embargo, se podría añadir un reloj en tiempo real (como el DS1307) con una batería, mediante el uso de la interfaz I²C.

Los esquemas del modelo A y el modelo B fueron lanzados el 20 de abril de 2012 por la fundación.

La aceleración por hardware para la codificación de vídeo (H.264) se hizo disponible el 24 de agosto de 2012, cuando se informó que la licencia permitiría

su uso gratuitamente; antes se pensó en anunciarlo cuando se lanzara el módulo de cámara. También se puso a la venta la capacidad para poder usar el codificación-decodificación de MPEG-2 y Microsoft VC-1.

3.3.1. Comparativa de modelos

La tabla comparativa de modelos se presenta a continuación.

Tabla III. **Tabla comparativa modelos Raspberry Pi**

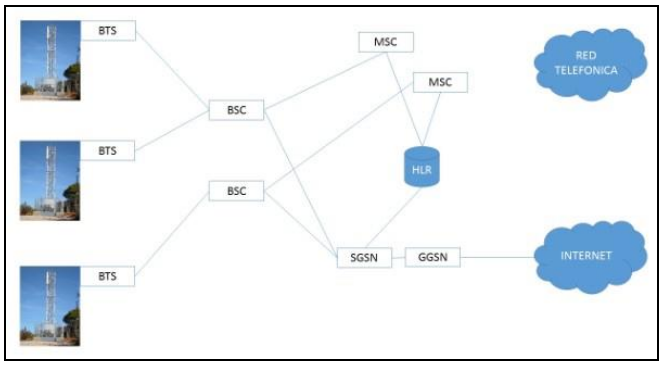
Hardware	**Raspberry Pi 1 Modelo A**	**Raspberry Pi 1 Modelo B**	**Raspberry Pi 1 Modelo B+**	**Raspberry Pi 2 Modelo B**
SoC	Broadcom BCM2835 (CPU + GPU + DSP + SDRAM + puerto USB)			Broadcom BCM2836 (CPU + GPU + DSP + SDRAM + puerto USB)
CPU	ARM 1176JZF-S a 700 MHz (familia ARM11)			900 MHz quad-core ARM Cortex A7
Instrucciones	RISC de 32 bits			
GPU	Broadcom VideoCore IV, OpenGL ES 2.0, MPEG-2 y VC-1 (con licencia), 1080p30 H.264/MPEG-4 AVC			
Memoria (SDRAM)	256 MiB (compartidos con la GPU)	512 MiB (compartidos con la GPU)		1 GB (compartidos con la GPU)
Puertos USB 2.0	1	2 (vía hub USB integrado)		4
Entradas de vídeo	Conector MIPI CSI que permite instalar un módulo de cámara desarrollado por la RPF			
Salidas de vídeo	Conector RCA (PAL y NTSC), HDMI (rev1.3 y 1.4), Interfaz DSI para panel LCD			
Salidas de audio	Conector de 3.5 mm, HDMI			
Almacenamiento integrado	SD / MMC / ranura para SDIO			MicroSD
Conectividad de red	Ninguna	10/100 Ethernet (RJ-45) via hub USB		
Periféricos de bajo nivel	8 x GPIO, SPI, I²C, UART			17 x GPIO y un bus HAT ID
Reloj en tiempo real	Ninguno			
Consumo energético	500 mA, (2.5 W)	700 mA, (3.5 W)	600 mA, (3.0 W)	800 mA, (4.0 W)
Alimentación	5 V vía Micro USB o GPIO header			
Dimensiones	85.60mm × 53.98mm (3.370 × 2.125 inch)			
Sistemas operativos	GNU/Linux: Debian (Raspbian), Fedora (Pidora), Arch Linux (Arch Linux ARM), Slackware Linux. RISC OS			

Fuente: elaboración propia.

4. RED CELULAR 3G

La telefonía móvil 3G es un servicio de comunicaciones inalámbricas que permite estar conectado de forma permanente a internet a través del teléfono móvil, el ordenador de bolsillo y el ordenador portátil. La tecnología 3G propone una mejor calidad y fiabilidad, una mayor velocidad de transmisión de datos y un ancho de banda superior. Con velocidades de datos de hasta 384 Kbps, es casi siete veces más rápida que una conexión telefónica estándar.

Figura 17. **Topología de red básica GPRS (2G)**



Fuente: *Topología de red básica GPRS*.
http://www.temastecnologicos.com/elementosmovil.html. Consulta: 8 de marzo de 2015.

La International Telecommunication Union (ITU) definió las demandas de redes 3G con el estándar IMT2000. Este estándar se desarrolló mediante un sistema móvil llamado UMTS (Universal Mobile Telephone System), este a su vez está desarrollado a partir de WCDMA, que es una tecnología móvil inalámbrica que aumenta las tasas de transmisión de datos de los sistemas GSM utilizando la interfaz aérea CDMA en lugar de TDMA (Time Division

Multiple Access), es por ello que 3G ofrece velocidades mucho más altas de datos en aparatos inalámbricos portátiles.

También UMTS se define como un sistema por capas. La capa de más arriba es la capa de servicios y, como su nombre lo señala, se encarga de los servicios, de su despliegue en forma rápida. En el centro se encuentra la capa de control que se preocupa de ayudar a la mejora de los procedimientos y permite que la capacidad de la red sea dinámica. En la zona más baja se encuentra la capa de conectividad, la que tiene como labor la transmisión de datos y el tráfico de voz. El primer país en implementar una red comercial 3G a gran escala fue Japón. En la actualidad, existen 164 redes comerciales en 73 países usando la tecnología WCDMA.

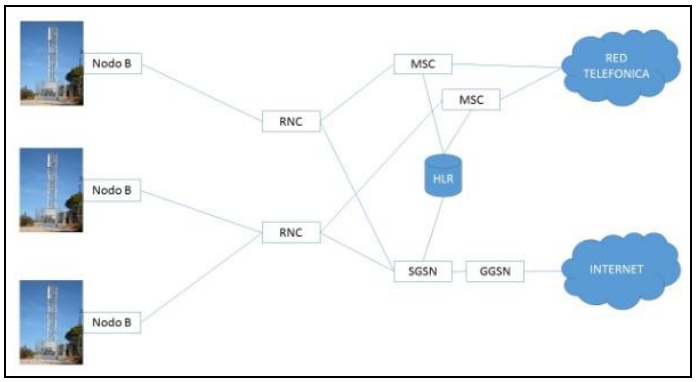
4.1. Evolución del 3G

3G evoluciona, de la segunda generación de sistema inalámbrico móvil (2G). Las redes 2G se construyeron principalmente para datos de voz y transmisiones lentas, debido a las altas expectativas de los usuarios se fueron produciendo cambios rápidos.

En Norteamérica, la evolución es a partir desde el TDMA, el cual cambiará a EDGE (Enhanced Data Rates for GSM Evolution) y después a UMTS. Según como expuso Erasmo Rojas (director para Latinoamérica y el Caribe de 3G Américas, organización que promueve el despliegue fluido de GSM y su evolución a 3G) al diario La Nación en el año 2007 cuando este tema recién comenzaba en Chile: “Esta red móvil que en algún momento se pensó que era sólo para hablar, hoy puede ayudar a disminuir la brecha de información. La ventaja de la red móvil es que las personas muchas veces necesitan procesar la información cuando están en movimiento”.

En Japón, se utilizan dos estándares 3G: W-CDMA usado por NTT DoCoMo (FOMA, compatible con UMTS) y SoftBank Mobile (UMTS), y CDMA2000, usado por KDDI. La transición por razones de mercado al 3G se completó en Japón durante 2006. La primera introducción de la tecnología 3G en el Caribe (2008) se hizo por América Móvil, que era anteriormente MIPHONE en Jamaica. La fase de implementación de esta red fue llevada a cabo por Huawei en conjunto con otras subcontratadas como TSF de Canadá.

Figura 18. **Topología de red básica UMTS (3G)**



Fuente: *Topología de red básica UMTS*.
http://www.temastecnologicos.com/elementosmovil.html. Consulta: 14 de marzo de 2015.

4.2. Seguridad

Las redes 3G ofrecen mayor grado de seguridad en comparación con sus predecesoras 2G. Al permitir a la UE autenticar la red a la que se está conectando, el usuario puede asegurarse de que la red es la intencionada y no una imitación.

En la conferencia BlackHat 2010 un *hacker* demostró que podía obtener números celulares e incluso escuchar las llamadas de teléfonos GSM cercanos, esto era logrado haciéndose pasar por una base (antena receptora/transmisora) de la telefónica AT&T en este caso.

Las redes 3G usan el cifrado por bloques KASUMI en vez del anterior cifrado de flujo A5/1. Aun así, se han identificado algunas debilidades en el código KASUMI. Además de la infraestructura de seguridad de las redes 3G, se ofrece seguridad de un extremo al otro cuando se accede a aplicaciones *framework* como IMS, aunque esto no es algo que sólo se haga en el 3G.

4.3. Ventajas y desventajas

Las ventajas y desventajas de la seguridad se presentan a continuación.

4.3.1. Ventajas

- El protocolo IP está basado en paquetes, pues solo se paga en función de la descarga, lo que supone, relativamente, un menor costo. Aunque dependiendo del tipo de usuario, también se podría calificar como desventaja.
- Velocidad de transmisión alta: fruto de la evolución de la tecnología, actualmente se pueden alcanzar velocidades superiores a los 3 Mbit/s por usuario móvil.
- Más velocidad de acceso.
- UMTS, sumado al soporte de protocolo de internet (IP), se combinan para prestar servicios multimedia y nuevas aplicaciones de banda ancha, como servicios de vídeotelefonía y vídeoconferencia.
- Transmisión de voz con calidad equiparable a la de las redes fijas.

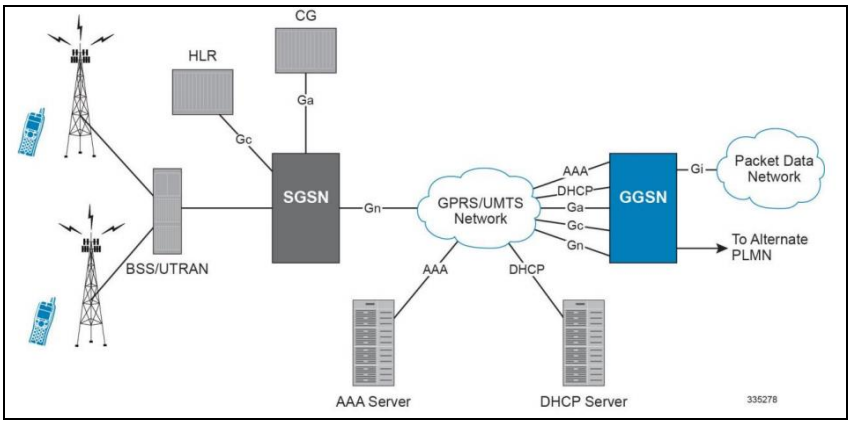
- Mayor velocidad de conexión ante caídas de señal.

Todo esto hace que esta tecnología sea ideal para prestar diversos servicios multimedia móviles.

4.3.2. Desventajas

- Cobertura limitada dependiendo de la localización, la velocidad de transferencia puede disminuir drásticamente (o incluso carecer totalmente de cobertura).
- Disminución de la velocidad si el dispositivo desde el que se conecta está en movimiento (por ejemplo, si se circula en automóvil).
- No orientado a conexión. Cada uno de los paquetes pueden seguir rutas distintas entre el origen y el destino, por lo que pueden llegar desordenados o duplicados. Sin embargo, el hecho de no ser orientado a conexión tiene la ventaja de que no se satura la red.
- Además, para elegir la ruta existen algoritmos que escogen qué ruta es mejor, estos algoritmos se basan en la calidad del canal, en la velocidad del mismo y, en algunos, oportunidad hasta en 4 factores (todos ellos configurables) para que un paquete escoja una ruta.
- Elevada latencia respecto a la que se obtiene normalmente con servicios ADSL. La latencia puede ser determinante para el correcto funcionamiento de algunas aplicaciones del tipo cliente-servidor como los juegos en línea.
- Elevada tasa de absorción específica (SAR)

Figura 19. **Topología de red básica GPRS/UMTS**



Fuente: *Topología de red básica GPRS/UMTS*. http://www.cisco.com/c/dam/en/us/td/docs/wireless/asr_5000/17-0/PDF/17-SGSN-Admin.pdf. Consulta: 15 de marzo de 2015.

4.4. Elementos de una red de datos

Los elementos de una red de datos se presentan a continuación.

4.4.1. BSC

Controla un determinado número de BTS de un área. Todas las BTS de dicha área se conectan a la BSC y, a través de ella, pasa todo el flujo de comunicaciones.

El elemento BSC controla el correcto funcionamiento de las BTS conectadas, maneja la configuración de cada una de ellas e incluso participa activamente cuando un usuario móvil pasa de una BTS a otra (*hand-over*). Con las generaciones 2,5 y 2,75 el elemento BSC diferencia el tráfico de voz y de datos, ya que a partir de ella siguen caminos separados.

4.4.2. RNC

Realiza una función similar al elemento BSC en la tercera generación. Las tecnologías 2G y 3G son muy diferentes y las funciones a realizar también son muy diferentes.

Actualmente se está implantando el concepto de Single RAN que intenta unificar las generaciones 2G y 3G en un único controlador que hace las funciones de BSC y RNC. Al igual que la BSC, la RNC discrimina entre conexiones de voz y de datos que, a partir de ella, siguen caminos separados.

4.4.3. HLR

Es el elemento de la red que almacena los datos de los usuarios. Para dar de alta un usuario en una red móvil se deben introducir los datos en el HLR correspondiente. En una red móvil suele haber un HLR por cada millón de abonados.

Por lo tanto, los elementos de la red móvil que consultan la información del usuario deben saber, según el usuario, cual es el HLR que contiene su información. La información almacenada es toda la información estática relativa al usuario como los desvíos o los servicios activados.

4.4.4. SGSN

Es un nodo de servicio GPRS, el cual tiene como función principal el dar acceso a los terminales móviles (teléfonos celulares) hacia la red de datos que puede ser internet o una red corporativa.

El SGSN es el primer punto principal en el que se autentifica un terminal al momento de realizar una conexión de datos.

Se encarga también del manejo de la movilidad de los celulares, llevando un registro de localización de los terminales, así como el enrutamiento y transferencia de los paquetes de datos. Se encarga del establecimiento de los túneles entre la RAN (BSC/RNC) y el GGSN.

Una tarea importante del SGSN es el de llevar la parte de facturación de los terminales que se encuentran en modo *roaming* por medio de registros llamados CDR.

El SGSN tiene varios servicios configurados como sgsn-service para 3G, gprs-service para 2G, estos dos son la parte de conexión hacia las RNC/BSC; Map Service que es la parte de acceso hacia el HLR; SMSC; sgtp service que es la conexión hacia el GGSN o también conocido como Gn que también es la puerta de enlace hacia otras redes celulares llamada Gp y el gtpp service que es para la parte de facturación.

Envía a los terminales vía el HLR el QoS (calidad de servicio), así como el perfil que dicho usuario va a utilizar.

4.4.5. GGSN

Es la puerta de enlace o punto central de conexión hacia el exterior o la PDN (Packet Data Network) de una red celular (red móvil), estas redes externas pueden ser internet o una red corporativa.

Son el punto de acceso para múltiples puntos de accesos llamados APN. (Access Point Network).

Dependiendo de la configuración, el GGSN puede manejar una parte de autentificación o autorización de navegación llamada Radius/Diameter, esto se puede realizar por APN.

En la parte de configuración de las APN, se puede configurar de tal forma que se pueden especificar el tipo de esquema de facturación que puede ser prepago o pospago.

En parte, se encarga del QoS, aunque el SGSN es el principal encargado, además de aplicar políticas y reglas de navegación con base en los datos transmitidos/recibidos por los celulares. Asignación de IP para uso del terminal dependiendo del APN solicitada.

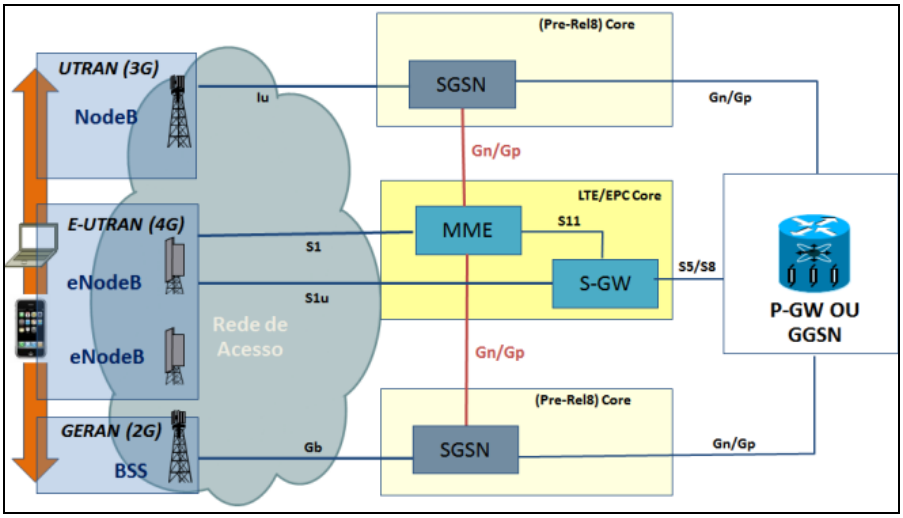
4.4.6. APN

APN, o Access Point Name, es el nombre de punto de acceso para GPRS o estándares posteriores (como 3G y 4G) que debe configurarse en el dispositivo móvil (bien sea un teléfono móvil u otro, como puede ser un módem USB), para que pueda acceder a redes computacionales (entre las que se puede incluir internet). Un punto de acceso es:

- Una dirección IP a la cual un móvil se puede conectar
- Un punto de configuración que es usado para esa conexión
- Una opción particular que se configura en un teléfono móvil

Una vez que el dispositivo se ha conectado, usa el servidor DNS para hacer el proceso llamado resolución de APN, que finalmente da la IP real del APN.

Figura 20. **Diagrama Packet Core, tecnologías GPRS/UMTS/LTE**



Fuente: *Diagrama Packet Core, Tecnologías GPRS/UMTS/LTE*. https://supportforums.cisco.com/discussion/11895496. Consulta: 17 de marzo de 2015.

4.4.7. Comparativa tecnológica red de datos

- GSM - CSD (2G): hasta 9,6 kbps en subida y bajada - prácticamente en desuso si se está realizando una llamada mientras se usa.
- GSM - GPRS (2'5G): hasta 80 kbps en bajada y 20 kbps en subida.
- GSM - EDGE (2'75G): hasta 236 kbps en bajada y 59 kbps en subida.
- 3G - UMTS (3G) - de 64 a 384 kbps de subida y bajada.
- 3G - HSPA (HSDPA+HSUPA) (3.5G) - hasta 7,2 mbps de subida y bajada.
- 3G - HSPA+ (3.75G) - hasta 22 Mbps de subida y bajada.

- 4G - LTE - la velocidad máxima en 4G es de 75 Mbps en bajada y 25 Mbps en subida. La velocidad media de descarga se estima entre 20 y 40 Mbps y la de subida entre 6 y 12 Mbps.

5. DISEÑO DE INTERFAZ

En esta sección se contempla el diseño del hardware necesario para la interacción de los elementos de interrogación a los que se tendrá acceso por medio de la Raspberry Pi como unidad de control.

Adicional al hardware necesario para la interrogación se contempla el diseño de la configuración de las distintas aplicaciones, así como los pasos necesarios para la instalación del sistema operativo que utilizará la Raspberry Pi para interactuar con los elementos e interfaces.

Las configuraciones de la Raspberry Pi contemplan estructurarla como un dispositivo de red capa 3 encargado del manejo de paquetes para establecer comunicación por medio del protocolo de transporte TCP/IP, utilizando una dirección IP pública o privada, dependiendo de las necesidades del cliente.

Adicional a esta configuración, se contempla la habilitación de comunicación serial, la cual se establecerá con el medidor eléctrico utilizando el protocolo rs232.

5.1. Diseño de hardware

Los factores del diseño de hardware que se utilizan son los siguientes.

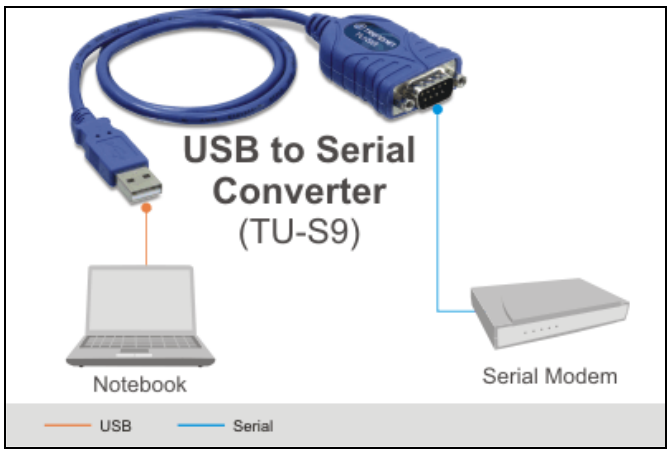
5.1.1. Interfaz serial a USB

Este convertidor de serial a USB permite conectar un dispositivo serial RS-232 de un módem a puerto USB en PC de escritorio o portátil.

- Compatible con las especificaciones USB 1,1.
- Admite interfaz serial RS-232.
- Admite hasta una transferencia de datos de 500 kbps.
- Se instala como un puerto COM, señales de control de módem *full* RS-232, señales de datos RS-232.

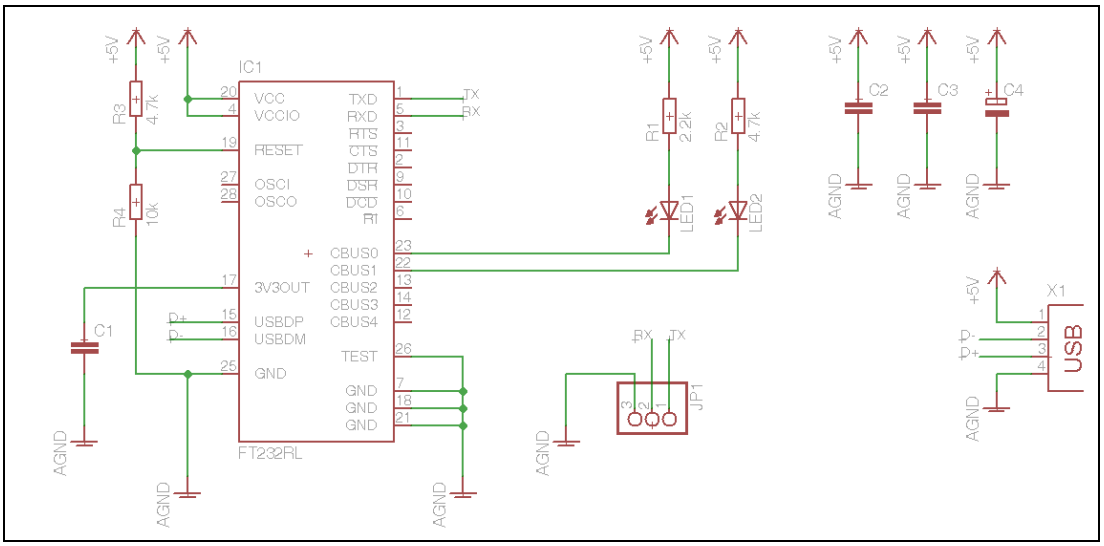
Este conversor es necesario para la comunicación serial desde la Raspberry Pi, debido a que dicha interfaz no posee una entrada serial con un puerto db9.

Figura 21. **Conversor de comunicación serial a USB**



Fuente: *Conversor de comunicación*.
http://www.trendnet.com/products/proddetail?prod=150_TU-S9&cat=32.
Consulta: 20 de marzo de 2015.

Figura 22. **Estructura interna de un conversor de serial a USB**



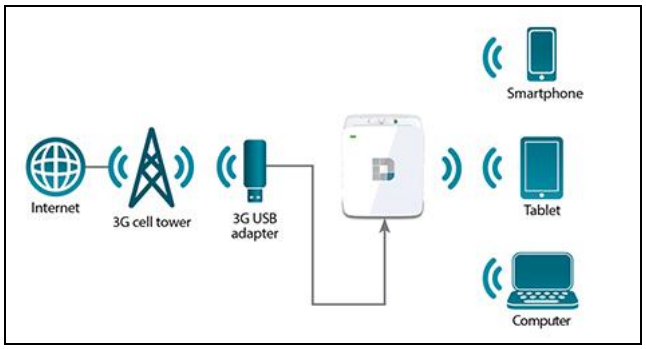
Fuente: elaboración propia, empleando EAGLE 5.4.

5.1.2. Módem 3G

Con un aspecto similar a una memoria USB, el módem USB 3G es un pequeño *gadget* que permite a un usuario acceder a internet a través de su PC portátil cuando no dispone de ninguna conexión a internet o cuando no se encuentra dentro de una zona wifi.

El módem USB 3G, una especie de módem inalámbrico de tipo wifi, utiliza la red de los operadores de telefonía para conectarse a internet. Al igual que los teléfonos móviles, el módem USB 3G posee un lugar reservado para una tarjeta SIM. Para que funcione, es necesario que previamente se haya suscrito a un plan en un operador de telefonía.

Figura 23. **Comunicación módem 3G**

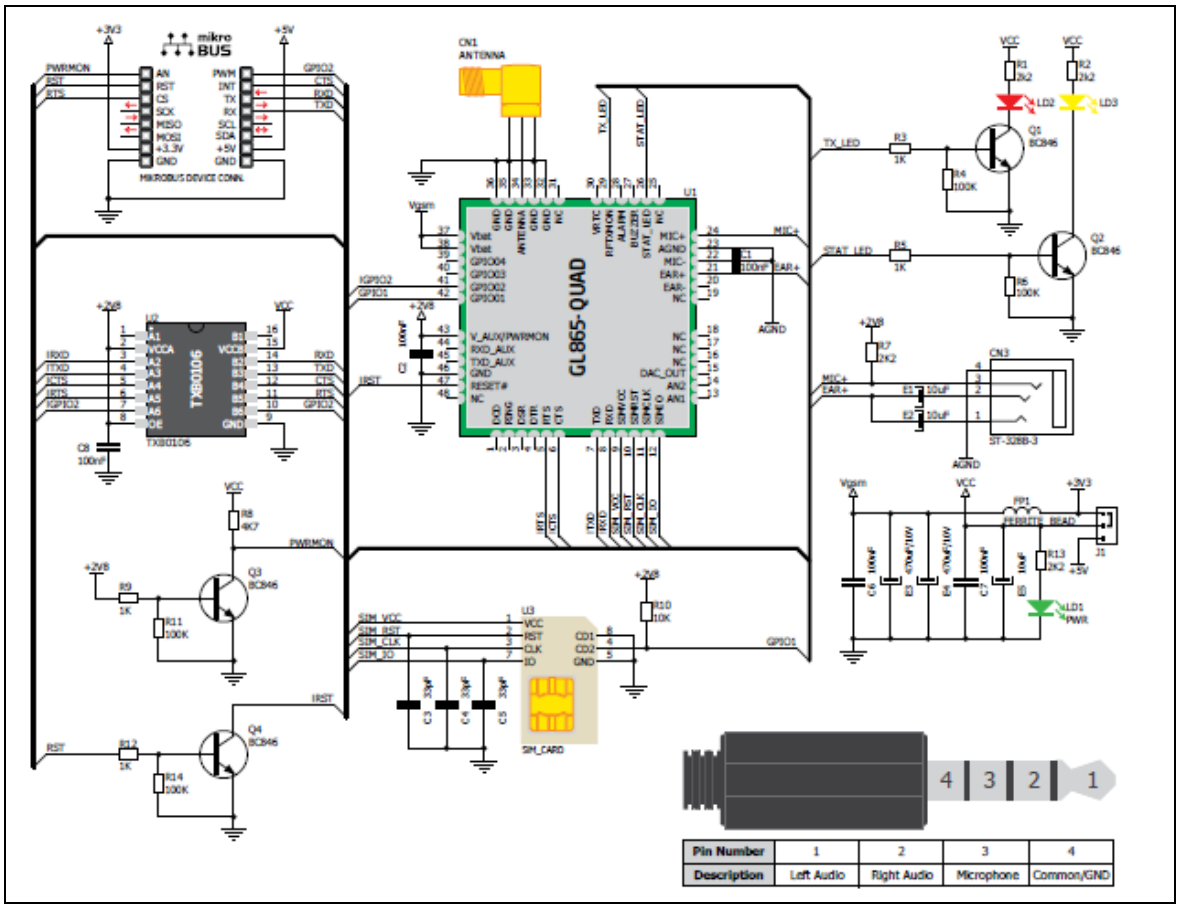


Fuente: *Comunicación módem 3G*. http://www.gsmred.com/gsm-gateway.htm. Consulta: 12 de marzo de 2015.

Figura 24. **Interfaz módem 3G**

Fuente: *Interfaz módem 3G*. http://www.open-electronics.org/gsmgprs-gps-modem-with-sim900sim908-module/. Consulta: 14 de marzo de 2015.

Figura 25. **Diagrama interno módem 3G**



Fuente: *Diagrama interno módem 3G*. http://www.mikroe.com/click/gsm/.
Consulta: 14 de marzo de 2015.

5.2. Instalación del sistema operativo

Lo primero que se debe hacer es descargar una imagen ISO de la distribución, se sugiere utilizar la distribución Raspbian, la cual es gratuita y es una versión de Debian.

Una vez se tenga la ISO descargada en la PC, se debe realizar un proceso con ella que consiste en “copiar” la ISO a la tarjeta de memoria SD, pero formateándola de forma que sea *booteable*.

Si se ubica en Windows, se puede hacer de forma fácil usando el programa Win32DiskImage o similares.

Si se ubica en Linux (como siempre, se prueba en una distribución de Kubuntu), el proceso se debería realizar sin problema con Startup Disk Creator o similares.

Una vez que el proceso anterior ha terminado, simplemente se introduce la tarjeta en el Raspberry PI y se inicia (basta con enchufarla a la corriente eléctrica).

Si está conectado a una pantalla y tiene teclado y ratón, se podrá hacer todo desde el mismo Raspberry, pero si no se tienen estos elementos, se conectará vía SSH (suponiendo que está conectado con el cable de red al *router*) desde el equipo principal. Ahora lo que se debe hacer es ejecutar el comando raspi-config con permisos de *sudo*, es decir:

sudo raspi-config

Este comando desplegará un menú en consola con distintas opciones, es prácticamente obligatorio extender la partición *root* (para usar todo el espacio de la SD) y conveniente cambiar la contraseña, configurar el *layout* del teclado a español, la zona horaria, entre otros.

Es mejor no tocar las opciones de *overclock* y *memory split* si no se sabe lo que se está haciendo, ya que se podría dañar la Raspberry PI.

Figura 26. **Configuración inicial Raspberry Pi**

Fuente: *Raspberry Pi*. http://www.frambuesapi.co/2013/08/10/tutorial-3-instalacion-y-configuracion-de-inicial-del-raspberry-pi-raspi-config/. Consulta: 25 de marzo de 2015.

Posterior a la configuración del sistema operativo, es necesario aplicar algunas configuraciones adicionales para permitir la comunicación con otras interfaces.

5.3. Configuración para uso módem 3G

La configuración de un módem 3G / 4G en una Raspberry Pi no es una tarea sencilla. El principal problema es que la mayoría de los módems USB actúan como dos dispositivos, un dispositivo de almacenamiento USB y un módem USB.

Cuando se conecta a la Raspberry Pi, el dispositivo, por lo general, lo reconoce en el modo de almacenamiento USB. Hay un programa llamado USB_ModeSwitch que se puede utilizar para hacer la conmutación.

Para conectar a la red celular el módem USB con la Raspberry Pi se debe utilizar los programas Classic ppp y Wvdial.

5.3.1. Instalación de programas módem 3G

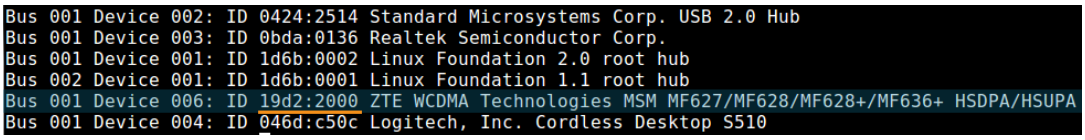
- Conectar la Raspberry Pi a una red LAN para tener acceso a internet
- Abrir la terminal
- *sudo apt-get update*
- *sudo apt-get install ppp usb-modeswitch wvdial*

5.3.2. Obtener los códigos de conmutación USB

- Se tiene que conseguir los códigos del dispositivo USB en el modo de almacenamiento USB y el modo de módem USB.
- Conectar el módem USB y reiniciar el Raspberry PI sin red LAN.
- Una vez reiniciado, abrir una ventana de la terminal y escribir: *lusb*

La salida será similar a la figura 27. El módem debe ser catalogado como uno de los dispositivos USB, se debe tener en cuenta los números subrayados. Estos son los códigos de los proveedores de los dispositivos.

Figura 27. **Código módem 3G USB**

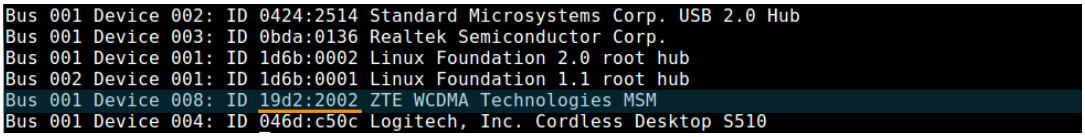


Fuente: *Código módem 3G USB*. http://www.thefanclub.co.za/how-to/how-setup-usb-3g-modem-raspberry-pi-using-usbmodeswitch-and-wvdial. Consulta: 19 de marzo de 2015.

- Tomar nota de estos números, en este caso es 19d2: 2000.
- Este valor será utilizado en el valor por defecto del producto.
- Reiniciar la Raspberry Pi con el módem conectado.
- Abrir una ventana de terminal y escribir: *sudo shutdown -r now*
- Una vez reiniciada la Raspberry Pi, ejecutar el siguiente comando.

La salida será similar a la figura 28. El módem debe aparecer, el segundo conjunto de números habría cambiado. Esto es debido al programa USB_ModeSwitch que cambiar el dispositivo a modo de módem USB.

Figura 28. **Código Target módem 3G**



Fuente: *Código módem 3G USB*. http://www.thefanclub.co.za/how-to/how-setup-usb-3g-modem-raspberry-pi-using-usbmodeswitch-and-wvdial. Consulta: 19 de marzo de 2015.

- Tomar nota de los nuevos números. En este caso, es 19d2: 2.002.
- Este valor se utilizará más adelante.

5.3.3. Configuración del archivo usb_modeswitch

Se tiene que crear un archivo de configuración personalizada para USB_ModeSwitch en el Raspberry Pi, porque cuando se reinicia el dispositivo esta opción no está siempre activa. algo más de información para nuestro archivo de configuración USB_ModeSwitch para que se puede hacer el cambio de forma manual.

- Abrir la terminal y escribir el siguiente comando, reemplazando los códigos 19d2 y 2000 con los códigos del paso 2.

  cd /tmp
  tar -xzvf /usr/share/usb_modeswitch/configPack.tar.gz 19d2\:2000

- Ahora, abrir el archivo extraído con un editor de texto como Leafpad. reemplazar los códigos indicados en el paso 2: *leafpad 19d2: 2000*
- El contenido del archivo debe tener un aspecto similar a la figura 29.
- Las partes importantes se muestran en azul.

Figura 29. **Modificación de archivo módem 3G**

```
# ZTE devices

TargetVendor=   0x19d2
TargetProductList="0001,0002,0015,0016,0017,0031,0037,0052,0055,0063,0064,0066,0091,0108,0117,0128,0157,2002,2003"

MessageContent="5553424312345678000000000000061e000000000000000000000000000000"
MessageContent2="5553424312345679000000000000061b000000020000000000000000000000"
MessageContent3="5553424312345670200000080000c85010101180101010101000000000000"

NeedResponse=1
```

Fuente: *Modificación de archivo módem 3G*. http://www.thefanclub.co.za/how-to/how-setup-usb-3g-modem-raspberry-pi-using-usbmodeswitch-and-wvdial. Consulta: 20 de marzo de 2015.

- Abrir el siguiente archivo /etc/usb_modeswitch.conf y agregar la información obtenida en el paso anterior.
- Ejecutar el siguiente comando en la terminal: *sudo leafpad /etc/usb_modeswitch.conf.*
- Agregar la siguiente información remplazando los códigos con los del dispositivo.

Figura 30. **Modificación de archivo Switch Mode**

```
DefaultVendor=0x19d2
DefaultProduct =0x2000

TargetVendor=0x19d2
TargetProduct =0x2002

MessageContent="5553424312345678000000000000061e000000000000000000000000000000"
MessageContent2="5553424312345679000000000000061b000000020000000000000000000000"
MessageContent3="555342431234567020000000800000c85010101180101010101000000000000"
```

Fuente: *Modificación de archivo Switch Mode*. http://www.thefanclub.co.za/how-to/how-setup-usb-3g-modem-raspberry-pi-using-usbmodeswitch-and-wvdial. Consulta: 22 de marzo de 2015.

5.3.4. Configuración del archivo wvdial

El siguiente paso es crear un archivo de configuración de wvdial para que se pueda conectar al proveedor de servicios.

- Abrir una ventana de la terminal y escribir: *sudo leafpad /etc/wvdial.conf*
- Remplazar el contenido del archivo con la siguiente información

Figura 31. **Modificación de archivo wvdial**

```
[Dialer 3gconnect]
Init1 = ATZ
Init2 = ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0
Init3 = AT+CGDCONT=1,"IP","internet"
Stupid Mode = 1
Modem Type = Analog Modem
ISDN = 0
Phone = *99#
Modem = /dev/gsmmodem
Username = { }
Password = { }
Baud = 460800
```

Fuente: *Modificación de archivo wvdial*. http://www.thefanclub.co.za/how-to/how-setup-usb-3g-modem-raspberry-pi-using-usbmodeswitch-and-wvdial. Consulta: 25 de marzo de 2015.

- Remplazar internet con el APN del proveedor de servicios.
- Cambiar el número de teléfono si se necesita marcar a un código diferente para conectarse.
- Remplazar nombre de usuario y contraseña si es necesario. Para dejar el nombre de usuario y contraseña en blanco {}.

5.3.5. Conectarse al APN de servicio

Para conectarse se tiene que verificar que el dispositivo está en modo de módem.

- Abrir un terminal y escribir: sudo usb_modeswitch -c /etc/usb_modeswitch.conf
- Para conectarse se debe de utilizar el siguiente comando: *wvdial 3gconnect*

5.4. Configuración de interfaz serial TCP

Ser2net permite acceder a los puertos serie a través de TCP, lo que convierte la Raspberry Pi en un servidor de consola. Está en los repositorios, pero no se puede instalarlo usando "apt-get" porque no es la última versión. Se descargará y cumplirá Ser2net:

wget http://downloads.sourceforge.net/project/ser2net/ser2net/ser2net-2.8.tar.gz

- Extraer los archivos: *tar -xzvf ser2net-2.8.tar.gz*
- Instalar el programa:

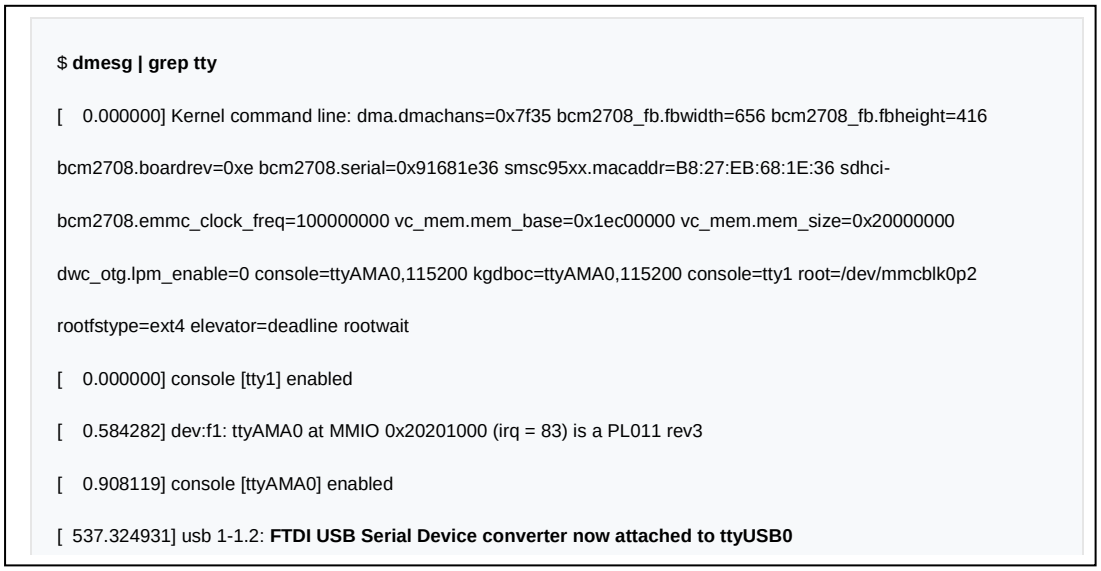
  cd ser2net-2.8/
  ./configure
  make
  sudo make install
- Una vez instalado Ser2net se eliminará las sobras:

  make clean

Antes de configurar Ser2net se necesita saber qué puerto USB utiliza el convertidor serial.

- Utilizar el siguiente comando.
- Configurar el archivo Ser2net, con el siguiente comando: *sudo vi /etc/ser2net.conf.*
- Agregar la siguiente línea: *4001:telnet:0:/dev/ttyUSB0:9600 8DATABITS NONE 1STOPBIT.*

Figura 32. **Modificación de archivo Ser2net**



```
$ dmesg | grep tty
[    0.000000] Kernel command line: dma.dmachans=0x7f35 bcm2708_fb.fbwidth=656 bcm2708_fb.fbheight=416
bcm2708.boardrev=0xe bcm2708.serial=0x91681e36 smsc95xx.macaddr=B8:27:EB:68:1E:36 sdhci-
bcm2708.emmc_clock_freq=100000000 vc_mem.mem_base=0x1ec00000 vc_mem.mem_size=0x20000000
dwc_otg.lpm_enable=0 console=ttyAMA0,115200 kgdboc=ttyAMA0,115200 console=tty1 root=/dev/mmcblk0p2
rootfstype=ext4 elevator=deadline rootwait
[    0.000000] console [tty1] enabled
[    0.584282] dev:f1: ttyAMA0 at MMIO 0x20201000 (irq = 83) is a PL011 rev3
[    0.908119] console [ttyAMA0] enabled
[  537.324931] usb 1-1.2: FTDI USB Serial Device converter now attached to ttyUSB0
```

Fuente: *Modificación de archivo Ser2net*. http://www.thefanclub.co.za/how-to/how-setup-usb-3g-modem-raspberry-pi-using-usbmodeswitch-and-wvdial. Consulta: 21 de marzo de 2015.

Se configura Ser2net para escuchar en el puerto TCP 4001 y utilizar el dispositivo / dev / ttyUSB0. La velocidad de transmisión de 9 600, 8 bits de datos, sin paridad y 1 bit de parada.

- Inicializar Ser2net: *ser2net –n*

- Para permitir que se inicialice Ser2net de forma automática cada vez que se reinicie la Raspberry Pi, se debe de modificar el siguiente archivo:

  sudo vi /etc/rc.local

- En la parte inferior de este archivo se encontrará 'exit 0', justo encima de esta línea es necesario agregar la siguiente: */usr/local/sbin/ser2net –n*

5.5. Configuración de interfaz de red

Debido a que la interrogación remota se debe realizar por medio de una IP publica o privada, dependiendo de la solución y un puerto TCP, es indispensable que la IP de cada interfaz de adquisición de datos sea configurada de forma estática, para ello se configurará de la siguiente forma.

- Para verificar las interfaces de red que se encuentran instaladas en la Raspberry Pi, se utiliza el siguiente comando: *Ifconfig –a*

- La interfaz de red que pertenece al módem 3G es la que lleva el nombre de ppp0, la cual se configurará con una IP asignada de forma estática, modificando el siguiente archivo de red: *sudo vi /etc/network/interfaces*

- En este archivo se modifican los siguientes parámetros, tomando en cuenta la información que el operador de telefonía ha asignado a cada SIM Card por medio de la configuración del APN corporativo.

  iface ppp0 inet static
  address <ip address>
  gateway <ip gateway>
  netmask <ip netmask>

5.6. Diseño de comunicación remota

El diseño de comunicación remota se presenta a continuación.

5.6.1. Diseño IP pública

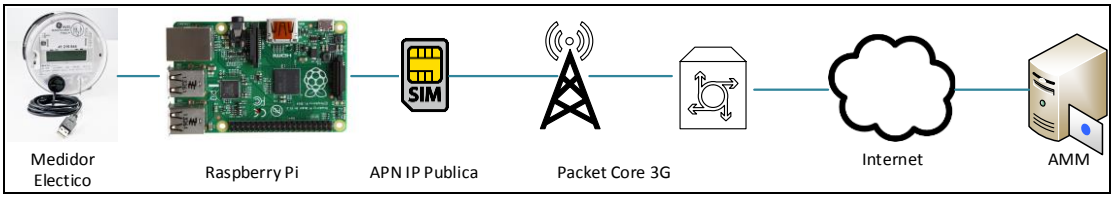
El diseño que contempla el uso de una IP pública es más sencillo de implementar, ya que al utilizar una dirección pública configurada en el APN de

la SIM Card puede ser alcanzada desde cualquier punto, debido a que este tipo de direcciones son enrutables desde internet.

Para esta implementación es necesario realizar los siguientes procedimientos:

- Conectar el medidor eléctrico por medio de la interfaz serial USB, validar que se tenga actualizado el controlador USB y que ha detectado el dispositivo.
- Cargar el software de control para permitir la conectividad de forma correcta al medidor eléctrico, para dicho paso es necesario que se establezca un puerto al TCP el cual será interrogado.

Figura 33. **APN IP/Pública**



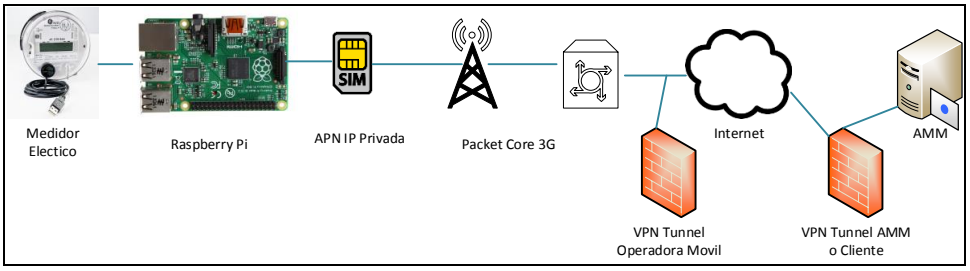
Fuente: elaboración propia.

5.6.2. Diseño IP privada

El diseño que contempla el uso de una IP privada debe tener configurado una VPN para establecer conectividad desde internet, debido a que una IP privada no puede ser alcanzada desde internet ya que no es una dirección única. Para ello es necesario establecer un túnel entre la IP del APN y cliente o AMM. Adicional a esto es necesario considerar los pasos siguientes:

- Conectar el medidor eléctrico por medio de la interfaz serial USB, validar que se tenga actualizado el controlador USB y que ha detectado el dispositivo.
- Cargar el software de control para permitir la conectividad de forma correcta al medidor eléctrico, para dicho paso es necesario que se establezca un puerto al TCP al cual será interrogado.

Figura 34. **APN IP privado**



Fuente: elaboración propia.

5.7. Análisis de costos de implementación

A continuación se presenta el análisis de costos de implementación.

Tabla IV. **Costos de implementación**

Descripción	**Costo**
Raspberry Pi modelo B	$ 42,98
Conversor serial USB	$ 8,35
Lector de Sim Card	$ 23,50
Case Raspberry Pi	$ 13,65
Cargador de Raspberry Pi	$ 3,21
Disipador térmico	$ 6,99
SD Card	$ 7,45
Precio total	$ 106,13

Fuente: elaboración propia.

5.8. Comparativa de precios con otras soluciones

La tabla comparativa de costos se presenta a continuación.

Tabla V. **Comparativa de costos**

Descripción	**Costo**
Interfaz Raspberry Pi	$ 106,13
Digi TransPort® WR21	$ 444,00

Fuente: elaboración propia.

6. MEDICION COMERCIAL

6.1. Antecedentes del Administrador del Mercado Mayorista

Los antecedentes del Administrador del Mercado Mayorista se presenta a continuación.

6.1.1. Historia

En 1996, el Gobierno de la República de Guatemala puso en marcha el ordenamiento de la industria eléctrica del país, emitiendo la Ley General de Electricidad, Decreto 93-96 y su reglamento en el Acuerdo Gubernativo 256-97. En el artículo 44 de la Ley se crea el Administrador del Mercado Mayorista (AMM), una entidad privada, sin fines de lucro.

6.1.2. Funciones

- La coordinación de la operación de centrales generadoras, interconexiones internacionales y líneas de transporte al mínimo costo para el conjunto de operaciones del mercado mayorista, en un marco de libre contratación de energía eléctrica entre agentes del mercado mayorista.
- Establecer precios de mercado de corto plazo para las transferencias de potencia y energía entre generadores, comercializadores, distribuidores, importadores y exportadores; específicamente cuando no correspondan a contratos libremente pactados.
- Garantizar la seguridad y el abastecimiento de energía eléctrica en el país.

6.1.3. Actividades

- Garantizar la seguridad del Sistema Nacional Interconectado (SNI) de energía eléctrica y el suministro, así como minimizar los costos mayoristas en el mercado de oportunidad.
- Prever y programar eficientemente el funcionamiento del mercado mayorista y del SNI.
- Realizar la valorización de las transacciones, pagos y cobros a los agentes de manera transparente.
- Operar en el Sistema Nacional Interconectado y administrar el mercado mayorista con objetividad y máxima transparencia dentro de las reglamentaciones del mercado mayorista.
- Velar por la obtención de la máxima eficiencia en el uso de los recursos.

6.2. Agentes y participantes

Los agentes del mercado mayorista están definidos en el Acuerdo Ministerial Número 195-2013, y son:

- Generadores
- Distribuidores
- Transportistas y comercializadores

Además de los agentes, se define también a los grandes usuarios. Cualquier agente y gran usuario es llamado en general participante, para poder ser agente o gran usuario del MM se debe cumplir con los siguientes requisitos básicos:

Tabla VI. **Integrantes del AMM**

Participantes	**Requisitos**
Generadores	Potencia máxima de por lo menos 5 MW
Distribuidores	Tener por lo menos 15 000 usuarios
Transportistas	Tener capacidad de transporte mínima de 10 MW
Comercializadores, importadores y exportadores	Comprar o vender bloques de energía asociada a una oferta firme eficiente o demanda firme de al menos 5 MW)
Grandes Usuarios	Demanda máxima de al menos 100 KW

Fuente: elaboración propia.

6.2.1. Obligaciones

- No realizar actos contrarios a la libre competencia.
- Cumplir con las normas emitidas por la Comisión Nacional de Energía Eléctrica.
- Obedecer las instrucciones de operación del Administrador del Mercado Mayorista.
- Instalar y mantener en buenas condiciones, los equipos de medición que le sean requeridos por el AMM.
- Los consumidores deben tener contratos de potencias que les permitan cubrir sus requerimientos de demanda firme.

6.2.2. Derechos

- Operar libremente en el mercado mayorista, de acuerdo a la ley.
- Acceso a la información sobre modelos y metodología utilizados por el AMM para la programación y el despacho.

6.3. Normativa de la medición comercial

Las normativas de la medición comercial son las siguientes.

6.3.1. Norma de Coordinación Comercial núm. 14

A continuación se presenta la norma de coordinación comercial no. 14.

6.3.1.1. Norma 14.8 Comunicaciones

Cada medidor o registrador oficial deberá contar obligatoriamente con un medio de comunicación vía internet (enlace IP) disponible en todo momento, para efectuar remotamente desde el AMM la lectura de memoria de acuerdo a los plazos establecidos en la regulación regional y nacional según corresponda. Deberá tener, además, la posibilidad de comunicación con una computadora mediante conexión con cable, interfaz óptica o cualquier otra herramienta inalámbrica, de tal forma que se pueda colectar la información del medidor oficial y el de respaldo sin cortar precintos.

El protocolo de comunicaciones, el formato de la información y la programación deberán ser compatibles con los que disponga el Administrador del Mercado Mayorista. De lo contrario, el participante responsable deberá proveer al Administrador del Mercado Mayorista los equipos y la programación necesarios para que el punto de medición pueda ser interrogado desde las instalaciones del Administrador del Mercado Mayorista.

CONCLUSIONES

1. La implementación de un sistema de interrogación que utilice la red celular con cobertura en el sitio de medición reduce los costos de infraestructura y ofrece una versatilidad en la solución debido a la movilidad que posee.

2. La utilización de un protocolo de comunicación como el TCP/IP garantiza el éxito en el envío y recepción de datos, porque este protocolo por sí mismo tiene distintas formas de garantizar y controlar el flujo correcto de transmisión.

3. El monitoreo por medio de un sistema de control reduce la cantidad de fallas en la comunicación remota, pues tiene la capacidad de rastrear diferentes elementos y dispositivos que intervienen en la misma.

4. El uso de sistemas embebidos en procesos de medición y control reduce considerablemente el uso de dispositivos electrónicos externos.

RECOMENDACIONES

1. Para una solución que requiera la implementación de una cantidad considerable de dispositivos de interrogación de medidores eléctricos, se debe utilizar la solución que contempla el uso de direcciones privadas configuradas en el APN.

2. Para el uso del dispositivo de interrogación de medidores eléctricos en condiciones ambientales extremas o intemperie, es necesario utilizar un *case* de protección metálico y con especificaciones que soporte temperaturas extremas y sellado térmico.

3. Utilizar un arreglo de dispositivos de medición por medio de una red LAN si el radio de separación entre un equipo y otro no es muy grande, esto para reducir la cantidad de SIM *Card*.

4. Para la implementación de este tipo de interfaces de interrogación de medidores eléctricos, es necesario garantizar que se tenga cobertura de red celular 3G, 2G para garantizar que la interrogación y acceso remoto sea exitosa.

5. Utilizar un sistema de protección y arreglo de baterías para garantizar que, si existe alguna falla eléctrica en el sistema de alimentación de la interfaz, se pueda tener acceso a ella y que no dependa de la disponibilidad energética de la red del lugar donde se encuentre instalado.

BIBLIOGRAFÍA

1. STALLINGS, William. *Data and computer communication*. 8a. ed. Estados Unidos; Pearson Prentice Hall, 2007. 120 p.

2. AMM. *Norma de Medición Eléctrica Comercial NCC14*. [en línea]. <www.cnee.gob.gt/pdf/normas/ncc14.pdf>. [Consulta: 26 de agosto de 2015].

3. AMM. *Migración a IP Medición Comercial*. [en línea]. <http://www.amm.org.gt/medicion_comercial.htm>. [Consulta: 26 de agosto de 2015].

4. AMM. *Alternativas de conectividad Medición Comercial*. [en línea]. <http://www.amm.org.gt/medicion_comercial.htm>. [Consulta: 26 de agosto de 2015].

5. NETWORK LESSONS. *Raspberry Pi as Cisco Console Server*. [en línea]. <http://networklessons.com/network-management/raspberry-pi-as-cisco-console-server/>. [Consulta: 26 de agosto de 2015].

6. RASPBERRY PI HQ. *How-To: Turn a Raspberry Pi into a WiFi router*. [en línea]. <http://raspberrypihq.com/how-to-turn-a-raspberry-pi-into-a-wifi-router/>. [Consulta: 26 de agosto de 2015].

7. *Hoja de características IC Max 232*. [en línea]. <http://www.ti.com/lit/ds/symlink/max232.pdf>. [Consulta: 26 de agosto de 2015].

8. *Descripción concepto de tecnología UMTS*. [en línea]. <http://www.3gpp.org/technologies/keywords-acronyms/103-umts>. [Consulta: 19 de septiembre de 2015].

9. *How to setup a USB 3G Modem on Raspberry PI using usb_modeswitch and wvdial*. [en línea]. <https://www.thefanclub.co.za/how-to/how-setup-usb-3g-modem-raspberry-pi-using-usbmodeswitch-and-wvdial>. [Consulta: 23 de enero de 2016].

10. *SGSN administration guide, StarOS Release 17*. [en línea]. <http://www.cisco.com/c/dam/en/us/td/docs/wireless/asr_5000/17-0/PDF/17-SGSN-Admin.pdf>. [Consulta: 23 de enero de 2016].

11. *GGSN administration guide, StarOS Release 17*. [en línea] http://www.cisco.com/c/dam/en/us/td/docs/wireless/asr_5000/17-0/PDF/17-GGSN-Admin.pdf. [Consulta: 23 de enero de 2016].

12. *Velocidades redes móviles*. [en línea] https://www.elhacker.net/diferencias-conexiones-3g-hsdpa umts.html. [Consulta: 23 de enero de 2016].

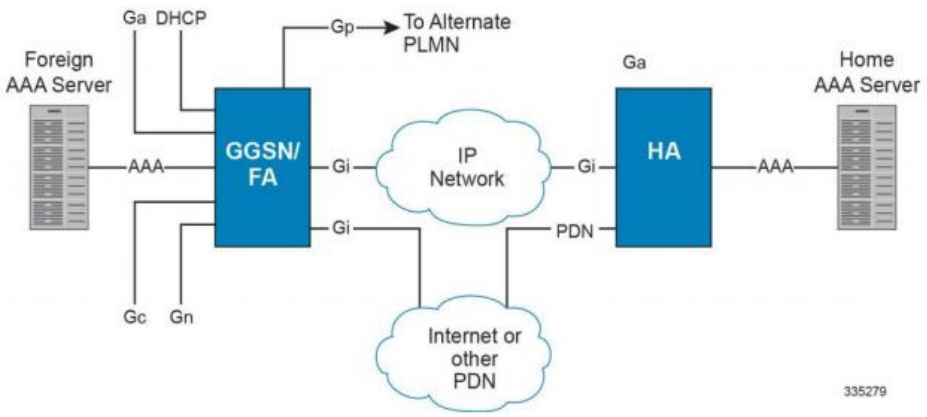
13. *Elementos de una red móvil*. [en línea] http://www.temas tecnologicos.com/elementosmovil.html. [Consulta: 23 de enero de 2016].

14. *Algoritmos de Cifrado túnel VPN*. [en línea]. <http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/>. [Consulta: 23 de enero de 2016].

15. *Tecnología VPN*. [en línea]. <http://www.networkingtool.net/2011/06/tecnologia-vpn.html>. [Consulta: 23 de enero de 2016].

APÉNDICE

GGSN despliegue para IP móvil o soporte de proxy IP móvil



Interfaces:

- Gn: esta es la interfaz utilizada por el GGSN para comunicarse con los SGSN en la misma GPRS / UMTS Red Pública Móvil Terrestre (PLMN). Esta interfaz sirve para la señalización y la ruta de datos para establecer y el contexto PDP del abonado. El GGSN se comunica con señales en la PLMN usando GPRS Protocolo de Túneles (GTP).

- La señalización o el control de los aspectos de este protocolo se conoce como el plano de control de GTP (GTPC), mientras el encapsulado del tráfico de datos del usuario se conoce como el Plano de Usuario GTP (GTPU).

- Ga: esta es la interfaz utilizada por el GGSN para comunicarse con la puerta de enlace de carga (CG). La carga gateway es responsable de enviar GGSN Carga de registros de datos (G-CDR) recibió del GGSN para cada Contexto PDP al sistema de facturación. El sistema soporta TCP y UDP como capa de transporte para esta interfaz. El GGSN se comunica con los GC en la PLMN usando GTP Prime (GTPP).

- Gc: esta es la interfaz utilizada por el GGSN para comunicarse con el Registro de Ubicación (HLR) a través de un GPO-MAP (Mobile Application Part) convertidor de protocolo. Esta interfaz se utiliza para la red iniciada PDP contextos. Para la red se inicia contextos PDP, el GGSN se comunicará con el convertidor de protocolo usando GTP a su vez, se comunicará con el HLR utilizando MAP sobre Sistema de Señalización 7 (SS7). Una interfaz Gc se puede configurar por contexto del sistema.

- Gi: esta es la interfaz utilizada por el GGSN para comunicarse con Packet Data Networks (PDN) externa a la PLMN. Ejemplos de RPD son Internet o intranets corporativas. Paquetes entrantes recibidos en esta interfaz podría iniciar una red solicitado contexto PDP si la MS es destino no está conectado actualmente. Para sistemas configurados como un GGSN / FA, esta interfaz se utiliza para comunicarse con HAs para IP y Soporte de proxy IP móvil.

- Una o más interfaces Gi se pueden configurar por contexto del sistema. Para IP móvil y Proxy Mobile IP, por lo menos una interfaz Gi debe configurarse para cada servicio FA configurado.

- Gp: esta es la interfaz utilizada por el GGSN para comunicarse con nodos de soporte GPRS (GSN, por ejemplo, GGSN y / o SGSN) en diferentes PLMNs. Dentro del sistema, una única interfaz puede servir tanto como un Gn y Gp una interfaz. Una o más interfaces Gn / Gp se pueden configurar por contexto del sistema.

- AAA: esta es la interfaz utilizada por el GGSN para comunicarse con autorización, autenticación y contabilidad (AAA) en la red. El sistema GGSN se comunica con el servidor AAA usando el dial de autenticación remota de protocolo de servicio de usuario (RADIUS). Esta es una interfaz opcional que puede ser utilizado por el GGSN para la autenticación de contexto PDP de abonado y contabilidad.

- DHCP: esta es la interfaz utilizada por el GGSN para comunicarse con un Dynamic Host Control Protocol (DHCP) Servidor. El sistema puede ser configurado como DHCP-Proxy o DHCP Client para proporcionar direcciones IP a la MS en contextos PDP de activación del servidor DHCP de forma dinámica.

- Gx: esta es una interfaz basada en protocolo Diameter opcional sobre el cual el GGSN comunica con una carga Regla Función (IRC) para el aprovisionamiento de las normas de carga que se basan en el análisis dinámico de los flujos utilizado para un Subsistema Multimedia IP (IMS) sesión.

- El sistema ofrece soporte mejorado para el uso del servicio Basado Política Local (SBLP) para el suministro y control de los recursos utilizados por el abonado IMS. También proporciona el flujo de carga

basado (FBC) mecanismo para cargar el suscriptor dinámicamente basándose en el uso de los contenidos.

- Gy: esta es una interfaz basada en protocolo Diameter opcional sobre el cual el GGSN comunica con una carga de función de disparo (CTF) del servidor que proporciona datos de facturación en línea. Soporte de interfaz Gy proporciona una línea interfaz que funciona con la función de inspección profunda de paquetes ECS carga. Con Gy, el tráfico de clientes puede ser cerrada y facturados en un estilo "en línea" o "prepago".

- Ambos modelos tiempo y basados en el volumen de carga son soportados. En todos estos modelos, tipos diferenciados se pueden aplicar a diferentes servicios basados en poco profunda o inspección profunda de paquetes.

- GRE: esta nueva interfaz de protocolo en la plataforma GGSN añade un protocolo adicional para apoyar a los usuarios móviles a conectarse a sus redes empresariales: encapsulación de enrutamiento genérico (GRE). GRE túnel es técnica para habilitar redes locales multiprotocolo a través de una red troncal protocolo único, para conectar redes no contiguas y permitir que las redes privadas virtuales a través de redes WAN.

- Este mecanismo encapsula los paquetes de datos desde un protocolo dentro de protocolos diferentes y transporta los paquetes de datos sin cambios a través de una red extranjera. Ello es importante señalar que tunelización GRE no proporciona seguridad para el protocolo de

encapsulado, ya que no hay cifrados involucrados (como IPSEC ofrece, por ejemplo).

Fuente: elaboración propia.

ANEXOS

Anexo 1. Configuración de APN Cisco ASR 5000

APN Creación y Configuración

```
configure
  context apn -noconfirm
    pdp-type {ipv4 [ipv6] | ipv6 [ipv4] | ppp}
    selection-mode {sent-by-ms | chosen-by-sgsn | subscribed}
    ip context-name
  end
```

Autenticación y Registro del APN

```
configure
  context <dst_ctxt_name>
    apn <apn_name>
      accounting-mode {none | gtpp | radius [no-interims] [no-early-pdus]}
      default authentication
    end
```

Grupo GTPP asociado al APN

```
configure
  context <vpn_ctxt_name>
    apn <apn_name>
      gtpp group <gtpp_group_name> [accounting-context <aaa_ctxt_name>]
    end
```

Continuacion del anexo 1.

Direcciones IP asociadas al APN

```
configure
  context <dst_ctxt_name>
    apn <apn_name>
      ip address alloc-method { dhcp-proxy [allow-deferred] [prefer-dhcp-options] |
      dhcp-relay | local [allow-deferred] | no-dynamic [allow-deferred] } [allow-userspecified]
end
```

Características de Cobro y Parámetros del APN

```
configure
  context <dst_ctxt_name>
    apn <apn_name>
      cc-sgsn {home-subscriber-use-GGSN | roaming-subscriber-use-GGSN | visitingsubscriber-use-
GGSN}+
      cc-home behavior <bit> profile <index>
      cc-roaming behavior <bit> profile <index>
      cc-visiting behavior <bit> profile <index>
      end
```

Parámetros adicionales de configuración del APN

```
  configure
    context <dst_ctxt_name>
      apn <apn_name>
        dns {primary | secondary} {<dns_ip_address>}
        mobile-ip required
        mobile-ip home-agent <ha_ip_address>
        ip source-violation {ignore | check [drop-limit <limit>]} [exclude-fromaccounting]
        restriction-value <value>
        timeout {absolute | idle | qos-renegotiate} <timeout_dur>
        timeout long-duration <ldt_dur> [inactivity-time <inact_dur>]
        long-duration-action detection
        long-duration-action disconnection [suppress-notification] [dormant-only] +
      end
```

Fuente: Raspberry Pi.

Anexo 2. **Configuración de APN de ejemplo**

Datos del APN

Nombre del APN: test.com

Tipo de APN: VPN

IP pool: 10.127.74.0/23

Tipo de IP Pool: Estático

VlanID: N/A

Next-Hop IP: N/A

```
configure
  context Gi
    ip pool test.com.P01 10.127.74.0 255.255.254.0 static group-name test.com.GP
    router ospf
      network 10.127.74.0/23 area 0.0.0.11
    exit
    apn test.com -noconfirm
      accounting-mode none
      gtpp group GCDR-TEST
      idle-timeout-activity ignore-downlink
      ims-auth-service Gx-Test
      dns primary 208.67.222.222
      dns secondary 8.8.8.8
      ip source-violation ignore
      ip address pool name test.com.GP
      credit-control-group Test
      active-charging rulebase Test
    exit
  exit
exit
```

Fuente: Raspberry Pi.