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

DISEÑO E IMPLEMENTACIÓN DE UN EQUIPO PARA MONITORIZACIÓN DE TEMPERATURA AMBIENTAL Y NIVELES DE SUMINISTRO ÉLECTRICO PARA LOS EQUIPOS EN UN NODO DE UNA RED DE TELECOMUNICACIÓN

Hugo Ismael Dardon Juárez
Asesorado por la Inga. Ingrid Salomé Rodríguez García

Guatemala, octubre de 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UN EQUIPO PARA MONITORIZACIÓN DE TEMPERATURA AMBIENTAL Y NIVELES DE SUMINISTRO ÉLECTRICO PARA LOS EQUIPOS EN UN NODO DE UNA RED DE TELECOMUNICACIÓN

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

HUGO ISMAEL DARDON JUÁREZ
ASESORADO POR LA INGA. INGRID SALOMÉ RODRÍGUEZ GARCÍA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, OCTUBRE DE 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Juan Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Guillermo Antonio Puente Romero
EXAMINADOR	Ing. Marvin Marino Hernández Fernández
EXAMINADOR	Ing. Julio César Solares Bascope
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

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:

DISEÑO E IMPLEMENTACIÓN DE UN EQUIPO PARA MONITORIZACIÓN DE TEMPERATURA AMBIENTAL Y NIVELES DE SUMINISTRO ÉLECTRICO PARA LOS EQUIPOS EN UN NODO DE UNA RED DE TELECOMUNICACIÓN

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 4 de agosto de 2009.

Hugo Ismael Dardon Juárez

Guatemala 8 de febrero del 2011

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

Estimado Ingeniero Gusman.

Me permito dar aprobación al trabajo de graduación titulado: **"DISEÑO E IMPLEMENTACIÓN DE UN EQUIPO PARA MONITORIZACIÓN DE TEMPERATURA AMBIENTAL Y NIVELES DE SUMINISTRO ELÉCTRICO PARA LOS EQUIPOS EN UN NODO DE UNA RED DE TELECOMUNICACIÓN"**, del señor Hugo Ismael Dardón Juarez, 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 ELECTRONICA
COLEGIADA 5,356

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

Ref. EIME 20. 2011
Guatemala, 14 de MARZO 2011.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingeniería Mecànica Elèctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: "DISEÑO E IMPLEMENTACIÓN DE UN EQUIPO PARA MONITORIZACIÓN DE TEMPERATURA AMBIENTAL Y NIVELES DE SUMINISTRO ELÉCTRICO PARA LOS EQUIPOS EN UN NODO DE UNA RED DE TELECOMUNICACIÓN", del estudiante, Hugo Ismael Dardón Juárez, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

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

Ing. Carlos Eduardo Guzmán Salazar
Coordinador de Electrónica

CEGS/sro

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

REF. EIME 29. 2011.

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; HUGO ISMAEL DARDÓN JUÁREZ titulado: "DISEÑO E IMPLEMENTACIÓN DE UN EQUIPO PARA MONITORIZACIÓN DE TEMPERATURA AMBIENTAL Y NIVELES DE SUMINISTRO ELÉCTRICO PARA LOS EQUIPOS EN UN NODO DE UNA RED DE TELECOMUNICACIÓN", procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

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

GUATEMALA, 27 DE ABRIL 2,011.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 416.2011

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: **DISEÑO E IMPLEMENTACIÓN DE UIN EQUIPO PARA MONITORIZACIÓN DE TEMPERATURA AMBIENTAL Y NIVELES DE SUMINISTRO ELÉCTRICO PARA LOS EQUIPOS EN UN NODO DE UNA RED DE TELECOMUNICACIÓN,** presentado por el estudiante universitario **Hugo Ismael Dardon Juárez,** autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, 19 de octubre de 2011.

/gdech

ACTO QUE DEDICO A:

Dios	Por ser la luz que ha iluminado día y noche mi camino.
Mis padres	Víctor Hugo Dardon Castillo y Edna Leonor Juárez Cobar.

AGRADECIMIENTOS A:

Dios Por darme vida y fuerza para culminar esta etapa de mi existencia.

Mis padres Víctor Hugo y Edna, por su apoyo incondicional en todo momento. Por crear en mí las bases que me sostienen en el camino de la vida y enseñarme con su ejemplo, que siempre es posible alcanzar las metas con dedicación, pasión y optimismo. Gracias por escucharme en los momentos de alegría, tristeza y preocupación; por apoyarme siempre que lo he necesitado y por quererme como lo hacen. Espero que esto sea un pequeño regalo a su esfuerzo, por brindarme el amor y la atención que siempre he tenido. Desde el fondo de mi corazón se los agradezco.

Mis hermanas Edna Marina y María Mercedes, por hacerme reír y disfrutar de la vida. Por enseñarme a ver la vida desde un punto de vista diferente y compartir conmigo todas las alegrías, tristezas y éxitos.

Mis compañeros de estudio y amigos de toda la vida	En especial a Wendy Barrios, Julio Morales, Christian Gómez, Carlos Boche, Carlos Arriola, David Cabeiro y Juan Carlos Argueta, por compartir conmigo momentos de alegría y tristeza pero dándonos fortaleza para siempre a continuar y culminar nuestras metas.
Mis compañeros y amigos de labores	Fernando Lemus, Pedro Mérida, Mario Silvestre, Juan Luis Guzmán, Jaime Matus, Fernando Mazariegos, Edwin Orozco, Gustavo Cifuentes, Aldo García, Magda Morales y Pedro Orellana, por compartir sus conocimientos y experiencias con entusiasmo de forma desinteresada, alentarme a culminar con las metas propuestas y compartir las alegrías y presiones laborales a las que nos hemos enfrentado diariamente.
Mi centro de estudios superiores	Universidad de San Carlos de Guatemala, por ser el ente que me formó a nivel profesional, dándome las herramientas necesarias para desarrollar un alto nivel académico y hacerme competitivo en el ámbito laboral.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
Bps	Bit por segundo.
MAC	Control de Acceso al Medio.
Gbps	Gigabits por segundo.
°C	Grados centígrados.
IP	*Intenet Protocol* (Protocolo de *Internet*).
kHz	Kilo Hertz por segundo.
Kbps	Kilobits por segundo.
Mbps	Megabits por segundo.
QoS	*Quality of Service* (Calidad de Servicio).

GLOSARIO

ACK Acuse de recibido (*ACKNOWLEDGEMENT*), en comunicaciones entre computadores, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado.

Amperio En el Sistema Internacional, es la unidad de intensidad de la corriente eléctrica.

BOOTP Estas son las siglas de *Bootstrap Protocol*. El cual es un protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente.

Bus Conjunto de conductores eléctricos en forma de pistas metálicas impresas sobre la tarjeta del equipo o computador, por donde circulan las señales que corresponden a los datos binarios con que opera el Microprocesador.

CARRIER Nombre dado a una empresa que transporta un producto o información utilizando su infraestructura y ofrece sus servicios al público en general.

CSU/DSU	Por sus siglas en inglés (*Channel Service Unit/Data Service Unit*), es un equipo con interfaces dígitales usado para conectar equipos terminales como Routers a un equipo dígital.
DHCP	Protocolo de configuración dinámica de *host* (sigla en inglés de *Dynamic Host Configuration Protocol*) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.
DNS	Sistema de Nombres de Dominio (*Domain Name System*) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a *Internet* o a una red privada.
FTP	Protocolo de Transferencia de Archivos (sigla en inglés de *File Transfer Protocol*) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor.
HTTP	Protocolo de Transferencia de Hipertexto (*Hypertext Tranfer Protocol*) es el protocolo usado en cada transacción de la *World Wide Web*.

IEEE	Corresponde a las siglas de (*Institute of Electrical and Electronics Engineers*) en español Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas.
LAN	Una red de área local, red local o LAN (del inglés *local area network*) es la interconexión de varias computadoras y periféricos. Su extensión está límitada físicamente a un edificio o a un entorno de 200 metros.
SMTP	Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo.
SSH	Intérprete de órdenes segura (*Secure Shell*) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.
TCP	Protocolo de Control de Transmisión (*Transmission Control Protocol*), es uno de los protocolos fundamentales en *Internet*.
WAN	Siglas del inglés *Wide Area Network*, son redes informáticas que se extienden sobre un área geográfica extensa.

RESUMEN

Las redes de telecomunicaciones son sistemas que transmiten información a través de líneas de un lugar a otro. Estas redes cuentan con nodos principales en los cuales se encuentran los equipos que conforman y mantienen operativas las redes. Estos puntos son de vital importancia ya que al ser la base de toda la red deben de contar con una temperatura adecuada así como de un suministro eléctrico ininterrumpido. En el presente trabajo de graduación se detalla el diseño de un equipo para monitorización de temperatura ambiental y niveles de suministro eléctrico. Este sistema se implementará en una red de telecomunicaciones existente, que proporciona diversidad de servicios a lo largo del país.

En el capítulo uno, se describe los problemas debido a energía eléctrica en un nodo de una red WAN, esto incluye el por qué de la necesidad de un servicio ininterrumpido, tipos de soluciones al problema de fallas eléctricas y un muestreo de los cortes de energía eléctrica suscitados en el país.

En el segundo capítulo, se abordan los conceptos básicos de redes, haciendo énfasis en los protocolos existentes, modelo OSI y ruteo.

En el capítulo tres, se abordan los conceptos básicos de la arquitectura de un microcontrolador, haciendo énfasis en las diferencias que existen con los microprocesadores y controladores. Posteriormente se detallan las funciones de cada elemento que lo compone y la amplia gama de opciones que brindan al programador. Adicionalmente, se da un pequeño esbozo de la etapa concerniente a la programación de microcontroladores.

En el cuarto capítulo, se describe a los sistemas de monitoreo, así como se da una explicación de las diversas funciones que brinda la herramienta de Solar Winds ORION.

Finalmente, en el capítulo quinto se enfoca toda la atención en el diseño e implementación del sistema generador de mensajes. En este apartado se detallan los elementos que forman parte del nuevo sistema y se explica el funcionamiento de cada uno de ellos. Adicionalmente se dedica una sección para explicar la lógica de programación utilizada.

Luego del diseño de la nueva herramienta, se detalla la etapa de implementación, donde se evalúa el desempeño del sistema. El capítulo quinto se finaliza con la estimación de costos del sistema completo.

OBJETIVOS

General

Diseñar un sistema que sea capaz de monitorear y a su vez generar mensajes por medio de correo electrónico para notificar las fallas y restablecimientos de suministro eléctrico, así como niveles de temperatura en el mismo nodo e implementarlo en un nodo existente.

Específicos

1. Definir los principios básicos y arquitectura de las redes WAN (*Wide-Area Network*).

2. Describir que es un microcontrolador y como está conformado.

3. Describir las ventajas y características de los sistemas de monitoreo.

4. Aplicar los conocimientos adquiridos a lo largo de la carrera en el diseño e implementación del sistema generador de mensajes a base de microcontroladores.

INTRODUCCIÓN

Actualmente las redes de telecomunicaciones que se encuentran establecidas en Guatemala, cuentan con varios nodos que son los cuales a su vez, albergan equipo activo que necesita permanecer con alimentación constante de energía eléctrica así como mantener cierta temperatura para su buen funcionamiento y no entorpecer la disponibilidad de los servicios.

Por el constante crecimiento y adelantos en el campo de la tecnología, se hace necesaria la automatización de muchos procesos, con el fin de incrementar la producción de los sistemas y economizar la operación de los mismos.

Para realizar el censado del suministro eléctrico se utiliza equipo capaz de llevar a cabo esta tarea, con el fin de que una persona desde el nodo central pueda revisar el equipo de forma remota, esto con el fin de desplazar personal al sitio antes de que el suministro de respaldo caiga o la temperatura del nodo alcance niveles altos y pueda perjudicar al equipo.

La comunicación hacia el equipo de monitoreo instalado en el nodo se realiza haciendo uso de la red WAN (*Wide-Area Network*). Este tipo de red permite varios tipos de comunicaciones, entre estos los protocolos TCP/IP y UDP son los más utilizados por sus versatilidades y bondades en las necesidades de comunicación actuales.

En Guatemala los servicios de transporte de datos o *Internet* que se prestan están creciendo cada vez más y por este motivo los nodos y equipos necesitan estar funcionando todo el tiempo con el fin de no interrumpir el flujo de información que viaja a través de cada nodo ya que esto representa pérdida de capital tanto para el cliente como para el carrier.

Por lo anterior, se ve la necesidad de implementar un sistema de monitoreo nuevo que pueda integrarse y complementar al sistema de respaldo actualmente instalado en cada uno de los nodos, con el fin de poder dar un diagnóstico y tomar una medida de acorde al problema que se pueda presentar en el nodo antes que éste cause inconvenientes en los equipos instalados en dicho nodo.

El sistema de monitoreo del suministro de energía eléctrica, pretende proveer de herramientas adicionales en el monitoreo de la red, con el fin de reducir los tiempos de falla. Este sistema es capaz de dar mediciones exactas tanto del suministro eléctrico como de la temperatura del nodo, mejorándose de esta forma el servicio prestado a los clientes y reduciendo las pérdidas de información por parte del cliente y evitando penalizaciones al carrier. El diseño e implementación del sistema de monitoreo se desarrollará a lo largo del presente trabajo de graduación, aportando una solución sencilla en la identificación de fallas y restablecimientos del suministro eléctrico.

1. PROBLEMAS DEBIDO A ENERGÍA ELÉCTRICA EN UN NODO DE UNA RED WAN

1.1. Energía eléctrica como servicio indispensable

Hace muchos años, cuando recién se iniciaba el uso de la energía eléctrica en Guatemala y su carga era en gran porcentaje lámparas incandescentes; la interrupción de servicio eléctrico no pasaba de ser un simple apagón sin mayores problemas ni consecuencias; hoy en día cuando se ha llegado a una completa comercialización e industrialización del mencionado servicio es muy importante la continuidad y necesidad para toda clase de consumidor.

El control de tránsito en nuestras grandes ciudades, el abastecimiento de agua potable, las comunicaciones por radio y cables, el funcionamiento de ascensores para grandes edificios, la energía eléctrica de un quirófano de los hospitales, la alimentación de un nodo de telecomunicaciones; son unos pocos de los ejemplos de la dependencia que a diario tenemos individual y colectivamente.

Normalmente en la actualidad los grandes centros productores de energía eléctrica se encuentran situados a grandes distancias de los consumidores, aumentando con esto la probabilidad de falla ya que no sólo puede afectar la avería de un elemento generador o dispositivos que separen a la planta generadora con los centros de carga; contactores, fusibles, aisladores y

protecciones en general; también afecta la línea de transmisión ya que puede ser afectada por descargas electro atmosféricas, sabotajes, caídas de árboles sobre el tendido. Es evidente pues, la posibilidad de falla y la necesaria continuidad del servicio en alguna forma.

1.2. Confiabilidad del equipo eléctrico

Los índices de confiabilidad básicos más útiles en el diseño de sistemas de distribución de energía eléctrica son:

- Frecuencia de interrupción del servicio
- Duración esperada de la interrupción del servicio

Estos 2 índices básicos se utilizan para calcular otros índices más útiles para el análisis que pretendemos hacer:

- Tiempo total esperado de interrupción por año (o cualquier otro período de tiempo).
- Disponibilidad o indisponibilidad del sistema, medidas en el punto donde se presa el servicio a la carga.

Este tipo de consideraciones son las bases que llevan a la necesidad de calcular el tiempo que ocurre una falla en la distribución del sistema de distribución eléctrico, es por esto que se hace tan necesario el garantizar que los equipos se encuentren trabajando ininterrumpidamente.

Para garantizar la alimentación ininterrumpida de energía eléctrica a los equipos se instalan en los nodos equipos electrógenos y sistemas ininterrumpidos de energía.

1.2.1. Grupos electrógenos y sistemas de suministro ininterrumpido de energía

Luego de determinarse la diversidad de causas capaces de producir fallas en un sistema eléctrico (y conocidos algunos datos estadísticos referentes a fallas del sistema nacional interconectado), 2 de las más importantes formas de mantener el servicio eléctrico emergente; las cuales son: plantas emergentes y sistemas de suministro ininterrumpido.

La mayor parte de equipo electromecánico y electrónico sofisticado opera con corriente alterna. Algunas veces este equipo se aplica a sistemas donde las interrupciones y los disturbios en la línea de energía AC no pueden ser tolerados, caso particular de los equipos de telecomunicaciones, por lo tanto se requieren medios de almacenamiento de energía que permitan mantener la operación de los equipos durante estas anormalidades. Un tipo de energía almacenada es el petróleo y sus productos, los cuales son utilizados en la máquinas diesel y turbinas de gas destinadas a excitar alternadores, los cuales alimentan la energía de corriente alterna (de aquí en adelante AC) al equipo crítico.

La mayoría de computadoras modernas son incapaces de tolerar cualquier interrupción en el suministro de energía. Incluso un corte momentáneo puede causar pérdidas de la memoria almacenada y el paro automático de los

procesos o máquinas controladas por el computador y el falseamiento de las comunicaciones cuando son utilizadas con ese propósito.

1.2.2. Plantas emergentes o grupos electrógenos

Las plantas generadoras accionadas por motores de combustión interna son muy conocidas. Las primeras máquinas eran llamadas plantas de luz, terminología totalmente descriptiva por su finalidad de proporcionar energía para lámparas eléctricas. Sin embargo, las modernas plantas accionadas por motores, suministran energía eléctrica tanto para obtención de luz como para otros usos domésticos e industriales.

En cierta manera la disponibilidad de la corriente suministrada por las compañías eléctricas y su constante expansión, han creado nuevos problemas al consumidor, debido a que la complejidad de sus tableros de mando como lo extenso de sus redes de distribución, los expone a la posibilidad de mayores interrupciones y fallas. La necesidad de poder disponer de un sistema más confiable obliga a los usuarios a depender cada día más de máquinas y aparatos movidos y controlados electrónicamente.

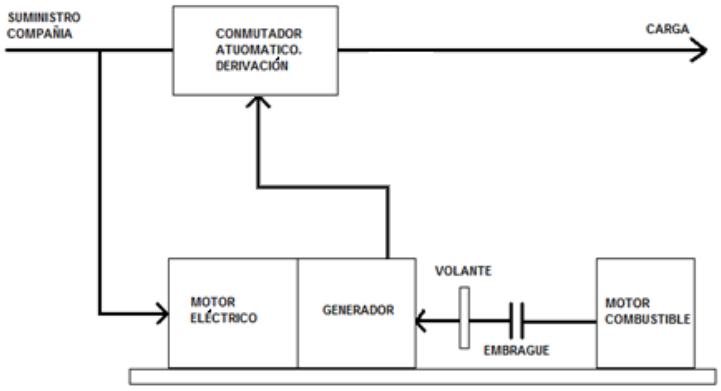
Considerando que puedan garantizarles un servicio más eficiente, por ejemplo lo que sucederá en un banco al producirse un corte en el suministro eléctrico, no pueden funcionar los sistemas de seguridad, luces, aparatos electrónicos de procesos de datos y demás servicios, lo cual además de incómodo es sumamente peligroso tanto para el personal como para los usuarios, debido a que se expone a cualquier tipo de atentado, por lo que es sumamente importante considerar un sistema que pueda garantizar un suministro continuo de corriente.

Lo mismo puede decirse de otras oficinas, cines, estadios, fábricas, escuelas y hospitales y todos aquellos lugares de alta concentración de público.

1.2.3. Diferentes tipos de suministro ininterrumpido de energía

Uno de los primeros sistemas de suministro ininterrumpido de energía estaba integrado por un motor eléctrico, un generador eléctrico, un motor de combustión interna y una gran masa rotativa (volante) que van acopladas a un eje común. La carga eléctrica se conecta a la salida del generador.

Figura 1. **Sistema de suministro ininterrumpido por motor de combustión interna**



Fuente: elaboración propia.

Funcionando normalmente, el motor eléctrico hace girar al eje. La energía para el motor eléctrico se obtiene del suministro normal de alimentación comercial. La entrada de combustible al motor diesel está cortada y un embrague mantiene desconectado el motor de combustión del eje general. Una

vez alcanzada la velocidad de régimen, la pesada masa rotativa actúa como un sistema mecánico de almacenamiento de energía.

Cuando se produce una interrupción en el suministro de energía comercial, se conecta la alimentación de combustible del motor y se activa el embrague, que acopla el motor de combustión al generador, el cual continuará alimentando a los consumidores, sin que se haya interrumpido dicho suministro ni un solo instante, debido a que el período durante el cual arranca el motor de combustión y alcanza su velocidad de régimen además del tiempo que tarda en ocurrir el acoplamiento del embrague, el generador es alimentado con energía del volante, el cual por su gran masa continúa girando por inercia aunque se interrumpa el suministro de energía comercial.

1.2.4. Suministro ininterrumpido de energía tipo estático

Este sencillo sistema de suministro de energía sin interrupción es considerado en la actualidad el más práctico de estos sistemas, siendo además eficientes en un alto porcentaje. A diferencia del primer sistema, éste usa como medio de almacenar energía un banco de baterías.

Básicamente está integrado por cuatro elementos fundamentales:

- Un rectificador o cargador de baterías
- Un banco de baterías
- Un inversor u ondulador estático
- Un conmutador automático

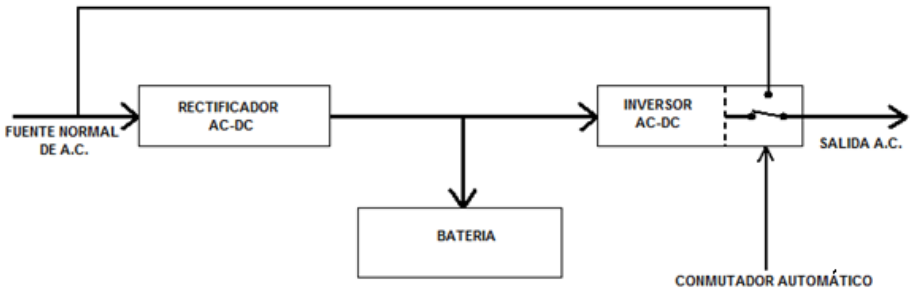
Este sistema consiste en un rectificador o cargador de baterías conectado a la fuente normal de energía eléctrica, estando acoplado el banco

de salida de éste. En otras palabras para hacer funcionar el inversor, la energía proviene del rectificador cuando hay suministro de energía comercial y las baterías actúan como un filtro, a la vez que reciben una carga continua de flotación que las mantiene a plena capacidad. Las cargas eléctricas críticas se encuentran a la salida del inversor. Cuando se interrumpe el servicio normal de energía el rectificador es sustituido por las baterías para alimentar el inversor.

1.2.4.1. Operación normal

- El rectificador es alimentado por la red comercial, transformando esta energía de corriente alterna (CA) a corriente directa (CD) completamente filtrada.
- La energía de CD proveniente del rectificador alimenta simultáneamente al inversor y a los bancos de baterías, los que mantiene a plena capacidad de carga.
- La CD suministrada al inversor es transformada por este nuevamente a CA la cual llega a los consumidores a través del *Switch* de transferencia.

Figura 2. **Sistema en operación normal**



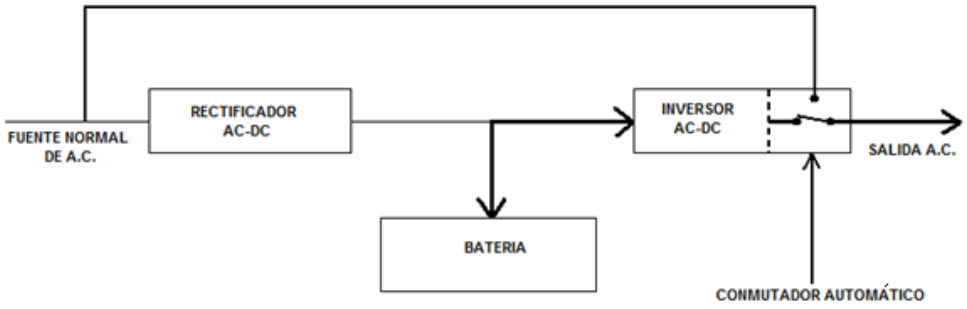
Fuente: elaboración propia.

1.2.4.2. Operación con falla de red comercial

Al fallar la red comercial sale de servicio el rectificador, lo que permite a la batería hacerse cargo de la alimentación del inversor en forma instantánea, sin que ocurra ninguna interrupción del servicio, lográndose en esta forma que los consumidores puedan contar con un servicio ininterrumpido de alimentación de energía.

Al normalizarse la red comercial, el sistema desarrollará las funciones de operación normal, con la única diferencia que la batería recibirá una corriente de carga mayor (carga de igualación) que permitirá su pronta recuperación de plena capacidad de energía perdida durante la descarga y la que pueda proporcionarle el rectificador debido a que ésta va de acuerdo al porcentaje de disponibilidad de capacidad del mismo, ya que simultáneamente debe alimentar al inversor, el cual exigirá más o menos corriente de acuerdo a las exigencias de los consumidores.

Figura 3. **Sistema en operación con falla de red comercial**



Fuente: elaboración propia.

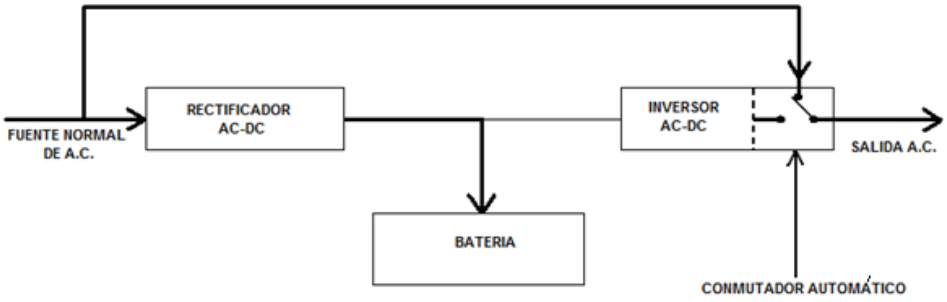
1.2.4.3. Operación con servicio de paso

Algunos sistemas de este tipo son diseñados para proporcionar este servicio; el cual consiste en que los consumidores son alimentados directamente de la red, la que simultáneamente suministra la energía de operación del rectificador, el cual se encarga de la alimentación de los bancos de baterías.

Este tipo de operación tiene el inconveniente de que al ocurrir suspensión del servicio de red, la alimentación de los consumidores se interrumpe durante el tiempo que tarda en cambiar de posición el *Switch* de transferencia (conmutador automático), sin embargo y a pesar de los riesgos de interrupciones momentáneas de servicio, las cuales son sumamente delicadas en procesos de computación, esta posición se utiliza cuando se tiene que realizar reparaciones o ajustes tanto en los rectificadores como en los

inversores, sin tener que interrumpir el suministro de energía a los consumidores. Facilitándose las labores de mantenimiento.

Figura 4. **Sistema en operación con servicio de paso**



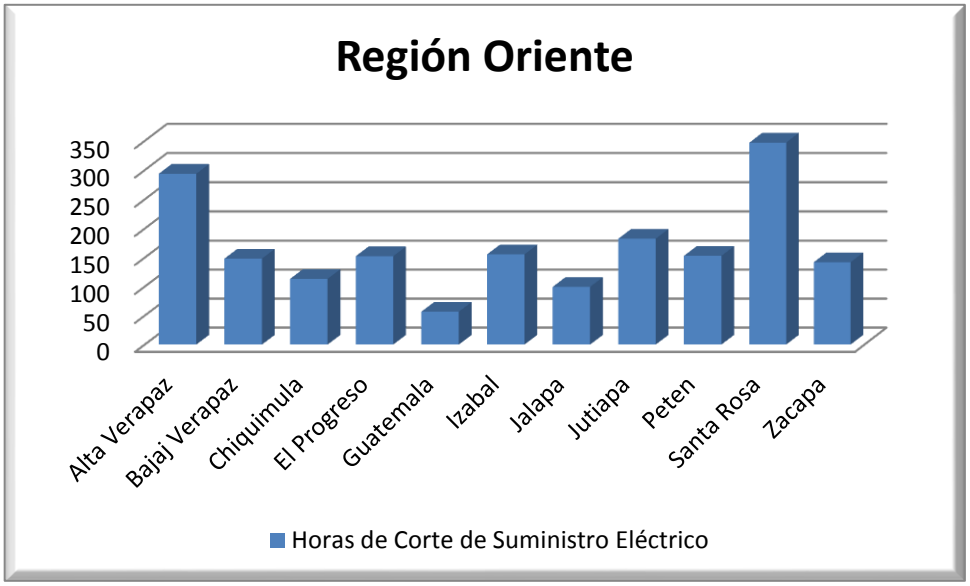
Fuente: elaboración propia.

1.3. Cortes de energía

En Guatemala los cortes de energía en la distribución a nivel nacional se pueden presentar por varios fenómenos tales como accidentes o fallas en algún transformador en alguna sub estación central, falla en una línea de transmisión principal, corte programado debido a mantenimiento, etc. Este último punto es el que con más frecuencia se suscita en nuestro país y es por esto que se ha analizado y encontrado que en el período del 18 de agosto del 2008 al 30 de septiembre del 2009 se tuvo en el territorio nacional un total de 4731,34 horas de indisponibilidad del suministro eléctrico.

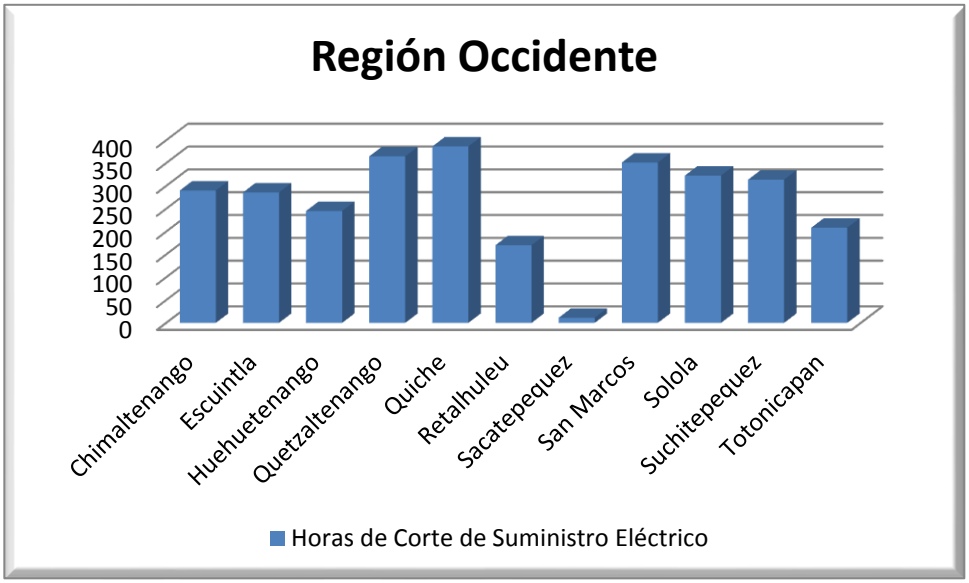
Estas 4731,34 horas se encuentran distribuidas por departamentos según se muestran en las siguientes gráficas.

Figura 5. **Horas de corte de suministro eléctrico Oriente**



Fuente: elaboración propia.

Figura 6. **Horas de corte de suministro eléctrico Occidente**



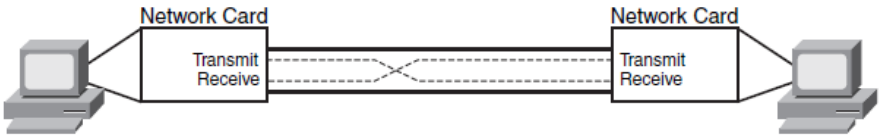
Fuente: elaboración propia.

2. TRABJO DE REDES FUNDAMENTALES

2.1. Introducción a los conceptos de redes de datos

En sus inicios la forma de transferir información de una computadora a otra era por medio de un disco magnético u otro medio físico el cual implicaba que las personas tenían que llevar la información físicamente de un punto a otro. Con el fin de solucionar este problema fueron creados programas para transferencia de archivos y las tarjetas de red que en un inicio sólo podían comunicar 2 computadoras, las cuales mediante el cruce de cables se podía utilizar un hilo del cable como transmisión y el otro como recepción.

Figura 7. **Diagrama de comunicación entre 2 computadoras**

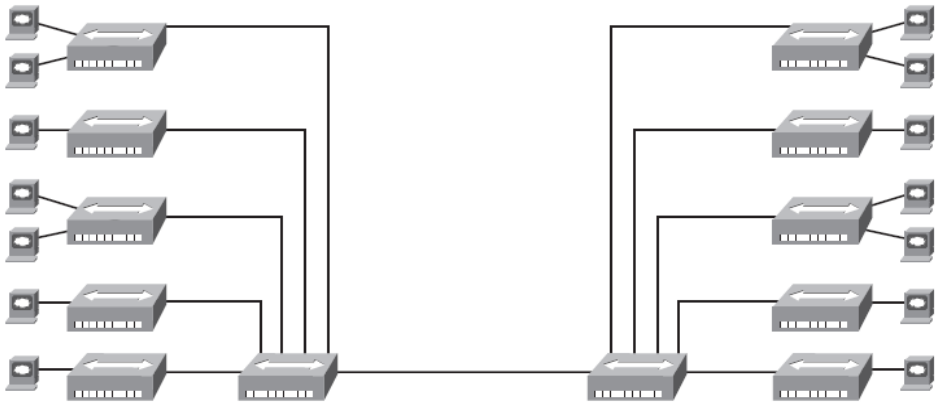


Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide, p. 9.

Este concepto funcionó perfectamente hasta que se quiso conectar varias computadoras, esto llevó a que se crearan los equipos concentradores (HUB), estos equipos realizaron las veces de repetir toda la información que recibían por parte de una computadora, esto causó que se pudieran conectar más de 2 computadoras sin necesidad de instalar más de 1 tarjeta de red a las mismas y

que todas las computadoras conectadas al HUB estuvieran comunicadas entre sí.

Figura 8. **Diagrama de 2 redes LAN**



Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide, p. 12.

.

El problema que se detectó con esta configuración fue el hecho que la información enviada por una PC era enviada a todas las demás que se encontraban conectadas, cuando quizá se quería sólo enviar información a una sola PC específica, este problema fue solucionado asignándole a cada tarjeta un número representativo único y agregando en el *software* de transferencia de archivos la instrucción a quien se quiere que se le envie el archivo, permitiendo que si la PC no era la que se mencionaba en la solicitud de envio se hiciera caso omiso de la solicitud de transferencia de datos.

Esto fue el fundamento de las comunicaciones entre computadoras, conforme estas comunicaciones fueron evolucionando presentando protocolos y conceptos como redes locales (LAN) y redes amplias (WAN).

2.2. Modelo TCP/IP y OSI

El término modelo de redes o arquitectura de red, se refiere a un conjunto organizado de los documentos. Individualmente, estos documentos describen una función necesaria para una pequeña red. Estos documentos pueden definir un protocolo, que es un conjunto de reglas lógicas que los dispositivos deben seguir para comunicarse. Otros documentos pueden definir algunos requisitos físicos para la creación de redes, por ejemplo, puede definir los niveles de voltaje y corriente utilizados en un determinado cable. En conjunto, los documentos referenciados en un modelo de red definen todos los detalles de cómo crear una red de trabajo completa.

Para crear una red de trabajo, los dispositivos de esa red tienen que seguir los detalles de referencia de un modelo de red en particular. Cuando varias computadoras y otros dispositivos de red aplican estos protocolos, especificaciones físicas, normas, y una conexión adecuada de los dispositivos, los equipos pueden comunicarse con éxito.

2.2.1. Arquitectura del protocolo TCP/IP

Este define una gran colección de protocolos que permiten a las computadoras comunicarse. TCP/IP define los detalles de cada uno de estos protocolos dentro de los documentos denominados Solicitudes de *Comments* (*Request For Comments*). Mediante la aplicación de los protocolos necesarios definidos en TCP/IP RFC, un computadora puede estar relativamente seguro de que podrá comunicarse con otros equipos que también cuente con la aplicación del protocolo TCP/IP.

Una fácil comparación puede hacerse entre teléfonos y computadoras que utilizan TCP/IP. Se va a la tienda a comprar un teléfono de uno de una docena de diferentes fabricantes. Cuando llegue a casa y conecte el teléfono al mismo cable en el que estaba conectado el teléfono antiguo, el teléfono nuevo funciona y es reconocido. Los vendedores de teléfonos conocer las normas para los teléfonos y construyen sus teléfonos para que coincida con éstas. Del mismo modo, un equipo que implementa los protocolos de red estándar definido por TCP/IP puede comunicarse con otros equipos que también utilizan los estándares TCP/IP.

Al igual que otras arquitecturas de redes, TCP/IP clasifica los distintos protocolos en diferentes categorías o capas.

Tabla I. **Modelos de arquitectura TCP/IP y ejemplos de protocolos**

Capa de Arquitectura TCP/IP	Ejemplo de protocolo
Aplicación	HTTP, POP3, SMTP
Transporte	TCP, UDP
Internet	IP
Capa de Acceso	Ethernet, Frame Relay

Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide. p. 22.

En la columna 1 se ven las distintas capas de arquitectura del protocolo TCP/IP y en la columna 2 se listan algunos de los protocolos más utilizados a nivel de cada capa. Si alguien construye una nueva aplicación, los protocolos utilizados directamente por la aplicación serían considerados protocolos de capa de aplicación.

Por ejemplo, cuando la World Wide Web (WWW) fue creado, un nuevo protocolo de capa de aplicación fue creada con el propósito de pedir las páginas web y la recepción de los contenidos de las páginas web. Del mismo modo, la capa de acceso a la red incluye los protocolos y estándares, tales como *Ethernet*. Si alguien hace un nuevo tipo de LAN, los protocolos se consideran una parte de la capa de acceso a la red.

2.2.1.1. Capa de aplicación

Los protocolos TCP/IP de la capa de aplicación brinda servicios al software de aplicación que se ejecuta en un computadora. La capa de aplicación no define la aplicación en sí, sino que define los servicios que necesitan las aplicaciones, tales como la capacidad de transferir un archivo en el caso de HTTP. En resumen, la capa de aplicación proporciona una interfaz entre el software que se ejecuta en un computadora y la red misma.

En esta capa se incluyen los procesos que usan los protocolos de la capa de transporte. Hay muchos protocolos de aplicación. La mayor parte proporcionan servicios de usuario y constantemente se añaden nuevos servicios. Algunos de los protocolos más conocidos de esta capa son:

- Telnet: protocolo que permite la conexión remota de terminales.
- FTP: utilizado para efectuar transferencias interactivas de ficheros.
- SMTP: éste es el protocolo que nos permite enviar correo a través de la red.

Estos tres protocolos hacen uso de los servicios orientados a la conexión TCP.

Algunos protocolos que, en cambio, usan los servicios de conexión UDP son:

- DNS: protocolo que traduce en direcciones IP los nombres asignados a los dispositivos de la red.
- NFS: protocolo que permite la compartición de ficheros por distintas máquinas de una red.
- RIP: utilizado por los dispositivos de la red para intercambiar información relativa a las rutas a seguir por los paquetes.

2.2.1.2. Capa de transporte

Los dos protocolos más importantes de esta capa son el TCP y el UDP. El primero se encarga de los servicios de envío de datos con detección y corrección de errores. El UDP proporciona servicios de envío de datagramas sin conexión.

El protocolo UDP proporciona a los programas de aplicación acceso directo al envío de datagramas, parecido al servicio que proporciona el IP. Este permite a las aplicaciones intercambiar mensajes con un mínimo de supervisión por parte del protocolo.

Este protocolo se usa principalmente en:

- Envío de pequeñas cantidades de datos, pues sería más costoso supervisar el establecimiento de conexiones y asegurar un envío fidedigno que retransmitir el conjunto de datos completo.

- Aplicaciones que se ajustan al modelo "pregunta-respuesta". La respuesta se puede usar como una confirmación a la pregunta. Si no se recibe respuesta, en un cierto período de tiempo, la aplicación, simplemente, vuelve a enviar la pregunta.

- Aplicaciones que tienen su propio sistema de verificar que el envío de datos ha sido fidedigno y no requieren este servicio de los protocolos de la capa de transporte.

Las aplicaciones que requieren de la capa de transporte en un servicio de transmisión de datos fidedigno, usan el protocolo TCP. Este protocolo verifica que los datos se envíen a través de la red adecuadamente y en la secuencia apropiada. Las características de este protocolo son:

- Fiabilidad
- Orientado a la conexión y al flujo de datos

Para lograr la fiabilidad, el TCP, se basa en un mecanismo de confirmación positiva con retransmisión (PAR, del inglés, *Positive Acknowledgement with Retransmition*).

Básicamente, este mecanismo consiste en que el emisor envíe los datos una y otra vez, hasta que reciba una confirmación de la llegada de los datos en perfecto estado.

Cada segmento de datos contiene un campo de chequeo que el sistema receptor usa para verificar la integridad de los datos. Para cada segmento recibido correctamente se envía una confirmación. Los segmentos dañados se eliminan. Tras un cierto período de tiempo, el emisor, volverá a enviar todos aquellos segmentos para los que no ha recibido confirmación.

El protocolo TCP es un protocolo orientado a la conexión. Este protocolo establece una conexión entre las dos máquinas que se comunican. Se intercambia información de control antes y después de la transmisión de los datos.

El TCP ve los datos que envía como un flujo continuo de bytes, no como paquetes independientes. Debido a esto, es necesario enviarlos en la secuencia adecuada. El TCP, se cuida de mantener esta secuencia mediante los campos de número de secuencia y número de confirmación de la cabecera de segmento.

En el paso, de información de control, que realiza el TCP, antes de establecer la conexión, se intercambian tres paquetes. Dicho intercambio se denomina "apretón a tres vías".

En el primer segmento, el emisor comunica al receptor, el número inicial de su secuencia. Esto se realiza poniendo este número en el campo número de secuencia de la cabecera del segmento, y activando el bit de sincronización de números de secuencia.

Cuando este segmento llega al receptor este contesta enviando:

- Su propio número inicial de secuencia, en el campo de número de secuencia y activando el bit de sincronización.
- La confirmación de recepción, indicando en el campo de confirmación el número inicial de secuencia del emisor y activando el bit de confirmación.

Cuando este segundo segmento llega al emisor este confirma la recepción del mismo, enviando un tercer segmento con el número de inicio de secuencia del receptor en el campo de número de confirmación y el bit de confirmación activado.

En este momento, el emisor tiene plena conciencia de que la máquina receptora esta operacional y lista para recibir sus datos, así pues se inicia el envío de los mismos.

Según se van recibiendo datos, el receptor irá indicando al emisor la correcta recepción de los mismos. Esto se realiza periódicamente, enviando al emisor un segmento con el bit de confirmación activado y el número de secuencia del último byte recibido correctamente. De esta forma nos evitamos el tener que enviar una confirmación con cada byte recibido.

En el campo de ventana de la cabecera de este mismo segmento se indica el número de bytes que el receptor es capaz de aceptar. Este número indica al emisor que puede continuar enviando segmentos siempre y cuando la longitud en bytes de estos sea inferior al tamaño de la ventana. Un tamaño de ventana cero indicará al emisor que detenga el envío de segmentos hasta recibir un segmento con tamaño de ventana mayor que cero.

Cuando el emisor termina de enviar los datos se establece otro "apretón a tres vías" que difiere del que ha tenido lugar como inicio de la conexión únicamente, en que en vez de llevar activado el bit de sincronización, los segmentos llevarán activado el bit de fin de transmisión de datos.

TCP es también responsable de enviar los datos recibidos a la aplicación correcta. La aplicación a la que se destina los datos está identificada por un número de 16 bits llamado número de puerto. El número de puerto, tanto del origen como del destino, se especifica en la cabecera de cada segmento.

2.2.1.3. Capa de internet

El protocolo más importante de esta capa y piedra base de toda la Internet es el IP. Este protocolo proporciona los servicios básicos de transmisión de paquetes sobre los cuales se construyen todas las redes TCP/IP. Las funciones de este protocolo incluyen:

- Definir del datagrama, que es la unidad básica de transmisión en *Internet*
- Definir el esquema de direccionamiento de *Internet*
- Mover los datos entre la capa de acceso a red y la capa de transporte
- Encauzar los datagramas hacia sistemas remotos. (*Routing*)
- Realizar la fragmentación y re-ensamblaje de los datagramas

El protocolo IP es un "protocolo sin conexión", es decir, no intercambia información de control para establecer una conexión antes de enviar los datos. En caso de que dicha conexión fuese necesaria, el IP delegará tal labor en protocolos de otras capas.

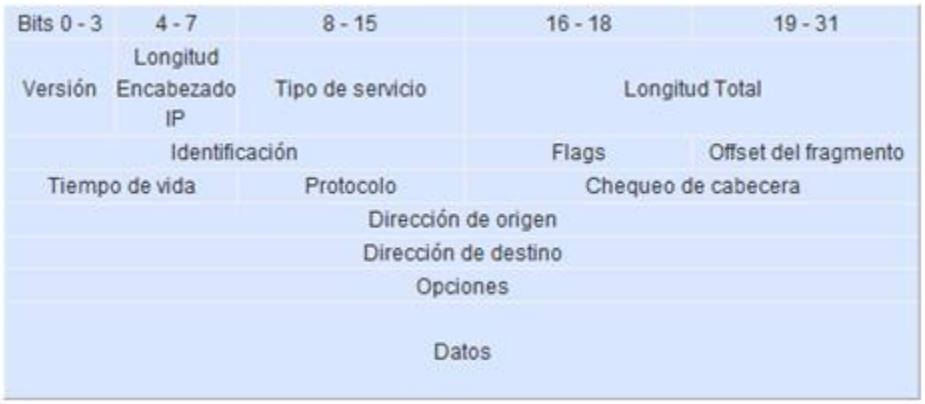
Este protocolo tampoco realiza detección de errores o recuperación de datos ante los mismos.

Los protocolos TCP/IP fueron diseñados para el intercambio de datos en ARPANET, que era una red de intercambio de paquetes. Un paquete es un bloque de datos que lleva consigo la información necesaria para enviarlo. Para aclarar esto podríamos comparar un paquete con una tarjeta postal, en la que no sólo escribimos un mensaje sino que además añadimos los datos pertinentes para que llegue a su destinatario, nombre, dirección, etc.

Una red de intercambio de paquetes usa esta información para cambiar los paquetes de una red a otra moviéndolos hacia su destino final. Cada paquete navega por la red independientemente de cualquier otro paquete.

El datagrama es el formato del paquete que define el IP. Un datagrama consta de dos partes, la cabecera y los datos.

Figura 9. **Estructura de un paquete IPv4**



Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide, p 102.

A la hora de enviar un datagrama, el IP comprueba la dirección de destino. Aquí surgen dos posibilidades:

- Que el destino sea una máquina de la red local. En este caso se envía el datagrama directamente a dicha máquina y listo.

- Que el destino sea una máquina perteneciente a otra red física. En este caso el IP encauzará el datagrama a través de *gateways* hacia su destino. El término inglés de este encauzamiento, normalmente más usado que el español, es *routing*.

Con la segunda posibilidad surge un problema más. Puesto que el datagrama va a atravesar distintas redes físicas, puede darse el caso de que su tamaño no sea adecuado para la transmisión a través de estas redes, pues cada tipo de red define un tamaño máximo para los paquetes que pueden circular por ella.

En este caso, cuando llegue al *gateway*, el IP fragmentará el datagrama en piezas más pequeñas, y a efectos de facilitar su ensamblaje posterior en la cabecera de cada pieza resultante se especificará a que datagrama pertenece y que posición tiene la pieza dentro del datagrama. Para el ensamblaje de las piezas se comprueban estos campos de la cabecera y otro más en el que se indica si hay más fragmentos que ensamblar o no.

Una vez que el datagrama llega a la máquina de destino, y en concreto a la capa de Internet, el IP habrá de enviarlo al protocolo correspondiente de la capa de transporte. Los protocolos de dicha capa tienen asignados unos números que los identifican y que quedan registrados en la cabecera del datagrama.

Otro protocolo definido en la capa de Internet es el ICMP, protocolo de control de mensajes en Internet. Dicho protocolo usa el sistema de envío de mensajes del IP para enviar sus propios mensajes.

Los mensajes enviados por este protocolo realizan las siguientes funciones:

- Control de flujo: cuando los datagramas llegan demasiado rápido a una máquina, de forma que esta no tiene tiempo para procesarlos, el ICMP de dicha máquina enviará al emisor de los datagramas un mensaje para que detenga el envío temporalmente.

- Detección de destinos inalcanzables: cuando no se puede alcanzar la dirección de destino de un datagrama, la máquina que detecta el problema envía a la dirección de origen de ese datagrama un mensaje notificando dicha situación.

- Redirección de rutas: cuando a un *gateway*, le llega un datagrama a enviar a una máquina, y existe otro *gateway* que resulta ser una opción mejor para enviar dicho datagrama, el primer *gateway* envía al emisor un mensaje comunicándole dicha situación para que el envío se haga a través del segundo *gateway*.

- Chequeo de sistemas remotos: una máquina que necesite saber si otra máquina de otra red está conectada y operacional le enviará un mensaje, llamado echo, que la otra máquina devolverá si está conectada y operando. El comando ping de Unix utiliza este protocolo.

2.2.1.4. Capa de acceso

Los protocolos de esta capa proporcionan al sistema los medios para enviar los datos a otros dispositivos conectados a la red. Es en esta capa es donde se define cómo usar la red para enviar un datagrama. Es la única capa de la pila cuyos protocolos deben conocer los detalles de la red física. Este conocimiento es necesario pues son estos protocolos los que han de dar un formato correcto a los datos a transmitir, de acuerdo con las restricciones que nos imponga, físicamente, la red.

Las principales funciones de los protocolos definidos en esta capa son:

- Encapsulación de los datagramas dentro de los marcos a transmitir por la red
- Traducción de las direcciones IP a las direcciones físicas de la red

2.2.2. Arquitectura del protocolo OSI

El modelo de referencia de Interconexión de Sistemas Abiertos (*OSI, Open System Interconnection*) fue el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, fue un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

Siguiendo el esquema de este modelo se crearon numerosos protocolos, por ejemplo X.25, que durante muchos años ocuparon el centro de la escena de las comunicaciones informáticas. El advenimiento de protocolos más flexibles donde las capas no están tan demarcadas y la correspondencia con los niveles

no era tan clara puso a este esquema en un segundo plano. Sin embargo, es muy usado en la enseñanza como una manera de mostrar cómo puede estructurarse una "pila" de protocolos de comunicaciones.

El modelo es considerado una arquitectura de redes, ya que especifíca el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usado como una gran herramienta para la enseñanza de comunicación de redes. Este modelo está dividido en siete capas:

2.2.2.1. Nivel físico (capa 1)

La Capa Física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico (medios guiados: cable coaxial, cable de par trenzado, fibra óptica entre otros tipos de conexión cableada; medios no guiados: radio, infrarrojos, microondas, láser y otras redes inalámbricas); características del medio (p.e. tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etc.) como a la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etc.).

Es la encargada de transmitir los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si ésta es uni o bidireccional (simplex, dúplex o full-dúplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

Se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable) o electromagnéticos (transmisión sin cables). Estos últimos, dependiendo de la frecuencia / longitud de onda de la señal pueden ser ópticos, de micro-ondas o de radio. Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

Sus principales funciones se pueden resumir como:

Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.

Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.

- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas.
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

Codificación de la señal

El nivel físico recibe una trama binaria que debe convertir a una señal eléctrica, electromagnética u otra dependiendo del medio, de tal forma que a pesar de la degradación que pueda sufrir en el medio de transmisión vuelva a ser interpretable correctamente en el receptor.

En el caso más sencillo el medio es directamente digital, como en el caso de las fibras ópticas, dado que por ellas se transmiten pulsos de luz.

Cuando el medio no es digital hay que codificar la señal, en los casos más sencillos la codificación puede ser por pulsos de tensión (PCM o *Pulse Code Modulation*) (por ejemplo 5 V para los "unos" y 0 V para los "ceros"), es lo que se llama codificación unipolar RZ. Otros medios se codifican mediante presencia o ausencia de corriente. En general estas codificaciones son muy simples y no usan bien la capacidad de medio. Cuando se quiere sacar más partido al medio se usan técnicas de modulación más complejas, y suelen ser muy dependientes de las características del medio concreto.

En los casos más complejos, como suelen ser las comunicaciones inalámbricas, se pueden dar modulaciones muy sofisticadas, este es el caso de los estándares Wi-Fi, en el que se utiliza codificación OFDM.

Topología y medios compartidos

Indirectamente, el tipo de conexión que se haga en la capa física puede influir en el diseño de la capa de enlace. Atendiendo al número de equipos que comparten un medio hay dos posibilidades:

- Conexiones punto a punto: que se establecen entre dos equipos y que no admiten ser compartidas por terceros.
- Conexiones multipunto: en la que más de dos equipos pueden usar el medio.

Así por ejemplo la fibra óptica no permite fácilmente conexiones multipunto (sin embargo, véase FDDI) y por el contrario las conexiones inalámbricas son inherentemente multipunto (sin embargo, véanse los enlaces infrarrojos). Hay topologías por ejemplo la topología de anillo, que permiten conectar muchas máquinas a partir de una serie de conexiones punto a punto (Directa entre dos máquinas).

Equipos adicionales

A la hora de diseñar una red hay equipos adicionales que pueden funcionar a nivel físico, se trata de los repetidores, en esencia se trata de equipos que amplifican la señal, pudiéndo también regenerarla. En las redes *Ethernet* con la opción de cableado de par trenzado (la más común hoy por hoy) se emplean unos equipos de interconexión llamados concentradores (repetidores en las redes 10Base-2) más conocidos por su nombre en inglés (hubs) que convierten una topología física en estrella en un bus lógico y que actúan exclusivamente a nivel físico, a diferencia de los conmutadores (switches) que actúan a nivel de enlace.

2.2.2.2. Capa de enlace de datos (capa 2)

Cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores, es decir, un tránsito de datos fiable a través de un enlace físico. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También puede incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Se hace un direccionamiento de los datos en la red ya sea en la distribución adecuada desde un emisor a un receptor, la notificación de errores, de la topología de la red de cualquier tipo. La tarjeta NIC (*Network Interface Card*, Tarjeta de Interfaz de Red en español o Tarjeta de Red) que se encarga de que tengamos conexión, posee una dirección MAC (control de acceso al medio) y la LLC (control de enlace lógico).

Los Switches realizan su función en esta capa siempre y cuando este encendido el nodo.

2.2.2.3. Capa de red (capa 3)

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan en castellano encaminadores, aunque es más frecuente encontrar el nombre inglés *routers* y, en ocasiones enrutadores.

Adicionalmente la capa de red lleva un control de la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red (similar a un atasco en un cruce importante en una ciudad grande). La PDU (Unidad de Datos del Protocolo, por sus siglas en inglés) de la capa 3 es el paquete.

Los routers trabajan en esta capa, aunque pueden actuar como *switch* de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas.

En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

2.2.2.4. Capa de transporte (capa 4)

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación.

Otra característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación. En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes.

Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte. Por ejemplo, la comunicación puede ser manejada para que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío.

Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión finalice. De la explicación del funcionamiento de esta capa se desprende que no está tan encadenada a capas inferiores como en el caso de las capas 1 a 3, sino que el servicio a prestar se determina cada vez que una sesión desea establecer una comunicación. Todo el servicio que presta la capa está gestionado por las cabeceras que agrega al paquete a transmitir.

En resumen, podemos definir a la capa de transporte como:

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que se esté utilizando. La PDU de la capa 4 se llama Segmentos, sus protocolos son TCP y UDP el primero orientado a conexión y el otro sin conexión.

2.2.2.5. Capa de sesión (capa 5)

Esta capa es la que se encarga de mantener y controlar el diálogo establecido entre los dos computadores que están transmitiendo datos de cualquier índole. Ofrece varios servicios que son cruciales para la comunicación, como son:

- Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta).
- Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo).
- Mantener puntos de verificación (*checkpoints*), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio.

Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

En conclusión esta capa es la que se encarga de mantener el enlace entre los dos computadores que estén transmitiendo datos de cualquier índole.

2.2.2.6. Capa de presentación (capa 6)

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras es un traductor.

Por todo ello, se puede resumir esta capa como aquella encargada de manejar la estructura de datos abstracta y realizar las conversiones de representación de los datos necesarios para la correcta interpretación de los mismos.

2.2.2.7. Capa de aplicación (capa 7)

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos

como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "GET index.html HTTP/1.0" para conseguir una página en html, ni lee directamente el código html/xml.

Entre los protocolos (refiriéndose a protocolos genéricos, no a protocolos de la capa de aplicación de OSI) más conocidos destacan:

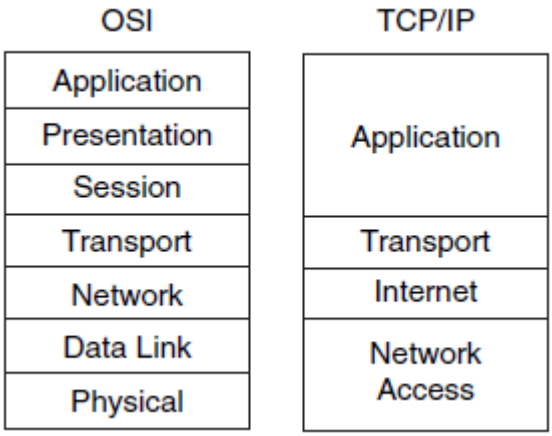
- HTTP (HyperText Transfer Protocol = Protocolo de Transferencia de Hipertexto) el protocolo bajo la www.
- FTP (File Transfer Protocol = Protocolo de Transferencia de Archivos) FTAM fuera de TCP/IP transferencia de ficheros.
- SMTP (Simple Mail Transfer Protocol = Protocolo Simple de Correo) (X.400 fuera de tcp/ip) envío y distribución de correo electrónico.
- POP (Post Office Protocol = Protocolo de Oficina de Correo)/IMAP: reparto de correo al usuario final.
- SSH (Secure Shell = Capa Segura) principalmente terminal remoto, aunque en realidad cifra casi cualquier tipo de transmisión.
- Telnet otro terminal remoto, ha caído en desuso por su inseguridad intrínseca, ya que las claves viajan sin cifrar por la red.

Hay otros protocolos de nivel de aplicación que facilitan el uso y administración de la red:

- SNMP (Simple Network Management Protocol)

- DNS (Domain Name Service)

Figura 10. **Modelos OSI y TCP/IP**



Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide.p. 33.

2.2.3. Fundamentos de redes LAN

Una red de empresa típica consta de varios sitios. Los dispositivos de usuario final conectarse a una LAN, que permite a las computadoras locales para comunicarse unas con otras. Además, cada sitio tiene un router que conecta a la red de área local (LAN) y a rede de área amplia (WAN), con la conectividad proporcionada por la red WAN entre los diferentes lugares. Con los routers y una WAN, las computadoras en diferentes lugares también pueden comunicarse.

2.2.3.1. Redes LAN modernas

El término Ethernet que se refiere a una familia de normas que en conjunto definen las características físicas y capas de enlace de datos del tipo más popular de LAN. Las diferentes normas varían en cuanto a la velocidad soportada, con velocidades de 10 megabits por segundo (Mbps), 100 Mbps y 1000 Mbps. (1 gigabit por segundo, o Gbps) es común en la actualidad.

Las normas también difieren en cuanto a la los tipos de cableado y la longitud permitida de los cables. Por ejemplo, el más comúnmente utilizado estándar de Ethernet permite el uso del cable par trenzado sin blindaje (UTP) de bajo costo, mientras que otras normas utilizan la fibra óptica la cual es más cara.

El cableado de fibra óptica podría valer la pena a pesar del coste en algunos casos, porque el cableado es más seguro y permite distancias mucho mayores entre los dispositivos. Para apoyar las necesidades de una amplia variedad de tipos físicos de LAN muchas variaciones de las normas de Ethernet se han creado.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) ha definido muchos estándares de Ethernet desde que asumió el proceso de normalización de internet en la década de 1980. La mayoría de las normas de definen una variación diferente en la capa física de Ethernet, con diferencias en la velocidad y los tipos de cableado. Además, para la capa de enlace de datos, el IEEE separa las funciones en dos subcapas:

- La Subcapa 802.3 Media Access Control (MAC)
- La Subcapa 802.2 Logical Link Control (LLC)

De hecho, las direcciones MAC reciben su nombre del estándar de la IEEE para esta parte inferior de la capa de enlace de datos de Ethernet.

Cada nuevo estándar de la capa física de la IEEE requiere muchas diferencias en esta capa. Sin embargo, cada una de estas normas de la capa física utiliza exactamente el mismo encabezado de 802,3 y cada uno utiliza la subcapa LLC superior también. La tabla II, enumera los estándares más comúnmente utilizados para la capa física Ethernet por la IEEE.

Tabla II. **Velocidades de protocolos**

Common Name	Speed	Alternative Name	Name of IEEE Standard	Cable Type, Maximum Length
Ethernet	10 Mbps	10BASE-T	IEEE 802.3	Copper, 100 m
Fast Ethernet	100 Mbps	100BASE-TX	IEEE 802.3u	Copper, 100 m
Gigabit Ethernet	1000 Mbps	1000BASE-LX, 1000BASE-SX	IEEE 802.3z	Fiber, 550 m (SX) 5 km (LX)
Gigabit Ethernet	1000 Mbps	1000BASE-T	IEEE 802.3ab	100 m

Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide. p. 46.

La tabla es conveniente para el estudio, pero los términos en la tabla tienen una pequeña explicación. Primero, hay que tener en cuenta que el término red Ethernet se utiliza a menudo en el sentido de "todos los tipos de Ethernet", pero en algunos de los casos se usa para significar "10BASE-T Ethernet." (Debido a que el término de Ethernet a veces puede ser ambiguo.) En segundo lugar, hay que notar que el nombre alternativo para cada tipo de Ethernet lista la velocidad en Mbps, es decir, 10 Mbps, 100 Mbps y 1000 Mbps.

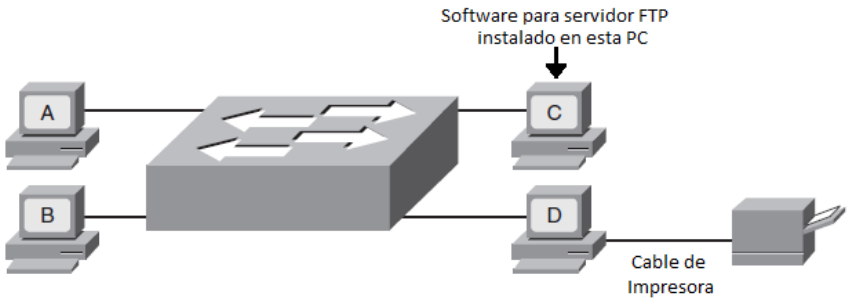
El T y TX en los nombres alternativos se refieren al hecho de que cada una de estas normas define el uso de cableado UTP, con la T se refiere a la T de par trenzado.

Para construir y crear una red LAN moderna, utilizando cualquiera de los UTP basado en los tipos de redes de área local Ethernet enumeradas en la Tabla 1, necesita los siguientes componentes:

- Los equipos deben tener una tarjeta de interfaz de red Ethernet (NIC) instalada.
- Un concentrador Ethernet o *switch* Ethernet.
- Cables UTP para conectar cada PC al concentrador o un conmutador.

La figura 11, muestra una LAN típica. Las NIC no se pueden ver, ya que residen en las PC. Sin embargo, las líneas representan el cableado UTP, y el icono en el centro de la figura representa un conmutador LAN.

Figura 11. **Diagrama de red LAN**



Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide. p. 47.

La mayoría de las personas pueden construir una red LAN como la mostrada en la figura 11, con prácticamente ningún conocimiento real del funcionamiento de las redes LAN. La mayoría de las computadoras contienen una NIC de Ethernet que se instaló en la fábrica. Los Switches no necesitan ser configurados para que se transmita el tráfico entre las computadoras. Todo lo que se tiene que hacer es conectar el cable de alimentación al tomacorriente y conectar por medio de cable UTP cada PC al conmutador. Entonces, las PCs deben de ser capaces de enviar tramas Ethernet de unos a otros.

Se puede utilizar una pequeña LAN para muchos fines, incluso sin una conexión WAN, estas pueden ser tales como:

- Intercambio de archivos: cada equipo puede estar configurado para compartir toda o parte de su sistema de archivos de manera que los otros equipos pueden leer, o, posiblemente, leer y escribir, los archivos en otra computadora. Esta función generalmente es simplemente parte del sistema operativo de la PC.

- Uso compartido de impresoras: las computadoras pueden compartir sus impresoras también. Por ejemplo, las computadoras A, B, y C en la figura 3 puede imprimir documentos en la impresora de la PC D. Esta función también normalmente es parte del sistema operativo de la PC.

- Las transferencias de archivos: una computadora podría instalar un servidor de transferencia de archivos (FTP), permitiendo así que otras computadoras puedan enviar y recibir archivos desde y hacia ese equipo.

- Juegos: el PC puede instalar software de juegos que permite que varios jugadores puedan jugar en el mismo juego.

2.2.3.2. Historia de *ethernet*

Como muchos otros protocolos de red temprana, *Ethernet* empezó su vida dentro de una sociedad que tenía que buscar resolver un problema específico. Xerox necesitaba una forma eficaz para que una nueva invención, llamada la computadora personal, pudiera ser conectada en sus oficinas. Fue así que *Ethernet* nació. Eventualmente Xerox unió fuerzas con Intel y Digital Equipment Corp. (DEC) para juntos desarrollar Ethernet, así el Ethernet original fue conocido como DIX Ethernet, haciendo referencia a DEC, Intel y Xerox.

Estas compañías dierón el trabajo del desarrollo de estándares para Ethernet a la IEEE a principios de 1980's. La IEEE formo dos comités que trabajaron directamente en Ethernet uno fue el comité IEEE 802,3 y el otro fue el comité IEEE 802,2. El comité 802,3 trabajo en los estándares de la capa física como una subparte de la capa de conexión de datos llamada Media Access Control (MAC). La IEEE le asignó a las otras funciones de la capa de conexión de datos al comité 802,2, llamando a esta capa de Logical Link Control (LLC). (El estándar 802,2 aplicado a Ethernet fue también aplicado a otros estándares IEEE para LANs tales como Token Ring.).

2.2.3.3. Cableado UTP

El estándar más utilizado el día de hoy es 10BASE-T (*Ethernet*), 100BASE-TX (Fast *Ethernet*, o FE), y 1000BASE-T (Gigabit *Ethernet,* o GE) usan cable UTP. Algunas diferencias claves existen, particularmente con el número de pares de cables necesarios en cada caso, y en la categoría del cable.

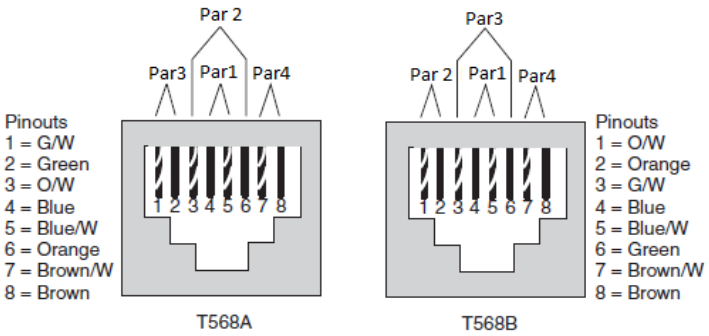
Cable UTP y conectores RJ45

El cableado UTP populares utilizados por las normas de Ethernet incluyen dos o cuatro pares de cables. Debido a que los cables dentro del cable son delgados y frágiles, el propio cable tiene en su exterior un saco de plástico flexible para apoyar los cables. Cada hilo de cobre tienen también un fino revestimiento de plástico para ayudar a evitar que el cable se rompa. El recubrimiento de plástico en cada hilo tiene un color diferente, por lo que es fácil mirar a ambos extremos del cable y de identificar los extremos de un cable individual.

Los extremos del cable suelen tener algún tipo de conector adjunto (normalmente conectores RJ-45), con los extremos de los cables insertados en los conectores. El conector RJ-45 tiene ocho ubicaciones específicas en las que los ocho hilos del cable se pueden insertar, llamado posiciones PIN, o simplemente alfileres. Cuando los conectores se agregan al final del cable, los extremos de los cables deben estar correctamente insertados en la posición correcta de pines.

Los diferentes estándares para los conectores son la TIA (*Telecomunications Industry Association)* y la EIA (*Electronics Industry Alliance*), definen los estándares para cables UTP por medio de código de colores para los hilos del cable como muestra la figura 12.

Figura 12. **Configuración RJ45**



Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide. p. 55.

2.2.4. Fundamentos de redes WAN

Las capas OSI físicas y de enlace de datos trabajan juntas para entregar los datos a través de una amplia variedad de tipos de redes físicas. Estándares de LAN y de protocolos definen el modo en que los diferentes equipos en una red se relacionan y trabajan en conjunto todo esto en una infraestructura relativamente cercana, por lo tanto, el término área-local en el acrónimo LAN. Las normas y protocolos WAN definir la manera en que redes entre los dispositivos que están relativamente lejos se interconectan, en algunos casos, incluso miles de área de millas de distancia, es de ahí el término amplia-área es utilizada para el acrónimo WAN.

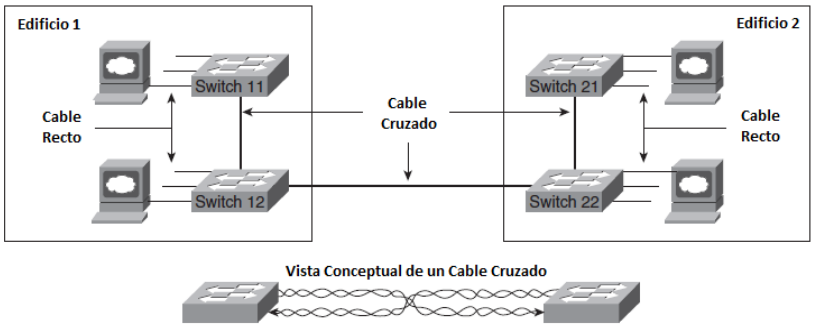
2.2.4.1. Capa 1 del modelo OSI para punto – punto WANs

La capa de OSI física, o la capa 1, define los detalles de cómo mover datos de un dispositivo a otro. De hecho, mucha gente piensa en la capa OSI 1 como "el envío de bits". Capas superiores encapsulan los datos, tal como se describió anteriormente. No importa lo que las otras capas OSI hagan, finalmente, el remitente de la información necesita transmitir los bits a otro equipo. La capa física del modelo OSI define las normas y los protocolos utilizados para crear la red física y así enviar los bits a través de esa red.

Una WAN punto a punto funciona como una troncal de *Ethernet* entre dos switches *Ethernet* de muchas maneras. Para verlo en perspectiva, veamos la figura 2.6, esta muestra una LAN con dos edificios y dos switches en cada edificio. Como una breve reseña, se debe recordar que varias tipos de *Ethernet* utilizan un par trenzado de cables para transmitir y otro par trenzado de recibir, a fin de reducir la interferencia electromagnética.

Normalmente, se utilizan cables rectos para conectar los dispositivos del usuario final y los switches. Para los enlaces troncales entre los switches se utilizan cables cruzados, ya que cada *switch* transmite en el mismo par de pins en el conector, por lo que el cable cruzado conecta un dispositivo de transmisión con el otro dispositivo de recepción. La parte inferior de la figura 13, muestra la idea básica detrás de un cable cruzado.

Figura 13. **Diagrama de pares cruzados en los routers**



Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide. p. 75.

Ahora imaginemos que los edificios están separados por más de 1000 Km. de distancia en lugar de uno al lado del otro. Inmediatamente se presentan dos problemas:

- Ethernet no es compatible con cualquier tipo de cableado que permita a un individuo ejecutar una troncal de 1000 Km. de distancia.
- Aunque Ethernet soporta una troncal de 1000 Km., no siempre se tienen los permisos necesarios para tender un cable de 100 Km. entre ambos edificios.

La gran diferencia entre LAN y WAN se refiere a cuán lejos los dispositivos pueden estar y aun así ser capaces de enviar y recibir datos entre ellos. Las redes LAN tienden a residir en un solo edificio o posiblemente, entre los edificios en un campus, por medio de cableado óptico aprobado para Ethernet. Las redes WAN suelen recorrer distancias más lejanas que las abarcadas por las redes LAN.

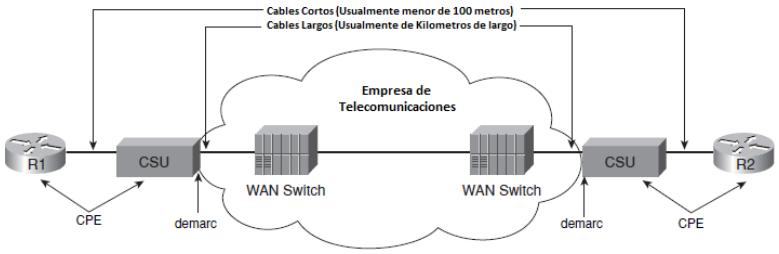
Para crear tales vínculos de larga duración de los circuitos, el cableado físico real es propiedad, instalado y administrado por una empresa que tiene el derecho de vía para tender cables en las calles. Debido a que una empresa se necesita para enviar datos a través del circuito de la WAN se le llama línea alquilada al canal de comunicación que brinda el proveedor para la comunicación entre las distintas LANs.

2.2.4.2. Conexiones WAN para la percepción del usuario

Los conceptos detrás de una conexión punto-a-punto son simples. En la figura 13, se asume que una WAN arrendada está formada gracias a la interconexión del proveedor, el cual brinda de cara a las LANs un par de cables trenzados para interconexión de ambas redes LAN a través de su red, para esto muchas tecnologías subyacentes deben de ser utilizadas para crear el circuito, y las empresas de telecomunicaciones utilizan una gran cantidad de la terminología que es diferente de la terminología de LAN.

La compañía telefónica rara vez realmente ejecuta la instalación de un cable de 1000 Km. de longitud. En su lugar, se construyen una amplia red e incluso corre cables extra de la oficina central local (CO) a su construcción (CO es sólo un edificio donde se localizan los dispositivos utilizados para crear su propia red). La figura 14, presenta algunos de los conceptos y términos clave relativos a los circuitos WAN.

Figura 14. **Diagrama de conexiones WAN**



Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide. p. 77.

Normalmente, los enrutadores se conectan a un dispositivo llamado unidad de servicio externo de canal / datos de servicio Unidad (CSU / DSU por sus siglas en inglés). El router se conecta a la CSU / DSU con un cable relativamente corto, típicamente menos de 50 pies de largo, porque el DSUs / CSU generalmente se instalan en un estante, cerca del router. Eso cables salen del edificio, corriendo a través del posteado instalado previamente por la empresa, esta puede ser también por subterráneo dependiendo de la infraestructura con que cuente la empresa.

La misma conexión física general existe en cada lado de la de punto a punto de enlace WAN.

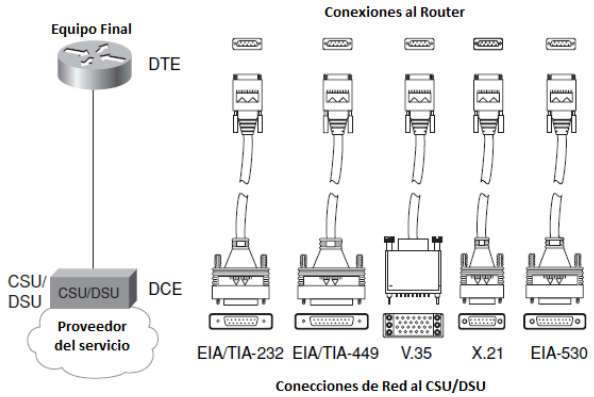
Normalmente, se le pide a la Empresa de Telecomunicaciones que el cable que ha de instalar y por el cual brinda está el servicio contratado lo haga en una sala especial, la mayoría, si no todas, las líneas de las telecomunicaciones terminar en la misma habitación. El término *Customer Premises Equipment* (CPE) se refiere a los dispositivos que se encuentran en el sitio del cliente.

2.2.4.3. Estándares de cableado para WAN

Cisco ofrece una gran variedad de diferentes tarjetas de interfaz WAN para sus routers, incluidas las interfaces en serie síncrona y asíncrona. Para cualquiera de los enlaces de punto a punto seriales o enlaces *Frame Relay*, el router utiliza una interfaz que soporta comunicación síncrona.

En los routers Cisco se utilizan una variedad de interfaces síncronas física de diferentes propiedades y tipos de conectores, como el 60-pin D-Connector Shell que se muestra en la parte superior del cable de dibujos en la figura 2.8. El cable que conecta el router a la CSU / DSU utiliza un conector que se adapte a la interfaz en serie router en el lado del router y un tipo de conector WAN estándar que coincide con la CSU / DSU en la interfaz de la CSU / DSU final del cable. La figura 15 muestra una conexión típica, con algunas de las opciones de cableado de serie de la lista.

Figura 15. **Tipos de interfaces físicas**



Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide. p. 79.

El ingeniero que despliega una red elige el cable sobre la base de los conectores de la router y la CSU / DSU. Más allá de esa elección, los ingenieros no necesitamos pensar en cómo los cables y pines funcionan. Muchos de los pernos se utilizan para el control de funciones, y algunos se utilizan para la transmisión de datos. Algunos pernos se utilizan para reloj, como se describe en la siguiente sección.

El cable entre la CSU / DSU y el de telecomunicaciones CO normalmente utiliza un conector RJ-48 para conectarse a la CSU / DSU, el conector RJ-48 tiene el mismo tamaño y forma que el conector RJ-45, conector utilizado para los cables de Ethernet. Muchos routers Cisco soportan interfaces seriales que tienen un interior CSU / DSU integrado. Con un interior CSU / DSU, el router no necesita un cable de conexión a una dirección externa CSU / DSU, porque la CSU / DSU es interna al router.

2.2.5. Fundamentos de direccionamiento IP y ruteo

RFC 791 define el protocolo IP, incluyendo varias clases diferentes de redes. IP define tres clases diferentes de direcciones de red utilizados por los diferentes equipos, direcciones llamadas direcciones IP de unidifusión. Estas tres clases de red se denominan A, B y C, además de estas 3 clases TCP/IP define la Clase D (*multicast*) y las direcciones de clase E (experimental) también.

Por definición, todas las direcciones en la misma clase A, B, C o de la red tienen el mismo valor numérico de parte de red de las direcciones. El resto de la dirección se llama la parte del host de la dirección.

Usando como ejemplo una oficina de correos, la parte de red de una dirección IP actúa como el *zip* (código postal), y la parte del equipo actúa como la dirección de la calle. Así como una máquina de clasificación de cartas distante sólo se preocupa por el código postal de una carta dirigida a usted, un router igual de distante que la máquina clasificadora de cartas sólo se preocupa por el número de red en la cual su dirección reside o pertenece.

Las redes clase A, B y C tienen una longitud diferente para la parte que identifica la red:

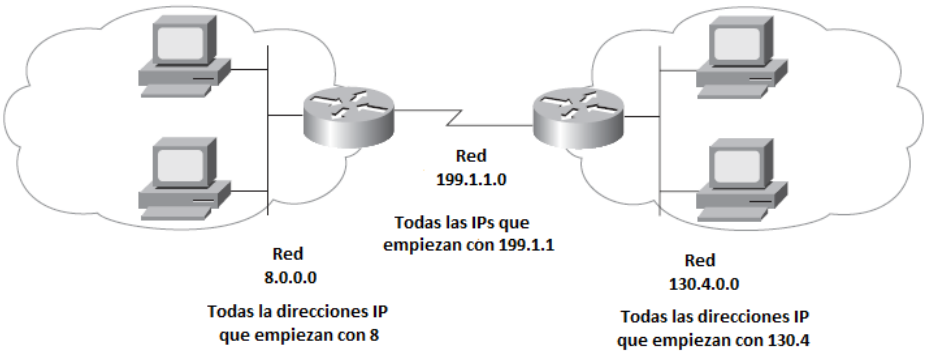
- Las redes de clase A tienen una longitud de 1 byte para la parte de la red. Eso deja a 3 bytes para el resto de la dirección, llamada también la parte del host.

- Las redes de clase B tienen una longitud de 2 bytes para la parte de la red, dejando 2 bytes para la parte del host de la dirección.

- Las redes de clase C tienen una parte de red de 3 bytes de longitud, dejando sólo 1 byte para la parte del host.

Por ejemplo, para la figura 16, la rede *Ethernet* 8.0.0.0 de la izquierda es una red de clase A, lo que significa que sólo 1 octeto (byte) se utiliza para la red parte de la dirección. Así, todos los hosts en la red 8.0.0.0 comienzan con 8. Del mismo modo, la red de clase B 130.4.0.0 se muestra junto a la red *Ethernet* a la derecha. Debido a que es una red de clase B, 2 octetos definen la parte de red, y todas las direcciones comienzan con 130,4 en los primeros 2 octetos.

Figura 16. **Red LAN de muestra**



Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide. p. 106.

Cuando se enumeran los números de red, la convención es escribir la parte de red de la serie, con todos los decimales ceros en la parte del equipo de la serie. Así, la red de clase A "8", que consiste en todas las direcciones IP que comienzan con 8, se escribe como 8.0.0.0. Del mismo modo, la red de clase B "130,4" que consiste en todas las direcciones IP que comienzan con 130,4, se escribe como 130.4.0.0, y así sucesivamente.

Ahora considere el tamaño de cada clase de red. Redes de clase A necesita 1 byte para la parte de red, dejando 3 bytes, o 24 bits, para la parte del host. Hay 224 diferentes valores posibles en la acogida de parte de las direcciones IP clase A. Así, cada red de clase A puede tener 224 direcciones IP distintas, excepto para dos direcciones de host reservados en cada red, como se muestra en la última columna de la tabla III, La tabla resume las características de la clase A, B, C y redes.

Tabla III. **Características de distintos tipos de redes**

Cualquier red de esta clase	Número de red Bytes(bits)	Número de Hosts Bytes (bits)	Número de direcciones por Red
A	1(8)	3(24)	2^{24} - 2
B	2(16)	2(16)	2^{16} - 2
C	3(24)	1(8)	2^{8} -2

Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide. P. 108.

La tabla IV, proporciona una mirada más cercana a la versión numérica de los tres números de red: 8.0.0.0, 130.4.0.0 y 199.1.1.0.

Tabla IV. **Ejemplo de redes**

Número de Red	Representación Binaria, con la parte de Host en Negrita
8.0.0.0	00001000 **00000000 00000000 00000000**
130.4.0.0	10000010 00000100 **00000000 00000000**
199.1.1.0	11000111 00000001 00000001 **00000000**

Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide. P. 109.

A pesar de que los números de red parecen direcciones debido a su formato de decimales con puntos, los números de red no pueden ser asignados a una interfaz que se utilizará como una dirección IP. Conceptualmente, los números de red representan el grupo de todas las direcciones IP en la red, similar a un código postal representa el grupo de todas las direcciones en una

comunidad. Sería confuso tener un solo número representando todo un grupo de direcciones, utilizaremos el mismo número como una dirección IP para un único dispositivo.

Además el número de red, un segundo valor decimal con puntos en cada red está reservada. Tenga en cuenta que el valor reservado en primer lugar, el número de red, tiene todos los números ceros binarios en la parte del equipo. El otro valor reservado es el que tiene todos los números unos binarios en el huésped. Este número se llama la emisión de la red de difusión o broadcast. Este número reservado no se puede asignar a un host para su uso como una dirección IP.

Sin embargo, los paquetes enviados a una dirección de broadcast se envían a todos los dispositivos en la red. Además, como el número de red es el más bajo valor numérico dentro de esa red y la dirección de difusión es el valor numérico más alto, todos los números entre la red número y la dirección de difusión son las direcciones válidas, útiles de propiedad intelectual que se puede utilizar para interfaces de dirección en la red.

IP routing

Armado con un mayor conocimiento de las direcciones IP, ahora se puede echar un vistazo más de cerca el proceso de enrutamiento IP. Esta explicación se centra en cómo el host de origen elige dónde enviar el paquete, así como la forma en que los routers seleccionan el lugar a rutear o envío de paquetes a su destino final.

Enrutamiento de host

Los hosts usan realmente una lógica simple de enrutamiento a la hora de elegir a dónde enviar un paquete. Está lógica en dos fases las cuales son como sigue:

Paso 1

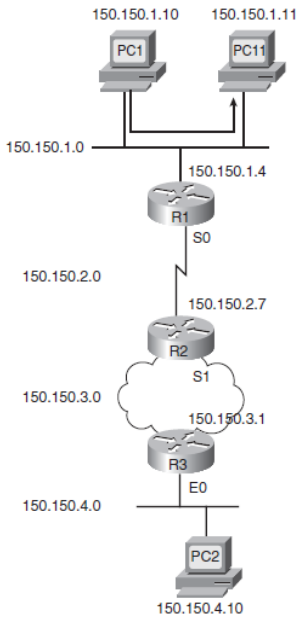
Si la dirección IP de destino está en la misma red en la que se encuentra el host emisor, envía el paquete directamente al host destinatario.

Paso 2

Si la dirección IP de destino no está en la misma red en la que se encuentra el host emisor, envía el paquete al default *Gateway* (un router o una interface Ethernet de la red).

Por ejemplo, considere la figura 17, vea la LAN en la parte de arriba de la figura. Esta tiene 2 PCs, nombradas como PC1 y PC11, además un router R1. Cuando la PC1 envía un paquete a la PC con dirección IP 150.150.1.11 (dirección IP de la PC11), la PC1 envía el paquete sobre la LAN Ethernet a la PC11, no hay necesidad de consultar al router.

Figura 17. **Red de ruteo**



Fuente: CCENT/CCNA ICND1 Official Exam Certification Guide. p. 115.

En el caso en que PC1 envié un paquete a la PC2 (150.150.4.10), la PC1 envía el paquete a su default *Gateway* 150.150.1.4, la cual es la interface del router R1, de esta manera es como se logra que siguiendo los saltos o rutas que contengan los routers involucrados en el camino hasta la PC2 hasta que se logra llegar al equipo deseado.

2.2.6. Fundamentos de transporte TCP/IP, aplicaciones TCP/IP y seguridad TCP/IP

Los protocolos de transporte son 2 TCP y UDP los cuales tienen diferentes funciones y aplicaciones en la comunicación entre 2 equipos.

TCP

Es un protocolo de comunicación orientado a conexión y fiable del nivel de transporte, actualmente documentado por IETF en el RFC 793. Es un protocolo de capa 4 según el modelo OSI, es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn.

Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP, SSH y FTP.

En la pila de protocolos TCP/IP, TCP es la capa intermedia entre el protocolo de internet (IP) y la aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe libre de errores, sin pérdidas y con seguridad.

Los servicios provistos por TCP corren en el anfitrión (host) de cualquiera de los extremos de una conexión, no en la red. Por lo tanto, TCP es un protocolo para manejar conexiones de extremo a extremo. Tales conexiones pueden existir a través de una serie de conexiones punto a punto, por lo que estas conexiones extremo-extremo son llamadas circuitos virtuales. Las características del TCP son:

- Orientado a la conexión: dos computadoras establecen una conexión para intercambiar datos. Los sistemas de los extremos se sincronizan con el otro para manejar el flujo de paquetes y adaptarse a la congestión de la red.

- Operación Full-Duplex: una conexión TCP es un par de circuitos virtuales, cada uno en una dirección. Sólo los dos sistemas finales sincronizados pueden usar la conexión.

- Error Checking: una técnica de checksum es usada para verificar que los paquetes no estén corruptos.

- *Acknowledgements*: sobre recibo de uno o más paquetes, el receptor regresa un *acknowledgement* (reconocimiento) al transmisor indicando que recibió los paquetes. Si los paquetes no son notificados, el transmisor puede reenviar los paquetes o terminar la conexión si el transmisor cree que el receptor no está más en la conexión.

- Control de flujo: si el transmisor está desbordando el buffer del receptor por transmitir demasiado rápido, el receptor descarta paquetes. Los *acknowledgement* fallidos que llegan al transmisor le alertan para bajar la tasa de transferencia o dejar de transmitir.

- Servicio de recuperación de Paquetes: el receptor puede pedir la retransmisión de un paquete. Si el paquete no es notificado como recibido (ACK), el transmisor envía de nuevo el paquete.

Los servicios confiables de entrega de datos son críticos para aplicaciones tales como transferencias de archivos (FTP por ejemplo), servicios de bases de datos, proceso de transacciones y otras aplicaciones de misión crítica en las cuales la entrega de cada paquete debe ser garantizada.

UDP

User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

Aplicaciones TCP/IP

- *Hypertext Transfer Protocol* o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la *World Wide Web*. HTTP fue desarrollado por el *World Wide Web Consortium* y la *Internet Engineering Task Force,* colaboración que culminó en 1999 con la publicación de una serie de RFC, siendo el más importante de ellos el RFC 2616, que especifica la versión 1.1. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse.

  Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador web o un spider) se lo conoce como "*user agent*" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos (URL). Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

  HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

- *Domain Name System* (o DNS, en español: sistema de nombre de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado al internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignados a cada uno de los participantes. Su función más importante, es traducir (*resolver*) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El DNS es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.mx es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.mx y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet. En un inicio, SRI (ahora SRI *International*) alojaba un archivo llamado *HOSTS* que contenía todos los nombres de dominio conocidos (técnicamente, este archivo aún existe - la mayoría de los sistemas operativos actuales todavía pueden ser configurados

para revisar su archivo hosts). El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo hosts no resultara práctico y en 1983, Paul Mockapetris publicó los RFCs 882 y 883 definiendo lo que hoy en día ha evolucionado hacia el DNS moderno. (Estos RFCs han quedado obsoletos por la publicación en 1987 de los RFCs 1034 y 1035).

Seguridad de redes

Años atrás, las amenazas de seguridad provienen de genios o estudiantes con mucho tiempo libre. El número de estas personas fueron relativamente pequeñas. Su motivación principal era demostrar que podría entrar en otra red. Desde entonces, el número de atacantes potenciales y la sofisticación de los ataques se han incrementado de manera exponencial.

Los ataques que antes requerían que los atacantes tuvieran un grado avanzado de conocimientos sobre informática ahora se pueden hacer con la facilidad de herramientas disponibles libremente descargándolas, y que hasta un estudiante promedio de secundaria puede descifrar cómo utilizar. Cada empresa y casi cada persona se conectan a Internet, lo que hace básicamente a todo el mundo vulnerable a los ataques.

El mayor peligro hoy en día pueden ser los cambios en la motivación de los atacantes. En vez de mirar para un desafío, o para robar millones, los atacantes de hoy pueden ser mucho más organizados y motivados. La delincuencia organizada intenta robar miles de millones para extorsionar a las empresas con la amenaza de una denegación de servicio (DoS) en los servidores del web público de las empresas. O robar la identidad y la información de la tarjeta de crédito para a veces robar a cientos de miles de personas con un sofisticado ataque.

Los ataques podrían provenir de los estados-nación o terroristas. No sólo podrían atacar organismos militares y gubernamentales, también podrían tratar de perturbar la infraestructura de servicios para empresas de servicios públicos y el transporte y las economías lisiadas.

3. MICROCONTROLADORES

3.1. Introducción a los microcontroladores

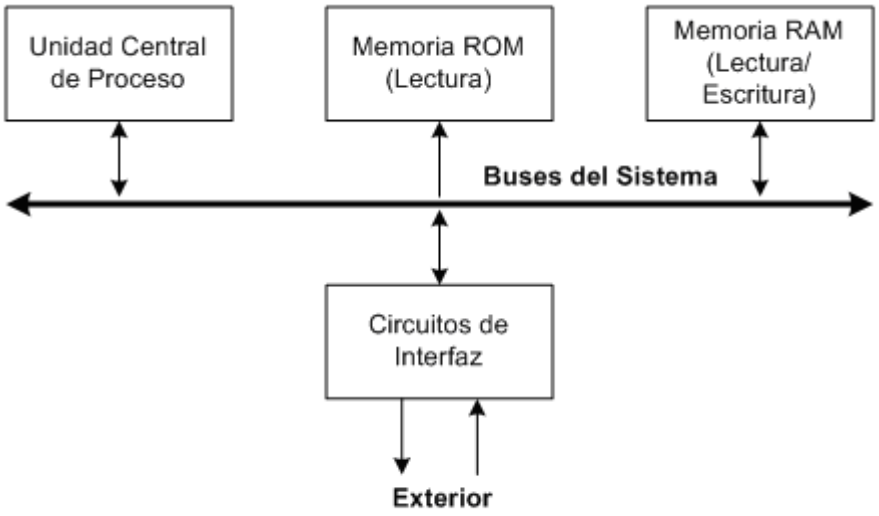
Desde la invención del circuito integrado, el desarrollo constante de la electrónica digital ha dado lugar a dispositivos cada vez más complejos. Entre ellos están los microcontroladores los cuales son circuitos integrados o chips que incluye en su interior las tres unidades funcionales de una computadora: unidad central de procesamiento, memoria y unidades de E/S (entrada/salida).

En el mercado existe una gran diversidad de microcontroladores. Una de las clasificaciones más importantes que se encuentran, se fundamenta en la capacidad que tienen los microcontroladores de manejar palabras de 4, 8, 16 ó 32 bits simultáneamente. Aunque las prestaciones de los microcontroladores de 16 y 32 bits son superiores a los de 4 y 8 bits, la realidad es que los microcontroladores de 8 bits dominan el mercado.

La razón de esta tendencia, es que los microcontroladores de 4 y 8 bits son apropiados para la gran mayoría de aplicaciones, lo que hace innecesario emplear microcontroladores más robustos y consecuentemente más caros.

Antes de ver que es un microcontrolador y analizar sus ventajas y desventajas, es útil hacer un repaso relacionado con la estructura de cualquier sistema programable que pueda hacer uso de un microcontrolador.

Figura 18. **Esquema general de un sistema programable**



Fuente: http:// www.abcdatos.com/tutoriales/tutorial/l9745.html.

La figura 18, representa el esquema general de cualquier sistema programable. Los elementos necesarios para su funcionamiento son los siguientes:

- La unidad central de proceso
- La memoria ROM del inglés *Read Only Memory* (sólo lectura)
- La memoria RAM del inglés *Random Access Memory* (lectura y escritura)
- Los circuitos de Interfaz
- Los buses de interconexión

La presencia de estos elementos básicos es indispensable y aun cuando no se representen tan claramente como en la figura 18, siempre existen.

La unidad central de proceso generalmente está constituida por un microprocesador, ésta ejecuta el programa que da vida a la aplicación. Los programas pueden ser muy diversos, puesto que, como es evidente, el que asegura la gestión de un termostato inteligente no tiene nada que ver con el que controla el correcto funcionamiento de una fotocopiadora. Sin embargo, éstos programas tienen en común el hecho de que muy raramente necesitan cálculos complejos y, en cambio, sí suelen incluir numerosas manipulaciones de la información de entrada y salida.

El programa se almacena en un segundo elemento, que es la memoria ROM. Esta memoria puede constituirse de diferentes formas: EPROM del inglés *Erasable Programmable Read Only Memory*, EEPROM del inglés *Electrically Erasable Programmable Read-Only Memory* y memoria flash. Cualquiera que sea la que se utilice es una memoria no volátil desde la que se ejecutará el programa una vez alimentado el sistema.

Para poder trabajar correctamente, el microprocesador necesita, a menudo, almacenar datos temporales en alguna parte, y aquí es donde interviene la memoria RAM. La memoria RAM es de lectura y escritura y no necesita ser de grandes dimensiones.

El último elemento y que generalmente, es el más importante en una aplicación susceptible de utilizar un microcontrolador es todo lo concerniente a los circuitos de interfaz con el mundo exterior, esta interfaz relacionará al microprocesador con elementos tan dispares como un motor paso a paso, una pantalla de cristal líquido o una botonera hexadecimal.

Lo que se pretende es hacerse de las herramientas necesarias para poder efectuar posteriormente el diseño e implementación del sistema de

monitorización de temperatura y suministro eléctrico en un nodo, para ello, a continuación se definen los conceptos básicos de los microcontroladores.

3.1.1. Diferencias entre controlador, microcontrolador y microprocesador

Un controlador es un dispositivo que se emplea para el gobierno de uno o varios procesos. Por ejemplo, el controlador que regula el funcionamiento de un horno eléctrico dispone de un sensor que mide constantemente su temperatura interna y actúa sobre las resistencias para mantener la temperatura dentro del rango establecido.

Aunque el concepto de controlador ha permanecido invariable a través del tiempo, su implementación física ha variado frecuentemente. Hace tres décadas, los controladores electrónicos se construían exclusivamente con componentes de lógica discreta, posteriormente se emplearon los microprocesadores que se rodeaban de integrados de memoria y puertos de entrada y salida sobre una tarjeta de circuito impreso. En la actualidad, todos los elementos del controlador se han podido incluir en un solo circuito integrado, conociéndose a este concepto con el nombre de microcontrolador.

Por lo tanto, un microcontrolador es un circuito integrado de alta escala de integración, que incorpora la mayor parte de los elementos que configuran un controlador y que contiene todos los componentes fundamentales de una computadora, aunque de limitadas prestaciones.

Finalmente, la diferencia entre un microprocesador y un microcontrolador radica en que un microprocesador es simplemente un elemento del

microcontrolador, formando lo que se conoce como la Unidad Central de Proceso (CPU del inglés *Central Process Unit*) que a su vez se divide en, la unidad de control, la unidad aritmética-lógica, los registros y dependiendo del procesador, la unidad de coma flotante.

3.2. Estructura del microcontrolador

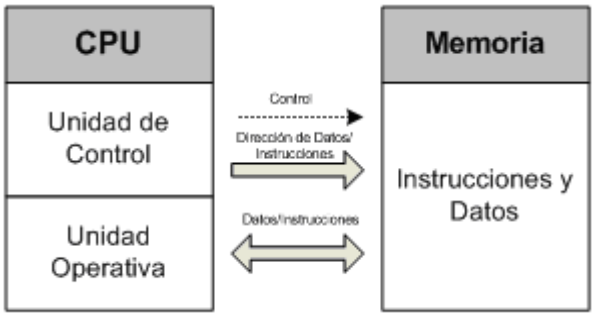
Al estar los microcontroladores en un solo circuito integrado, su estructura fundamental y sus características básicas son muy parecidas. Todos disponen de procesador, memoria de datos, memoria de instrucciones, líneas de entrada y salida, oscilador de reloj y módulos controladores de periféricos. Sin embargo, cada fabricante intenta enfatizar los recursos más idóneos para las aplicaciones a las que se destinan preferentemente.

En este apartado se hace un recorrido de todos los elementos que se hallan en la mayoría de los microcontroladores, además de hacer énfasis en las características especiales del microcontrolador 16F877 utilizado en la etapa de diseño e implementación.

Existen dos tipos de arquitecturas, la arquitectura Harvard y la arquitectura Von Neumann. Inicialmente todos los microcontroladores adoptaron la arquitectura clásica de Von Neumann, pero en el presente se impone la arquitectura Harvard.

La arquitectura de Von Neumann se caracteriza por disponer de una sola memoria principal donde se almacenan datos e instrucciones de forma indistinta. A dicha memoria se accede a través de un sistema de buses único (direcciones, datos y control).

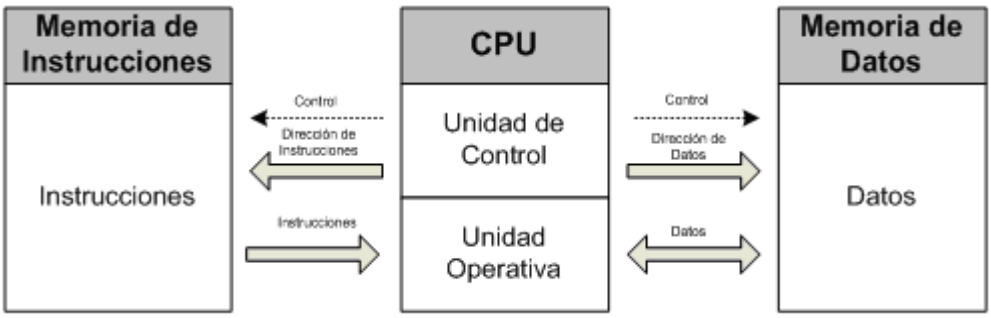
Figura 19. **Arquitectura Von Neumann de un microcontrolador**



Fuente: http://www.unicrom.com/Tut_arquitectura_microcontrolador.asp.
21 abril 2010

Por otro lado, la arquitectura Harvard dispone de dos memorias independientes entre sí, una que contiene sólo instrucciones y otra, sólo datos. Ambas disponen de sus respectivos sistemas de buses de acceso, permitiendo de esta manera la realización de accesos (lectura o escritura) simultáneos en ambas memorias. Los microcontroladores utilizados en la solución responden a la arquitectura Harvard.

Figura 20. Arquitectura Harvard de un microcontrolador



Fuente: http://www.unicrom.com/Tut_arquitectura_microcontrolador.asp.
21 abril 2010

3.3. Elementos del microprocesador

Los microprocesadores están construidos con diferentes arquitecturas las cuales tienen sus diferentes ventajas una sobre la otra según se ha visto anteriormente, sin embargo estos poseen elementos que los componen en forma general independiente del tipo de arquitectura que se tenga, de estos elementos hablaremos en el siguiente apartado.

3.3.1. Unidad central de proceso

Es el elemento más importante del microcontrolador y determina sus principales características, tanto a nivel de *hardware* como de *software*.

La unidad central de proceso se encarga de direccionar la memoria de instrucciones, recibir el código de operación de la instrucción en curso, su decodificación y la ejecución de la operación que implica la instrucción, así como el almacenamiento del resultado.

Existen tres orientaciones en cuanto a la arquitectura y funcionalidad de los procesadores actuales.

3.3.1.1. Computadores con juego de instrucciones complejo

Estos procesadores disponen de más de 80 instrucciones en su repertorio de programación, estas ofrecen al programador muchas más herramientas de manejo y procesamiento de información, pero tienen el inconveniente que debido a la complejidad de algunas instrucciones, el procesador requiere de muchos ciclos de reloj para poder ejecutar las operaciones. Generalmente a esta filosofía se le refiere como CISC del inglés *Complex Instruction Set Computer.*

3.3.1.2. Computadores con juego de instrucciones reducido

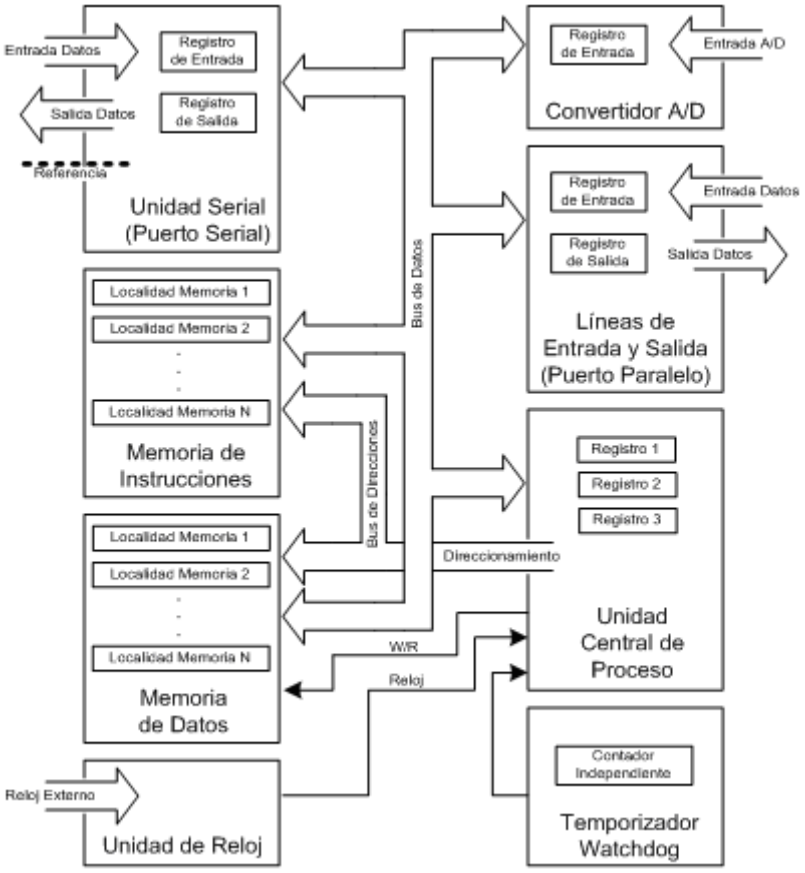
Tanto la industria de los computadores comerciales como la de los microcontroladores están migrando hacia la filosofía RISC del inglés *Reduced Instruction Set Computer*. En estos procesadores el repertorio de instrucciones es muy reducido y las instrucciones son simples y generalmente se ejecutan en un solo ciclo de reloj.

La sencillez y rapidez de las instrucciones permiten optimizar el *hardware* y el *software* del procesador. El microcontrolador utilizado en la solución responde a la filosofía RISC.

3.3.1.3. Computadores con juego de instrucciones específico

En los microcontroladores destinados a aplicaciones muy concretas, el juego de instrucciones, además de ser reducido, es específico, esto quiere decir, que las instrucciones se adaptan a las necesidades de la aplicación prevista. Esta filosofía se ha referido con el nombre de SISC del inglés *Specific Instruction Set Computer*.

Figura 21. **Arquitectura de un microcontrolador**



Fuente: diseño e implementación de un sistema generador de mensajes en una red de telemedida, ante fallas del suministro de energía eléctrica. p. 30.

3.3.2. Memoria

En los microcontroladores la memoria de instrucciones y datos está integrada en el mismo chip. Una parte debe ser no volátil (tipo ROM), y se destina a contener el programa de instrucciones que gobierna la aplicación.

Otra parte de memoria es volátil (tipo RAM), y se destina a guardar las variables y los datos.

La memoria RAM en estos dispositivos es de poca capacidad pues sólo debe contener las variables y los cambios de información que se produzcan en el transcurso del programa. Por otra parte, como sólo existe un programa activo, no se requiere guardar una copia del mismo en la memoria RAM pues se ejecuta directamente desde la memoria ROM.

Según el tipo de memoria ROM que dispongan los microcontroladores, la aplicación y utilización de los mismos es diferente. A continuación se describen las cinco versiones de memoria no volátil que se pueden encontrar en los microcontroladores del mercado.

3.3.2.1. Memoria ROM con máscara

Es una memoria no volátil de sólo lectura cuyo contenido se graba durante la fabricación del integrado. El elevado coste del diseño de la máscara sólo hace aconsejable el empleo de los microcontroladores con este tipo de memoria, cuando se precisan cantidades superiores a varios miles de unidades.

3.3.2.2. Memoria OTP

La memoria OTP del inglés *One Time Programmable*, permite al usuario cargar el código del programa una sola vez en la memoria del microcontrolador. La versión OTP es recomendable cuando es muy corto el ciclo de diseño del producto, o bien, en la construcción de prototipos y series muy pequeñas.

Tanto en este tipo de memoria como en la memoria EPROM, se suele usar la encriptación mediante fusibles para proteger el código contenido.

3.3.2.3. Memoria EPROM

Los microcontroladores que disponen de memoria EPROM pueden borrarse y grabarse muchas veces. La grabación se realiza, como en el caso de las memorias OTP, con un grabador gobernado desde una computadora. Si posteriormente se desea borrar el contenido, estos disponen de una ventana de cristal en su superficie por la que se somete a radiación ultravioleta durante varios minutos hasta lograr el borrado.

Las cápsulas son de material cerámico y son más caros que los microcontroladores con memoria OTP que están hechos con material plástico.

3.3.2.4. Memoria EEPROM

Se trata de memorias de sólo lectura, tanto la programación como el borrado, se realizan eléctricamente desde el propio grabador y bajo el control programado de una computadora. Es muy cómoda y rápida la operación de grabado y borrado. No disponen de ventana de cristal en la superficie.

El número de veces que puede grabarse y borrarse una memoria EEPROM es finito, por lo que no es recomendable una reprogramación continúa. Son muy idóneos para la enseñanza y la ingeniería de diseño. Un inconveniente es que este tipo de memoria es relativamente lenta.

El microcontrolador elegido para este proyecto está provisto de este tipo de memoria, ofreciendo una gran flexibilidad y facilidad al programador en la etapa de diseño.

3.3.2.5. Memoria flash

Se trata de una memoria no volátil, de bajo consumo, que se puede escribir y borrar. Funciona como una memoria ROM y una memoria RAM pero con la diferencia que consume menos potencia y es más pequeña.

A diferencia de la memoria ROM, la memoria *flash* es programable en el circuito. Es más rápida y de mayor densidad que la memoria EEPROM.

La alternativa *flash* está recomendada frente a la EEPROM cuando se precisa gran cantidad de memoria de programa no volátil. Es más veloz y tolera más ciclos de escritura y borrado.

Las memorias EEPROM y *flash* son muy útiles al permitir que los microcontroladores que las incorporan puedan ser reprogramados en circuito, es decir, sin tener que retirar el circuito integrado de la tarjeta. Así, un dispositivo con este tipo de memoria incorporado al control del motor de un automóvil permite que pueda modificarse el programa durante la rutina de mantenimiento periódico, compensando los desgastes y otros factores tales como la compresión, la instalación de nuevas piezas, etc. La reprogramación del microcontrolador puede convertirse en una labor rutinaria dentro de la puesta a punto.

3.3.3. Buses de comunicación

Para lograr la comunicación entre los elementos del microcontrolador, es necesario interconectarlos por medio de tres buses o canales de información. Los buses utilizados para trasladar la información son los siguientes.

3.3.3.1. Bus de control

A través de este bus se envían las señales que controlan los distintos dispositivos del microcontrolador. Es el encargado de manejar el sentido de la información. Si se desea acceder a la memoria de lectura en lugar de un puerto de salida, este bus se encarga abrir el camino para acceder a la memoria de lectura y anula la comunicación hacia los demás periféricos.

3.3.3.2. Bus de datos

A través de este bus viaja la información que se manipulará es transferida de una unidad a otra para ser procesada o desplegada. En la etapa de diseño e implementación se hace uso de un microcontrolador que tiene una capacidad de 8 bits de datos.

3.3.3.3. Bus de direcciones

Este bus de comunicación se utiliza para encontrar la ubicación de la información que se va a manipular. En una memoria de lectura y/o escritura,

cada palabra guardada (información) está asociada a una localidad de memoria que posee una dirección hexadecimal. Cuando se desea obtener información de la memoria, el procesador traslada la dirección hexadecimal hacia la memoria a través del bus de direcciones, con este valor, la memoria ubica la palabra solicitada y la retorna a través del bus de datos para su manipulación.

3.3.4. Puertos de entrada y salida

Los puertos de entrada y salida permiten al microcontrolador interactuar con los elementos que lo rodean. Por medio de estos, un microcontrolador puede manejar un motor paso a paso, acceder a localidades de memorias externas, controlar una pantalla de cristal líquido (LCD del inglés *Liquid Crystal Display*), etc.

Es muy importante conocer los niveles de voltaje y corriente que se manejan, con la finalidad de evitar daños tanto al microcontrolador como a los elementos externos.

El dispositivo microcontrolador utilizado en este diseño maneja voltajes de salida y entrada de 5 voltios para un uno lógico y cero voltios para un cero lógico.

3.3.5. Reloj principal

Todos los microcontroladores deben disponer de un circuito oscilador que genere una onda de alta frecuencia. Cada microcontrolador posee un rango de frecuencias a la cual puede operar satisfactoriamente. Al momento de diseñar,

hay que tomar en cuenta que el aumentar la frecuencia del reloj supone disminuir el tiempo en que se ejecutan las instrucciones, pero lleva aparejado un incremento en el consumo de energía.

Generalmente, el circuito de reloj está incorporado en el microcontrolador y sólo se necesitan unos pocos componentes externos para seleccionar y estabilizar la frecuencia de trabajo. Dichos componentes suelen consistir en un cristal de cuarzo, un resonador cerámico o una red R-C. Para el presente caso, se hace uso de un cristal de cuarzo de 20 MHz.

3.3.6. Recursos especiales

Cada fabricante oferta numerosas versiones de una arquitectura básica de microcontrolador. En algunas amplía las capacidades de las memorias, en otras incorpora nuevos recursos, en otras reduce las prestaciones al mínimo para aplicaciones muy simples, etc. La labor del diseñador es encontrar el modelo mínimo que satisfaga todos los requerimientos de su aplicación, minimizando el coste final del producto.

Entre los principales recursos específicos que incorporan los microcontroladores podemos mencionar:

- Temporizadores
- Perro guardián o *watchdog*
- Protección ante fallo de alimentación
- Estado de reposo o de bajo consumo
- Conversor analógico/digital
- Conversor digital/analógico

- Comparador analógico
- Modulador de anchura de impulsos (PWM del inglés *Pulse Width Modulation*)

3.3.6.1. Temporizadores

Se emplean para controlar períodos de tiempo (temporizadores) y para llevar la cuenta de acontecimientos que suceden en el exterior (contadores).

Para la medida de tiempos se hace uso de un registro al cual se carga un valor definido, este valor se irá incrementando o decrementando, según sea el caso, en función de los impulsos de reloj, algún múltiplo de este o cambios de flanco en alguna línea de entrada. Cuando el valor del registro se desborda y llega a cero, el microcontrolador produce un aviso que puede ser utilizado para ejecutar alguna rutina establecida.

3.3.6.2. Perro guardián o *watchdog*

El perro guardián consiste en un temporizador que cuando se desborda, provoca un reinicio automático en el sistema. Para evitar que el microcontrolador se reinicie automáticamente, debe preverse en el código refrescar o re-inicializar el registro que concierne al perro guardián, para ello existe una instrucción que reinicia el conteo del perro guardián evitando con ello el desborde y por ende el reinicio del sistema.

Este recurso es de vital importancia cuando se tiene un microcontrolador que funciona sin el control de un supervisor y de forma continuada las 24 horas

del día. La ventaja principal que brinda este recurso, es que el microcontrolador tiene la capacidad de reiniciarse completamente cuando sufre un bloqueo inesperado en el sistema.

3.3.6.3. Protección ante fallo de alimentación

Se trata de un circuito que reinicia al microcontrolador cuando el voltaje de alimentación (V_{DD}) es inferior a un voltaje mínimo. Mientras el voltaje de alimentación sea inferior al voltaje mínimo, el dispositivo se mantiene reiniciado, comenzando a funcionar normalmente cuando sobrepasa dicho valor.

3.3.6.4. Estado de reposo ó de bajo consumo

Son abundantes las situaciones reales de trabajo en que el microcontrolador debe esperar a que se produzca algún acontecimiento externo que le ponga de nuevo en funcionamiento. Para ahorrar energía, (factor clave en los equipos portátiles), los microcontroladores disponen de una instrucción especial, que obliga al microcontrolador a pasar a un estado de reposo o de bajo consumo, en el cual los requerimientos de potencia son mínimos. En dicho estado se detiene el reloj principal y sus circuitos asociados, quedando el microcontrolador únicamente sensible a las interrupciones. Al activarse una interrupción ocasionada por un acontecimiento esperado, el microcontrolador regresa a su operación normal y reanuda su trabajo.

3.3.6.5. Conversor analógico/dígital

Los microcontroladores que incorporan un conversor analógico/digital suelen disponer de un multiplexor que permite aplicar a la entrada del conversor diversas señales analógicas y convertirlas en valores digitales que son guardados en registros internos del microcontrolador para ser procesados. Este módulo es muy utilizado en aplicaciones de digitalización de señales.

3.3.6.6. Conversor dígital/analógico

A la inversa que el recurso anterior, este convertidor transforma los datos digitales obtenidos del procesamiento del microcontrolador, en señales analógicas de salida en algún puerto del integrado.

3.3.6.7. Comparador analógico

Algunos modelos de microcontroladores disponen internamente de un amplificador operacional que actúa como comparador entre una señal fija de referencia y otra variable. La salida del comparador proporciona un nivel lógico “1” ó “0” cuando una de las señales sea mayor o menor que la otra.

3.3.6.8. Modulador de anchura de impulsos

Es un módulo que proporciona en una línea de salida impulsos de anchura variable. Estos son utilizados generalmente para manejar la potencia de motores pequeños.

3.3.6.9. Puertos de comunicación

Los puertos de comunicación ofrecen al microcontrolador la posibilidad de comunicarse con otros dispositivos externos que trabajan bajo algún protocolo específico, entre estos podemos mencionar:

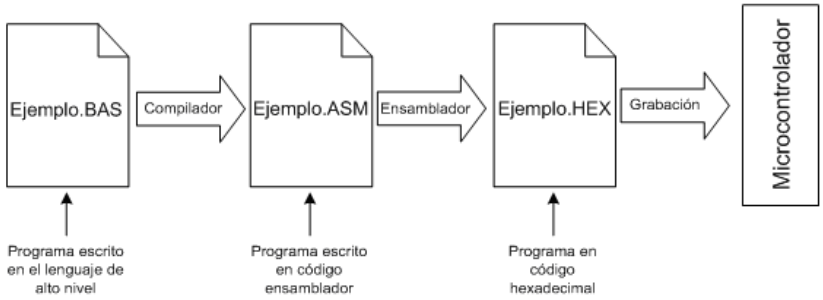
- Puerto UART del inglés *Universal Asynchronous Receiver Transmitter*, es un adaptador de comunicación serie asíncrona.
- Puerto USART del inglés *Universal Synchronous Asynchronous Receiver Transmitter,* es un adaptador de comunicación serie síncrona y asíncrona.
- Puerto paralelo esclavo, utilizado para la conexión con otros microprocesadores.
- Puerto USB del inglés *Universal Serial Bus*, es un adaptador de comunicación serial de reciente creación.

3.4. Herramientas de programación

La programación es una de las partes más importantes de cualquier diseño con microcontroladores, esta definirá la eficiencia y desempeño del sistema. Para lograr un buen resultado, se debe conocer las diferentes etapas de programación y las herramientas disponibles para la simulación y prueba del código del programa ó código fuente.

A continuación se detallará cada una de las fases que implica la programación de microcontroladores.

Figura 22. **Fases de programación**



Fuente: diseño e implementación de un sistema generador de mensajes en una red de telemedida, ante fallas del suministro de energía eléctrica. p. 42.

3.4.1. Lenguaje de alto nivel

Con el avance de la tecnología, cada vez se proveen de más y mejores herramientas que facilitan a los programadores el diseño del código fuente para el microcontrolador. Los lenguajes de alto nivel se caracterizan por expresar algoritmos de una manera adecuada a la capacidad cognitiva humana, en lugar de la capacidad ejecutora de las máquinas, es decir, que son lenguajes más orientados al entendimiento humano.

La programación en un lenguaje de alto nivel (como C++ ó Basic) permite disminuir el tiempo de desarrollo de un producto. No obstante, si no se programa con cuidado, el código resultante puede ser mucho más ineficiente que el programado en el lenguaje ensamblador.

Los lenguajes de alto nivel crean un archivo de texto que contiene cada una de las sintaxis propias del lenguaje. Una vez que el diseñador termina la programación, el código fuente debe pasar a una fase denominada compilación. Por medio de la compilación el software puede analizar si todas las líneas cumplen con las sintaxis establecidas por el lenguaje. Si existiera algún error de sintaxis, este es anunciado para el que programador pueda detectarlo y corregirlo. De lo contrario, si todas las sintaxis son correctas, el compilador crea un nuevo archivo que contiene el programa en código ensamblador.

3.4.2. Lenguaje ensamblador

El código ensamblador puede obtenerse de dos formas, la primera, mediante la compilación de una código fuente realizado en un lenguaje de alto nivel, tal y como se explicó anteriormente, y la segunda, programando en un lenguaje que soporte la programación en código ensamblador.

La programación en lenguaje ensamblador permite desarrollar programas muy eficientes, ya que otorga al programador el dominio absoluto del sistema. Los fabricantes suelen proporcionar el programa ensamblador de forma gratuita y en cualquier caso siempre se puede encontrar una versión gratuita para los microcontroladores más populares.

3.4.3. Lenguaje máquina

El lenguaje máquina es el único que entiende directamente el procesador. Este lenguaje utiliza el alfabeto binario conformado por unos y ceros. Los códigos en lenguajes máquina se consiguen al momento de ensamblar el código ensamblador recién obtenido. El archivo que se origina del ensamble, está formado por valores hexadecimales que representan los unos y ceros del código, estos valores son cargados al microcontrolador a través de un programa y equipo especial para cada microcontrolador.

3.4.4. Depuración y simulación

Además de los programas especializados en la programación de microcontroladores, existen herramientas igualmente importantes para el desarrollo de proyectos.

La depuración es una herramienta que comúnmente está incluida en los programas de programación. Con esta herramienta se puede evaluar el programa escrito para encontrar errores lógicos en el código diseñado. Muchas veces los errores no son provocados por una mala sintaxis, sino por una mala programación de condiciones.

Otra herramienta importantísima en el desarrollo de proyectos lo conforman los simuladores. Los simuladores son capaces de ejecutar en una computadora o tarjeta los programas realizados para el microcontrolador. Los simuladores permiten tener un control absoluto sobre la ejecución de un programa, siendo ideales para la depuración de los mismos.

Hoy en día existen simuladores más sofisticados que permiten al diseñador introducir señales en las líneas de entrada del microcontrolador y poder reflejar las respuestas de este, en un puerto serial, en una matriz de puntos, en una pantalla de cristal líquido, etc.

4. HERRAMIENTAS DE MONITOREO

4.1. Introducción a las herramientas de monitoreo

El término Monitoreo de red describe el uso de un sistema que constantemente revisa el funcionamiento de los equipos en una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico u otras alarmas. Es un subconjunto de funciones de la administración de redes.

Mientras que un sistema de detección de intrusos monitorea una red por amenazas del exterior (externas a la red), un sistema de monitoreo de red busca problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red (u otros dispositivos).

Por ejemplo, para determinar el estatus de un servidor web, software de monitoreo puede enviar, periódicamente, peticiones HTTP (Protocolo de Transferencia de Hipertexto) para obtener páginas; para un servidor de correo electrónico, enviar mensajes mediante SMTP (Protocolo de Transferencia de Correo Simple), para luego ser retirados mediante IMAP (Protocolo de Acceso a Mensajes de Internet) o POP3(Protocolo Post Office).

Comúnmente, los datos evaluados son tiempo de respuesta y disponibilidad (o uptime), aunque estadísticas tales como consistencia y fiabilidad han ganado popularidad. La generalizada instalación de dispositivos de optimización para redes de área extensa tiene un efecto adverso en la

mayoría del software de monitoreo, especialmente al intentar medir el tiempo de respuesta de punto a punto de manera precisa, dado el límite visibilidad de ida y vuelta.

Fallas de peticiones de estado, tales como que la conexión no pudo ser establecida, tiempo de espera agotado, entre otros, usualmente produce una acción desde del sistema de monitoreo. Estas acciones pueden variar; una alarma puede ser enviada al administrador, ejecución automática de mecanismos de controles de fallas, etcétera.

Monitorear la eficiencia del estado del enlace de subida se denomina Medición de tráfico de red.

4.2. Descripción de la herramienta *Solar Winds*

El sistema de administración de red de TCP/IP se basa en el protocolo SNMP (*Simple Network Management Protocol*), que ha llegado a ser un estándar de ipso en la industria de comunicación de datos para la administración de redes de computadora, ya que ha sido instalado por múltiples fabricantes de puentes, repetidores, ruteadores, servidores y otros componentes de red.

Para facilitar la transición de SNMP a CMOT (*Common Management Information Services and Protocol Over TCP/IP*), los dos protocolos emplean la misma base de administración de objetos MIB (*Management information Base*).

Para hacer más eficiente la administración de la red, la comunidad de TCP/IP divide las actividades en dos partes:

- Monitoreo, o proceso de observar el comportamiento de la red y de sus componentes, para detectar problemas y mejorar su funcionamiento.
- Control, o proceso de cambiar el comportamiento de la red en tiempo real ajustando parámetros, mientras la red está en operación, para mejorar el funcionamiento y repara fallas.

Es del inciso a, de donde se encuentra la aplicación *Orion Solar Winds* la cual presenta varias aplicaciones y bondades para el monitoreo de las redes WAN y LAN.

Orion Network Performance Monitor es una aplicación de administración de desempeño de fácil comprensión basada en la administración de fallas, disponibilidad y ancho de banda de la red que permite a los usuarios ver las estadísticas en tiempo real y la disponibilidad de su red directamente desde el navegador de red.

La aplicación *Orion Network Performance Monitor* monitoreará y recogerá datos de enrutadores, switches, servidores, y cualquier otro dispositivo con SNMP disponible. Adicionalmente, Orion monitorea carga de la CPU, utilización de memoria, y espacio de disco disponible. Orion NMP es una aplicación de disponibilidad administrada altamente escalable, capaz de monitorear desde 10 hasta más de 10 000 nodos.

Una de las características más destacables de la aplicación *Orion Network Performace Monitor* es su motor de alerta el cual permite configurar alertas para cientos de situaciones e incluye la habilidad de definir las dependencias de los dispositivos. Mientras, el motor de reportes de *Orion* permite sacar datos que se necesiten desde la base de datos de *Orion* y visualizarlos en la red o directamente en el escritor de reportajes. Aparte de toda la información que se

despliega también tiene la posibilidad de realizar la notificación de las llamadas alarmas previamente configuradas a cuentas de correos por medio de un servidor de correo configurado.

4.3. Configuración de la herramienta *Solar Winds* para monitorización de dispositivos

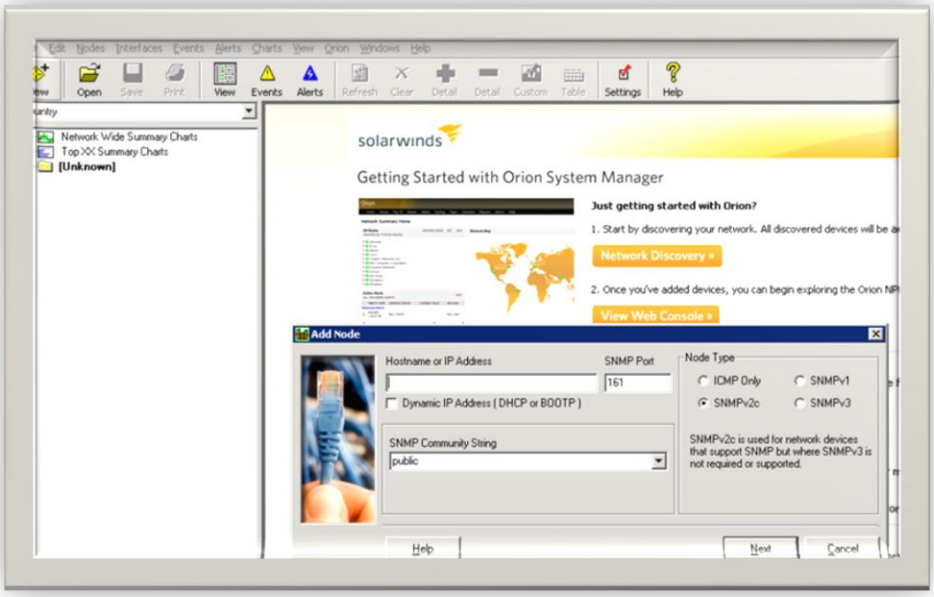
Para empezar a configurar el monitoreo de un equipo en el sistema de monitoreo *ORION* primero se debe de asignar al equipo una dirección IP y luego se debe de crear y corroborar todas las rutas para que el sistema pueda alcanzar con facilidad el equipo. Una vez cumplido con lo anteriormente explicado se procederá a ingresar los equipos.

4.3.1. Ingreso de equipo

Abrir la ventana *Orion Network Performance Monitor*, una vez aquí se debe de pinchar el icono New esto mostrara una ventana donde debemos de ingresar la IP del equipo, puerto SNMP habilitado para el equipo (si lo tiene), el nombre de la comunidad SNMP (si lo tiene), también se puede indicar que tipo de nodo es por medio del monitoreo ICMP (Ping), SNMPv1, SNMPv2 o SNMPv3, esto dependiendo de la tecnología que soporte el equipo a monitorear.

Luego de terminar de seleccionar las prestaciones que deseamos para nuestro equipo se presiona el botón Next para finalizar de ingresar el equipo y empezar a llevar las estadísticas del mismo.

Figura 23. **Ingreso de equipos**

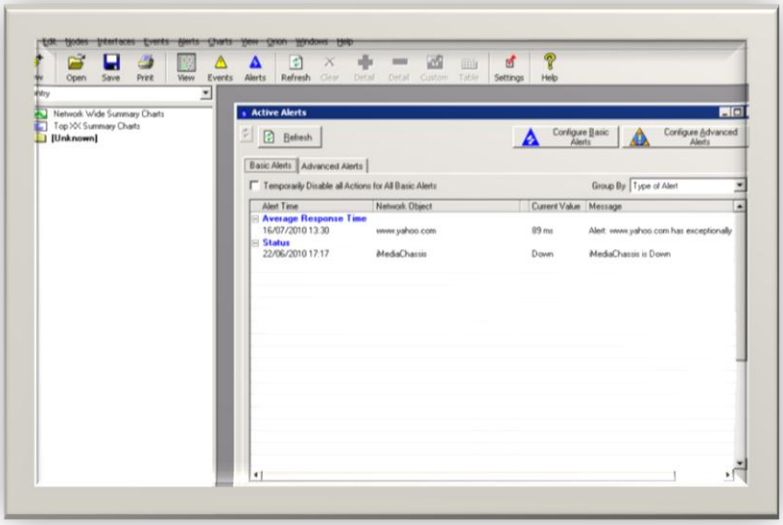


Fuente: *print screen.*

4.3.2. Configuración de alarmas y notificaciones

Este tipo de configuración se realiza en la ventana de *Orion Network Performance Monitor*, aquí se presiona el icono *Alerts*, esto hará aparecer la ventana de *Active Alerts*.

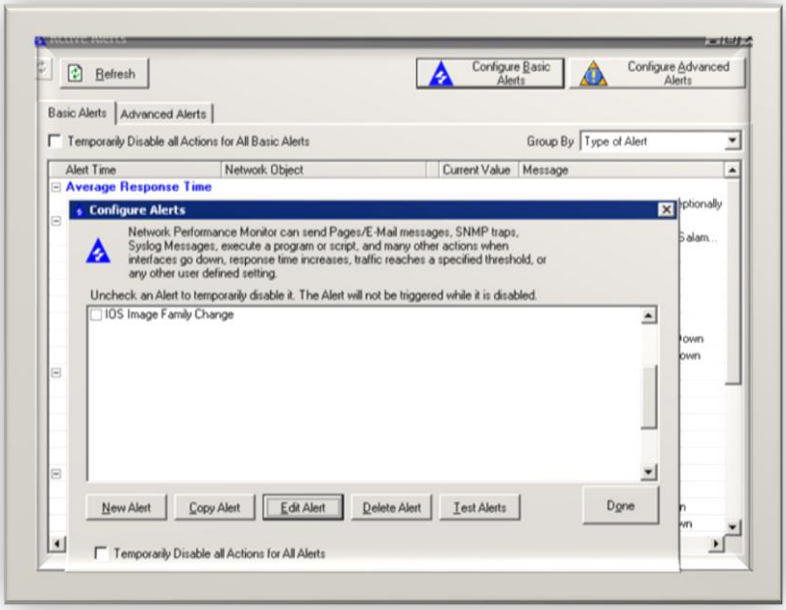
Figura 24. **Configuración de alarmas 1**



Fuente: *print screen.*

Una vez en esta ventana se debe presionar el botón *Configure Basic Alerts* lo que hará aparecer la ventana *Configure Alerts*, aquí se debe de presionar escoger el botón de *New Alert* lo que hará que la se pueda configurar una nueva alarma.

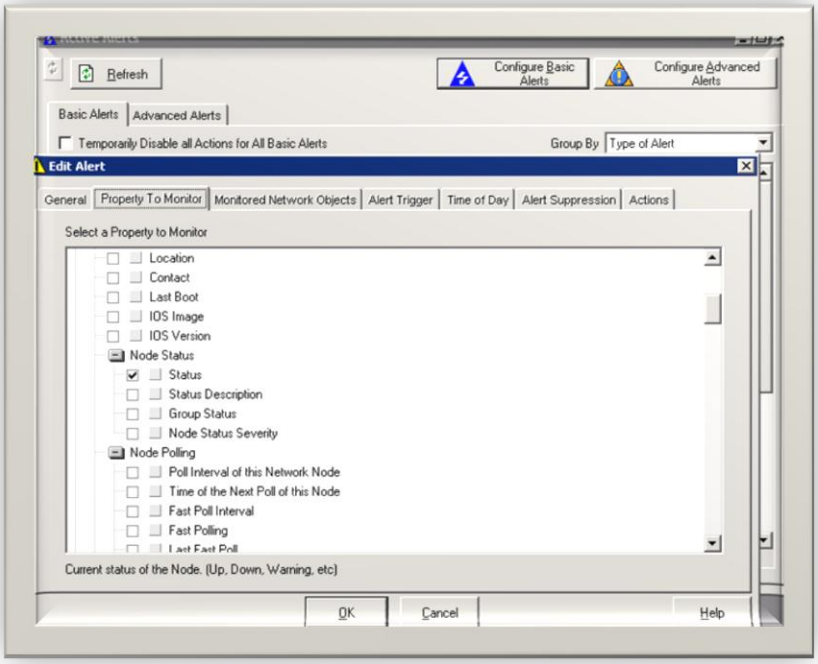
Figura 25. **Configuración de alarmas 2**



Fuente: *print screen.*

Luego de Ingresar el nombre de la alarma se puede elegir que tipo de alarma se desea, esto se hace en la pestaña *Property To Monitor*, aquí se pueden escoger varios tipos de alertas, en nuestro caso seleccionaremos la categoría *Node Status* y la opción *Status*, esta permite analizar si el equipo se encuentra caído o se encuentra activo.

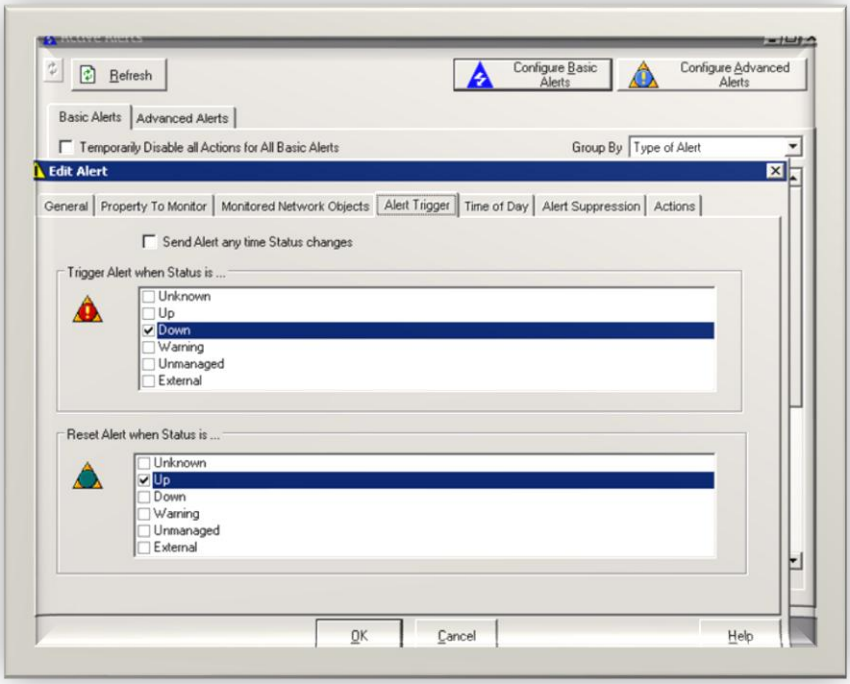
Figura 26. **Configuración de alarmas 3**



Fuente: *print screen.*

Luego de seleccionar la propiedad del equipo a monitorear nos dirigimos a la pestaña *Alert Trigger* en la cual se debe configurar cuando se activara la alarma y cuando se desactivará.

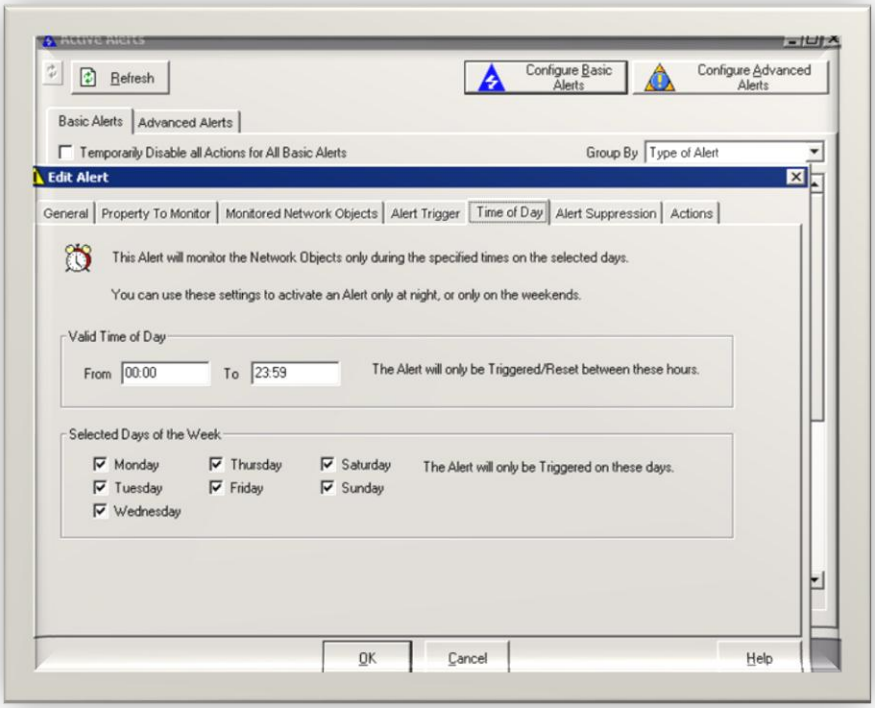
Figura 27. **Configuración de alarmas 4**



Fuente: *print screen.*

Luego en la pestaña *Time of Day* se puede especificar el horario en que queremos que se mantenga activa la alarma, se puede escoger el período de tiempo por medio del ingreso de la hora de inicio y la hora de finalización, también se puede escoger que días de la semana se desea monitorear el equipo. Cabe mencionar que la hora en el equipo que posee el *Solar Winds Orion* debe de estar siempre bien configurado para evitar problemas.

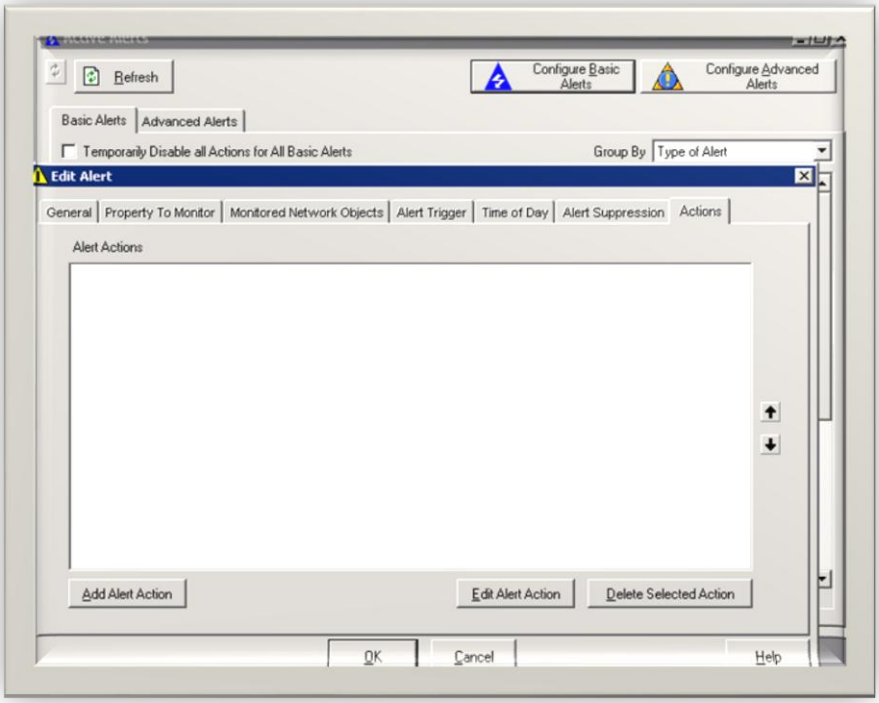
Figura 28. **Configuración de alarmas 5**



Fuente: *print screen.*

Luego se va a la pestaña titulada *Actions* en la cual se configurara el envió de correo electrónico por medio de un servidor de correo. Para realizar esto se debe presionar el botón *Add Alert Action*.

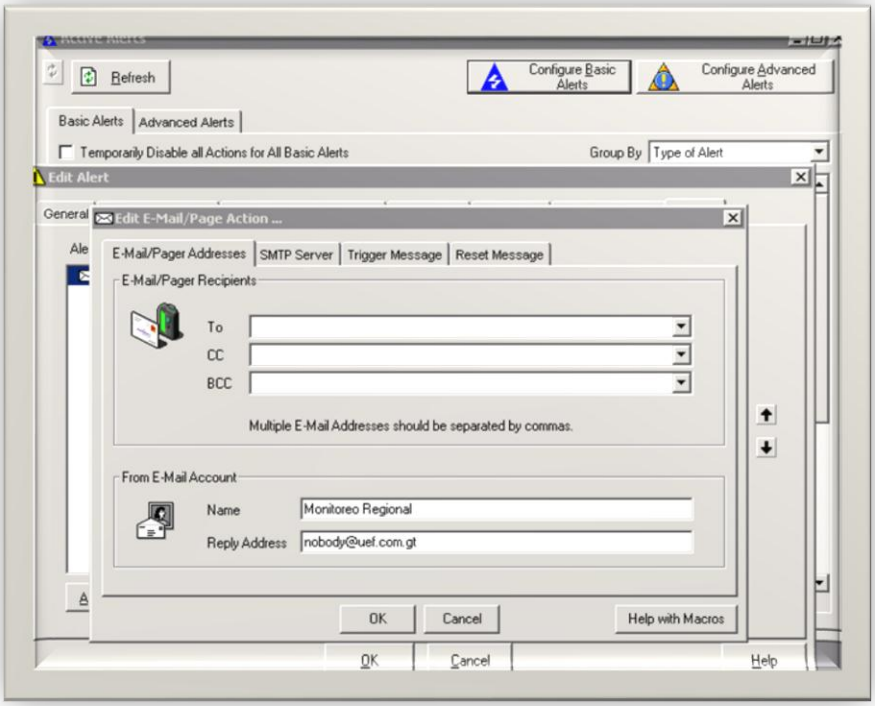
Figura 29. **Configuración de alarmas 6**



Fuente: *print screen.*

Inmediatamente después aparecerá una ventana con 4 pestañas en las cuales en la primera *E-Mail/Pager Addresses* se debe de ingresar las direcciones de correo de las personas se deseen que aparezcan como remitente para los correos que se generaran en caso de un evento.

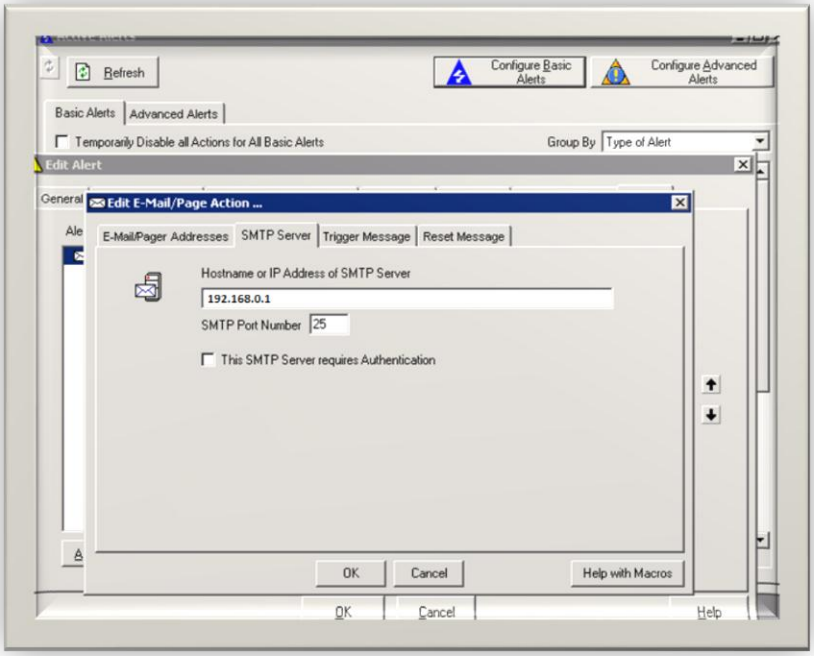
Figura 30. **Configuración de alarmas 7**



Fuente: *print screen.*

En la pestaña SMTP *Server* se debe de ingresar la dirección y el puerto SMTP del servidor de correo a través del cual se esteran enviando los correos.

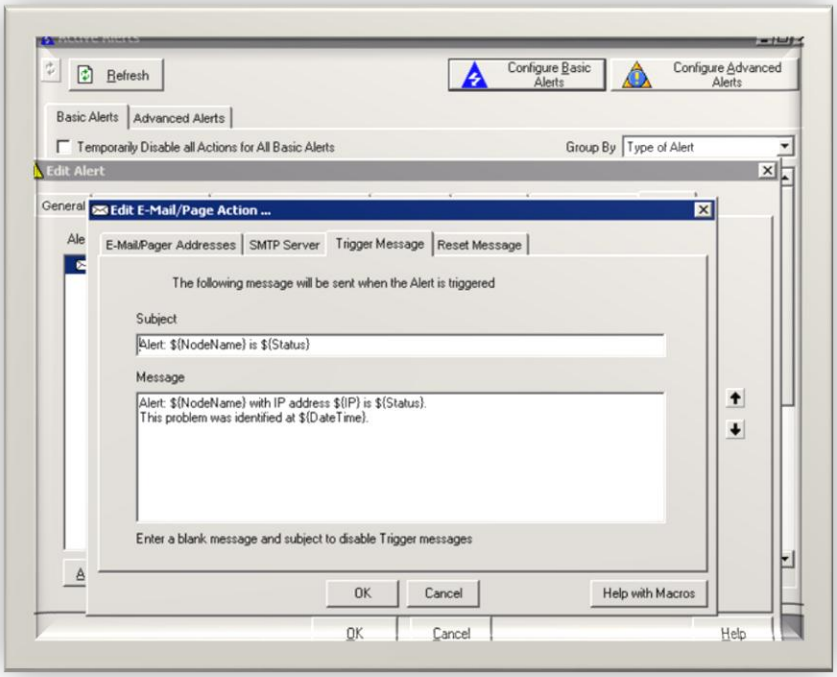
Figura 31. **Configuración de alarmas 8**



Fuente: *print screen.*

En la pestaña *Trigger Message* se configura el título y cuerpo del mensaje a enviar, esta opción se realizará para el correo que estará enviando el programa al activarse la alarma, y luego en la pestaña de *Reset Message* se configura exactamente lo mismo pero para cuando se resetea la alarma.

Figura 32. **Configuración de alarmas 9**



Fuente: *print screen.*

Luego de configurar todos estos pasos se presiona el botón OK y luego nuevamente se debe oprimir el botón OK , al regresar a la ventana *Configure Alerts* se puede probar que toda la configuración realizada previamente se encuentre funcionando adecuadamente por medio del botón *Test Alerts* el cual realizara una simulación de la activación de una alarma.

5. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA GENERADOR DE MENSAJES

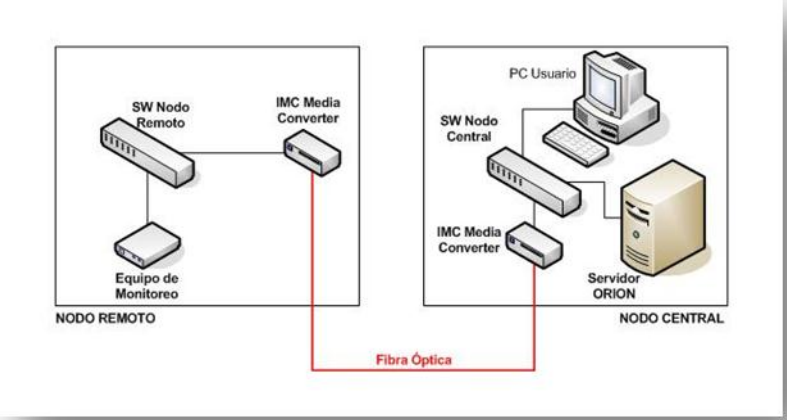
5.1. Etapa de diseño

Una de las etapas más importantes en la fabricación de equipos lo constituye la etapa de diseño, en ella se define el alcance, flexibilidad, limitaciones y prestaciones del sistema. A continuación se detalla brevemente la creación del sistema.

5.1.1. Elementos del sistema monitorizado

La red en la cual se implementará el sistema de monitoreo consta de equipos interconectados entre sí por medio de equipos *Media Converters* que se encargan de convertir los impulsos eléctricos a impulsos ópticos, esto debido a que para grandes distancias las redes se interconectan por medio de fibra óptica la cual permite la transmisión de una mayor cantidad de información.

Figura 33. **Diagrama de red**



Fuente: elaboración propia.

Los requerimientos para integrar el sistema de monitoreo a un nodo de comunicación son los siguientes:

- Diseño del equipo de monitorización del suministro eléctrico y temperatura.
- Establecer una comunicación directa entre el puerto Ethernet del equipo de monitorización de temperatura y suministro eléctrico y el servidor donde se encuentra instalado el sistema de monitorización ubicado en el nodo central para permitir el monitoreo del equipo.
- Implementar una fuente de voltaje de respaldo para suministrar corriente al equipo de monitorización al momento que ocurra una falla de energía eléctrica.
- Proveer de un punto de medición de 110VAC, para monitorear el suministro de energía eléctrica en el nodo.

5.1.1.1. Diseño de equipo para la monitorización de temperatura y suministro eléctrico

Como se menciona en el primer punto, el sistema debe ser capaz de medir la temperatura del ambiente del nodo de telecomunicaciones así como medir la alimentación de dicho sitio.

Además de esto el equipo al momento de alcanzar una medición de temperatura o voltaje fuera de los parámetros correctos debe de ser capaz de desactivar el puerto 7 tcp por el cual se implementa *Echo Request* en el protocolo ICMP, esto hará que en el servidor que cuenta con el programa de monitoreo se active la alarma configurada y se proceda a notificar al usuario.

Una vez el usuario se encuentre notificado se puede ingresar al equipo de monitoreo utilizando el puerto 80 tcp y utilizando una interfaz web para desplegar los valores.

De igual manera al regresar los valores normales de temperatura y alimentación el sistema deberá de volver a activar el puerto 7 tcp para permitir que el sistema de monitoreo instalado en el servidor notifique al usuario el restablecimiento de la alarma.

5.1.1.2. Comunicación ethernet entre los equipos

La comunicación *Ethernet* entre los equipos requiere de configurar una *Vlan* determinada a la cual se pueda crear una red privada y a esta poder incluir el equipo de monitorización de temperatura y suministro eléctrico y al servidor con el software de monitorización a utilizar.

En cada nodo el equipo encargado del manejo de las *Vlans* es un *Switch* en el cual debe de tener nombrada la *Vlan* seleccionada al igual que todos los equipos activos encargados de transmitir el tráfico en la red.

La internase a la cual se conectara el equipo de medición de voltaje y temperatura debe de estar configurada en modo *Access* para la *Vlan* que se ha destinado para llevar el tráfico de la red creada.

Debido a las grandes distancias entre los diferentes nodos el medio de comunicación entre nodos deben de ser a través de fibra óptica utilizando equipos *Media Converter* los cuales son los encargados de convertir las señales eléctricas a señales.

5.1.1.3. Fuente de voltaje de respaldo

Un punto muy importante a cumplir es la implementación de una fuente de voltaje de respaldo. La función principal de la fuente de respaldo, es proveer de energía eléctrica a los equipos conectados, después de que ocurre una falla en el suministro eléctrico. Generalmente, las fuentes de respaldo están compuestas por bancos de batería o generadores de energía eléctrica a base

de combustibles. Para aplicaciones pequeñas, lo más común es encontrar fuentes de respaldo compuestas por baterías.

Para seleccionar el tamaño y características de una batería, es necesario considerar el voltaje y corriente del sistema. La corriente define el consumo de energía que realiza cada uno de los equipos energizados, mientras que el voltaje define la diferencia de carga eléctrica que existe entre los polos de la fuente de alimentación a la que opera el sistema.

Para que el sistema de monitorización instalado pueda funcionar correctamente al momento que ocurra una falla de energía eléctrica en el nodo, deben existir por lo menos tres equipos energizados, el equipo de monitorización, que servirá para alertar al servidor encargado de monitorizar y al momento de poder ingresar a revisar el status del nodo a través del equipo instalado, el *Switch*, el cual es el que le da acceso al equipo de monitoreo a la red, y el *Media Converter*, el cual es el encargada de comunicar el nodo hacia los demás puntos de la red. Por lo anterior, la planta celular y el generador de mensajes son los equipos que definirán las características principales de la batería de respaldo.

Según las hojas de especificaciones de los elementos del equipo de monitorización instalado en el nodo, este tiene un consumo de corriente máximo de 0,1 amperio, el *Switch* por el cual se comunicara el equipo de monitorización tiene un consumo de 1,3 amperios y los *Media Converters* tienen un consumo de 1 amperio cada uno y son necesarios 2 para poder tener como mínimo una ruta de redundancia para cada nodo, por tal caso el consumo total de los *Media Converters* es de 2 amperios. Para encontrar la corriente total del sistema, únicamente se suman las corrientes individuales, en este caso 2(1)+1,3+0,1=3,4 amperios.

Con lo que respecta al voltaje de alimentación, según las especificaciones del fabricante, el *Switch* y *Media Converters* pueden operar entre 110 VAC y 220 VAC, el transformador que alimenta el equipo de equipo de monitorización opera también entre los valores que los otros 2 equipos. Esto define que el voltaje del sistema (voltaje común) es de 110 VAC.

Después de definir el voltaje y la corriente total del sistema, se debe considerar el tiempo de operación de los equipos al momento que falle el suministro primario. Entre los parámetros más importantes de una batería se encuentra el amperio-hora. Este parámetro define la cantidad de corriente que puede proveer la batería en el transcurso de una hora.

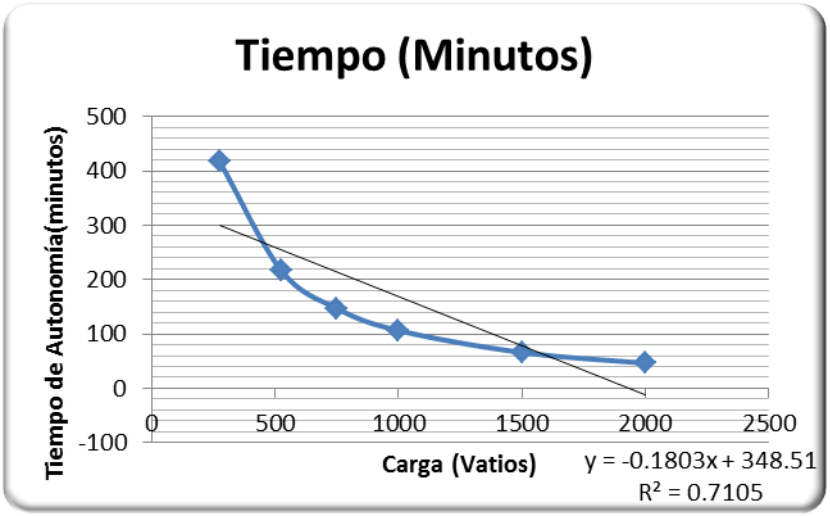
Por ejemplo, si la batería indica 3,2 amperios-hora, ésta será capaz de proveer 3,2 amperios de forma constante durante una hora, luego de cumplirse la hora, el valor de voltaje comenzará a decaer pudiendo ocasionar problema en el funcionamiento de los equipos.

Por lo anterior, si se desea que los equipos del sistema se mantengan en operación por lo menos una hora, necesitamos un UPS capaz de darnos tal capacidad de autonomía, aunque en la realidad la capacidad de autonomía que debería de tener el sistema es de 4 horas, esto ya que de esta forma estaríamos asegurando que se cuenta con tiempo suficiente para restablecer la energía al recibir la alarma por parte del equipo de monitoreo.

Por lo anteriormente explicado, es necesario un UPS que proporcione aproximadamente 400 Watts, en el mercado se puede encontrar el equipo APC Smart-UPS XL 3 000 VA 120 V *Tower/Rack Convertible* y con una batería adicional APC *Smart-UPS Ultra Battery Pack* 48 V, el cual proporciona una salida de tensión nominal de 120 V y una potencia máxima configurable de

3 000 VA, el desempeño de este equipo referente a la autonomía respecto a la carga conectada se puede apreciar en la gráfica mostrada a continuación.

Figura 34. **Gráfico de autonomía equipo SUA3000XL**



Fuente: APC.

5.1.1.4. Monitoreo de temperatura y del suministro de energía eléctrica

El sistema de monitoreo es capaz de medir los cambios tanto en la temperatura ambiente como la perdida de voltaje en el suministro eléctrico que alimenta al nodo de telecomunicaciones.

Para establecer cuando ocurre un evento en la temperatura, el sistema cuenta con un censor capaz de medir constantemente la temperatura del nodo.

En el caso del suministro de energía eléctrica se realiza una medición en un punto toma de corriente de 110 VAC a través del cual, el equipo de monitoreo chequea constantemente el estado del suministro de energía eléctrica, pudiendo detectar la caída y el restablecimiento del suministro de energía eléctrica.

5.2. Ingeniería de programación

El sistema de monitoreo está controlado por un microcontrolador que se encarga de monitorear y administrar la habilitación del puerto de ping así como de permitir visualizar la información que censa constantemente, esto referente a la temperatura del nodo y del suministro eléctrico. La programación de este equipo se desarrolla en una lógica de decisiones que evalúa los estados de diferentes variables para definir el procedimiento a realizar.

Para el buen desarrollo de la fase de programación, la primera etapa debe contemplar un diagrama de flujo que defina todos los caminos posibles en el funcionamiento del equipo. Esta fase es la más importante en la ingeniería de programación, ya que a través de ella se definirá el alcance, seguridad, fiabilidad y robustez del sistema.

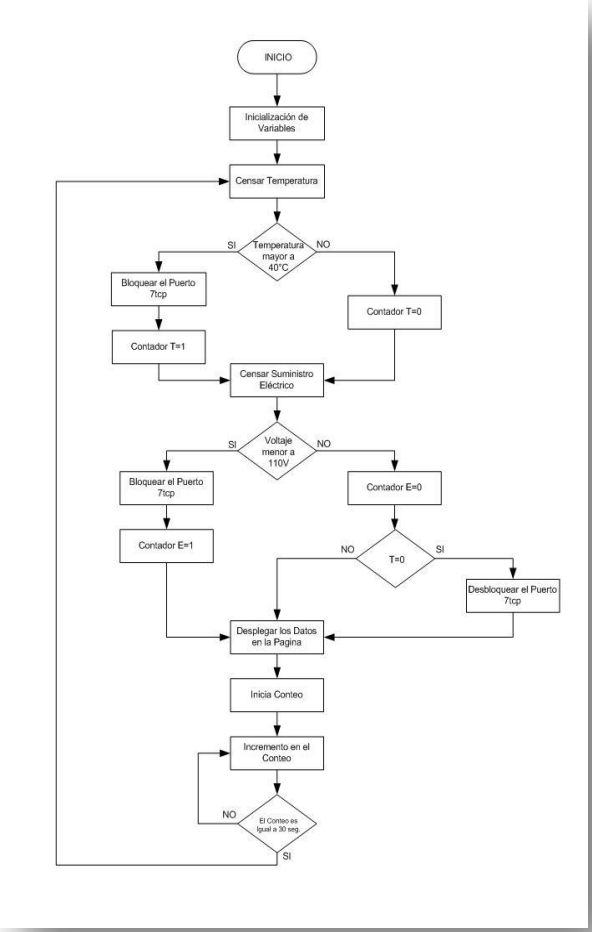
El sistema de monitoreo debe cumplir con los siguientes requerimientos:

- Identificar la falla y restablecimiento de la misma, ya sea por temperatura o por nivel de voltaje del suministro eléctrico del nodo.
- Deshabilitar el puerto 7 tcp para con esto hacer notar que hay un problema en el nodo.

- Poder desplegar en cualquier momento la información recabada a través de una página web que se almacena en el microcontrolador.

Tomando en cuenta estos requerimientos, se diseña el diagrama de flujo para la programación del equipo generador de mensajes. En la figura 35, se puede apreciar la lógica utilizada.

Figura 35. **Diagrama Lógico**



Fuente: elaboración propia.

Después de definir los procedimientos que realizara el sistema de monitoreo, se hace uso de programas dedicados que permiten trasladar la lógica presentada en el diagrama de flujo, a un código de ceros y unos que entenderá el microcontrolador. Este código es cargado a la memoria del microcontrolador para que comience a ejecutar las rutinas establecidas.

5.3. Implementación del sistema

Una vez explicado cada uno de los elementos del sistema generador de mensajes y sus requerimientos, se centra la atención en la implementación del sistema completo.

5.4. Requerimientos del sistema

Este proyecto pretende integrar a un bajo costo, el sistema de monitoreo de temperatura y suministro de energía eléctrica a una red ya existente y que cuenta con un sistema de monitoreo por caídas, por lo tanto, el sistema busca aprovechar cada uno de los recursos existentes, obteniendo de ellos lo necesario para el funcionamiento de los nuevos elementos.

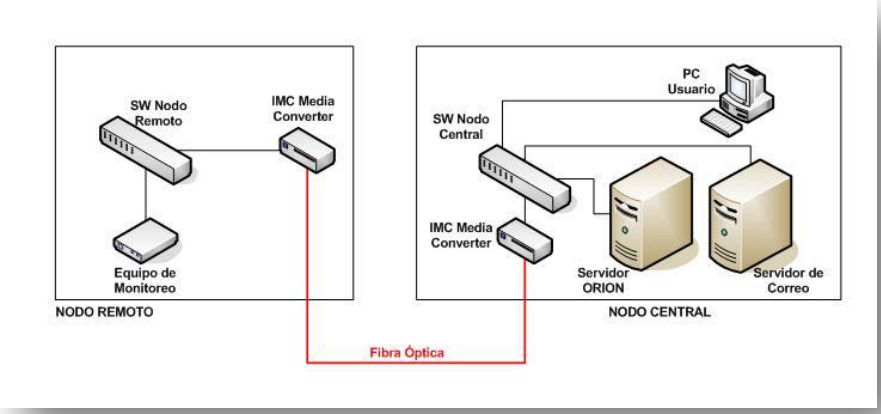
Básicamente los requerimientos del sistema son los siguientes:

- Alimentación de 110 VAC, que provea el suministro de energía eléctrica a la fuente de alimentación y proporcione un punto de medición para el censor del equipo.
- Cables de interconexión que permitan la comunicación Ethernet entre el Switch y el equipo de monitoreo.

5.5. Integración del sistema de Monitoreo

En la figura 36, se presenta el sistema completo que integra al equipo de monitoreo con los demás elementos existentes en la red.

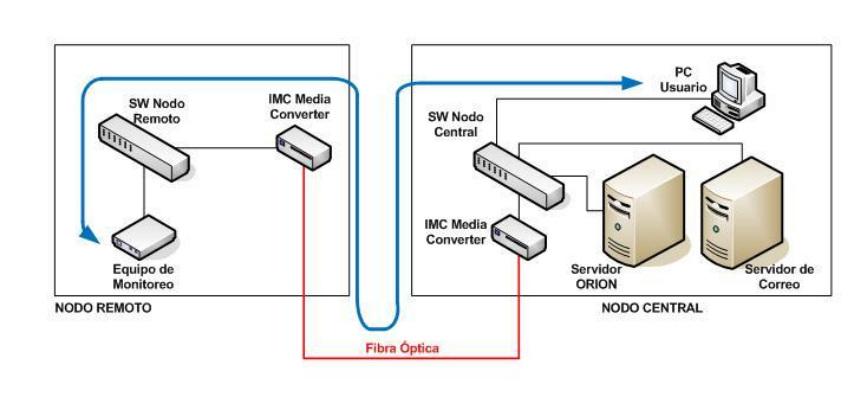
Figura 36. **Diagrama del Sistema Completo de Monitoreo**



Fuente: elaboración propia.

Cuando el usuario desee realizar una revisión, por medio de una PC que tenga acceso a la LAN en la que se encuentra configurado el equipo de monitoreo remoto, al establecer la comunicación el usuario podrá visualizar los valores de temperatura y voltaje de alimentación del nodo por medio de una interfaz Web.

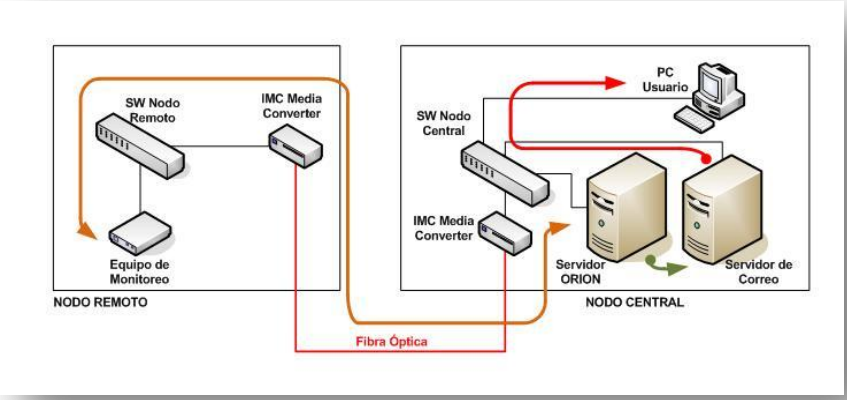
Figura 37. **Verificación de Interfaz Web del Equipo de Monitorización**



Fuente: elaboración propia.

Por otro lado, cuando exista una falla o un restablecimiento de energía eléctrica o un alto nivel de temperatura, el equipo de monitoreo alarmara el puerto 7 tcp para que por medio del servidor de monitoreo se envíen los mensajes de correo para notificar al usuario y que este pueda tomar acciones antes de que el servicio del nodo se vea afectado.

Figura 38. **Generación de Alarmas**



Fuente: elaboración propia.

5.6. Fase de prueba del prototipo

Luego de la integración, el sistema entra a una fase de prueba y evaluación de desempeño. El prototipo de este sistema se implementó el 13 de julio del 2010. A partir de esta fecha, se llevó a cabo un cuadro de control para verificar las fallas en el suministro eléctrico y problemas de temperatura en el nodo.

Las caídas de suministro eléctrico percibidas y alarmados por el prototipo fueron confirmados por el centro de operaciones de red que se encarga de monitorear los ramales de distribución de energía eléctrica.

En la tabla V, se presenta parte del historial de las fallas registradas por el sistema de monitoreo de suministro eléctrico y temperatura.

Tabla V. **Registro de fallas**

Evento Registrado	Fecha	Hora	Observaciones
Falla de Energía	13/07/2010	11:00	Falla simulada (Prueba del equipo)
Reestablecimiento	13/07/2010	11:04	Reestablecimiento simulado (Prueba del equipo)
Falla de Energía	13/07/2010	11:22	Falla simulada (Prueba del equipo)
Reestablecimiento	13/07/2010	11:26	Reestablecimiento simulado (Prueba del equipo)
Falla de Energía	04/08/2010	17:12	Falla confirmada
Reestablecimiento	04/08/2010	17:34	Reestablecimiento confirmado
Falla de Energía	18/08/2010	23:56	Falla confirmada
Reestablecimiento	19/08/2010	00:07	Reestablecimiento confirmado
Falla de Energía	19/09/2010	14:26	Falla confirmada
Reestablecimiento	19/09/2010	14:29	Reestablecimiento confirmado
Falla de Energía	21/09/2010	08:08	Falla confirmada
Reestablecimiento	21/09/2010	08:11	Reestablecimiento confirmado

Fuente: elaboración propia.

Los niveles de temperatura detectados por el prototipo se midieron 2 veces al día y fueron comparados con los censores del *Switch* instalado en el nodo.

En la tabla VI, se presenta parte del historial de las temperaturas registradas por el sistema de monitoreo de suministro eléctrico y temperatura.

Tabla VI. **Registro de fallas**

Fecha	Hora	Temperatura Registrada (°C)	Temperatura según Switch (°C)
13/09/2010	12:02	30	31
13/09/2010	18:00	31	32
15/09/2010	12:09	31	32
15/09/2010	18:01	32	33
17/09/2010	12:01	30	31
17/09/2010	18:04	31	32
20/09/2010	12:01	31	32
20/09/2010	18:10	30	31
22/09/2010	12:06	31	32
22/09/2010	18:03	30	31
24/09/2010	06:00	29	30
24/09/2010	14:02	31	32

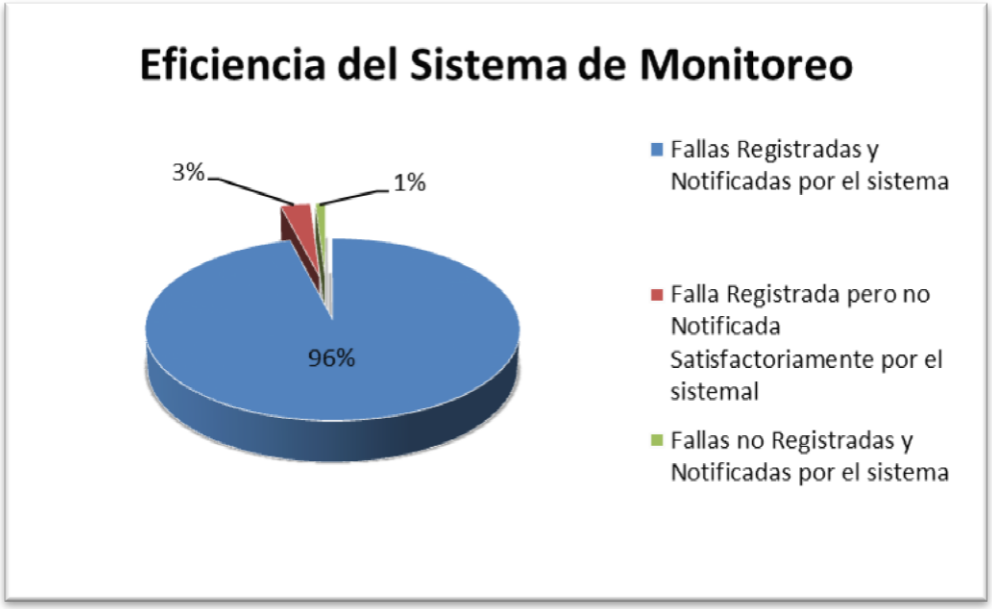
Fuente: elaboración propia.

5.7. Evaluación de desempeño

La evaluación del desempeño del prototipo se ha realizado en base a los datos capturados por el equipo de monitorización de temperatura y niveles de energía eléctrica y los registros de fallas del centro de operaciones de red.

Según se puede confirmar que el equipo reporta el 96% de fallas y restablecimientos del suministro de energía eléctrica.

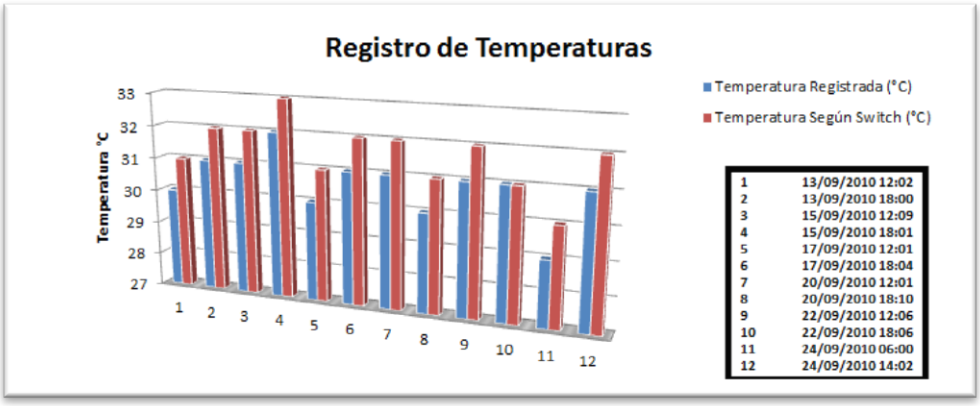
Figura 39. **Eficiencia del Sistema de Monitoreo**



Fuente: datos obtenidos del desempeño del sistema.

En el caso de las lecturas de la temperatura podemos apreciar que la temperatura captada por el equipo de monitoreo de temperatura y el equipo referencia en este caso el *Switch* instalado en el nodo difiere por 1°C aproximadamente, esto es debido a que el sensor de temperatura del *Switch* censa la temperatura interna del mismo mientras que el equipo de monitoreo censa la temperatura ambiente que rodea el equipo, a pesar de este detalle el equipo de monitoreo coincide en un 99% con el *Switch*.

Figura 40. **Registro de Temperaturas**



Fuente: datos obtenidos de las mediciones del sistema.

5.8. Estimación de costos

Los costos presentados den la tabla VII, corresponden a los precios encontrados en el mercado del presente año. Varios de los elementos del sistema generador de mensajes de texto ante fallas del suministro eléctrico no se encuentran en el mercado guatemalteco, lo que obliga a recurrir al mercado internacional. Por lo anterior, debe considerarse tiempos en envió y costos de transporte para la provisión.

Tabla VII. **Estimación de costos**

	Cantidad	Costo Unitario	Subtotal
PIC16F877	1	Q 71.63	Q 71.63
Socket DIP40	1	Q 4.35	Q 4.35
Oscilador 20MHz	1	Q 21.24	Q 21.24
Socket Oscilador	1	Q 4.35	Q 4.35
Leds	3	Q 22.23	Q 66.69
Conector Macho Alimentación/Sensor	2	Q 5.43	Q 10.86
Conector Hembra Alimentación/Sensor	2	Q 4.25	Q 8.50
Pines para conector de alimentación	2	Q 1.09	Q 2.18
Transformador de Celular	2	Q 50.00	Q 100.00
Capacitor 1µf	4	Q 0.62	Q 2.48
Resistencias	12	Q 1.48	Q 17.76
Capacitor 100µf 50V	1	Q 0.77	Q 0.77
Cable	2	Q 19.76	Q 39.52
Placa Impresa y montaje	1	Q 345.80	Q 345.80
Regulador 5V	1	Q 20.00	Q 20.00
Modulo Ethernet	1	Q 161.50	Q 161.50
DS1820	1	Q 127.50	Q 127.50
Caja de Protección	1	Q 300.00	Q 300.00
TOTAL			**Q1,305.13**

Fuente: elaboración propia.

El valor expresado en la tabla VII, representa únicamente el costo del producto, no se incluye mano de obra ni impuestos.

CONCLUSIONES

1. Las redes WAN son una tecnología que presta servicios de comunicación tanto de datos como de voz. Por medio de las redes WAN se puede establecer una comunicación bidireccional entre dos equipos geográficamente distantes, proveyéndoles de un canal de comunicación para la transmisión y recepción de datos.

2. En el período de prueba del sistema se pudo detectar un 96% de las fallas totales en el nodo instalado, lo cual convierte al sistema en una herramienta confiable para uso en la operativa diaria del personal encargado del buen funcionamiento de la red del carrier.

3. En el sistema de monitoreo del suministro de energía eléctrica y temperatura de un nodo de telecomunicaciones, el microcontrolador cumple con la función esencial de llevar a cabo todas las rutinas y procedimientos establecidos para el buen funcionamiento las mediciones de los distintos parámetros y poder desplegarlos.

4. Un sistema de monitoreo presenta el apoyo ideal para verificar el estado de los distintos equipos que conforman una red de telecomunicaciones, también permite la rápida notificación de eventos que afecten la operación de los distintos equipos.

5. Con la implementación del sistema de monitoreo del suministro eléctrico y temperatura en un nodo de telecomunicaciones, se logra mejorar el tiempo

de respuesta en una incidencia por falta de energía eléctrica en un nodo de la red.

6. El sistema de monitoreo de temperatura y suministro eléctrico en un nodo de telecomunicación ayuda por medio de la detección temprana de cualquier evento que afecte a los equipos instalados en los distintos nodos, a reducir el tiempo de indisponibilidad de los enlaces lo cual evita que el carrier caiga en penalizaciones monetarias por parte de sus clientes.

RECOMENDACIONES

1. Realizar periódicamente limpieza física de los equipos de monitoreo, equipo activo y conectores de cableado instalados en los Nodo con el fin de prevenir que estos se averíen.

2. Revisar el estado de las baterías y llevar el control de la vida útil de estas de acuerdo a las especificaciones del fabricante.

3. Mantener actualizado a la última versión disponible de software la herramienta de monitoreo y sistema operativo, esto con el fin de garantizar el desempeño óptimo de la aplicación.

4. Tomar las medidas de seguridad necesarias para que el equipo en el cual se encuentra instalada la herramienta de monitoreo no sea manipulado por personal no autorizado.

5. Mantener personal calificado en puntos estratégicos de la red con equipo y herramienta necesaria para solventar los problemas detectados por el sistema de monitoreo de temperatura ambiental y niveles de suministro eléctrico en cualquier nodo de la red WAN.

BIBLIOGRAFÍA

GUALDA GIL, Juan Andrés. *Electrónica industrial : Técnicas de potencia*. 2ª ed. México: Marcombo, 1992. 496 p. ISBN-10: 8426708439.

MANO, Morris. *Diseño digital***.** 3ª ed. México: Prentice Hall, 2005. 532 p. ISBN 9702604389.

MAZARIEGOS LANSEROS, Fernando. "Diseño e implementación de un sistema generador de mensajes en una red de telemedida, ante fallas del suministro de energía eléctrica". Trabajo de graduación de Ing. Electrónico. Facultad de Ingeniería, Universidad San Carlos de Guatemala, 2008. 93 p.

ODOM, Wendell. *CCENT/CCNA ICND1 Official Exam Certification Guide.* 2ª ed**.** Estados Unidos: Cisco Press, 2008. 641 p. ISBN 978-1-58720-182-0.

PREDKO, Myke. Programming & customizing *PICmicro microcontrollers.* 2ª ed. Estados Unidos: McGraw-Hill, 2000. 960 p. ISBN-10: 0071361723.