UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

TESIS DE LICENCIATURA QUE PARA OBTENER EL TITULO

“INGENIERO ELÉCTRICO-ELECTRÓNICO”

TESIS: DISEÑO DE UNA RED WI-FI:” CASO DE ESTUDIO ZONA RURAL”

PRESENTA:

FELIPE DE JESÚS CADENA PERALTA

DIRECTOR DE TESIS: M. I. AURELIO SÁNCHEZ VACA

CIUDAD UNIVERSITARIA 2012

AGRADECIMIENTOS

A la ***Universidad Nacional Autónoma de México*** por haberme formado cultural, profesional y socialmente.

A la ***Facultad de Ingeniería*** y a todos mis profesores de la misma que me supieron transmitir todos sus conocimientos y experiencias con el único afán de forjarme como un buen ingeniero.

Un agradecimiento especial a mis sinodales al ***M. I. Aurelio Sánchez Vaca, Ing. Gonzálo López de Haro, M. E. Alejandra Vargas Espinosa de los Monteros, M. I. Eduardo Alarcón Ávila y al Ing. Cruz Sergio Aguilar Díaz***, por el inmenso apoyo y guía para la obtención de esta tesis.

Y a todos aquellos que de una u otra manera colaboraron mediante observaciones, pláticas y conocimientos en la realización de está tesis.

A todos ellos gracias.

Felipe de Jesús Cadena Peralta

DEDICO ESTA TESIS

A mi madre, Celia:

Por su enorme sacrificio, amor, tenacidad, confianza y por que sin su apoyo no hubiera sido posible este gran logro en mi vida, ya que fue, es y será siempre una pieza muy importante en mi vida.
Muchas gracias mamita

A mi padre Felipe:

A quien me dedicó su tiempo, amor, me educó, me cuidó y me supo llevar durante este tiempo para poder cumplir todas mis metas.
Muchas Gracias papito

A mis hermanas Graciela y Jeovana:

Por perdonar mis errores, por aceptarme tal y como soy, por haberme ayudado cuando lo necesité y porque siempre estuvieron conmigo.
Muchas gracias las amo

A Arely:

Por brindarme su amor, cariño y comprensión.
Muchas gracias

A mí mentor y amigo Miguel Figueroa:

Quien me motivó y confío en mí, por su apoyo incondicional y por su enorme paciencia.
Muchas gracias

A mis amigos Marduk e Ígor:

Quien me apoyaron cuando más lo necesité, por sus consejos y su enorme comprensión.
Muchas gracias

A mis Madres Myrna y José:

Desde el primer día que las conocí me brindaron su amor, cariño y comprensión.
Muchas gracias

A mi amigo Erick:

Quien me apoyo cuando más lo necesite y quien sin recibir nada a cambio fue una pieza importante en la terminación de está tesis.
Muchas gracias

Contenido

A. Objetivos Generales 4
B. Introducción 5
1) Conceptos teóricos de una red Wi-Fi 6
1.1) Diferencia entre una red inalámbrica y una red cableada Ethernet 6
1.2) Tipos de redes inalámbricas 8
1.2.1) WPAN (Wireless Personal Area Network) 9
1.2.2) WLAN (Wireless Local Area Network) 10
1.2.3) WMAN (Wireless Metropolitan Area Network-WiMax) 10
1.2.4) WAN (Wireless Area Network) 10
1.2.5) Banda estrecha o angosta (Narrowband) 11
1.2.6) Espectro Extendido (Spread Spectrum) 11
1.3) Protocolos típicos de redes inalámbricas 14
1.3.1) Infraestructura-BSS 14
Caso 1: Estrella 14
Caso 2: Punto a punto 15
1.3.2) Punto a punto (AD-HOC) 15
1.3.3) MESH 15
1.4) Normalización de las redes inalámbricas 16
1.4.1) Alianzas de tecnología inalámbrica 17
1.5) Componentes de una red inalámbrica. 18
1.5.1) Punto de acceso (ACCESS POINT) 18
1.5.2) Adaptador de red 18
1.5.3) Switch 19
1.5.4) Router 19
1.5.5) Identificador SSID (Service Set Identifier) 19
1.6) Protocolo de comunicación 19
1.6.1) Características principales del protocolo TCP/IP 21
1.6.2) Direcciones IP 21
1.7) Conceptos básicos de seguridad en redes inalámbricas 802.11 22
1.7.1) Mecanismos y factores de seguridad 24
1.7.2) Los factores de seguridad se definen en un entorno inalámbrico pueden reducirse en cinco elementos básicos: 24
1.8) Problemas de seguridad en redes Wi-Fi 25
1.8.1) Problemas inherentes a su medio de transmisión 25
1.8.1.1) Puntos de acceso mal configurados 25
1.8.1.2) Punto de acceso no autorizado (Rogue) 25
1.8.2) Ataques particulares a Wi-Fi 25
1.8.2.1) Ataques pasivos 26
1.8.2.2) Ataques activos 26
1.8.2.3) Tipo de ataque DoS 26
1.8.2.4) Ataques avanzados 27
1.9) Evolución de la seguridad en redes 802.11 29
1.9.1) Requerimientos para tener una red inalámbrica segura 30
1.9.2) WEP 30
1.9.2.1) Elemento de cifrado WEP 31
1.9.2.2) Vulnerabilidades de WEP 32
1.9.3) WPA 33

1.9.3.1) WPA y sus actualizaciones *34*
1.9.3.2) Modos de funcionamiento de WPA *35*
1.9.4) WPA2 ..... *36*
1.9.4.1) 802.11i: La Solución de Seguridad del IEEE para WLANs *37*
1.9.4.2) Protocolos Utilizados en 802.11i *38*
1.10) 802.11i precisa los protocolos *42*
1.9.1) WRAP Y CCMP *42*
1.10.2) MIC *42*
1.10.3) RSN *43*
1.9.4) Beneficio y problemáticas de 802.11i *44*
1.9.5) Resumen de las normas de seguridad para WLANs *45*
2) La Telemedicina (e-salud) *46*
2.1) Breve historia de la Telemedicina *46*
2.2) Telemedicina en México *48*
2.2) ¿Qué es la Telemedicina? *49*
2.3) Medios de comunicación y tecnología requerida para el funcionamiento de una red de Telemedicina *50*
2.3.1) Niveles de atención *50*
2.4) Unidades requeridas para la transmisión de una red en Telemedicina vía satelital *57*
2.5) Telemedicina a nivel Mundial *58*
2.6) Zona Rural *59*
2.7) Localidades rurales en México *60*
3) Herramientas Diagnósticas *61*
3.1) Introducción *61*
3.2) Historia Clínica *61*
3.1.2) Lista de problemas *62*
3.1.3) Planes iníciales de acción *63*
3.1.4) Notas de evolución *64*
3.2) El Teorema de Bayes *65*
3.3) Diferentes tipos de diagnósticos *67*
3.3.1) El cambio de peso *67*
3.3.2) Cambio en el apetito *69*
3.3.3) Sudoración anormal *71*
3.3.4) Escalofrío *72*
3.3.5) Fiebre *73*
3.3.6) Pruebas de laboratorio *76*
3.3.7) Radiografías *77*
3.3.8) Ultrasonografías y Resonancia magnética *78*
3.3.9) Gammagrafías *78*
3.3.10) Biopsia *78*
3.3.11) Fiebre de origen oscuro (FOO) *78*
3.3.12) Debilidad o Astenia *79*
3.3.13) Agudeza visual *80*
3.3.14) Hipoacusia *82*
3.3.15) Acúfenos *84*
3.3.16) Otorrea y otorragía *85*
3.3.17) Otalgia *85*
3.3.18) Vértigo *86*
3.3.19) Rinorrea *87*

3.3.20) Epistaxis *87*
3.3.21) Alteraciones del gusto *88*
3.4) Tipos de exploración complementaria *89*
3.4.1) Alimentación *89*
3.4.2) Sodio y cloro *90*
3.4.3) Ocupación *90*
3.4.4) Tabaquismo *90*
3.4.5) Alcoholismo e ingestión de bebidas alcohólicas *91*
3.4.6) Fármacodependencia *92*
3.5) Errores en el diagnóstico *93*
4) Diseño de la red Wi-Fi *95*
4.1) Diámetro de una red *96*
4.2) Redundancia de una red *96*
4.3) Tecnología PoE (Power over Ethernet) *97*
4.4) Consideraciones para la elección del switch para la red Wi-Fi *98*
4.5) Switch con Tecnología PoE (Power over Ethernet) *99*
4.6) RJ45 ..... *100*
4.7) Protocolos de enrutamiento *101*
4.8) Simulación de la red *103*
5) CONCLUSIONES *109*
GLOSARIO *110*
BIBLIOGRAFÍA *119*
MESOGRAFÍA *120*

A. Objetivos Generales

Definir los parámetro necesarios para el diseño de una red Wi-Fi, que sirva de enlace entre hospitales y médicos especializados con las comunidades rurales de bajos recursos, con la finalidad de hacer un diagnostico médico a distancia y con base en este, establecer acciones que puedan auxiliar en el tratamiento del paciente.

Es importante tomar en cuenta la brecha tecnológica e ideológica que en una zona rural normalmente prevalece, considerando la cultura, ideología, creencias religiosas y prácticas médicas de la misma.

B. Introducción

La comunicación es un elemento fundamental en el actuar médico, por lo que es necesario estudiar las condiciones para establecer una red inalámbrica en una zona rural, donde es necesario realizar un estudió para poder introducir la tecnología en una zona donde a lo mejor no se cubren las necesidades básicas.

Es necesario estudiar los ataques que se realizan a las redes inalámbricas para poder tenerlas en cuenta cuando se está configurando, es necesario conocer las características de los dispositivos que componen la red para poder establecer mecanismo de defensa en el robo de la información.

La propuesta de solución para el problema expuesto, consiste en diseñar una red inalámbrica con el programa Cisco Packet Trace que fue proporcionado por el Laboratorio de Redes de la Facultad de Ingeniería de Ingeniería de la UNAM.

En la simulación se muestran los protocolos de enrutamiento OSPF y el EIGRP más ocupados en la vida profesional y se ocupa la tecnología Power over Ethernet, descrita en está tesis y tomando en cuenta los niveles de atención de la telemedicina y las características de las zonas rurales.

1) Conceptos teóricos de una red Wi-Fi

Una red Wi-Fi es aquella que conecta dispositivos sin la necesidad de utilizar cables como medio de comunicación.

Las redes Wi-Fi están ganando mucha popularidad en casas y oficinas, debido a que los dispositivos que se conectan inalámbricamente a la red pueden ser incorporados a redes cableadas existentes con mayor facilidad, favoreciendo costos de adecuación de la red (como tendido de cables por ejemplo) y dando una mayor movilidad a los dispositivos, resolviendo así muchos problemas de conectividad en lugares de difícil acceso.

Los elementos que se necesitan para proveerse de una red Wi-Fi incluyen:

- Tarjeta de red inalámbrica.
- Access Point o puntos de acceso.
- Router Wireless que llevaran incorporado una antena Wi-Fi.
- Switch

Estos elementos los describiré más detalladamente en el capítulo 1.15 de esta tesis.

Para poder establecer la red inalámbrica requerida es importante hablar del medio de transmisión utilizado para la transmisión de los paquetes datos.

Las ondas electromagnéticas viajan en el vacío a 300,000 Kilómetros por segundo, teniendo una velocidad variable que depende del medio en que se transmiten.

Los principales factores que afectan las comunicaciones de radio son:

Distorsión: Deformación de una señal en cuanto a su amplitud, frecuencia ó fase.

Atenuación: Es la pérdida de potencia por la señal al transitar por cualquier medio de transmisión.

Interferencia: Es cualquier proceso que altera, modifica o destruye una señal durante su trayecto en el canal existente entre el transmisor y el receptor.

Reflejo: Cambio de dirección de las ondas electromagnéticas que inciden sobre una superficie o cuerpo.

Asincronía: Cuando la señal pierde su sincronía o es susceptible de desarrollarse con independencia del desarrollo de otros procesos.

1.1) Diferencia entre una red inalámbrica y una red cableada Ethernet

Una red cableada envía señales eléctricas a través de un medio físico, ***Wi-Fi*** envía señales de Radio Frecuencia a través del aire.

El cable es un medio exclusivo, mientras que el aire es un medio compartido**,** por lo tanto, la información que se transmite por el cable es privada, a diferencia de la que se transmite por el aire que es pública**.** El alcance aproximado de las ondas de radio frecuencia en las redes ***Wi-Fi*** es de 100 metros**.**

El hecho de que la información en las redes inalámbricas ***Wi-Fi*** viaje por el aire, y no por cable, genera grandes problemas de seguridad. En la siguiente tabla se muestran algunas diferencias.

Red cableada Ethernet	Red inalámbrica Wi-Fi
Envía la información a través de un medio exclusivo**:** CABLE.	Envía la información a través de un medio compartido: AIRE.
Envía señales eléctricas.	Envía energía, ondas de radio frecuencia.
La información que se transmite por cable no puede ser vista por extraños.	La información que se transmite por el aire puede ser vista por cualquiera.

Tabla 1.1 Diferencias entre una red Ethernet y una Wi-Fi

Las redes inalámbricas se diferencian de las cableadas en las dos primeras capas del modelo OSI.

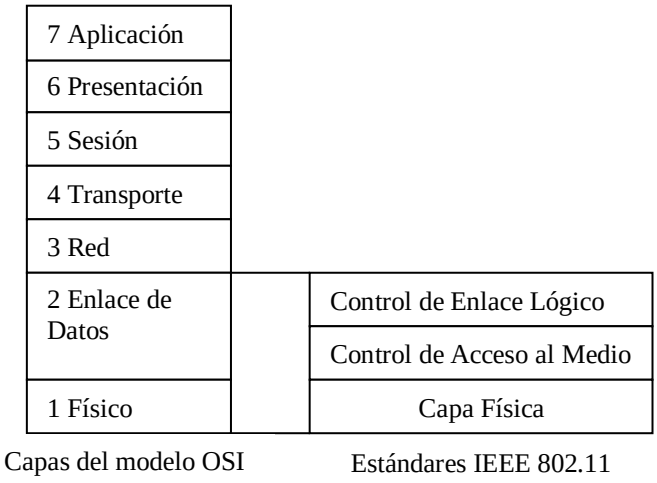


Figura 1.1

La capa física se encarga de las señales de radiodifusión a transmitir a nivel de bits.

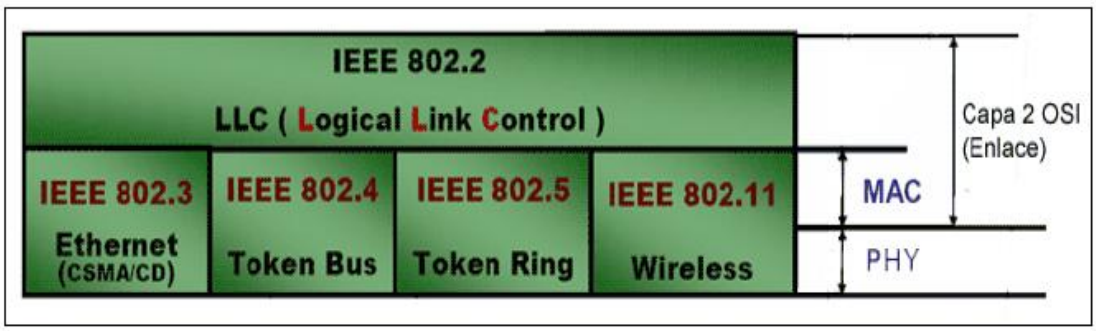


Figura 1.2 Visualización de la división de las capas 1 y 2

La segunda capa, enlace de datos, se divide en dos subcapas y tiene funciones de control de flujo e integridad de las comunicaciones:

LLC – Control Lógico de Enlace (Logical Link Control) ó 802.2

MAC – Control de acceso al Medio (Media Access Layer)

La subcapa LLC, también comunica a la capa 1 y 3

La subcapa MAC tiene una dirección de 20 bytes en base hexadecimal, es única a nivel mundial y es establecida por el fabricante para identificar cada dispositivo en la red.

Es por eso que está capa es conocida como capa de ***direccionamiento MAC***.

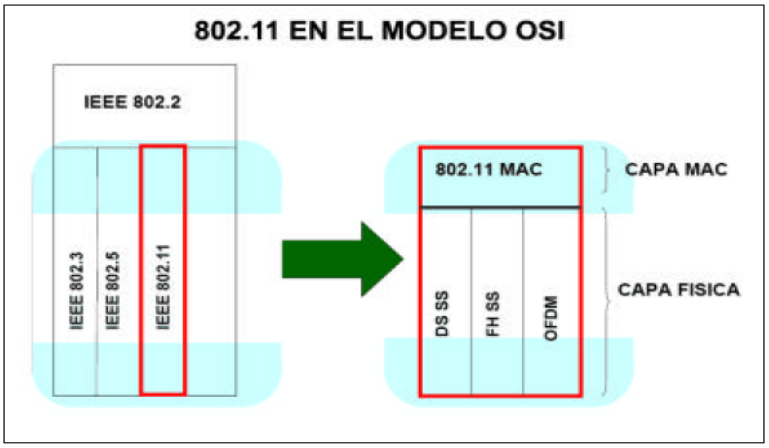


Figura 1.3 Métodos de señalización en 802.11 bajo el modelo OSI

Ambas capas se encuentran implementadas en los dispositivos de red, los cuales tienen procesadores dedicados únicamente a estas tareas.

Adicionalmente una red Ethernet convencional utiliza un protocolo de acceso al medio denominado CSMA/CD Acceso múltiple con sensor de portadora / Detección de colisiones (Carrier Sense Multiple Access / Collision Deteccion).

1.2) Tipos de redes inalámbricas

Las redes inalámbricas difieren de las convencionales en la capa física y en la capa de enlace de datos, según el modelo OSI.

La capa física indica como son enviados los bits de una estación a otra, mientras que la de enlace de datos describe cómo se empaquetan nuevamente los datos y el modelo de verificación de los bits

Figura 1.4 Funciones de las capas del modelo OSI

para que no contengan errores.

Al cambiar los cables por otros medios de naturaleza similar, no importa sobre qué medios de red subyacente se opera, es posible construir una red que opere sobre cualquier medio (cable coaxial, alambre de par trenzado, fibras de radio, ondas de radio, etc.).

La clasificación de redes inalámbricas se describe en la siguiente tabla:

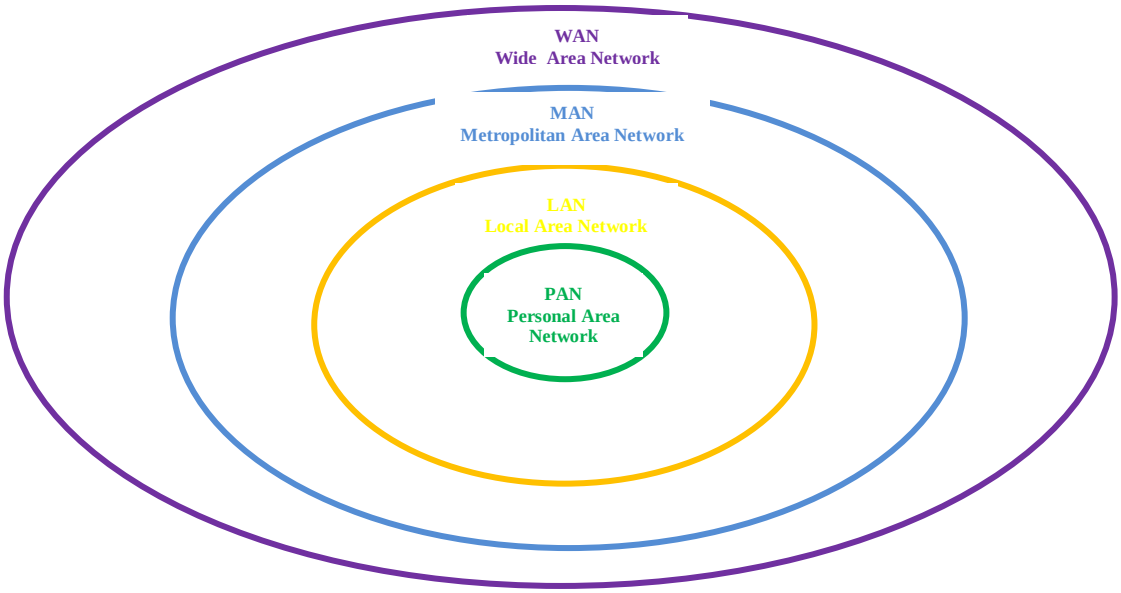


Figura 1.5 Clasificación de redes inalámbricas

1.2.1) WPAN (Wireless Personal Area Network)

Es una red que cubre 10 metros como máximo, normalmente utilizadas para dispositivos portátiles personales.

Esta comunicación de dispositivos *peer-to-peer* normalmente no requiere de altos índices de transmisión de datos y esto da como beneficio bajo consumo de energía haciendo a la WPAN adecuada para dispositivos móviles pequeños (celulares, PDAs o cámaras digitales).

El grupo de trabajo de IEEE 802.15 ha definido tres clases de WPANs que se diferencian por su rango de transmisión de datos, consumo de energía y calidad de servicio (QoS).

a) Las WPANs con un rango de transmisión de datos elevada (802.15.3) diseñado para aplicaciones multimedia que requieren altos niveles de QoS.
b) Las WPANs con un rango medio de transmisión de datos (802.15.1/Bluetooht)
c) que maneja una cantidad de tareas que van desde teléfonos celulares hasta comunicación con PDAs y tienen QoS apropiado para aplicaciones de voz.
d) La RL-WPANs con un rango bajo de transmisión de datos (802.15.4).

1.2.2) WLAN (Wireless Local Area Network)

Es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros. Existen varios tipos de tecnologías:

a) **Wi-Fi** (o IEEE 802.11) con el respaldo de WECA (Wireless Ethernet Compatibility Alliance) ofrece una velocidad máxima de 54 Mbps en una distancia de varios cientos de metros.
b) **hiperLAN2** (*High Performance Radio LAN 2.0*), estándar europeo desarrollado por ETSI (*European Telecommunications Standards Institute*). HiperLAN 2 permite a los usuarios alcanzar una velocidad máxima de 54 Mbps en un área aproximada de cien metros, y transmite dentro del rango de frecuencias de 5150 y 5300 MHz.

1.2.3) WMAN (Wireless Metropolitan Area Network-WiMax)

a) ***WiMax (Worldwide Interoperaability for Microwave Access):*** Es una red con transmisión inalámbrica estándar (802.16) de datos que, gracias a su ancho de banda, permite el despliegue de servicios fijos de voz, acceso a internet, comunicaciones de datos en redes privadas, y video bajo demanda.

Wimax ofrece conexiones de velocidades similares al ADSL, lo que lo convierte en el principal candidato para la base de las redes Metropolitanas de acceso a Internet, además de servir de apoyo para facilitar las conexiones en zonas rurales, y usarse en el mundo empresarial para implementar las comunicaciones internas.

1.2.4) WAN (Wireless Area Network)

Es una red capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente.

Las tasas de transmisión en redes WAN se extienden generalmente a partir de 1200 bit/s hasta 24 Mbit/s, a pesar de algunas conexiones, tales como cajeros automáticos y líneas arrendadas[1] pueden llegar a velocidades superiores a 156 Mbit/s.

Las redes WAN mas utilizadas son las líneas telefónicas, enlaces de microondas y vía satélite.

Los métodos para transferir información en redes inalámbricas pueden clasificarse en sistemas de banda angosta (***Narrowband***) y en sistemas basados en espectro Disperso o Expandido (***Spread Spectrum).***

[1] Línea Arrendada.- Es una conexión punto-a-punto entre dos ordenadores o redes de área local (LAN).

	WPAN	WLAN	WMAN	WAN
Standards	Bluetooth	802.11a, 11b, 11g, HiperLAN2	802.11 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G
Velocidad	< 1 Mbps	2 a 54+Mbps	22+ Mbps	10 a 384 Kbps
Rango	Corto	Medio	Medio	Largo
Aplicaciones	Peer-to-Peer Device-to-Device	Enterprise Networks	Fixed, last mile Access	PDAs, teléfonos móviles, acceso celular

Tabla 1.2 Clasificación de redes inalámbricas

1.2.5) Banda estrecha o angosta (Narrowband)

Un sistema de radio de banda angosta transmite y recibe información del usuario sobre una frecuencia específica. Un radio de banda angosta mantiene la frecuencia de la señal de radio tan estrecha como es posible, sólo para pasar la información.

Una técnica usada para evitar interferencia indeseable entre los canales de comunicación, es coordinar cuidadosamente diferentes usuarios sobre diferentes canales de frecuencia.

Para reforzar la seguridad y evitar interferencias en un sistema de radio, se hace uso de frecuencias separadas. El radio receptor filtra todas las señales, excepto aquellas que están sobre la frecuencia para la cual es diseñado.

Desde el punto de vista cliente, una desventaja de la tecnología de banda angosta es que la terminal del usuario debe obtener una licencia de la Comisión Federal de Telecomunicaciones (COFETEL) para cada sitio donde sea empleado.

1.2.6) Espectro Extendido (Spread Spectrum)

El protocolo **IEEE 802.11** o **Wi-Fi** es un estándar de protocolo de comunicaciones del IEEE que define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todos los mismos protocolos. El estándar original de este protocolo data de 1997, era el **IEEE 802.11**, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz.

Los productos 802.11 usan técnica de espectro extendido para transmitir sus señales, la cual es una tecnología de banda amplia desarrollada por militares estadounidenses que proveen comunicaciones seguras, confiables y de misión crítica.

La tecnología de espectro extendido esta diseñada para intercambiar eficiencia en ancho de banda por confiabilidad, integridad y seguridad.

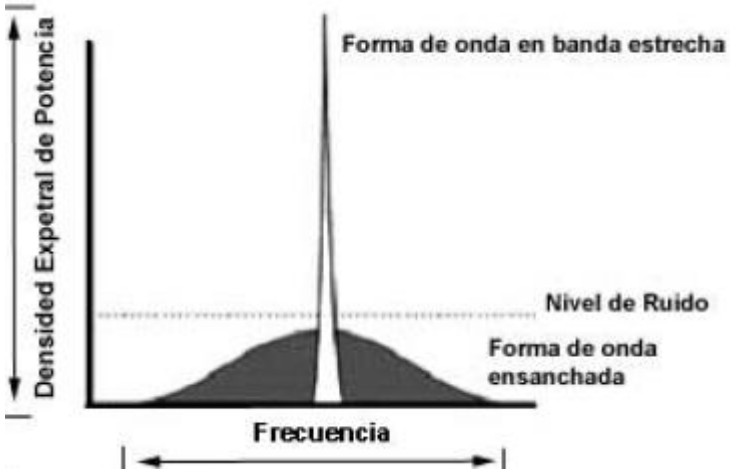


Figura 1.6 Espectro Extendido y Angosto

Existen dos tipos de espectro extendido disponibles para 802.11:

a) Salto de frecuencia (Frecuency Hopping Spread Spectrum)
b) Secuencia directa (Direct Sequence Spread Spectrum)

a) Espectro Extendido con Salto de Frecuencia (FHSS)

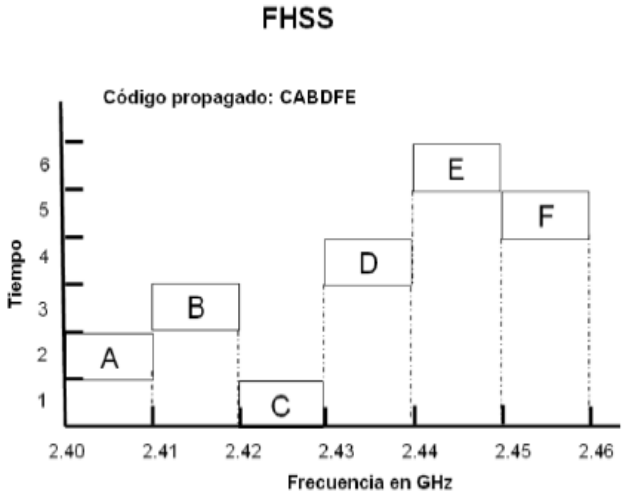


Figura 1.7 Espectro extendido con salto de Frecuencia

Está tecnología aparece después de la segunda Guerra Mundial y utiliza una portadora de banda angosta que cambia de frecuencia cada 400 milisegundos, en una secuencia establecida previamente antes de la transmisión. En la figura I.6 la secuencia sería 2, 3, 1, 4, 6, 5. El transmisor y el receptor deben de estar sincronizados, comunicándose por un canal de control que cambia de frecuencia a cada momento.

El ***FHSS*** es utilizado para comunicaciones a corta distancia, en aplicaciones por lo general se tiene una cantidad de receptores cercanas el punto de acceso. Utiliza 75 subcanales de 1MHz cada uno.

Esta tecnología está siendo desechada y solo un proveedor de chips la sigue soportando.

b) Espectro Extendido con Secuencia Directa (DSSS)

El ***DSSS*** genera un patrón de bits redundante llamado chip de 11 elementos. Cada bit al ser transmitido es convertido a código chip. Es por eso que si uno ó mas bits se daña, técnicas estadísticas embebidas dentro del transmisor podrán recuperar la señal original sin necesidad de retransmisión.

Esta técnica divide la banda ISM[2] 2.4 GHz en 14 canales con 22 Mhz cada uno. El desempeño de DSSS puede mejorar al aumentar la señal de reloj o la complejidad de la modulación.

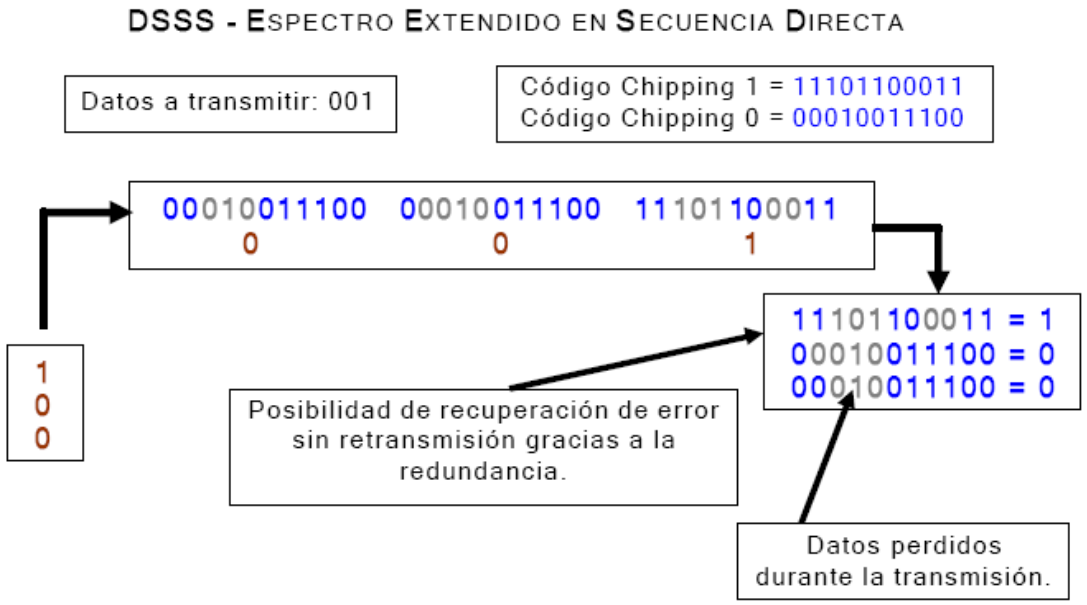


Figura 1.8 Código chip de 11 elementos por cada bit a transmitir

c) Ventajas y Desventajas del espectro extendido

El espectro extendido tiene muchas propiedades únicas y diferentes que no se pueden encontrar en ninguna otra técnica de modulación.

Ventajas:

- Resiste todo tipo de interferencia, tanto las intencionadas como las malintencionadas (más conocidas con el nombre de jamming), siendo más efectivo que las de banda estrecha.
- Tiene la habilidad de eliminar o aliviar el efecto de las interferencias multitrayecto.
- Se puede compartir la misma banda con otros usuarios.
- Confidencialidad de la información transmitida gracias a los saltos seudo aleatorios.
- FHSS es mejor contra las interferencias.

Desventajas:

- Utilización de mayor ancho de banda. DSSS la utiliza más eficiente que FHSS.
- La implementación de los circuitos es en algunos casos más compleja.
- Incompatibilidad. FHSS y DSSS no pueden coexistir.
- Velocidad máxima de 2 Mbps en FHSS debido a su limitación de frecuencia de1Ghz.

[2] Banda ISM. –Banda Industrial, Scientific and Medical

1.3) Protocolos típicos de redes inalámbricas

1.3.1) Infraestructura-BSS

Esta configuración se logra al instalar el Punto de Acceso cuya cobertura es llamada célula, cada una de estás contribuye a formar lo que se le denomina arquitectura celular también conocida como BBS[3].

Cada punto de acceso actúa como regulador de tráfico entre los diferentes equipos móviles. Tiene por lo general una cobertura de 100 metros a la redonda, dependiendo del número y tipos de obstáculos que haya en la zona.

Un punto de acceso permite la conectividad a la red cableada, con lo cual, las estaciones inalámbricas pueden ser agregadas fácil y rápidamente a la red corporativa; permitiendo hacer uso de los recursos bajo la misma infraestructura.

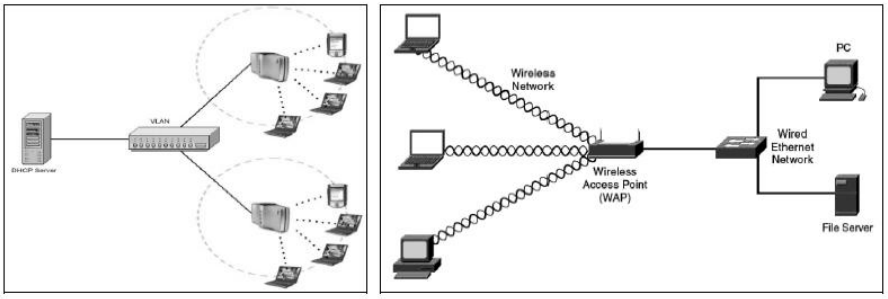


Figura 1.9 Redes inalámbricas operando en modo de infraestructura

Caso 1: Estrella

La topología estrella es la más utilizada en redes inalámbricas, es la tecnología usada para un *hotspot (punto de conexión a internet)*.

Frecuentemente se utiliza está topología con otras para mejorar el rendimiento de la red inalámbrica.

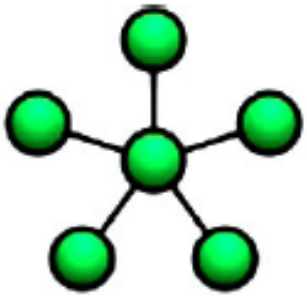


Figura I.9 Configuración estrella

Configuración	***Nodo 1***	***Nodo 2***
Modo	Infraestructura	Infraestructura
SSID	Definir MI_SSID	Conectar a MI_SSID
Canal	Definir el canal x	Descubrir el canal
Dirección IP	Normalmente tiene un servidor DHCP (si cuenta con características de enrutamiento)	Normalmente toma la IP que se le asigna por DHCP

Tabla 1.3 Configuración típica de una red Estrella

[3] BBS.-Basic Service Set-Conjunto de Servicios Básicos

Caso 2: Punto a punto

Esta topología puede ser parte de una topología estrella, de una simple línea entre dos puntos.

Figura 1.10 Configuración Punto a apunto

Configuración	*Nodo 1*	*Nodo 2*
Modo	Infraestructura	Infraestructura
SSID	Definir MI_SSID	Conectar a MI_SSID
Canal	Cualquier canal	Cualquier canal
Dirección IP	Normalmente fija	Normalmente fija
Dirección MAC	Puede referirse a la MAC del otro nodo	Puede referirse a la MAC del otro nodo

Tabla 1.4 Configuración típica de un enlace punto a punto

1.3.2) Punto a punto (AD-HOC)

Esta configuración, denominada IBSS[4], AD-HOC ó P2P[5], los equipos móviles se conectan unos con otros, sin necesidad que exista un punto de acceso, utilizando una **tarjeta de red inalámbrica** para llevar acabo dicha conexión.

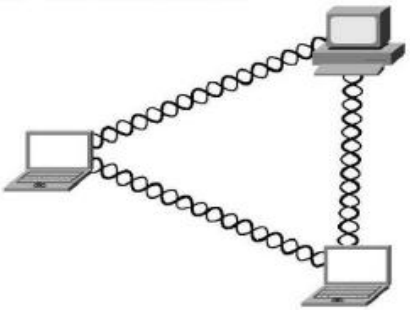


Figura 1.11 Red inalámbrica Ad-Hoc

Configuración	*Nodo 1*	*Nodo 2*
Modo	Ad-Hoc	Ad-Hoc
SSID	MI_SSID	MI_SSID
Canal	Debe de ser convenido y conocido por todos	Debe de ser convenido y conocido por todos
Dirección IP	Normalmente fija	Normalmente fija

Tabla 1.5 Configuración típica de una red Ad-Hoc

1.3.3) MESH

Son aquellas en las que se mezclan las dos topologías de las redes inalámbricas, la topología Ad-hoc y la topología infraestructura. Básicamente son redes con topología de infraestructura pero que permiten unirse a la red a dispositivos que a pesar de estar fuera del rango de cobertura de los puntos de acceso están dentro del rango de cobertura de alguna tarjeta de red (TR) que directamente o indirectamente está dentro del rango de cobertura de un punto de acceso (PA).

Permiten que las tarjetas de red se comuniquen entre sí, independientemente del punto de acceso. Esto quiere decir que los dispositivos que actúan como tarjeta de red pueden

[4] IBSS.-Independ Basic Service Set-conjunto de Servicios Básicos Independientes.
[5] P2P.-Point to Point-Punto a Punto.

no mandar directamente sus paquetes al punto de acceso sino que pueden pasárselos a otras tarjetas de red para que lleguen a su destino.

Para que esto sea posible es necesario el contar con un protocolo de enrutamiento que permita transmitir la información hasta su destino con el mínimo número de saltos.

Este protocolo tiene un problema, debido que los saltos entre nodos provoca retardos que se van añadiendo unos a otros.

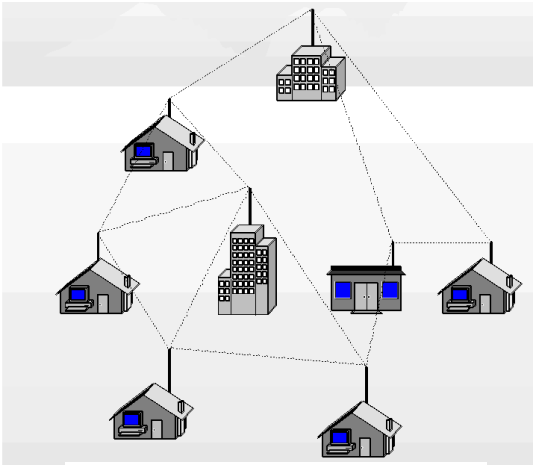


Figura 1.12 Red inalámbrica Mesh

1.4) Normalización de las redes inalámbricas

Hay instituciones que se encargan de establecer los estándares y normas a escala mundial, para tener una base común de referencia en la cual se pueda trabajar de manera ordenada en el desarrollo tecnológico como en otras áreas del conocimiento.

En el desarrollo de una nueva tecnología, se hace necesaria la existencia de recomendaciones, para permitir a los productos una operación adecuada entre sí y se cumpla con un mínimo de calidad y funcionalidad.

La normalización o estandarización es la redacción y aprobación de documentos técnicos con las siguientes características:

1) Contienen especificaciones técnicas de aplicaciones.
2) Son elaboradas por consenso de las partes interesadas:

    2.1 Fabricantes
    2.2 Administradores
    2.3 Usuarios y consumidores
    2.4 Centro de investigación y laboratorios
    2.5 Asociaciones y Colegios profesionales

3) Están basadas en los resultados de la experiencia y el desarrollo tecnológico.
4) Son aprobados por organismos nacionales, regionales o internacionales de normalización.
5) Están disponibles al público.

Las normas establecen un lenguaje común de comunicación entre los diferentes agentes que participan en las transacciones comerciales, jurídicas, tecnológicas y son un modelo necesario de confianza entre sus participantes.

Los siguientes organismos crean, desarrollan, definen y proponen estándares internacionales oficiales a la industria a través de un proceso abierto a las compañías y son:

IEEE → Institute of Electrical and electronics Engineers
IETF → Internet Engineering Task Force
ISO → International Standard Organization
ITU → International Telecommunications Union
ETSI → European Telecommunications Standards Institute

IEEE: Es el Instituto de Ingenieros Eléctricos y Electrónicos fue creado en Estados Unidos en 1963 a partir de otras instituciones como el AIEE (American Institute of Electrical Engineers) y el IRE (Institute of Radio Engineers). Es una asociación sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros en telecomunicaciones, en computación, eléctricos electrónicos, en informática. Su trabajo es promover la creatividad, el desarrollo y la integración para compartir y aplicar los avances de la tecnología de la información, electrónica y ciencias en general en beneficio de la humanidad y de los mismos profesionales.

IETF: Es el grupo de ingenieros para Internet, tiene como objetivo en contribuir en la ingeniería del Internet, actuando en diversa áreas como transporte, encaminamiento y seguridad. Fue creada en Estados Unidos en 1986.

ISO: La organización Internacional para la estandarización, es una organización internacional no gubernamental, compuesta por representantes de los cuerpos de estandarización nacionales, que producen estándares nacionales, estándares mundiales industriales y comerciales.
ISO coopera estrechamente con la Comisión Electrotécnica Internacional (IEC), que es la responsable de la estandarización de los equipos electrónicos.
ISO no es un acrónimo; proviene del griego, que significa igual.

ITU: La Unión de Telecomunicaciones Internacional, es el organismo especializado en las Naciones Unidas en cargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.

ETSI: Instituto de Estándares y Telecomunicaciones Europeo, produce estándares de Telecomunicaciones usados en Europa.

1.4.1) Alianzas de tecnología inalámbrica

Las alianzas tecnológicas se forman para introducir un protocolo o una tecnología específica y prever interoperabilidad y certificación de productos de diferentes compañías que utilizan esta tecnología o protocolo.

BLUETHOOTHSIG: Utiliza tecnología de radio frecuencia para prever conectividad a Internet, a computadoras portátiles, teléfonos móviles u otros dispositivos móviles formando redes conocidas como Redes de Área Personal (PAN).

HIPERLAN1, HIPERLAN ALLIANCE E HIPERLAN2 GLOBAL FORUM: Organizaciones Europeas que utilizan enlaces de radio de alto desempeño en las frecuencias en el rango de 5 GHz.

HOMERF: Basada en una especificación para comunicaciones inalámbricas en hogares conocida por sus siglas en inglés SWAP (Shared Wireless Access Protocol). El HRFFW (Grupo de Trabajo para Radio frecuencia Casera) se fundó para preveer los cimientos aun amplio rango de dispositivos al establecer una especificación abierta a la industria de comunicaciones digitales inalámbricas, entre PCs y dispositivos domésticos alrededor de los hogares.

ALIANZA WI-FI: Se formo en agosto de 1999 por las compañías 3Com, Aironess gíreles Communications, Harris Semiconductor, Lucent Technologies, Nokia y Symbol Technologies. Certifica la interoperabilidad de productos WLAN y promueve el término WI-FI como el nombre de marca global para los productos basados en 802.11. Solo aquellos productos que pasan las pruebas de la Alianza WI-FI se les permiten referirse como WI-FI certificados. A estos se les requiere llevar un sello de identificación en sus paquetes que indique tanto su estatus de certificación, así como la banda de radio frecuencia en la que opera (2.5 GHz para 802.11 b/g y 5GHz para 802.11 a).

1.5) Componentes de una red inalámbrica.

1.5.1) Punto de acceso (ACCESS POINT)

Es un dispositivo inalámbrico central de una red inalámbrica ***WI-FI*** (Wireless) que por medio de ondas de radio frecuencia (RF) recibe información de diferentes dispositivos móviles y la transmite a través de cable al servidor de la red cableada.

Figura 1.13 Punto de acceso inalámbrico

1.5.2) Adaptador de red

Figura 1.14 Adaptador de red

Es una tarjeta de red inalámbrica, conocida como ***NIC*** por sus siglas en inglés ***(Network Interface Card – Tarjeta de Interface de Red).*** Permite a un equipo conectarse con otros equipos inalámbricos o con punto de acceso.

1.5.3) Switch

Es un equipo que trabaja en capa dos del modelo OSI, a nivel de MAC (dirección física de una red), entonces los switch no buscan direcciones IP sino direcciones MAC y esto hace posible que los dispositivos se puedan comunicar en una red.

Figura 1.15 switch

1.5.4) Router

Es un equipo de capa tres del modelo OSI y trabaja a nivel de IP, cada dispositivo de la red debe tener una asignada, el router es un dispositivo que conecta dos o más redes.

Figura 1.16 Router

1.5.5) Identificador SSID (Service Set Identifier)

Este identificador es definido durante la configuración del equipo inalámbrico. Permite definir a que red pertenece.

1.6) Protocolo de comunicación

Soporta los sistemas operativos de redes habituales, lo que es una gran ventaja para los usuarios que pueden seguir utilizando sus aplicaciones habituales, con independencia del medio empleado. El protocolo soportado es el ***TC/IP***, aunque se pude utilizar cualquier otro. Utilizaremos este protocolo por la familiaridad de este en la facultad.

E protocolo ***TC/IP*** este ya lo hemos utilizado indirectamente y lo confunden con un solo protocolo cuando en realidad son varios, y uno de los más importantes es el IP.

TC/IP se esconde uno de los protocolos más usados en el mundo.

TC/ IP (Transmisión Control Protocol/Internet Protocol), en el año de 1973 la DARPA (Defense Advance Research Projects Agency) inició un programa de investigación de tecnologías de comunicación entre redes de diferentes características. El proyecto se basaba en la transmisión de paquetes de información, y tiene por objetivo la interconexión de redes. De este proyecto surgieron dos redes: Una de investigación, ARPANET, y una de uso exclusivamente militar, MILNET. Para comunicar las redes, se desarrollaron varios protocolos. El protocolo de Internet y los protocolos de control de transmisión.

Posteriormente estos protocolos se englobaron en el conjunto de protocolos TC/IP. En 1980, se incluyó en el UNIX 4.2 de BERKELEY, y fue el protocolo militar estándar de 1983. Con el nacimiento en 1983 de Internet, este protocolo se popularizó. ARPANET dejo de funcionar oficialmente en 1990.

El propósito de ***TC/IP*** es proporcionar los protocolos necesarios de transmisión de la información independientemente de la red o equipo utilizado, aplicándose en organizaciones que precisaban establecer conexiones entre distintos tipos de LAN, ***TCP/IP*** ha sido elevado de forma inmediata al dominio de la Internet, ya que el modelo básico en Internet es el modelo Cliente/servidor. El clientes un programa que le solicita a otro un servicio. El servidor es el que proporciona este servicio. La arquitectura de Internet esta basada en capas. Esto hace más fácil implementar otros protocolos. El conjunto de protocolos ***TC/IP*** al estar integrado plenamente en Internet, también dispone de esta arquitectura.

El protocolo ***TC/IP*** trabaja definiendo una red de intercambio por paquetes, lo que significa que la información a las computadoras se transmiten en partes: una parte esta conformada por los paquetes que contienen una "carga" de datos y, la otra, por la información de cabecera que identifica el envío, constituida por la dirección del destino y los códigos de corrección de errores. Algunas ordenes requieren tan sólo un único paquete, la transmisión de archivos de gran extensión se dividen en múltiples paquetes, debiendo incluir una secuencia de números indicativos del orden según el cual los paquetes se deben reensamblar en el sistema de destino.
Una de las características más importantes del protocolo TC/IP es su esquema de direccionamiento en la red, el cual proporciona una forma de direccionar diferentes redes, así como los nodos de las mismas. Este esquema es extensivo, dando cabida a millones de posibles direcciones en una escala global.

Las direcciones de Internet son registradas y asignadas por el ***NIC (Network Interface Card – Tarjeta de Interface de Red),*** a fin de evitar conflictos aunque no es esencial registrar las direcciones, si tan sólo se tratara de establecer una conexión entre redes en un ámbito reducido.

El protocolo ***TCP*** proporciona un servicio de comunicación que forma un circuito, es decir, que el flujo de datos entre el origen y el destino parece que sea continuo. ***TCP*** proporciona un circuito virtual el cual es llamado una conexión. El protocolo ***TCP*** corresponde al estrato de sesión y transporta el modelo ***OSI. TCP*** recibe información de las aplicaciones que operan en niveles superiores en la pila de protocolos, y es

responsable desempaquetado y la transmisión a través de la red. ***TCP*** pasa a ***IP*** los paquetes que crea.

El protocolo IP corresponde al estrato de red en el modelo OSI. Este se encarga de crear los paquetes de información, y es el responsable de añadir las direcciones IP de origen y destino. Algo que IP no puede proporcionar es la garantía de que los paquetes llegaran a su destino, y en el orden adecuado. Por este motivo TCP añade información a cada uno de los paquetes que este módulo crea, en la que incluye datos de identificación y su ubicación. Si ***IP*** pierde un paquete ***TCP*** es el responsable de determinar cuál es el paquete perdido, y de volverlo a enviar.

1.6.1) Características principales del protocolo TCP/IP

- Independencia de tecnologías de redes. Ya que no está basado sobre el hardware de ningún vendedor en especial. Los protocolos ***TCP/IP*** definen la unidad de transmisión como datagramas y especifican cómo transmitir datagramas en una red.
- Interconexión universal (Puede funcionar en máquinas de cualquier tamaño). Una red de ***TCP/IP*** permite la comunicación de cualquier pareja de computadoras que forman parte de la red. A cada computadora se le asigna una dirección, que es reconocida por todos los equipos integrantes de la red. Cada datagrama lleva la dirección de origen y destino. Las computadoras intermedias usan la dirección de destino para tomar decisiones de ruteo.
- Acuse de recibo entre computadoras que dialogan. Los protocolos ***TCP/IP*** proporcionan un acuse de recibo sólo entre las dos computadoras que dialogan y no entre máquinas sucesivas que forman parte de la trayectoria.

1.6.2) Direcciones IP

La dirección Internet Protocolo ***(IP)*** de un nodo de direccionamiento lógico, es independiente de la dirección física asigna por la tarjeta de red por el fabricante de la misma. La dirección ***IP*** es independiente de la configuración de la red. La dirección ***IP*** tiene la misma forma, no importa el tipo de red que se usa. Este formato es el valor numérico de 4 bytes (32bits), que sirve para identificar, tanto a la red, como al nodo de la misma. Cada dirección ***IP*** debe de ser única y consta de cuatro números decimales, separados por puntos, los paquetes pueden atravesar cualquier tipo de red. En cada uno de los tipos de red, el protocolo ***TCP/IP*** se encarga de asignar una dirección ***IP*** a un nodo físico, para poder realizar el tránsito. Los paquetes contienen las direcciones ***IP*** del remitente, lo cual permite que el destinatario pueda reclamar los datos, en caso de ser necesario. La dirección **IP** permite identificar tanto a la red como al nodo que corresponde al remitente. Una de direccional ***IP*** consiste en unirse a la comunidad ***DARPA Internet***, contando con el ***NIC***. Si no se está interesado en registrarse oficialmente una red, se pueden elegir números arbitrarios que se rijan con el esquema de direccionamiento ***IP***. Es bueno que se utilice el esquema ***DARPA Internet***, por si en el futuro se precisa entrar en contacto con algún punto de acceso externo. La dirección ***IP*** de 4 bytes se divide en dos partes: una de ellas para identificar la red y la otra para identificar al nodo (computadora). De esta manera, la parte que corresponde a la red,

debe ser siempre la misma para todos los nodos que la conforman, en tanto que la parte que identifica al nodo, ha de ser única y diferente para cada equipo conectado a dicha red.

Existen diversos esquemas para la asignación de estos números:

I) Esquema de direccionamiento clase A:

El primer byte es la dirección de la red, y los tres últimos la del nodo. El rango para el primer byte es de 1 a 126, lo cual permite un total de 126 redes diferentes, con 16 millones de nodos cada una.

II) Esquema de direccionamiento clase B:

Los dos primeros bytes identifican a la red, y los dos últimos, el nodo. El rango para el primer byte es de 128 a 191, quedando el segundo para identificaciones más finas. Esto permite un total de 16,000 redes con 65,000 nodos.

III) Esquema de direccionamiento clase C:

Los tres primeros bytes identifican a la red y el último es la dirección del nodo, lo cual permite un total de 2 millones de redes diferentes con 254 nodos cada una.

Es posible dividir una red en varias subredes, para así poder hacer uso de múltiples tipos de medios, o bien para reducir la congestión, disminuyendo el número de puestos de trabajo de la red. Cuando existen subredes, las direcciones ***IP*** constan de una dirección de red, una dirección de subred y la dirección del nodo. La parte de dirección que corresponde al nodo en la dirección ***IP***, se divide para incluir las direcciones de la subred y del nodo. Para las redes externas, la red total seguirá apareciendo como único conjunto, con una única dirección.

1.7) Conceptos básicos de seguridad en redes inalámbricas 802.11

Los objetivos fundamentales que se deben tener en cuenta para la seguridad son:

La confidencialidad de los datos: Solo las personas autorizadas pueden ver la información.

La integridad de los datos: Todos los usuarios autorizados deben de estar seguros de los datos que obtienen son precisos y que no fueron modificados.

La disponibilidad de los datos: Los usuarios autorizados deben tener acceso a la información que necesiten, en cualquier momento.

La seguridad se puede dividir en seis requisitos. La mayoría de ellos hacen uso de técnicas de criptográficas.

a) Identificación: Está relacionada con los nombres de los usuarios y con la forma en que éstos se identifican en un sistema informativo.

b) Autentificación: Es todo aquello que tiene que ver con una contraseñas, tarjetas inteligentes, etc. Es el método que utilizan los usuarios para demostrarle al sistema que son legítimos.

c) Control de acceso: Son los privilegios y requerimientos concedidos a los usuarios para que puedan acceder y realizar determinadas funciones en un sistema informático.

d) Confidencialidad: Garantiza a las personas autorizadas la privacidad de la información y comunicaciones, a través del uso de mecanismo de cifrado o encriptación para hacer frente a observaciones no autorizadas.

e) Integridad: Abarca aquellos procesos que se ocupan de la prevención y detección de la falsificación, pérdida o daño de los mensajes de datos mientras son transmitidos.

f) Imposibilidad de rechazo: Es aquel en que los datos y solicitudes auténticas sean procesos brindado al cliente el servicio solicitado. Las firmas digitales forman un papel esencial en este servicio.

Los ataques en las redes son típicamente dos:

Ataques activos: Estos ataques son relativamente sencillos de identificar, ya que implica la modificación del flujo y disponibilidad de datos transmitidos a la creación de un flujo falso de datos, pudiendo en subdividirse en cuatro categorías:

a) La adición: Se refiere a la introducción de datos al flujo de la información.

b) La modificación: Es una alteración a la información original.

c) La saturación: Inhabilita a un equipo en seguir procesando sus servicios.

d) La eliminación: Se refiere a los datos transmitidos eliminados, así como los registros y archivos completos.

Ataques Pasivos: Estos están dirigidos a vulnerar la confidencialidad de la información al buscar interceptar el flujo de información sin alterar su contenido las cuales le hace difícil de identificar.

Una técnica muy sutil puede consistir en:

- **Obtención de la información y datos:** Si la información no está encriptada es posible verla.
- **Obtención del origen y destinatario de la comunicación:** Leyendo las cabeceras de los paquetes monitoreados.

- **Monitoreo del volumen de tráfico:** Intercambio entre las entidades monitoreadas, obteniendo así información acerca de actividad o inactividad inusuales.
- **Monitoreo de las horas habituales:** Monitoreo de intercambio de datos entre las entidades de comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar ya que no provoca ningún alteración en los datos, sin embargo, es posible evitarlos mediante encriptamiento de la información.

Si consideramos que una de las aplicaciones más comunes de las redes convergentes es el uso de voz (VoIP[6]) y datos de redes inalámbricas por el mismo canal, el impacto de un ataque DoS[7] sobre el canal de datos implicaría que tanto el sistema de operación transaccional como el telefónico se verán afectados.
Cuando las redes proveen el medio de comunicación de voz, multimedia y datos, entre otros, la seguridad se convierte en un tema prioritario como el de esta tesis.

1.7.1) Mecanismos y factores de seguridad

Los mecanismos de seguridad poseen tres componentes principales:

a) Formación secreta, como claves, contraseñas, conocidas como las entidades autorizadas.
b) Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios
c) Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envíe qué a quién y cuándo.

Es importante notar que los sistemas de seguridad requieren una administración de seguridad. La administración comprende dos campos amplios:

1) Seguridad en la generación, localización y distribución de la información secreta, de modo que solo puede ser accedida por aquellas entidades autorizadas.

2) La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

1.7.2) Los factores de seguridad se definen en un entorno inalámbrico pueden reducirse en cinco elementos básicos:

1) Robos
2) Control de accesos
3) Autenticación
4) Encriptación
5) Barreras

[6] VoIP -Voz sobre IP (VoiceOver IP).
[7] DoS - Negación del Servicio (Denial Of Service).

1.8) Problemas de seguridad en redes Wi-Fi

1.8.1) Problemas inherentes a su medio de transmisión

La diferencia principal de los entornos wirelass con los entornos de cable tradicionales, como con Ethernet radica en los medios donde se transmiten los datos.

Algunos de los riesgos son similares a las de las redes cableadas, otros son agravados por la conectividad inalámbrica y varios más son nuevos.

La fuente más importante de los riesgos inalámbricos son las señales que pueden ser escuchadas por intrusos desde fuera de los linderos físicos de su empresa.

1.8.1.1) Puntos de acceso mal configurados

La mala configuración de un punto de acceso inalámbrico es muy común, si al adquirir el equipo inalámbrico no se cambia la configuración que trae por defecto, sin seguridad alguna, los riesgos que se corren son altísimos ya que el SSID de todos los proveedores son conocidos y ninguna opción de seguridad (WEP o WPA) es habilitada inicialmente.

Cualquier persona desde el exterior capta la señal del punto de acceso, tendrá la posibilidad de navegar gratis en Internet, emplear ese punto de ataque hacia las demás redes y luego desconectarse para no ser detectado, robar software e información, introducir virus o software maligno.

Un punto de acceso mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la compañía.

1.8.1.2) Punto de acceso no autorizado (Rogue)

Es aquél que ha sido instalado sin la autorización ni el consentimiento de los administradores de la red. Por lo cual no está en la administración de los expertos en tecnologías de la información ni bajo las políticas de seguridad para la red.

Los puntos de acceso "rogue" son un problema inclusive si la compañía no tiene red inalámbrica, ya que empleados buscan mejorar su productividad instalan inconscientemente un punto de acceso para uso personal en la red sin entender los riesgos de seguridad para la red. Los puntos de acceso "rogue" son utilizados por hackers para atacar redes inalámbricas.

1.8.2) Ataques particulares a Wi-Fi

Con la variedad e herramientas disponibles en Internet, libros y revistas, un hacker novato puede ejecutar una multitud de ataques como si fuera recetas de cocina.

1.8.2.1) Ataques pasivos

Las redes inalámbricas son especialmente vulnerables a los taques pasivos, ya que el único requisito es estar en el área de cobertura.

El primer paso es conseguir una asociación de la red inalámbrica. En las redes que utilizan autenticación abierta o nula (Open System) el proceso es transparente, aumentando la complejidad en lo sistemas de autenticación Shared Key. En estos casos la autenticación es posible tras la captura de cierto número de paquetes para develar la clave, existiendo varias herramientas para facilitar dicha tarea.

Es posible obtener datos, información, direcciones MAC de los equipos de origen y destino, direcciones IP, horario de uso, volumen y monitoreo de tráfico que está presente en el entorno inalámbrico.

Se realiza espionaje al escuchar todo lo que se transmite durante y dentro del canal de comunicación.
Los ataques pasivos son muy difíciles de detectar ya que no alterar los datos.

1.8.2.2) Ataques activos

Son ataques en los cuales se llevo a cabo la modificación de los mensajes, paquetes o archivos.

Suplantación: El ataque personifica aun usuario autorizado y por lo tanto obtiene privilegios no autorizados.

Repetición: El atacante monitorea la transmisión y retransmite mensajes como un usuario legitimo.

Modificación de mensajes: El atacante altera un mensaje legítimo al borrarlo, agregarlo, cambiarlo o reordenándolo.

Negación de servicio (DoS): Es un ataque que impide a la victima usar totalmente o parcialmente los servicios o comunicaciones de su red.

Este tipo de ataque puede estar dirigido a:

- Un usuario, para impedir realizar conexiones salientes de la red.
- Una organización completa, para detener su tráfico entrante y saliente a ciertos servicios de red, tales como la página Web de la organización.

1.8.2.3) Tipo de ataque DoS

Existen diferentes ataques DoS clásicos. La mayoría se basan en las debilidades del protocolo TCP/IP. Las mejoras de los fabricantes y una configuración apropiada de red

han hecho que los ataques DoS sean difíciles e imposibles de realizar. En la siguiente tabla se presentan algunos ataques DoS.

Tipo de ataque DoS	*Descripción*
Inundación (Flood)	Es el más antiguo de los ataques DoS. El atacante simplemente envía más tráfico que el que la víctima puede soportar, esto requiere que el atacante tenga una conexión de red más rápida que la víctima, este ataque es el menos sofisticados tecnológicamente, pero es el más difícil de prevenir.
Toque de la muerte (Ping of Death)	Se basa en un error de la pila de los protocolos TCP/IP de Berkley, el cual también existía en la mayoría de los sistemas que copiaron el código de la universidad de Berkley, el toque de la muerte simplemente envía un paquete de sondeo mayor de 65,535 byte a la víctima.
Sincronía (SYN)	En el protocolo TCP/IP, el enlace de conexión de red es realizado con mensajes SIN y ACK, el sistema que dese comunicarse envía mensaje de solicitud SYN, al sistema de destino, y el sistema de destino responde con un mensaje ACK. En un ataque SYN, el atacante inunda al destinatario con mensajes SYK engañosos para aparecer estar en una dirección de Internet inalcanzable, esto llena y sobrepasa el espacio para mensajes SYN en el equipo destino, impidiendo que otros sistemas de red se puedan comunicarse con este.
Bloqueo (Teardrop)	Utiliza el algoritmo de fragmentación de los paquetes IP para enviar paquetes dañados a la víctima. Esto, lo confunde y puede bloquearse.
Smurf	El atacante envía una solicitud de contestación (ping) a una dirección de emisión masiva (broadcast) desde otro equipo en la red. Esta solicitud es modificada para hacerla parecer que viene de la dirección de la red de la víctima, cada equipo dentro del dominio de emisión de esa red, enviara una respuesta a la víctima.
DoS Distribuido (DDoS)	Es un ataque DoS ejecutado dentro de una gran cantidad de sitios, que han sido comprometidos por un gusano, caballo de Troya o por un hacker manualmente. Esos equipos comprometidos son usualmente controlados con un software sofisticado cliente servidor tal como Trinoo, Tribe Flood Network, Stalchedaht, TFN2K, Shaft y Mstream. Puede ser muy difícil defenderse y combatir ataques DDoS.

Tabla 1.6 Tipos de ataques DoS

1.8.2.4) Ataques avanzados

Estos tipos de ataques se dividen en:

a) Ataque de Diccionario: Es aquel en el que se intenta que cada palabra de un diccionario es un posible password de un mensaje encriptado. Ya que los usuarios utilizan password muy sencillos.

Existen dos métodos para mejorar los ataques de diccionario:

1. El primero consiste en utilizar un diccionario más grande o varios diccionarios.
2. El segundo consiste en una manipulación de palabras del diccionario.

b) Ataque de Fuerza Bruta: Consiste en intentar todas las posibles claves, códigos combinaciones o contraseñas hasta encontrar el correcto. La dificultad de estos ataques depende de varios factores:

¿Qué tan larga sea la clave?
¿Cuántos valores posibles pueda cada componente de la llave tener?

¿Cuánto tiempo tomará intentar cada clave?

c) Asociación Maligna o Accidental: Un hacker puede forzar a una estación de trabajo a conectarse, sin que está lo sospeche, a una red 802.11 no deseada o ficticia o alterar la configuración de la estación para operar en modo de red ad-hoc.

Los hacker configuran una computadora portátil con un punto de acceso suave usando cualquiera de las herramientas gratuitas para hacker tales como HostAP, Airnsarf y Hotspotter, o alguna herramienta comercialmente disponibles.

Así pues cuando la estación de trabajo de la víctima transmite una solicitud para asociarse con un punto de acceso, el punto de acceso suave del hacker responde a esa petición y establece una conexión entre los dos. A continuación el punto de acceso suave provee una dirección IP a la estación del trabajo de la víctima. Una vez echo esto, el hacker puede escudriñar la estación de la víctima con herramientas diseñadas para encontrar vulnerabilidades bajo Windows.

d) Robo de Identidad (Mac Spoofing): El robo de la identidad de un usuario es una amenaza seria para las redes inalámbricas.

Aún cuando el SSID y las direcciones MAC actúan como un número de identificación personal (PIN) al verificar la identidad de los clientes autorizados, los estándares de encriptación no son una garantía.

Los hacker con conocimiento pueden elegir direcciones MAC o SSID autorizadas y robar ancho de banda, bajar archivos o dañarlos y ejecutar la destrucción de la red entera.

Éste ataque son similares a los ataques efectuados en redes cableadas, y las herramientas para realizar esos ataques en redes cableadas pueden ser usados en redes inalámbricas. Entrar en medio de una sesión de comunicaciones es un problema en redes cableadas, este proceso es mucho más fácil en las redes inalámbricas ya que una estación que transmite no es capaz de detectar la presencia de estaciones con la misma dirección MAC o IP, usando software softAP, un hacker puede fácilmente convertir un dispositivo inalámbrico en un punto de acceso suave y posicionar el punto de acceso en medio de la sesión de comunicación.

El ataque de hombre en medio más sofisticado roba el protocolo de saludo y desafío para ejecutar un ataque de des-autenticación, este ataque expulsa a un usuario de un punto de acceso, ocasionando que ese usuario busque otro punto de acceso al cual conectarse, con el punto de acceso SoftAP, del hacker funcionando, el usuario se reconecta a la computadora portátil del hacker.

Ahora el hacker con una interfaz inalámbrica diferente, se conecta a la red inalámbrica real, pasando todo el tráfico de autenticación a través de él, la víctima es ajena a esto, y pasando todos los datos a través del equipo del hacker. Este escenario es posible ya que las VPNs establecen su conexión en la capa 3 del modelo OSI, mientras que las capas inalámbricas existen debajo de las VPN, en las capas 1 y 2.

Una vez conectado el hacker puede usar herramientas tales como DSNIFF, Ettercap, IKEcrack u otras herramientas para revertir la seguridad de la VPN hasta que el tráfico este en texto o este usando una encriptación débil de fácil rompimiento, este es un problema común para la mayoría de los protocolos de VPNs, tales como IPSEC, PPTP, SSH, SSL y L2TP.

Solo un sistema de detección de intrusos altamente capaz y que monitoree las 24 hrs, puede detectar esos tipos de ataques en redes inalámbricas.

e) Ataque de inyección de tráfico a la red: Es un nuevo desarrollo de negación (DoS), éste ataque explota dispositivos inalámbricos mal configurados y su objetivo es la red entera. Cuando un punto de acceso es conectado a una sección no filtrada de la red corporativa, emite tráfico de red, tal como "Spanning Tree" (802.1D), OSPF, RIP, HSRP y otro tráfico dirigido o diseminado, al hacer esto los paquetes inician ataques que derriban los equipos de las redes inalámbricas y cableadas e impulsan a disolver la infraestructura entera de la red interna, incluidos los hubs, ruteadores y switches.

El algoritmo "Spanning Tree" asegura una topología libre de ciclos infinitos (loops), para redes que contienen puentes paralelos y segmentos de Ethernet múltiples.
Los loops ocurren cuando hay rutas alternas entre los clientes (hosts), si existe un loops en una red extensa, los puentes podrían enviar tráfico a hosts Ethernet falsos o erróneo indefinidamente, incrementando el tráfico y reducir el rendimiento de la red al punto donde la red para de responder.

Un hacker puede inyectar tráfico sobre el segmento de red inalámbrica y será propagado a través de la red completa, esto crea un ataque de DoS al insertar intencionalmente loops dentro de la red.

Ataques de ruteo son otros ataques de moda DoS, un hacker puede utilizar herramientas tales como IRPAS o Routing Atack Tool para inyectar actualizaciones de ruteo falsas dentro de la red, cambiando la puerta (gatewey) por defecto o destruyendo las tablas de ruteo, cualquier punto de acceso falso en la red que no esta filtrado por una puerta abre la red a este ataque dañino.

También cabe mencionar la utilización de computadoras conectadas a Internet cuyo nivel de procesamiento y de seguridad son bajos, estas son usadas en conjunto para:

- Atacar-Ataque distribuido de negación de servicio (DoS).
- Romper llaves de seguridad.
- Decodificar algoritmos de seguridad.

1.9) Evolución de la seguridad en redes 802.11

802.11 inicia con un mecanismo llamado WEP cuyas fallas hacen que la alianza Wi-Fi desarrolle un conjunto temporal de soluciones denominada WPA, las cuales resuelven los requerimientos inmediatos de la industria.

El IEEE seguía trabajando en su estándar 802.11i y ante su lentitud se consolida la segunda versión temporal de seguridad WPA2, la cual incluye más elementos de seguridad como encriptación AES que demanda mayor capacidad de procesamiento, por lo cual se requiere de equipo nuevo.

Tanto WPA, como WPA2 no son estándares. Sin embargo como han sido la solución temporal mientras se desarrolla es estándar de la IEEE, se les trata como tales.

Después de tres borradores y casi cuatro años de diseño el IEEE logra el esperado estándar 802.11i, este se basa en todos los adelantos logrados por WPA2.

1.9.1) Requerimientos para tener una red inalámbrica segura

Los organismos de estándares como el IEEE, el IETF y la alianza Wi-Fi han definido tres áreas básicas de seguridad para tener una red inalámbrica segura:

- ***Autenticación:*** Método que certifica, válida y controla el acceso de los usuarios y dispositivos a la red.
- ***Confidencialidad:*** Para brindar privacidad las comunicaciones se encriptan.
- ***Integridad:*** Aquellos procesos que prevén y detectan la falsificación de los mensajes de datos. Los paquetes transmitidos deben estar originados por los emisores.

1.9.2) WEP

WEP (Wired Equivalent Privacy-Privacidad Equivalente al Cableado) inicia en con las WLANs en 1999, desarrollado por voluntarios del IEEE cuyo objetivo era brindar seguridad a las redes inalámbricas al proveer ***integridad, confidencialidad y autenticación.***
Poco tiempo después de salir al mercado este mecanismo, ya mostraba serías fallas de seguridad, software gratuito que puede descargarse de Internet, permite que ataques automatizados sobre WEP puedan ser llevados a cabo con facilidad.

La integridad en WEP: Se aplica un algoritmo de comprobación de integridad CRC-32 a los datos a transmitir, lo que genera un valor de integridad (ICV).

El ICV y los datos se depositan en paquetes que se envía al receptor, el receptor ejecuta el mismo algoritmo sobre los datos del paquete recibido y compara su resultado con el ICV que recibió como parte del paquete, si ambos ICV son iguales el mensaje será considerado como integro, de lo contrario, el paquete y por ende los datos han sido alterados.

Es fácil observar que este mecanismo no es a prueba de colisiones ni de ataques, ya que se puede llegar el mismo valor de ICV con diferentes datos dentro del paquete transmitido.

La confidencialidad en WEP: Se logra al habilitar WEP y se configura una clave secreta en cada una de las estaciones y puntos de acceso del sistema WLAN.

Cuando una estación trata de conectarse con punto de acceso, éste replica con un texto aleatorio, que constituye el desafío (challenge), la estación debe utilizar su clave secreta para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse, el punto de acceso descifra la respuesta utilizando su clave y compara con el texto de desafío original que envió. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y lo acepta dentro de la red, de lo contrario el punto de acceso lo rechaza evitando que la estación acceda a la red.

***La autenticación** en WEP: Existen dos tipos de autenticación.*

- ***Sin encriptación o autenticación abierta (Open System):*** No se requiere de absolutamente ninguna configuración especial, el cliente solicita acceso a la red ofreciendo su SSID y su dirección MAC para se identificada. Si el SSID es igual al del punto de acceso obtiene una dirección IP, con la cual se comunicara a partir de este momento.

- ***Encriptada o de clave compartida (Shared Key):*** Se requiere habilitar la opción WEP y configurar todos los dispositivos inalámbricos con la misma clave, manualmente, siendo esta guardada en su chip de configuración. El cliente transmite y recibe, encriptando y desencriptando, todas sus comunicaciones con dicha clave.

1.9.2.1) Elemento de cifrado WEP

VI= Vector de inicialización de 24 bits, cuyo rango va de 0 a $2^{24} = 16{,}777{,}215$.
C= Clave secreta de 40 bits o 64 bits, conocida en todos los dispositivos.
RC4= Mecanismo de encriptación.
CRC32= Algoritmo para verificar la integridad de los datos.
T= Texto a transmitir.

Pasos para cifrar:

1) Se obtiene el ICV^2 al calcular el CRC32 de los datos a transmitir. ICV= CRC32 (T)
2) Se forma la semilla (seed) al concatenar C y VI. Z= C+VI.
3) Se ejecuta el RC4 sobre Z. Se obtiene (K), el Keystream. K= RC4 (Z).
4) Se ejecuta el método Xor^2 sobre el ICV y K. Se obtiene (TC), Texto Cifrado.
TC= Xor (ICV, K).
5) Se forma el paquete a enviar: VI+TC. El VI viaja sin cifrar. P= IV+TC.

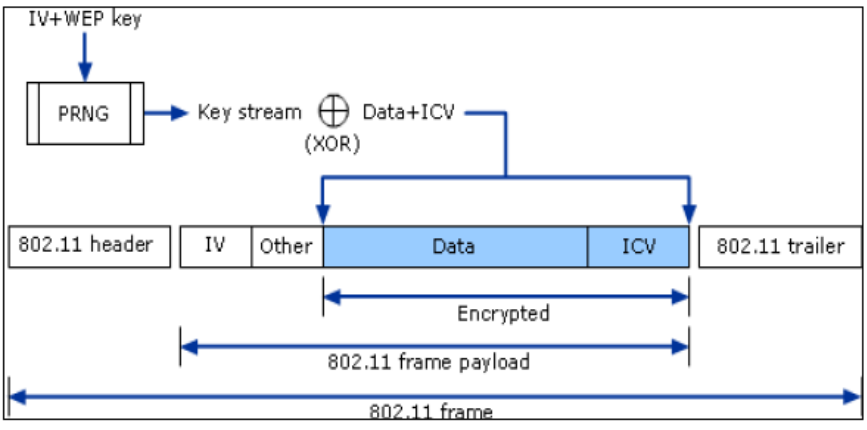


Figura 1.17 Cifrado de WEP

Pasos para descifrar:

1) Se recibe el paquete que contiene el VI el Texto Cifrado. P= VI+TC
2) Se genera la semilla ya que se conoce el VI y la clave secreta compartida. Z= C+VI
3) Se aplica el RC4 sobre la semilla para obtener el Keystream. K= RC4 (Z).
4) Se ejecuta el Xor a K y los datos recibidos (TC), se obtiene el Texto original (T). T= Xor (TC, K).

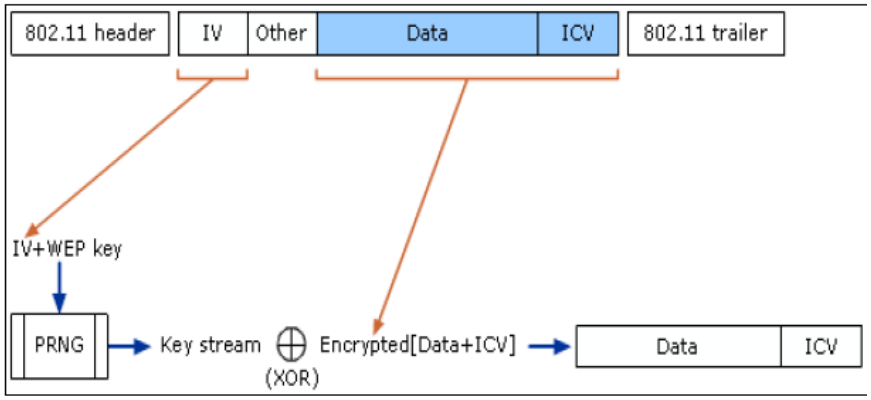


Figura 1.18 Descifrado WEP

El Keystream actúa como una mascara o valor constante para ejecutar el Xor y así cifrar y descifrar la información. El VI viaja sin cifrar y es cíclico o fijo, es decir es visible y se repite, lo que hay que esperar es que al hacer el Xor entre el Keystream y texto cifrado se obtenga el mismo resultado.

De hacerlo se habrá encontrado la clave secreta (C).

1.9.2.2) Vulnerabilidades de WEP

1. Clave WEP estática: Se usa la misma clave WEP en todos los dispositivos.

2. Vector de inicialización (VI) de 24 bits: Los valores van desde 0 hasta $2^{24} = 16{,}777{,}215$. Es un número que se incrementa por cada paquete enviado para encriptar los datos.
   En una red con tráfico se reiniciaría en forma cíclica y el valor del VI se repetirá, al seleccionar los VI repetidos de la cadena de datos, un atacante puede coleccionar suficientes datos para averiguar la clave WEP. Adicionalmente este valor es transmitido como texto sin cifrar.

3. Programa gratuititos: Programas que se bajan de Internet pueden recuperar la clave WEP.

4. La desencriptación no autorizada y la violación de la seguridad de los datos: Una vez que la clave WEP es revelada, un hacker puede transformar el texto cifrado a su forma original y entender los datos, al entender el algoritmo, un hacker

puede usar la clave WEP obtenida para modificar el texto cifrado y reenviar un mensaje modificado al receptor. Exponiendo con esto a la red inalámbrica a ataques pasivos y activos.

5. Administración pobre de la clave: Una clave de WEP es tecleada manualmente en cada dispositivo inalámbrico para habilitar WEP, desafortunadamente, no existen mecanismo para renovar la clave WEP, una vez que la clave WEP esta en riesgo, por ejemplo, un empleado deja la compañía, la clave tiene que ser cambiada para mantener la seguridad. El cambio de claves puede ser aplicable en un ambiente casero o en un pequeño negocio, sin embargo, en un ambiente empresarial con cientos de dispositivos móviles esta tarea se convierte en una misión casi imposible.

6. Punto de acceso sin autenticación: WEP solamente provee un método para que las tarjetas de red autentiquen puntos de acceso, no existe forma para que los puntos de acceso autentiquen a las tarjetas de red, como resultado, es posible para un hacker enviar los datos a puntos de acceso a través de una ruta alterna no autorizada, por ejemplo, un punto de acceso instalado por un hacker.

7. WEP no esta activado por defecto sino cuando esta disponible.

La industria no podía esperar al estándar 802.11i hasta fines del 2003, se estaba demandando un ambiente inalámbrico más seguro inmediatamente. En respuesta, la alianza Wi-Fi, junto con el IEEE, desarrollo el WPA (Wi-Fi Protected Access- Acceso Protegido Wi-Fi), en un esfuerzo por atender las vulnerabilidades de WEP y ofrecer un estándar de seguridad fuerte e interoperable al mercado en el primer cuatrimestre del 2003.

1.9.3) WPA

Wi-Fi Protected Access, es decir, Acceso Protegido para redes inalámbricas, presentado en abril del 2004 por la alianza Wi-Fi en la ciudad de Las Vegas durante el evento Network Interop.

WPA es una solución de seguridad temporal cuyo objetivo es resolver todas las vulnerabilidades de WEP, mientras no están preparados los primeros dispositivos que implementan el 802.11i, los principales fabricantes, agrupados bajo la conocida alianza Wi-Fi, se han puesto de acuerdo en este estándar provisional de seguridad.

WPA se basa en un subconjunto de aspectos que se han extraído del futuro estándar 802.11i incluyendo las siguientes tecnologías para atender las vulnerabilidades WEP.

- 802.1X: Estándar creado por la IEEE en el 2001 para proporcionar un control de acceso en redes cableadas basado en el uso de puertos, las estaciones trataran de conectarse a un puerto del punto de acceso, el punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentique.

- EAP: Protocolo de Autenticación Extendido (Extensible Authentication Protocol), definido en la RFC 2284, lleva acabo las tareas de autenticación, autorización y contabilidad, el EAP fue diseñado originalmente para el protocolo Punto a Punto (Point to Point Protocol), aunque WPA lo utiliza entre la estación y un servidor RADIUS. Esta forma de encapsulamiento de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP Over LAN).

- TKIP: Protocolo de Integridad de Llave Temporal (Temporal Key Integrity Protocol), es el protocolo encargado de la generación de una llave para cada trama.

- MIC: Código de Integridad de los mensajes (Message Integrity Code), código que verifica la integridad de los mensajes, también conocido como Michael.

En teoría WPA puede operar simultáneamente con equipos basados todavía en 802.11 y WEP, aunque con la desventaja de que las claves de cifrado no son dinámicas, esta limitación es muy importante ya que reduce su funcionalidad casi al mismo nivel que WEP, aunque la integridad obtenida con Michael es una ventaja.

La alianza Wi-Fi no recomienda este método de trabajo mixto debido a que casi invalida las ventajas de WPA y en sus pruebas de certificación verifica que, si es soportado, no sea el modo por defecto.
La experiencia de los usuarios indica que es difícil conseguir esta interoperabilidad entre productos de diferentes marcas e incluso entre los de la misma marca.

Otra limitación de WPA es que no da soporte a redes inalámbricas, cuya topología es, ad-hoc.

1.9.3.1) WPA y sus actualizaciones

WPA requiere actualización de todos sus componentes que intervienen en una red inalámbrica:

- Firmware de puntos de acceso y tarjetas de red.

- Los controladores de los dispositivos.

- Software instalado en los equipos cliente.

Los dispositivos de red inalámbricos (puntos de acceso y tarjetas de red), requieren una actualización de firmware, esto es necesario para incorporar TKIP, Michael, AES y un elemento de información nuevo que emiten los puntos de acceso.

Los primeros productos con WPA comenzaron a salir al mercado a mediados del 2005 por que la implementación no es trivial y lleva tiempo, algunos modelos de CISCO, 3Com y otras empresas, ya disponen de la correspondiente descarga en sus sitios Web, otra circunstancia muy reciente es que muchos fabricantes dan prioridad a sus productos más recientes, ofreciendo actualizaciones sólo para productos 802.11g y dejando de

lado los Wi-Fi originales (802.11a y 802.11b) y otros productos ni siquiera ofrecen alguna actualización.

Windows XP o Windows 2003 el controlador de la tarjeta deberá ser capaz de soportar los servicios de WPA.

Microsoft manifiesta que ha trabajo con muchos fabricantes de hardware inalámbrico para que estos incluyan actualizaciones de firmware para la instalación del nuevo controlador para Windows XP, de forma que al instalar el controlador en este sistema operativo también se automatiza su firmware de forma automática.

El software del cliente es el que consigue que el sistema operativo pueda sacar partido a todas las mejoras que las actualizaciones de firmware y de controlador han proporcionado. El único sistema operativo que ofrece soporte para WPA es Windows XP y se puede descargar la correspondiente actualización gratuita en:

1.9.3.2) Modos de funcionamiento de WPA

WPA puede funcionar de 2 modos:

1. Con un servidor AAA, RADIUS o IAS normalmente, es el modo indicado para las empresas y requiere un servidor configurado para desempeñar las tareas de autenticación, autorización y contabilidad.

2. con clave inicial compartida (PSK), este modo está orientado para usuarios domésticos o pequeñas redes, denominadas SoHo (Small Office Home Office), no requiere un servidor AAA, sino que utiliza una clave compartida en las estaciones y puntos de acceso, al contrario que WEP, esta clave solo se utiliza como punto de inicio para la autenticación, pero no para el cifrado de datos.

WPA adopta al 802.1x para atender el problema de la autenticación y escalabilidad de usuarios en WEP. 802.1x inicialmente esta diseñado para redes cableadas pero es también aplicable a redes inalámbricas.

El estándar 802.1X consta de tres elementos:

1. Un suplente: Un dispositivo inalámbrico que desea conectarse a la red y ser autenticado.

2. Un servidor de autenticación: Es un sistema de autenticación, tal como un servidor RADIUS o IAS, el cual maneja la autenticación 802.1x fue diseñado para utilizar servidores RADIUS, cuya especificación se puede consultar en la RFC 2058.

   Estos servidores fueron creados para inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica.

3. Un autenticador: Es un dispositivo que actúa como un intermediario entre un suplicante y un servidor de autenticación, usualmente es un punto de acceso.

La autenticación del cliente se lleva acabo mediante el protocolo EAP (Extensible Authentication Protocol) y un servidor RADIUS.

Esta autenticación mutua en 802.1X involucra varios pasos:

1. Un suplicante inicia una conexión con un autenticador, el cual, detecta la solicitud de inicio y habilita el puerto del suplicante, sin embargo, todo tráfico incluyendo DHCP, http, FTP, SMTP Y POP3, es bloqueado excepto 802.1x.

2. El autenticador requiere la identidad del suplicante.

3. El suplicante responde con su identidad al autenticador, que pasa, la identidad a un servidor de autenticación.

4. El servidor de autenticación certifica la identidad del suplicante, una vez autenticado, un mensaje de aceptación es enviado al autenticador, este cambia el puerto del suplicante a un estatus de autorización.

5. El suplicante solicita la identidad del servidor de autenticación, el servidor de autenticación pasa su identidad al suplicante.

6. Una vez que el suplicante autentica la identidad de un servidor de autenticación, todo tráfico es permitido.

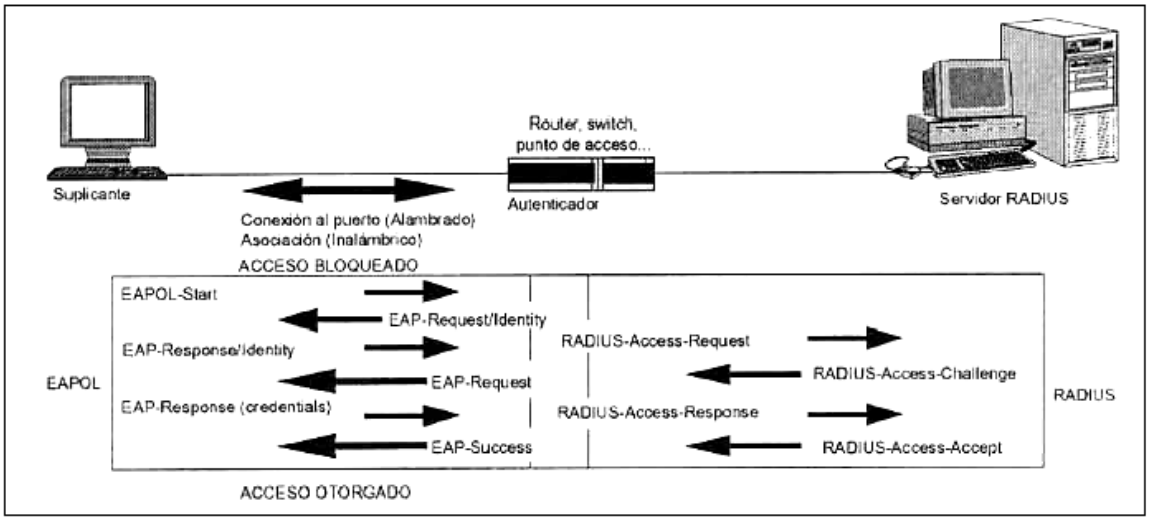


Figura 1.19 Diálogo detallado del suplicante-Autenticador-Servidor RADIUS

1.9.4) WPA2

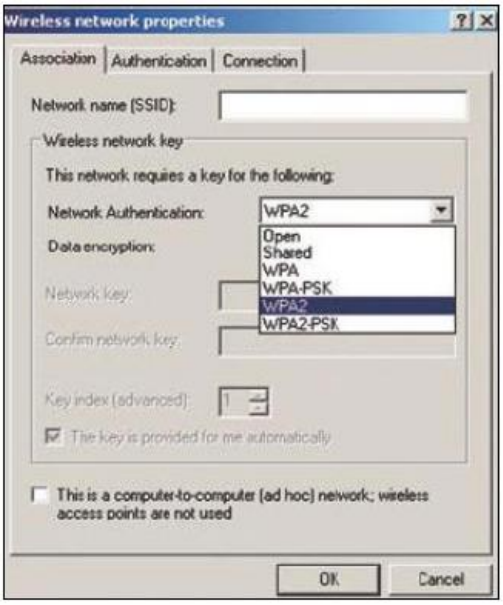
Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA basada en el estándar 802.11i y utiliza un algoritmo de encriptación llamado AES-CCMP.

WPA2 soporta TKIP, AES-CCMP, Ad-Hoc, IBSS, 802.1x/EAP, PSK y movilidad rápida, al pre-autenticar el usuario en los puntos de acceso existentes en la

infraestructura de red, permitiendo al usuario sin tener que autenticarse con cada uno de ellos. Adicionalmente se requiere de un servidor AAA como RADIUS o IAS para uso corporativo con requerimientos de alta seguridad.

WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard).



1.20 Configuración de la red WPA2

1.9.4.1) 802.11i: La Solución de Seguridad del IEEE para WLANs

El nuevo estándar de seguridad, el 802.11i, para WLANs es la solución que el IEEE diseñó para resolver los problemas de WEP:

- La encriptación no estaba siendo usada apropiadamente.
- No había manera de prevenir la falsificación de mensajes.
- Las llaves de encriptación eran reutilizadas, permitiendo con esto que los datos fueran leídos sin saber la llave de encriptación.
- La autenticación no funcionaba, ya que transmitía al aire todo lo necesario para que un atacante se autenticara ante la red.

El grupo de trabajo de 802.11i, conformados por expertos en seguridad, liberó esta solución en junio de 2004. Utilizó más de tres años en la especificación y tres borradores fueron publicados durante su desarrollo.

Algunos participantes en la solución de seguridad 802.11i fueron Intel, Cisco, Agere, Broadcomm,, Hi-FN, Microsoft, RSA Labs y muchos otros. Representantes de muchas Universidades como el MIT (Instituto de Tecnología de Massachusetts), Certicom y Berckley.

El comité "i" precedió a trabajar en cuatro líneas separadas:

1. Mejorar Autenticación: Protocolo 802.1x, que requiere de un servidor de autenticación.

2. Inventar un nuevo algoritmo de encriptación: CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), protocolo de respuesta a la codificación en bloque encadenado al código del mensaje de autenticación y utiliza al algoritmo AES para encriptación.

3. Diseñar una solución temporal para WEP resultando en WPA: TKIP y 802.1x.

4. Asegurarse de que las llaves no fueran reutilizadas para desligar la protección de los datos de autenticación. Ya que cada vez que un cliente se asocia con un punto de acceso se genera una llave de sesión que será usada como la base de la encriptación.

WPA2/802.11i añade encriptación mejorada vía AES (CCMP). Soporte a redes en modo Ad-Hoc ó IBSS y una característica llamada "pre-autenticación", la cual permite movilidad al usuario entre las redes inalámbricas conectadas en la misma infraestructura al pre-autenticar en los puntos de acceso al usuario ya autenticado en alguno de ellos.

Uno de los motivos de retraso de WPA2 fue el de dar tiempo a los fabricantes de chips para poder soportar AES en los nuevos productos. AES requiere más poder de cómputo que el débil WEP.

Algunos fabricantes han agregado AES en su hardware en sus conjuntos de chips, mientras que otros lo han implementado. Los usuarios pueden esperar que la transición de WPA a WPA2 vaya mejor que la de WEP a WPA, la cual fue larga, lenta y en muchos casos una promesa vacía para los productos existentes. Afortunadamente, los fabricantes tienen el incentivo de los productos 11g basados en una velocidad inalámbrica mayor como estímulo principal de actualización.

La administración de estándares China (SAC- Standards Administration of china) desarrolló su propio estándar de encriptación inalámbrica, conocido como WAPI (Wired Authentication and Privacy Infraestructure). WAPI es incompatible con el 802.11i

1.9.4.2) Protocolos Utilizados en 802.11i

El 802.11i define nuevos estándares y se basa en mucho estándares existentes.

802.11i utiliza los protocolos existentes:

802.1x (EAPol): Usado para encapsular los mensajes EAP en redes inalámbricas Ethernet. De esta manera no importa cual sea el método EAP utilizando.

EAP: EAP (Extensible Authentication Protocol) es un protocolo de seguridad de según capa del modelo OSI, empleado en la etapa de autenticación del proceso de seguridad, con lo cual se provee la capa final de seguridad para las redes inalámbricas.

Este estándar provee control de acceso basado en puertos así como autenticación mutua entre clientes y puntos de acceso usando un servidor de autenticación.

Es un protocolo que 802.IX utiliza para administrar la autenticación mutua y el método de autenticación puede ser password, certificados PKI u otras formas de autenticación.

El EAP es un autenticador que no necesita entender los detalles sobre los métodos de autenticación, el autenticador simplemente actúa como interceptor de paquetes EAP a ser enviados de un suplicante a un servidor de autenticación, en el cual la autenticación en sí se lleva a cabo.

Existen diversas variantes del protocolo EAP, según la modalidad de autenticación que se emplee, se puede hablar de dos grupos de variantes, las que emplean certificados de seguridad y las que utilizan contraseñas.

Las variantes de EAP que emplean certificados de seguridad son las siguientes:

- EAP-TLS: este es un estándar desarrollado por la compañía Microsoft y definido ene el RFC 2716, utiliza un certificado X.509 para realizar la autenticación, en lugar de la combinación usuario/password, requiere de instalar certificados en los clientes y en servidor y proporciona autenticación mutua fuerte (el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEB. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transparent Layer Substrate).

- EAP-TTLS: Desarrollada por Funk Software y Certicom, proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor, agilizando el proceso, esto garantiza la autenticación del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que establece la sesión TLS, utilizando otro método tal como PAP, CHAP, MS-CHAP o MS-CHAP V2, con lo cual el suplicante se identifica con una combinación nombre/contraseña.

- PEAP: Desarrollado por Microsoft, Cisco y RSA Security, funciona de manera parecida a EAPTTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor y provee protección a métodos mas antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

El empleo de certificados permite una autenticación fuerte entre cliente y servidor, sin embargo posee también varias desventajas:

- La administración de los certificados de seguridad puede ser costosa y complicada, especialmente en los esquemas donde se necesitan certificados en los clientes y en el servidor, es necesario comprar los certificados a una autoridad de certificación (CA) conocida o montar una CA propia.

- El diálogo de autenticación es largo, esto ocasiona que el proceso sea algo demorado, siendo especialmente molesto para usuarios que tienen que reautenticarse con mucha frecuencia.

- La manipulación del certificado puede ser engorrosa para el usuario, en muchos casos se elige instalar el certificado en la terminal del usuario, con lo cual, si la terminal es robada y el certificado es el único nivel de seguridad que se posee, la seguridad de la red estaría en riesgo, la otra solución sería llevar el certificado en una tarjeta inteligente, lo que obligaría a instalar hardware adicional en las terminales para leer dichas tarjetas.

Las variantes de EAP que utilizan contraseñas son las siguientes:

- EAP-MD5: emplea un nombre de usuario y una contraseña para la autenticación, la contraseña se transmite cifrada con algoritmos MD5, su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a taques de diccionario. Además, el cliente no tiene manera de autenticar al servidor y el esquema no es capaz de generar claves WEP dinámicas.

- LEAP: Esta variante es propiedad de la compañía CISCO, este emplea un esquema de nombre de usuario y contraseña y soporta claves dinámicas WEP, y al ser una tecnología de CISCO, exige que todos los puntos de acceso sean de esta marca y que el servidor RADIUS sea compatible con LEAP.

- EAP-SPEKE: Emplea el método SPEKE (Simple Password-authenticated Exponential Key Exchange), que permite verificar que tanto clientes como servidores comparten una información secreta (en esta caso, una contraseña) a través de un medio inseguro y sea comprobado que el método es muy seguro, aun con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados, muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

RADIUS: Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cable modem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red o Network Access Server) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como

PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

RADIUS fue desarrollado originalmente por Livingston Enterprises para la serie PortMaster de sus Servidores de Acceso a la Red, más tarde se publicó como RFC 2138 y RFC 2139. Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría puede gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. A menudo se utiliza SNMP para monitorear remotamente el servicio.

Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes).

RADIUS es extensible; la mayoría de fabricantes de software y hardware RADIUS implementan sus propios dialectos.

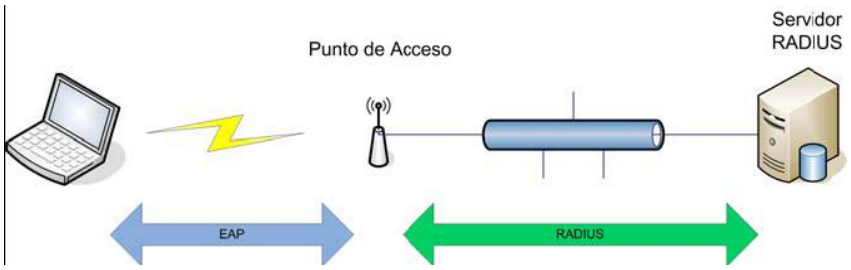


Figura 1.21 Autenticación EAP con RADIUS

TKIP: Es un protocolo de llave temporal (Temporal Key Integrity Protocol) es otro elemento derivado del 802.11i, está diseñado para corregir las vulnerabilidades conocidas de WEP en el área de encriptación de datos, específicamente TKIP repara la falla de seguridad del uso cíclico de llaves en WEP.

El paquete de TKIP está compuesto de tres partes:

1. Una llave dinámica y temporal, incrementada de 40 bits en WEP a 128 bits en TKIP, la cual es compartida por los clientes y los puntos de acceso.
2. una dirección MAC de un dispositivo cliente.
3. Un vector de inicialización de 48 bits describe un número de secuencias de paquete.

Está combinación garantiza que varios clientes usen diferentes llaves.

Para ser compatible con hardware existente, TKIP usa el mismo algoritmo de encriptación (RC4) usado en WEP, que solamente una actualización en software es

requerida para implementar TKIP, comparando con WEP, TKIP cambia las llaves temporales cada 10,000 paquetes y esta distribución dinámica deja a los hackers un pequeño espacio para romper la llave TKIP.

MICHAEL: Es usado para asegurar la integridad de los datos, el código de integridad de mensajes (MIC) es un mensaje de 624 bits calculado usando el algoritmo de Michael, su finalidad es detectar posibles cambios en el contenido del paquete debido a errores de transmisión o manipulación intencional.

PSK: Existe un caso en la implementación de 802.1X, en ambientes de usuarios pequeños tal como en hogares o pequeños negocios, un servidor de autenticación puede ser una opción para autenticar, un mecanismo de llave compartida con antelación (PSK-Pre Shared Key) es usado y la llave compartida es puesta tanto en el suplicante como en el autenticador manualmente.

Su único requerimiento es compartir una clave entre los diferentes clientes que se van autenticar contra un determinado punto de acceso que también la conoce, si la clave de un cliente inalámbrico coincide con la del correspondiente AP se le otorga acceso, denegándolo en caso contrario. Esta clave no se envía la AP al intentar la autenticación sino que es el origen de un trabajo criptográfico que finalmente conduce a la autenticación, por lo que no es posible averiguar rastreando las emisiones, esta claro que no es tan seguro como el uso de un servidor RADIUS pero será más que suficiente en entornos que necesiten conectar de forma segura a pocos equipos.

1.10) 802.11i precisa los protocolos

1.9.1) WRAP Y CCMP

El WRAP[8] es un protocolo de encriptación en el estándar 802.11i, está basado en el modo AES de compensación de un libro de códigos o símbolos OCB[9].

Los problemas con respecto a los derechos de propiedad de este protocolo, reclamado por sus diferentes grupos han causado que el IEEE introduzca el CCMP[10] en el estándar 802.11i y hacer de WRAP un componente opcional de RSN[11].

CCMP utiliza una estructura de llaves jerárquicas, basadas en pares de llaves y llaves de grupo. Las fases operacionales son: descubrimiento, autenticación, administración de llaves y transferencia de datos.

1.10.2) MIC

El verificador de integridad de mensajes (MIC-Message Integrity Check), es también parte del 802.11i y tiene una función muy similar al ICV utilizado en WEP.

---

[8] WRAP.- Wireless Robust Authentication Protocol-Protocolo Inalámbrico de Autenticación Robusta
[9] OCB.- Offset Codebock
[10] CCMP.- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
[11] RSN.-

Sin embargo el ICV solo protege al contenido del paquete, pero no su encabezado. El MIC protege a ambos al paquete y al encabezado.

El MIC es un campo adicional de 8 bytes que está entre la posición de datos de una trama 802.11 y los 4 bytes del Valor de Comprobación de Integridad (ICV- Integrity Check Value).

El algoritmo que implementa el MIC es conocido como Michel, el cual también implementa un contador de tramas, lo cual detiene ataques de repetición.

Algunos analistas se refieren a MIC como un componente de TKIP.

1.10.3) RSN

Es un protocolo que reemplaza al TKIP y que sirve para negociar el tipo de cifrado a utilizar y establecer comunicaciones seguras con cada dispositivo inalámbrico en la WLAN.

RSN utiliza el 802.1x para autenticar dispositivos inalámbricos a la WLAN y proporciona las llaves dinámicas requeridas, todo esto con un bajo nivel de procesamiento en el autenticador, generalmente el punto de acceso.

RSN funciona de la siguiente manera:

1. La tarjeta inalámbrica del cliente, envía una solicitud de sondeo.

2. El punto de acceso inalámbrico envía una respuesta de sondeo con una trama de intercambio de información RSN.

3. La tarjeta de red inalámbrica solicita autenticación a través de uno de lo métodos aprobados.

4. El punto de acceso proporciona autenticación para la tarjeta inalámbrica.

5. La tarjeta de red inalámbrica envía una solicitud de asociación con una trama de intercambio de información.

6. El punto de acceso envía una respuesta de asociación.

Los conjuntos de administración y autenticación de llaves soportados por RSN son:

CÓDIGO	SIGNIFICADO
00:00:00:1	Autenticación y manejo de llaves 802.1x
00:00:00:2	Sin autenticación y manejo de llaves 802.1x

Tabla 1.7 Llaves de Administración y Autenticación RSN

Los cifrados soportados por RSN son:

CÓDIGO	SIGNIFICADO
00:00:00:1	WEP
00:00:00:2	TKIP
00:00:00:3	WRAP
00:00:00:4	CCMP
00:00:00:3	WEP-104

Tabla 1.8 Cifradores soportados por RSN

1.9.4) Beneficio y problemáticas de 802.11i

Beneficios:

- Canal encriptado y seguro antes de iniciar autenticación a nivel capa 2 del modelo OSI.
- Asociación y autenticación segura.
- Des-asociación y des-autenticación seguras.
- Negociación de cifrado: Adopta a los diferentes modos de cifrado en la misma WLAN, el 802.11i requiere que los dispositivos anuncian sus capacidades de encriptación, activando el tipo de cifrado apropiado basado en las capacidades mutuas de los equipos.
- Nuevo algoritmo de verificación de mensajes: MIC
- Metodología EAP para autenticar: EAP-TLS o cualquier otra.
- Soporte de movilidad (Roaming) al pre-autenticar los puntos de acceso al usuario.
- Encriptación reforzada con la implementación de encriptación AES-CCMP.
- Es compatible con redes IBSS y Ad-Hoc.

Beneficios:

- Requerimientos adicionales de hardware, para poder implementar AES.
- Para tener una WLAN que cumpla con el estándar 802.11i en su totalidad, se requiere cambiar todos los equipos inalámbricos de la(s) red(es) instaladas.
- Debilidad ante ataques DoS y no obliga al uso específico de un método EAP.

- Tendremos que esperar tanto la mercadotecnia, implementación y costos para 802.11i

1.9.5) Resumen de las normas de seguridad para WLANs

En la tabla 1.5 se tiene un comparativo de las diferentes normas de seguridad que han sido desarrolladas a la fecha tanto por la Alianza Wi-Fi y el IEEE.

Norma / Características	WEP	WPA	802.11i (RSN, WPA2)
Algoritmo de Cifrado	RC4	RC4 (TKIP)	Rijndael (AES-CCMP)
Llave de Encriptación	40-bits	128-bits (TKIP)	128-bits (CCMP)
Vector de Inicialización	24-bits	48-bits (TKIP)	48-bits (CCMP)
Llave de Autenticación	Ninguna	64-bits (TKIP)	128-bits (CCMP)
Integridad de los Datos	CRC-32	Michael (TKIP)	CCM
Integridad del Encabezado	No	Michael	CCM
Distribución de Llaves	Manual	802.1x (EAP)	802.1x (EAP)
Llave única para:	Red	Paquete, Sesión, Usuario	Paquete, Sesión, Usuario
Llave Jerárquica	No	Proviene de 802.1x	Proviene de 802.1x
Negociación Cifrada	No	Si	Si
Seguridad Ad-Hoc	No	No	Si (IBSS)
Pre-Autenticación (Red Cableada)	No	No	Utiliza 802,1x (EAPOL)

Tabla 1.9 Cuadro comparativo de las normas de seguridad Inalámbricas

2) La Telemedicina (e-salud)

En este capítulo describiré un poco la historia de la Telemedicina a nivel Mundial y en nuestro país para poder establecer una relación con la zona rural y no cometer errores culturales e ideológicos en la instalación de la red inalámbrica.

2.1) Breve historia de la Telemedicina

La historia de la Telemedicina se ha desarrollo junto con las Telecomunicaciones (el telégrafo, el teléfono, la radio, la televisión y los enlaces por satélite se han aprovechado para uso médico desde el primer momento de su invención).

Desde inicios de 1900 se ha usado la medicina a distancia y existen ejemplos de equipos que fueron desarrollados para la transmisión de resultados de rayos X a través del telégrafo en Australia.

Se tienen referencias del uso de sistemas de radiotelegrafía ya en 1920 en los países nórdicos y en Italia para asistencia marítima.

La Telemedicina existe como tal desde fines de la década de 1950. Una de las primeras implementaciones se efectuó en la Universidad de Nebraska en los Estados Unidos y consistió en un circuito cerrado de televisión bidireccional comunicado por microondas, que se usó para tratamiento a distancia y educación médica.

Otro proyecto importante utilizó una conexión vía satélite entre un hospital de Anchorage, Alaska con otro de Sacramento en California.

El desarrollo de la Telemedicina hasta su nivel actual ha pasado por muchas etapas, y resulta indudable que ha estado relacionado con aspectos tecnológicos.

El creciente nivel de complejidad que desde la década de 1960 han ido adoptando las Telecomunicaciones, ha revolucionado este campo. Primeramente, las comunicaciones telefónicas han sufrido un cambio que va desde la telefonía electromecánica de los primeros tiempos, hasta los tendidos digitales de fibra óptica de alta velocidad de hoy en día.

La Administración Espacial y Aeronáutica Nacional (NASA), cuya sede se encuentra ubicada en los Estados Unidos, jugó un papel muy importante en los comienzos del Desarrollo de la Telemedicina. Los esfuerzos de la NASA en Telemedicina comienzan en los años 60, cuando el hombre decide volar hacia el espacio. Durante la Misión fueron Telemedidos los parámetros fisiológicos de los trajes espaciales y la nave espacial.

Estos primeros esfuerzos y el incremento en comunicaciones satelitales promovieron el desarrollo de la Telemedicina y descubrieron muchos de los Equipos Médicos de Salud de hoy.

Dentro de los primeros proyectos tenemos:

a) Tecnología Espacial aplicada para Asistencia Médica a una Reservación India en Arizona**.** Esta comienza en los años 1972-1975 y prestaba Servicio Médico a los Astronautas y a los Indios de la Reservación. Esta prestaba Servicios de Rayos X y Electrocardiograma. Luego fue enlazado con los Hospitales Públicos y Especialistas vía radar, microondas y transmisión de audio.
b) Requerimientos de Vídeo para Diagnóstico Médico Remoto. El propósito principal fue para investigar el uso de satélites en el envío de señales de vídeo para mejorar la calidad de la Asistencia Médica en Alaska.

El advenimiento de las comunicaciones vía satélite a finales de los 60's fue decisivo pues contribuyó al nivel actual de la Telemedicina permitiendo la transmisión remota de imágenes de televisión.

Cuba no ha estado exenta de esta experiencia y desde la década de 1970 ha experimentado en la transmisión de señales a través del teléfono o radio, con la finalidad de buscar mayor calidad del diagnóstico mediante consulta de segunda opinión, con la finalidad de brindar una atención adecuada a su población, por ende ha venido trabajando sistemáticamente en diferentes alternativas acordes con el desarrollo mundial.

En Europa comienza en 1980 en el Hospital Universitario de Tromso (Noruega) el uso de la Telemedicina.

En 1986 se hace en Noruega la 1ª videoconferencia entre médicos.

Para 1989, se crea en Francia el Instituto Europeo de Telemedicina.

En Inglaterra actualmente existen 4 centros que usan la Telemedicina: Aberdeen, Powys, London (Gay´s hospital and Hammersmith hospital) and Queen´s University in Belfast.

En Italia desde 1987 hasta 1990 el Instituto de Radiología de la Universidad de L´Aquila fue el primero en usar protocolos Standards.

En España en 1990, la Dirección General de Telecomunicaciones patrocina el proyecto REVISA (Red de Videoteléfonos Sanitarios) de las Islas Canarias.

En 1996 una compañía privada llamada TELE-Rx se ha establecido en el sur de España, ofrece servicios de diagnósticos Tele-radiológicos.

En Cuba a partir de 1998, se decide por el Ministerio de Salud Pública, abordar de conjunto con el grupo de la electrónica del SIME, la implementación de una Red de Telediagnóstico para el Sistema Nacional de Salud, soportada en la Red Telemática de la Salud, INFOMED, la cual brinda el soporte necesario de Telecomunicaciones, para el tráfico de la información e implementado con el Sistema PATRIS y REX, producidos por EICISOFT, iniciándose en una primera etapa en 8 hospitales Clínico Quirúrgicos y Pediátricos de subordinación provincial, un Hospital Especializado y un Instituto de Investigación y Desarrollo de subordinación nacional.

Sin embargo, la mayor revolución en este campo, la brindó el advenimiento de la computación, que posibilitó el almacenamiento masivo de datos médicos y su transferencia a otros sitios para ser consultados.

Las primeras implementaciones de Telemedicina y computadoras ofrecían la posibilidad de consultar grandes bases de datos e Historias Clínicas, y de proveer educación médica a distancia.

En los últimos 10 años es, sin embargo cuando hace eclosión la computación gráfica, modificando todas las prácticas médicas por la posibilidad de incorporar imágenes a las herramientas con que había contado la Telemedicina hasta ese momento.

Y, finalmente, el advenimiento de las grandes redes de computadoras, y entre ellas la Internet, transformó a la Telemedicina en un recurso al alcance de grandes sectores de la población y la comunidad médica.

Todas estas experiencias, sirvieron de base para que en los últimos años la Telemedicina haya recibido un impulso muy importante gracias al desarrollo de las Tecnologías de la Información y las Comunicaciones. Resulta evidente el interés creciente de los sectores público y privado por explotar las capacidades de los sistemas de telecomunicación avanzados para su uso en la mejora de los servicios de salud. Estados Unidos en primer lugar, en Australia, Canadá y también en menor medida en Europa, existen ya numerosos programas y redes de Telemedicina en funcionamiento estable, que se han visto multiplicados con el desarrollo de Internet, la telefonía móvil y las nuevas redes de telecomunicaciones de banda ancha.

2.2) Telemedicina en México

El Ingeniero Guillermo González Camarena en 1948 en la octava asamblea de médicos cirujanos fue el primero en instalar un circuito cerrado con cámara de orticón para la enseñanza de la cirugía y un año después, durante la siguiente asamblea, los cirujanos tuvieron el privilegió de presenciar las primeras pruebas de televisión a colores con el sistema tricromático y posteriormente este sistema fue colocado en la Facultad de Medicina de la UNAM para la enseñanza didáctica de la cirugía.

El ISSSTE es la institución pionera en México, y es el programa de esta institución en la que más logros se han tenido a lo largo de su desarrollo. Con el creciente desarrollo de las Telecomunicaciones se han buscado nuevas aplicaciones que ayuden al hombre y la Telemedicina busca esta aplicación en el sector de la salud humana, esto con el fin de dar asistencia a distancia clínico-sanitaria y médico a médico.

La responsable de este proyecto es la ahora directora del programa de Telemedicina del ISSSTE la M. en C. Amanda Gómez, la idea surgió cuando ella y un médico que la acompañaba en un evento realizado en Estados Unidos se dieron cuenta que en ese país y Rusia habían realizado un enlace con un fin médico.

En el año de 1993 se le presentó el proyecto al subdirector del ISSSTE, quien se vio muy interesado, ya que el proyecto era prometedor y sobre todo por que iba a evitar

traslados innecesarios de pacientes lo cual haría que se redujeran gastos, pero mejor aún que se autofinanciaría la red en muy poco tiempo.

En 1995 se realizó un proyecto piloto que consistió en hacer un enlace vía satélite entre un hospital de Tuxtla Gutiérrez y el Centro Médico 20 de Noviembre en el Distrito Federal.

Las pruebas hechas en este piloto, se realizaban a través de la transmisión de video, voz y datos, la cual tuvo una duración de cuatro meses y que durante este tiempo se evitaron 52% de los traslados que se hacían anteriormente en este hospital con lo que se llegó a la conclusión que era autofinanciable.

Los aspectos técnicos que tomaron en cuenta para la mejor realización del proyecto, está la calidad del vídeo la cual debe ser muy buena para muchas especialidades, con lo que se estableció como mínimo una conexión de 256 Kbps y la consideración de equipos periféricos como estetoscopio electrónico, electrocardiógrafo, escáner para rayos X, cámara de documentos y videograbadora.

Además de un ancho de banda para el enlace final de 512 Kbps para contar con buena calidad de los elementos antes mencionados (video, audio y datos). Para la conexión existían dos alternativas conexión vía satélite o fibra óptica, pero la última tenía algunos inconvenientes, tanto técnicos como económicos. Así no tanto la tecnología satelital, ya que permitía la reutilización de canales.

Por esto el programa de Telesalud ISSSTE-México ha sido declarado como programa prioritario por el gobierno federal, por lo que ha quedado exento del pago del segmento satelital destinado al apoyo de la educación y la salud.

Entonces se decidieron por reutilizar la portadora, un ancho de banda satelital que posibilita el enlace ida y vuelta a cualquier hora del día. En 1995 se asignaron 10 portadoras, y el equipo se preparó para las siguientes etapas. Un año después se instalaron ocho en hospital 20 de noviembre, hospital 1º de octubre, Tuxtla Gutiérrez, Villahermosa, Tampico, Veracruz y Hermosillo.

2.2) ¿Qué es la Telemedicina?

Es el uso de la informática y Telecomunicaciones para la asistencia sanitaria, de médico a médico con fines clínicos.

Sirve para intercambiar información médica de cualquier tipo por medios electrónicos de comunicación para mejorar la calidad de las prestaciones médica. También puede ser definida como la provisión del cuidado de la salud a través de una combinación de las telecomunicaciones y las tecnologías multimedia con médicos expertos.

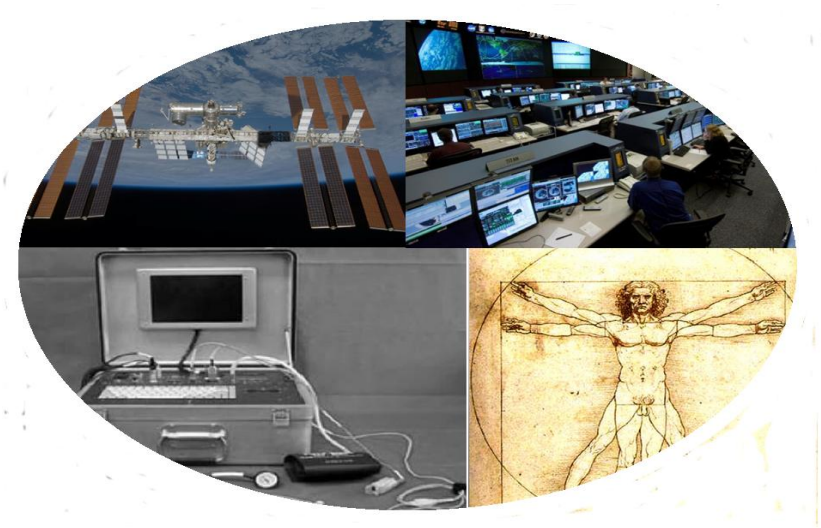


Figura 2.1 La Telemedicina

2.3) Medios de comunicación y tecnología requerida para el funcionamiento de una red de Telemedicina

2.3.1) Niveles de atención

Son las diferentes etapas que se presentan en los servicios de salud dentro de una entidad federativa.

A) Primer Nivel: En este nivel de atención el servicio es brindado en clínicas familiares por médicos generales y enfermeras, es aquí donde se atiende entre el 80% y el 85% de la población.

En éste nivel se necesita una plataforma sencilla que permita entablar una comunicación multimedia entre el hospital de referencia y la unidad local, para esto se puede utilizar una plataforma que cuente con una PC que tenga el sistema operativo Windows de Microsoft.

Dentro del equipo multimedia de la PC, deben de estar incluidas tanto las bocinas, como el micrófono y la cámara Web, con lo que se permitirá el intercambio de datos, imagen, vídeo y voz de mediana calidad, debe de contar al menos con una línea telefónica, tener un dispositivo de fax, el ancho de banda que debe tener la conexión a Internet puede ser desde 56 kbps hasta 128 Kbps.

Figura 2.2 PC para el primer nivel

Los aparatos mínimos para hacer un buen diagnóstico en el ***primer nivel*** son:

1) Estetoscopio: También conocido como fonendoscopio, es un dispositivo usado en medicina para oír los sonidos internos del cuerpo humano; fue inventado por

René-Théophile-Yaciente Laennec en 1816. Generalmente usado en la auscultación de los latidos cardíacos o lo ruidos respiratorios mayormente, aunque algunas veces, también se usa para escuchar otros ruidos.

Los estetoscopios estándares no proporcionan ninguna amplificación, lo que viene a limitar su uso. Este estetoscopio, utiliza circuitos amplificadores operacionales diferenciales para amplificar más que un estetoscopio estándar e incluye filtros activos pasa banda para eliminar frecuencias indeseadas y el ruido de fondo.

Figura 2.3 Estetoscopio

Figura 2.4 báscula

2) Báscula: Aparato que es de utilidad para pesar. Existen diferentes tipos y modelos, los cuales varían en escala y precisión dependiendo del uso que se les vaya a dar.

3) Termómetro: Es un instrumento que fue inventado y fabricado para poder medir la temperatura. Desde su invención ha evolucionado mucho, principalmente desde que se empezaron a fabricar los termómetros electrónicos digitales.

Los termómetros iniciales que se fabricaron se basaban en el principio de la dilatación, por lo que se prefiere el uso de materiales con un coeficiente de dilatación alto de modo que, al aumentar la temperatura, la dilatación del material sea fácilmente visible. El metal base que se utilizaba en este tipo de termómetros ha sido el mercurio encerrado en un tubo de cristal que incorporaba una escala graduada.

Figura 2.5 Termómetro de mercurio

Figura 2.6 Termómetro digital

El creador del primer termoscopio fue Galileo Galilei; éste podría considerarse el predecesor del termómetro. Consistía en un tubo de vidrio que terminaba con una esfera en su parte superior que se sumergía dentro de un líquido mezcla de alcohol y agua. Al calentar el agua, ésta comenzaba a subir por el tubo. Sanctorius incorporó una graduación numérica al instrumento de Galilei, con lo que surgió el termómetro.

4) Esfigmomanómetro: Instrumento médico usado para la medición de la **presión arterial.** La palabra proviene del griego *sphygmós*, pulso; *manós*, no denso y *metron*, medida. También es conocido popularmente como "tensiómetro" o "baumanómetro".

Figura 2.7 Esfigmomanómetro

El esfigmomanómetro puede ser de varios tipos: los tradicionales de columna de mercurio, los aneroides (de aguja en un dial circular) y los digitales. Con el uso de estos instrumentos se puede medir la presión o tensión arterial de manera indirecta, ya que se comprime externamente a la arteria y a los tejidos adyacentes y se supone que la presión necesaria para ocluir la arteria, es igual a la que hay dentro de ella.

B) Segundo Nivel: En este nivel de atención se cuenta con el servicio de cuatro especialidades troncales: Ginecología, Pediatría, Medicina Interna y Cirugía, aquí se atiende del 15% al 17% de la población.

En éste nivel se necesita una plataforma que permita establecer una videoconferencia de buena calidad entre el hospital de referencia y las unidades locales, para esto se puede utilizar una plataforma que cuente con una PC que tenga el sistema operativo Windows de Microsoft incluir dentro de las aplicaciones, el software utilizado por los equipos periféricos, dentro del equipo multimedia de la PC, deben de estar incluidas tanto las bocinas, como el micrófono y la cámara Web, con lo que se permitirá el intercambio de datos, imagen, video y voz de buena calidad.

Como para este nivel se necesita una videoconferencia de buena calidad, es muy recomendable que se tenga un canal exclusivo de comunicación, con esto se mantendrá la privacidad y confiabilidad de la información que se intercambie durante la comunicación.

Las unidades tanto locales como de referencia, deberán contar con los equipos periféricos médicos que necesiten para dar su diagnóstico, dependiendo del nivel que les corresponda, debe de contar con una o varias líneas telefónicas, un dispositivo de Fax y el ancho de banda mínimo que debe tener la conexión a Internet es de 256 Kbps.

Figura 2.8 Segundo nivel de atención

Los aparatos mínimos para hacer un buen diagnóstico en el ***segundo nivel*** son:

***1) Laboratorio de análisis clínicos*:** Un laboratorio clínico engloba un conjunto de estudios específicos los cuales proporcionan una mayor información diagnóstica en la evaluación del funcionamiento de los diversos sistemas en el organismo, e intentan simplificar al médico la obtención de la información clínica.

Para que los servicios de un laboratorio tengan validez oficial, deben ser avalados por un químico responsable con registro ante la Secretaría de Salud, además de que debe contar con el equipo necesario para realizar la mayoría de los análisis clínicos que en forma rutinaria son solicitados por todo médico profesional. Su objetivo es brindar análisis de calidad a la comunidad en general.

Figura 2.9 Laboratorio de análisis clínico

2) Rayos X: Los rayos X son una radiación electromagnética de la misma naturaleza que las ondas de radio, las ondas de microondas, los rayos infrarrojos, la luz visible, los rayos ultravioleta y los rayos gamma. La diferencia fundamental con los rayos gamma es su origen: los rayos gamma son radiaciones de origen nuclear que se producen por la desexcitación de un nucleón de un nivel excitado a otro de menor energía y en la desintegración de isótopos radiactivos, mientras que los rayos X surgen de fenómenos extranucleares, a nivel de la órbita electrónica, fundamentalmente producidos por desaceleración de electrones. La energía de los rayos X en general se encuentra entre la radiación ultravioleta y los rayos gamma producidos naturalmente.

Los rayos X fueron descubiertos de forma accidental en 1895 por el físico alemán **Wilhelm Conrad Roentgen** mientras estudiaba los rayos catódicos en un tubo de descarga gaseosa de alto voltaje. A pesar de que el tubo estaba dentro de una caja de cartón negro, Roentgen vio que una pantalla de platinocianuro de bario, que casualmente estaba cerca, emitía luz fluorescente siempre que funcionaba el tubo. Tras realizar experimentos adicionales, determinó que la fluorescencia se debía a una radiación invisible más penetrante que la radiación ultravioleta. Roentgen llamó a los rayos invisibles "rayos X" por su naturaleza desconocida.
Los rayos X son radiaciones electromagnéticas cuya longitud de onda va desde unos 10 nm hasta 0,001 nm (1nm o nanómetro equivale a 10-9 m). Cuanto menor es la longitud de onda de los rayos X, mayores son su energía y poder de penetración.

Los rayos X se utilizan principalmente en traumatología y ortopedia, en neumología para placas de tórax y en urgencias analizando el abdomen.

Las ventajas de este procedimiento son que es barato, seguro y mediante él se puede identificar el requerimiento de un estudio más preciso.

3) Incubadoras: Es un aparato o cámara construido para mantener organismos vivos en un entorno favorable para su crecimiento; las incubadoras mantienen condiciones de temperatura y grado higrométrico constantes, con el propósito de recibir temporalmente a recién nacidos prematuros.

Figura 2.10 Incubadora

4) Quirófano: El quirófano es un lugar o instalación acondicionada de tal manera que cuenta con el equipo, instrumental esterilizado y especializado, y con una limpieza lo más impecable posible, ya que en este lugar los médicos cirujanos intervienen u operan a las personas que necesitan someterse a una operación para que puedan recuperar su salud, la cual ha sido afectada o dañada por algún mal, como puede ser algún tumor maligno, enfermedad, accidente, etc.

Figura 2.11 Quirófano

También puede ser utilizado para practicar una cesárea, para realizar un transplante o para realizar muchas cosas más, todo con el fin de ayudar a que los pacientes recuperen o preserven su salud.

5) Cámara de Documentos: Este dispositivo periférico tiene la funcionalidad de un escáner, pero además ofrece una mayor resolución en cuanto a la calidad de las imágenes que son captadas a través de dicho equipo, por lo que su utilización en la transmisión de documentos de un sitio remoto a otro de referencia es de gran ayuda, ya que permite observar de manera clara desde documentos y radiografías, hasta la piel y uñas de alguna persona.

Figura 12 Cámara de documentos

La cámara de documentos es una herramienta de presentación que se puede utilizar para mostrar transparencias, texto, objetos 3-D, y objetos microscópicos.

Una cámara de documentos puede mostrar claramente objetos 3D, documentos e incluso imágenes microscópicas en una TV o en un proyector S-Vídeo.

C) Tercer Nivel: En este nivel de atención se atienden subespecialidades y en hospitales especializados como el Primero de Octubre, Zaragoza y Adolfo López Mateos, ubicados en el D.F. en México.

En éste nivel se necesita una plataforma que permita establecer una videoconferencia de buena calidad entre el hospital de referencia y las unidades locales, para esto se puede utilizar una plataforma que cuente con una PC que tenga el sistema operativo Windows de Microsoft, incluir dentro de las aplicaciones el software utilizado por los equipos periféricos, dentro del equipo multimedia de la PC, deben de estar incluidas tanto las bocinas, como el micrófono y la cámara Web, con lo que se permitirá el intercambio de datos, imagen, vídeo y voz de buena calidad, para este nivel se necesita una videoconferencia de buena calidad, es muy recomendable que se tenga un canal exclusivo (dedicado) de comunicación, con esto se mantendrá la privacidad y confiabilidad de la información que se intercambie durante la comunicación.

Figura 2.13 Transmisión de una consulta

Las unidades tanto locales como de referencia, deberán contar con los equipos periféricos médicos que necesiten para dar su diagnóstico, dependiendo del nivel que les corresponda, debe de contar con una o varias líneas telefónicas, tener un dispositivo de Fax y el ancho de banda mínimo que debe tener la conexión a Internet es de 512 Kbps.

Los aparatos mínimos para hacer un buen diagnóstico en el ***tercer nivel*** son:

1) Oftalmoscopio: Es un instrumento para observar aumentado el fondo del ojo de un paciente , donde se localiza la retina. Fue inventado por ***Hermann von Helmholtz*** en 1851.

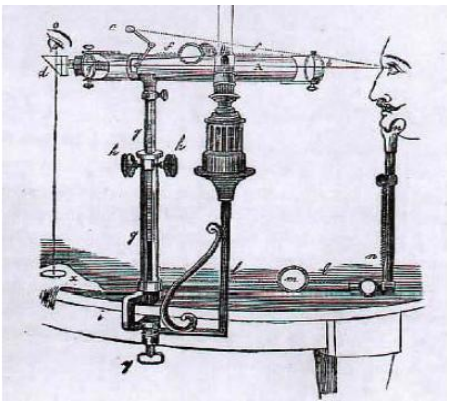


Figura 2.14 Oftalmoscopio fijo de Liebreich

Mediante la observación directa de las estructuras oculares no sólo es posible detectar patologías o anormalidades inherentes al ojo, sino también alteraciones sistémicas como diabetes, hipertensión arterial o procesos neurológicos. O sea que el ojo es como una ventana a través de la cual pueden realizarse muchas evaluaciones clínicas.

El oftalmoscopio directo es un aparato manual con una luz con la que, a través de la parte central no plateada de un espejo angulado, puede verse la retina iluminada.

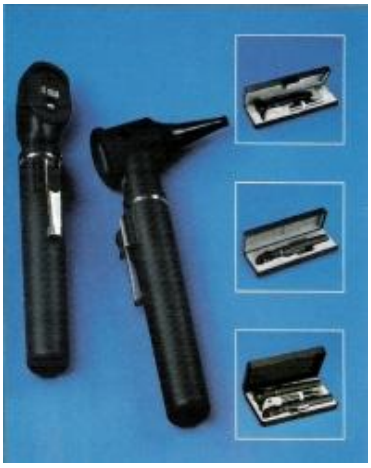


Figura 2.15 Oftalmoscopio Rini-Mini 3009 RIESTER

Los nuevos oftalmoscopios tienen una serie de aperturas para usar en diferentes situaciones:

- ***Apertura pequeña*****:** facilita la visión del fondo en pupilas no dilatadas; así se evita el reflejo del haz de luz sobre el borde pupilar.

- ***Apertura grande*****:** para ojos con pupilas dilatadas y examen de las estructuras oculares anteriores.

- ***Apertura de fijación*****:** tiene dos líneas cruzadas perpendicularmente, lo que permite un fácil diagnóstico de fijación excéntrica si al hacer mirar al paciente el punto donde se cruzan las líneas, ésta no cae directamente en la mácula.

A su vez las líneas están graduadas, para medir no sólo el grado de fijación excéntrica sino también las lesiones maculares o coroideas.

1. Apertura de hendidura**:** ayuda a determinar niveles en lesiones, en particular tumores y edema de papila.

2. Filtro de cobalto**:** si se instila una gota de fluoresceína en la superficie o cular, es posible evaluar lesiones de las estructuras externas del ojo.

3. ***Luz aneritra*****:** al eliminar el espectro rojo del haz de luz, resalta estructuras, principalmente las vasculares. Además puede usarse con todos los tipos de aperturas.

Entre los rayos luminosos que retornan y el ojo del examinador, hay una recamara giratoria de lentes, que suelen oscilar desde +30 a -30 dioptrías, y corrigen cualquier error de refracción inherente, ya sea del paciente o del examinador. Mediante el cambio

en el poder de las lentes y variando la distancia del examinador al paciente, pueden evaluarse otras estructuras, por ejemplo:

a) Con +15 D y a 5 cm del paciente se pueden evaluar córnea e iris.

b) Con +6 D y a 15 cm del paciente, se evalúa el cristalino. En la misma posición, haciendo mirar al paciente a derecha e izquierda, y abajo y arriba, pueden observarse opacidades vítreas.

2) Electrocardiógrafo: Es un aparato electrónico que capta y amplía la actividad eléctrica del corazón a través de electrodos colocados en las 4 extremidades y en 6 posiciones precordiales.

Figura 2.17 Electrocardiógrafo

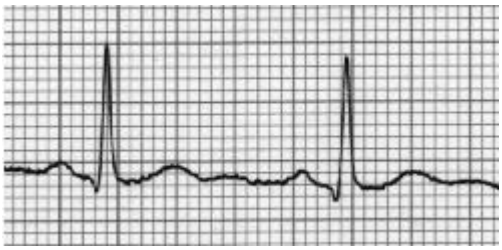


Figura 2.16 Electrocardiograma

El electrocardiograma (ECG/EKG, del alemán Elektrokardiogramm) es el gráfico que se obtiene con el electrocardiógrafo para medir la actividad eléctrica del corazón en forma de cinta gráfica continua. Es el instrumento principal de la electrofisiología cardiaca y tiene una función relevante en el cribado y diagnóstico de las enfermedades cardiovasculares.

***3) Otoscopio*:** El otoscopio es un instrumento que posee una fuente de luz, un lente con aumento y un dispositivo donde insertar espéculos auditivos (conos) de diferentes tamaños, nos sirve para realizar una exploración del conducto auditivo externo y para evaluar el oído medio a través de la visualización directa del tímpano.

Un **otoscopio** consta de 3 partes:

***a)* El mango,** que contiene la batería para la fuente de luz.

***b)* La cabeza,** que contiene la bombilla y una lente de aumento.

c) El cono, que se inserta en el conducto auditivo.

Figura 2.18 Otoscopio

4) Dermatoscopio: Es un instrumento que permite observar la piel con mayor precisión y sirve para obtener una imagen aumentada y más clara de las características, lesiones de la piel o de un lunar en específico.

Figura 2.19 Dermatoscopio

Emplea un sistema de lentes ópticos, con una luz incidental que ilumina la piel y permite un aumento con el lente que va desde 10X - 50X.

Un dermatoscopio permite diferenciar entre estructuras melanocíticas y no malanocítas, y observar de forma precisa las lesiones pigmentadas de la piel.

Principalmente se compara el volumen, tamaño, área, color, forma y densidad de algún lunar que se analice.

También permite valorar la profundidad de las arrugas.

5) Cámara de Documentos: Ver figura 2.12

d) Centro Médico: En este nivel de atención se atienden casos cuya naturaleza requieren de investigación y desarrollo de nuevos métodos para el tratamiento y control de la enfermedad, además de realizar operaciones de trasplante de órganos, en México se cuenta con el Centro Médico Nacional Siglo XXI y con el Hospital 20 de Noviembre.

Figura 2.20 Cuarto de cirugía del centro Médico siglo XXI

En éste nivel se necesita una plataforma que permita establecer una videoconferencia de alta calidad entre el hospital de referencia y las unidades locales, para esto se puede utilizar una plataforma que cuente con una PC que tenga el sistema operativo Windows de Microsoft, incluir dentro de las aplicaciones, el software utilizado por los equipos periféricos, dentro del equipo multimedia de la PC, deben de estar incluidas tanto las bocinas, como el micrófono y la cámara Web, con lo que se permitirá el intercambio de datos, imagen, video y voz de buena calidad, para este nivel se necesita una videoconferencia de buena calidad, es muy recomendable que se tenga un canal exclusivo (dedicado) de comunicación, con esto se mantendrá la privacidad y confiabilidad de la información que se intercambie durante la comunicación.

Las unidades tanto locales como de referencia, deberán contar con los equipos periféricos médicos que necesiten para dar su diagnóstico, dependiendo del nivel que les corresponda, debe de contar con una o varias líneas telefónicas, tener un dispositivo de Fax y el ancho de banda mínima para la conexión a Internet es de 512 Kbps.

2.4) Unidades requeridas para la transmisión de una red en Telemedicina vía satelital

a) Unidad Maestra: Es la unidad con mayor capacidad, ya que cuenta con la infraestructura necesaria para atender y controlar a las unidades regionales y a las unidades remotas.

Figura 2.21 Unidad Maestra

Esta unidad cuenta con una antena de radio y potencia mayor que las antenas de las unidades remotas y regionales, doble modem, redundancia en radios, emisión y edición del canal de Tele-educación.

Figura 2.22 Unidad Regional

b) Unidad Regional: *Es* la unidad que cuenta con la infraestructura necesaria para atender y controlar a las unidades remotas.

Esta unidad cuenta con una antena de radio y potencia mayor que las antenas de las unidades remotas, y menor (en cuanto a tamaño y potencia) que la antena de la unidad maestra, doble modem y redundancia en radios.

c) Unidad Remota: Es la unidad que cuenta con la infraestructura necesaria para atender y controlar casos sencillos (de primer nivel de atención).

Figura 2.23 Unidad Remota

Esta unidad cuenta con una antena VSAT, un modem y un radio.

La VSAT (terminal de muy pequeña apertura) es una estación terrena del Servicio Fijo por Satélite (geoestacionario) utilizada para una gran variedad de aplicaciones en el campo de las telecomunicaciones, que incluye las comunicaciones de datos interactivas y por lotes en diversos protocolos, operación de redes con conmutación de paquetes, servicios de voz, transmisión de datos y vídeos y operación en red en una vasta área.

2.5) Telemedicina a nivel Mundial

En los últimos años, empresas multinacionales comienzan a realizar pilotos con equipos especialmente diseñados para realizar telemedicina (Unidades de Telemedicina). Esto ha ocurrido por un desarrollo más intenso de las telecomunicaciones y el desarrollo de software específicos, que mediante grandes compresiones de archivos, logra la transmisión de sonido y vídeo en tiempo real, permitiendo una comunicación de carácter fluido entre el paciente y el médico ubicado distante de él.

Estos equipos, utilizan simplemente las líneas telefónicas o bandas de ancho relativamente pequeñas para lograr una transmisión apropiada. Asociados a estos equipos, se incorporan estetoscopios electrónicos, capaces de transmitir en tiempo real los sonidos del corazón y pulmón, permitiendo que el paciente sea atendido por una enfermera o incluso por una auxiliar de enfermería. En el otro extremo, un médico especialista evalúa los antecedentes transmitidos por el mismo paciente, o incluso con antelación por la enfermera, dejando un registro en una base de datos.

Los sonidos transmitidos por el estetoscopio son similares a los obtenidos al escuchar directamente al paciente y permiten eventualmente hacer diagnósticos de neumonías, derrames, soplos cardíacos, etc. Asimismo, es posible contar con una cámara **dermatoscópica**, que envía imágenes de alta definición para ser evaluadas a distancia

por dermatólogos, permitiendo el seguimiento de lesiones sospechosas o la derivación en caso necesario.

Otra de las unidades que se pueden adicionar, es un electrocardiógrafo que tiene la posibilidad de conectarse a través de una red a la unidad de diagnóstico de telemedicina. La recepción también es en el mismo instante y puede quedar almacenada la computadora central o el de la misma unidad para ser interpretado en otro momento. También se puede incorporar un otoscopio y un oftalmoscopio, que de la misma manera que el dermatoscopio pueden realizar diagnósticos de precisión a distancia. Otro de los equipos es un esfigmomanómetro, que en forma electrónica es capaz de transmitir la información de la presión arterial.

Según fuentes del **NIH** (Nacional Institutes of Health) de Estados Unidos, en la actualidad se están desarrollando 260 programas a nivel mundial relacionados con telemedicina; se han publicado 11 587 artículos, y existen 138 congresos o seminarios que involucran este tema.

2.6) Zona Rural

Una zona rural es la que no se encuentra localizada dentro de las zonas delimitadas como urbanas.

El número de habitantes que tiene una población determina si ésta es rural o urbana. De acuerdo con el INEGI, una población se considera rural cuando tiene menos de 2500 habitantes, mientras que la urbana es aquella donde viven más de 2500 personas.

Las principales causas de muerte son enfermedades del corazón, tumores malignos, diabetis mellitus y accidentes.

De acuerdo al INEGI se dan en este orden:

1. Diabetis mellitus.
2. Enfermedades isquémicas del corazón.
3. Cirrosis y otras enfermedades crónicas del hígado.
4. Enfermedad cerebrovascular.
5. Enfermedad pulmonar obstructiva crónica.
6. Infecciones respiratorias agudas bajas.

La situación actual de la salud rural nos habla de la existencia de un importante rezago del campo mexicano en esta materia.

La población rural, en general, presenta mayores necesidades de salud que la población urbana, y el acceso que tiene a los recursos y servicios que requiere para atenderlas es considerablemente menor.

Los problemas de rezago se concentran en las comunidades rurales dispersas y en la periferia de las grandes ciudades.

La causa fundamental de estos problemas es la pobreza y su solución definitiva depende de la posibilidad de incrementar el nivel de bienestar general.

El vivir en un área rural limita el acceso a cuidados médicos especializados a tiempo, los residentes en estás áreas tiene por tanto un cuidado médico debajo del estándar, ya que los médicos especialistas se localizan en zonas donde se concentra la población.

2.7) Localidades rurales en México

Un pueblo indígena es aquel que desciende de poblaciones que habitaban en el territorio actual del país al iniciar la colonización y que conservan sus propias instituciones sociales, económicas, culturales y políticas o parte de ellas.

En México hay 51,606 localidades divididas en:

1. Localidades de interés o con presencia de población indígena con 1,535
2. Localidades con menos de 40% de población indígena con 22,797
3. Localidades con más de 40% de población indígena con 24,090
4. Localidades con cinco viviendas o menos con 3,184

En el Distrito Federal hay 266 localidades distribuidas de la siguiente manera:

5. Localidades de interés o con presencia de población indígena con 31
6. Localidades con menos de 40% de población indígena 144
7. Localidades con más de 40% de población indígena 68
8. Localidades con cinco viviendas o menos 23

En el Estado de México hay 2526 localidades distribuidas de la siguiente manera:

9. Localidades de interés o con presencia de población indígena con 252
10. Localidades con menos de 40% de población indígena 1812
11. Localidades con más de 40% de población indígena 442
12. Localidades con cinco viviendas o menos 20

Figura 2.24 Localidades indígenas

3) Herramientas Diagnósticas

En este capítulo trataré de describir las enfermedades más frecuentes que se presentan en la zona rural y algunos aparatos médicos que son necesarios en un nosocomio, mostrar que tan difícil es diagnosticar una enfermedad sino se hace con el equipo médico necesario y poder brindar una herramienta más con la red inalámbrica al profesional de la salud.

3.1) Introducción

En este capítulo trataremos el ***Expediente clínico orientado por problemas (ECOP)*** este fue propuesto por L. Weed en 1969 ha sido adoptado por muchos establecimientos médicos y escuelas de medicina en México y en el mundo.

La responsabilidad de los profesionales dedicados a mantener la salud y el bienestar de las personas no es darle más años de vida, sino más vida a sus años.

La opinión de la mayoría que lo utilizan es de que, no sólo tiene virtudes de simplicidad y la lógica, sino que, en efecto, constituye un excelente instrumento para ayudar a mejorar la calidad de la atención médica de los enfermos, a la vez que contribuye poderosamente a la educación y a la investigación clínica en medicina.

El expediente clínico orientado por problemas está compuesto por la historia clínica o relato patográfico, lista de problemas, lista de problemas, lista de planes iniciales y notas de evolución.

3.2) Historia Clínica

Es una lista de síntomas principales, seguida de la narración del padecimiento actual, durante el cual se permite al paciente la comunicación controlada y complementada por las oportunas preguntas del médico.

Conviene que está primera etapa se complemente con un número preciso y definido de datos obtenidos tanto por interrogatorio como por la exploración física del paciente, es útil contar con una forma diseñada (machote), dotado de espacio suficiente para que la persona que haga la historia clínica describa, con la amplitud que sea necesaria y con su estilo propio, el padecimiento actual.

Está historia clínica incluye un conjunto de datos que deben ser invariablemente llenados durante el estudio clínico del enfermo.

De esta manera no se permite que la fatiga, la prisa o el temperamento dicten y determinen el número y características de los datos que deben ser contestados; estos datos son determinados por cada institución, hospital, clínica, grupo médico o médico individual en una función de variables como son: población que utiliza sus servicios,

características de edad, ocupación, situación económica, exposición a factores patogénicos, morbilidad y mortalidad de la población.

Es importante resaltar que no pueden ser iguales los datos que deben buscarse en un paciente hospitalizado que en una clínica de pediatría o geriatría.

En algunos expedientes convencionales es común que existan varías historias clínicas realizadas por estudiantes y médicos de diverso rango.

A menudo los datos que se registran en una historia clínica no aparecen o están en contradicción con los que señala la otra. Esta duplicación de historia es indeseable y refleja falta de comunicación y de integración en el trabajo clínico.

3.1.2) Lista de problemas

Todo paciente se presenta al médico por que tiene uno o más problemas que el percibe o que el médico descubre.

Hay varias clases de problemas como uno enfermedad (por ejemplo, diabetes mellitus), un síndrome (por ejemplo, disfagia), un signo (por ejemplo, esplenomegalia), un síndrome psíquico (por ejemplo, ansiedad) o un problema social (por ejemplo, un esposo sin empleo). Cada uno de estos problemas requiere una acción.

Todos ellos deben aparecer en una hoja intitulada "lista de problemas", cada uno con su número correspondiente y con la fecha en que el problema fue identificado por el médico. El número estará asociado siempre al problema correspondiente y no se utilizará jamás para otro problema en el mismo paciente.

Los problemas de cualquier paciente pueden clasificarse en dos grupos:

a) ***Problemas Activos:*** Que son actuales y que demandan acciones médicas a corto o a largo plazo.

b) ***Problemas Inactivos:*** Problemas que no demanden ninguna acción por estar aparentemente resueltos o por algunas otras razones.

La lista de problemas es sumamente útil para integrar un expediente bien organizado. Permite obtener una visión panorámica total del paciente, ayudando así o evitar la peligrosa fragmentación que ha surgido como consecuencia de la especialización médica.

Cualquier médico que no conozca al paciente puede, en escasos segundos, enterarse del conjunto de sus problemas, lo cual permite actuar inteligentemente en caso necesario.

Ejemplo de lista de problemas		
Nombre del establecimiento		
Ficha de identificación del paciente		
Lista de problemas		
Fecha	***No. de problemas activos***	***Problemas inactivos***
26-IV-2008	1. *Diabetis Mellitus*	
26-IV-2008	2. Hipertensión intracraneana $\xrightarrow{(5\text{–}VI\text{–}2008)}$ cisticercosis cerebral	
26-IV-2008	3. Disfagia $\xrightarrow{(29\text{–}VI\text{–}2008)}$ esofagitis péptica	
26-IV-2008	4. Esplenomegalia $\xrightarrow{(30\text{–}VI\text{–}2008)}$ no confirmada	
26-IV-2008	5. Ansiedad	
26-IV-2008	6. Esposo sin empleo	
26-IV-2008	7. Hipercalcemia $\xrightarrow{(31\text{–}VI\text{–}2008)}$ no confirmada	
26-IV-2008		8.Historia de infarto al miocardio
26-IV-2008		9.Historia de asma

Figura 3.1 Lista de Problemas

3.1.3) Planes inículales de acción

Cada problema genera un plan de acción. La función primaria del médico clínico es tratar al paciente para aliviar de la manera más efectiva posible al conjunto de alteraciones patológicas en sus aspectos biológicos, psicológicos y sociales.

La hoja titulada "Planes de Acción" sirve para que se señalen allí los planes que surgen lógicamente de cada problema. Dicha hoja deberá llenarse una vez que se hayan establecido las listas de problemas.

Los planes iniciales de acción se escribirán por problemas, comúnmente incluirán tres tipos de acción diagnósticas, terapéuticos y de educación al paciente.

Ejemplo de planes iniciales de acción	
Nombre del establecimiento	
Ficha de identificación del paciente	
Planes Iniciales de Acción	
26-VI-2008	***No 1. Diabetes mellitus:***
	Dx. Buscar complicaciones cardiovasculares, renales y oculares de la diabetes: radiografías del tórax; ECG examen general de orina, química sanguínea, consulta con oftalmología dietética.
	Rx. Intentar control con medidas exclusivamente; en caso de resultar insuficiente, dar tolbutamida; dieta para diabético de 1500 calorías.
	Educación al paciente: se inicia con una explicación de lo que es la diabetes; uso de clinitest y cuidado de los pies.
	No 2. Hipertensión Intracraneana:
	Dx. Radiografías de cráneo; consulta con neurología.
	Rx. Sintomático: ácido acetilsalicílico, 600 mg c/4 a 6 horas.
	No 3. Disfagia:
	Dx. Buscar lesión orgánica esofágica: radiografía de esófago; considerar esofagoscopia y estudios manométricos.
	Rx. Dieta de 1500 calorías,
	No 4. Ansiedad:
	Dx. Intentar conocer mejor al paciente y sus problemas personales; en caso de ser necesario, solicitar psiquiátrica.

Figura 3.2 Planes iniciales de acción

3.1.4) Notas de evolución

Se escriben por problemas y, en condiciones ideales, aparecen en las mismas hojas que las notas escritas por médicos tratantes, enfermeras, dietistas, consultantes, trabajadores sociales, etc.

Para cada problema, cuya evolución se desea registrar, el médico deberá organizar su información en cuatro partes:

a) ***Datos subjetivos:*** La información proporcionada por el paciente.

b) ***Datos objetivos:*** Todo cambio en los datos de exploración física, datos de laboratorio, de gabinete y reportes de especialistas consultados.

c) ***Interpretación:*** Evaluación y comentarios que surgen como resultado de los datos obtenidos.

d) ***Nuevos planes de acción:*** Estos se dividen en nuevos planes de acción, los cuales, esta dicho, se dividen en planes diagnósticos, terapéuticos y educativos para el paciente.

El expediente se convierte en un instrumento valioso para optimizar la atención médica y para la educación médica del propio facultativo y de quienes revisen sus expedientes. Se describen las notas más importantes en un expediente clínico.

- ***Nota de salida. Nota de defunción:*** La nota final, a la salida del paciente o a resultas de su defunción, no es más que una nota de evolución final, más detallada, en la que describen los datos principales relacionados con todos y cada uno de los problemas del enfermo, la interpretación, las conclusiones diagnósticas, las acciones y los resultados obtenidos.

- ***Notas de los consultantes:*** Todo consultante deberá escribir su reporte en las hojas de notas de evolución. Empezará por identificar el problema para cuya solución ha sido llamado, anotando su número y título. A continuación escribirá, brevemente, sus conclusiones o sus recomendaciones principales.

- ***Hoja de concentración de datos clínicos; hoja de concentración de datos de laboratorio:*** Las hojas de concentración de datos clínicos y de laboratorio, los cuadros y gráficas, constituyen variantes de las notas de evolución, alas que a menudo sustituyen con ventaja al proporcionar una imagen visual, objetiva y de conjunto de la evolución de datos y problemas.

- ***Notas de enfermería:*** Las notas de enfermería constituyen un componente muy valioso del expediente clínico. Cuando se escriben con meticulosidad, cuidado e inteligencia, suelen aportar información muy valiosa para el médico y demás integrantes del equipo de salud que atiende al enfermo. Las notas de enfermería deben ser escritas por problemas, tal como aparecen numerados y titulados en la lista de problemas colocada al principio del expediente. Si la enfermera identifica un problema que no aparece consignado en la lista de problemas puede anotarlo como nuevo problema, siguiendo la secuencia antes señalada.

3.2) El Teorema de Bayes

El Teorema de Bayes es muy utilizado en Telemedicina para sacar las probabilidades de los indicadores costo oportunidad, costo beneficio y costo eficiencia, son muy importantes estos indicadores para encontrar sitios óptimos, de impacto social y de autofinanciamiento del proyecto.

Sea $E_1, E_{2,}....,E_n$ una partición de espacio muestral S, y sea A cualquier evento. Entonces, para todo i,

$$P(Ei \mid A) = \frac{P(Ei)P(A \mid Ei)}{P(E_1)P(A \mid E_1) + P(E_2)P(A \mid E_2) + ... + P(E_n)P(A \mid E_n)}$$

Utilizando la definición de probabilidad condicional obtenemos

$$P(Ei \mid A) = \frac{P(Ei \cap A)}{P(A)} = \frac{P(Ei)P(A \mid Ei)}{P(E_1)P(A \mid E_1) + P(E_2)P(A \mid E_2) + ... + P(E_n)P(A \mid E_n)}$$

Aquí hemos usado el teorema de la multiplicación, $P(Ei \cap A) = P(Ei)P(A \mid E_i)$, para obtener el denominador utilizamos

$$P(A) = P(E_1)P(A \mid E_1) + P(E_2)P(A \mid E_2) + ... + P(E_n)P(A \mid E_n)$$

Demostrando esta ecuación.

Sea $E_1, E_2, ...E_n$ una partición de espacio muestral S, y sea A cualquier evento. Entonces

$$P(A) = P(E_1)P(A \mid E_1) + P(E_2)P(A \mid E_2) + ... + P(E_n)P(A \mid E_n)$$

Puesto que los Ei forman una partición de S, los Ei son disjuntos por pares y $S = E_1 \cup E_2 \cup ... \cup E_n$

Luego

$$A = S \cap A = (E_1 \cup E_2 \cup ... \cup E_n) \cap A = (E_1 \cap A) \cup (E_2 \cap A) \cup ... \cup (E_n \cup A)$$

Y los $E_i \cap A$ son también disjuntos por pares. En está forma,

$$P(A) = P(E_1 \cap A) + P(E_2 \cap A) + ... + P(E_n \cap A)$$

Según el teorema de la multiplicación $P(E_i \cap A) = P(E_i)P(A \mid E_i)$; luego

$$P(A) = P(E_1)P(A \mid E_1) + P(E_2)P(A \mid E_2) + ... + P(E_n)P(A \mid E_n)$$

Ejemplo: En cierta zona rural, el 4% de los hombres y el 1% de las mujeres se enferman de gripe en el mes de diciembre. Además, el 60% de la población son mujeres. Ahora bien, si se selecciona al azar un persona de la zona rural y enferma de gripe, ¿Cuál es la probabilidad de que la persona enferma de gripe sea mujer?

Solución:

Sea A= (personas enfermas de gripe en el mes de diciembre)

Buscamos P (W|A)

P (W)=población de mujeres=60%

P (A|W)=Mujeres enfermas de gripe =1%

P (M)=Población hombres=40%

P A|H)=Hombres enfermos de gripe=4%

Según el teorema de Bayes es:

$$P(W \mid A) = \frac{P(W)P(A \mid W)}{P(W)P(A \mid W) + P(W)P(A \mid H)} = \frac{(60\%) * (1\%)}{(60\%) * (1\%) + (40\%) * (4\%)} = \frac{3}{11}$$

3.3) Diferentes tipos de diagnósticos

Los diferentes tipos de diagnósticos se basan en los diferentes cambios físico, psicológicos, patológicos, sociales, etc. Presentes en el paciente.

3.3.1) El cambio de peso

Es el resultado de la suma de cuatro componentes del cuerpo humano: protoplasma, fluidos extracelulares, tejido adiposo y esquelético, en la proporción de 50, 25, 18 y 7% respectivamente.

La causa más importante de adelgazamiento lento es la pérdida de protoplasma, la que se manifiesta, en el aspecto bioquímico, por desequilibrio negativo de nitrógeno, potasio y fósforo y, en aspecto clínico por atrofia muscular, En cambio, la causa más importante de pérdida rápida es la deshidratación, manifestada, en el aspecto bioquímico, por pérdida de agua y electrolitos y, en el aspecto clínico, por sequedad de mucosa, pérdida de la turgencia cutánea, oliguria e hipertensión arterial.

Las dos causas más comunes de aumento de peso son el aumento de tejido adiposo y de líquido extracelular.

En la obesidad (tejido adiposo) hay disminución de la densidad del cuerpo y disminución de nitrógeno, potasio, fósforo, agua y electrolitos, y del punto de vista clínico hay aumento de grosor de los pliegues cutáneos y del perímetro del abdomen, los brazos y los muslos.

El liquido extracelular abarca tanto el espacio intersticial como el comportamiento vascular da lugar al aumento de la presión venosa.
Con la pérdida de peso constituye uno de los síntomas más importantes de la patología, y a menudo es indicativa de la existencia de una enfermedad grave.

Conviene clasificarla de la siguiente manera:

a) ***Pérdida de peso en presencia de apetito aumentado***. Debe presentarse en:

- Diabetes mellitus.

- Hipertiroidismo.
- Absorción intestinal deficiente.
- Feocromocitoma.
- Síndrome carcinoide.

b) ***Pérdida de peso en presencia de anorexia y disminución de la ingesta***. Debe presentarse en:

- Depresión psíquica.
- Enfermedad hepática.
- Neoplasias malignas.
- Insuficiencia suprarrenal o hipofisaria.
- Intoxicaciones endógenas.
- Anorexia nerviosa.
- Infecciones crónicas.
- Enfisema pulmonar avanzado.
- Obstrucción pilórica.
- Enfermedades crónicas del aparato digestivo.

Aumento de peso suele deberse a la ***obesidad*** o a ***edemas.***

a) La obesidad: Es el resultado del desequilibrio positivo entre la ingestión de alimentos y el consumo energético.

b) Las consecuencias principales de ***edema son*** las siguientes:

- Insuficiencia cardiaca digestiva.
- Insuficiencia hepática crónica.
- Nefropatías con síndrome nefrótico.
- Edemas idiomáticos.
- Gastroenterapías con pérdida de proteínas.
- Desnutrición avanzada.
- Trastornos locales de circulación venosa y linfática.

3.3.2) Cambio en el apetito

Las bases fisiológicas del hambre no son bien definidas. Se acepta la existencia de centro reguladores localizados en el hipotálamo que consta de una porción denominada interna llamada ***centro de la saciedad.***

Se sigue aceptando que el hipotálamo ejerce un papel esencial en la modulación del hambre y el apetito y del comportamiento alimenticio gracias a que integra y organiza una gran cantidad de señales, y mantiene la homeostasia nutricional de los animales y del hombre.

Hoy en día existen dos sistemas: El periférico y central, cuyos mensajes o señales nerviosas y hormonales son integrados finalmente en el hipotálamo.

- ***El sistema periférico:*** Es responsable de señales que promueven la sensación de saciedad y la interrupción de la actividad alimentaria. La vía nerviosa consiste en impulsos nacidos en los interruptores de distensión, localizados en el estómago que, a través de los nervios vagos, alcanzan el núcleo del tracto solitario y de allí sigue hacia estructuras límbicas e hipotalámicas. La vía hormonal consiste en péptidos, entre los cuales destaca la colecistocina, neuropéptidos que transmiten mensajes de saciedad desde receptores gastrointestinales hasta diversos niveles del cerebro, incluyendo los núcleos paraventriculares del tracto solitario.

- ***El sistema central:*** Incluye un gran número de péptidos, aminas y aminoácidos. Algunos estimulan al comportamiento alimentario (opioides, neuropéptidos Y, péptidos YY, hormona hipotalámica liberadora de la hormona de crecimiento, noradrenalina, ácido aminobutírico, orexina A y B y galanina. Para poner en evidencia la complejidad de los mecanismos que regulan el hambre y apetito, es preciso añadir los siguientes factores: estímulos olfatorios, gustativos y visuales procedentes de los alimentos, características fisicoquímicas de los alimentos ingeridos, factores psicológicos, culturales y sociales.

La disminución del apetito y su pérdida total se presentan en:

a) Todos los estados infecciosos y febriles.

b) Infecciones digestivas.

- Gastritis atrófica.
- Cáncer de estómago.
- Cáncer de páncreas.
- Enfermedades agudas y crónicas del hígado.

- Cáncer en otros segmentos del aparato digestivo.

c) Intoxicaciones exógenas.

- Alcoholismo.
- Tabaquismo.
- Fármacos: digital, anfetaminas, metronidazol, agentes quimioterapéuticos, etc.

d) Intoxicaciones endógenas.

- Uremia crónica.
- Cetosis diabética.

e) Radioterapia.

f) Enfermedades endocrinas.

- Insuficiencia hipofisario.
- Insuficiencia tiroidea.
- Insuficiencia suprarrenal.

e) Trastornos psíquicos.

- Anorexia nerviosa.
- Depresión.

g) Enfermedades neoplásicas

Es particularmente interesante el síndrome psicológico denominado bulimia nerviosa por su frecuencia creciente en mujeres clase media y alta y escolaridad elevada.

El aumento del ***apetito*** o ***bulimia, hiperorexia, hiperfagía o polifagía*** se presentan en los siguientes casos:

a) Trastornos digestivos.

- Úlcera péptica.
- Parásitos intestinales.

b) Trastornos endocrinos y metabólicos.

- Diabetes mellitus, sobre todo en sus fases precoces.

- Hipoglucemia.
- Obesidad.
- Hipertiroidismo.
- Acromegalia.
- Uso de esteroides, insulina, hipoglucemiantes por vía oral y ciproheptadina.

3.3.3) Sudoración anormal

Las glándulas sudoríparas humanas son de dos tipos: apocrinas y ecrinas.

Las ***glándulas apocrinas*** se localizan principalmente en la región axilar y anogenital.

Las ***glándulas ecrinas*** actúan con la regulación de la temperatura corporal, además, responden principalmente a estímulos parasimpáticos mediados por acetilcolina, y son inhibidas por los alcaloides de la belladona; la magnitud de la sudoración fluctúa en función de la elevación de la temperatura de la piel o de la sangre circulante. La sudoración es componente importante del sistema de termorregulación.

El aumento de la sudoración se puede ver en los siguientes casos:

- ***Estados febriles:*** El fenómeno de la sudoración en el momento de la defervescencia es común en muchos padecimientos febriles como paludismo, fiebre recurrente y fiebres de los procesos piogénicos. Hay infecciones en las que el sudor es particularmente intenso y continuo, por lo que alcanza un cierto valor de diagnóstico: reumatismo cardioarticular agudo, fiebre de malta, tuberculosis, brucelosis, abscesos pulmonares y endocarditis bacteriana.
- ***Linfomas:*** Es característica de la enfermedad de Hodking.
- ***Enfermedades del sistema nervioso:*** Hay hiperhidrosis en casos de lesiones de los centros hipotalámicos de la termorregulación y en enfermedades del sistema nervioso simpático. De ahí que se observen algunos casos de tabes, siringomielia, tumores medulares, lesiones del simpático cervical y torácico.
- ***Enfermedades endocrinas:*** Existe hiperhidrosis en el hipertiroidismo, en el climaterio y en la hipoglucemia. En el primer caso es continua, mientras en los otros sobreviene con accesos con bochorno, y con otros síntomas de hipoglucemia en el último caso.
- ***Enfermedades de debilidad***: Tiene carácter típico de la debilidad en general es la transpiración, que va desde moderada hasta copiosa.

- ***Trastornos circulatorios***: El sudor frío es muy típico de la insuficiencia circulatoria aguda, angina de pecho, infarto del miocardio, trombosis mesentérica y otros cuadros de hipertensión grave.

- ***Ansiedad***: Es bien conocida la hiperhidrosis palmar que se presenta durante estados de ansiedad.

- ***Medicación antidepresiva***: Los antidepresivos tricíclicos y los inhibidores selectivos de la recaptura de serotonina pueden ocasionar diaforesis acentuada.

- ***Síndrome de abstinencia de sedantes y opioides***: Sus manifestaciones más frecuentes son ansiedad, intranquilidad motora, irritabilidad, lagrimeo, sudoración, dilatación pupilar, anorexia, náuseas, vomito, diarrea, dolor abdominal, dolores musculoesqueléticos, temblor e insomnio.

- ***Hiperhidrosis gustativa***: Consiste en sudoración de la extremidad cefálica (cuero cabelludo, frente, cara y cuello) se presenta cuando el paciente acaba de ingerir alimentos es un fenómeno patológico que se observa en pacientes diabéticos con neuropatía autónoma avanzada o en sujetos con antecedentes de patología de la glándula parótira, cáncer de cuello y secuelas de herpes zóster.

3.3.4) Escalofrío

Es una sensación de frío que recorren la espalda y obliga a una contracción brusca, todos los músculos del cuerpo se contraen en repetidos espasmos, el cuerpos se encoge, los miembros se repliegan sobre el tronco, los dientes entrechocan, la piel palidece y las pulsaciones se aceleran.

El escalofrío se presenta en las siguientes condiciones:

- ***Infección de comienzo brusco:*** El escalofrío anuncia la neumonía típica, viruela, erisipela, tifus recurrente y paludismo.

- ***En presencia de un foco infeccioso con invasión en la sangre por los gérmenes:*** Septicemias, pielitis, cistitis, colecistitis, colangitis, flebitis y abscesos.

- ***Exposición al frío:*** Hay personas con sensibilidad especial a la hipotermia, que se extrémese al menor deceso de temperatura o la menor corriente de aire. Esta sensibilidad ocurre con la edad.

- ***Estados emotivos:*** En las emociones agradables pueden haber escalofríos leves y en los momentos de terror extremo, alcanza grados extremos.

- ***Administración intermitente de antipiréticos:*** En la administración de aspirina y otros antipiréticos puede causar una depresión de la temperatura.

3.3.5) Fiebre

Como otras funciones biológicas, la temperatura corporal es baja (36° C o menos en la madrugada y 37.4° C o más por la tarde) dentro de esos límites algo elásticos, constituye una constante celosamente guardada por mecanismos homeostáticos que mantiene un equilibrio dinámico entre los mecanismos que generan calor y los que lo disipan.

Entre los primeros destaca el hígado (gracias a sus funciones metabólicas) y el corazón, a los que se añade el sistema musculoesqueléticos cuando entra en actividad.
Los segundos consisten en la disipación de calor a través de la piel y, en grado mucho menor, de los pulmones. El centro regulador, llamado ***centro de control térmico*** se localiza en el núcleo preóptico del hipotálamo anterior y logra su objetivo homeostático estimulando el sistema nervioso autónomo para que se genere vasodilatación cutánea y escalofríos, según la temperatura corporal central tiende a subir o bajar, respectivamente.

La elevación de la temperatura corporal se presenta dos síndromes diferentes de ***hipertermia y fiebre***.

La hipertermia se puede presentar cuando la producción de calor está aumentada por el ejercicio físico, tormenta hipertiroidea, descarga de catecolaminas procedentes de un Feocromocitoma o acción de anestésicos. También se presentan cuando hay interferencia de calor como insolación, vendajes oclusivos, fármacos que inhiben la sudoración y deshidratación. La hipertermia puede deberse a estados patológicos del centro hipotalámico, como infecciones, tumores, trastornos vasculares, traumatismo o efectos tóxicos de fármacos.

El síndrome febril se debe a pirógenos endógeno, sustancias que sólo recientemente se han identificado la interleucina-1 y el factor necrosante tumoral llamado caquectina. Aun no se sabe si la fiebre es útil para los humanos en su defensa antiinfecciosa, pero evidente puede ser nociva en los niños puede causar convulsiones; en los adultos altera la sensibilidad y llega a causar delirio; y en los ancianos o personas con patologías cardiovasculares o pulmonares puede precipitar la producción de arritmias, hipotensión arterial, isquemia e insuficiencia cardiaca congestiva, ya que grado centígrado de alza térmica determina un aumento de 15% en el consumo de oxígeno.

Infecciones en las que el diagnóstico se hace por manifestaciones clínicas distintas de la fiebre.

a) Infecciones de sintomatología principalmente digestiva.

- Enteritis por gérmenes patógenos.
- Hepatitis aguda por virus.
- Amibiasis hepática.
- Colecistitis, colangitis.

- Abscesos intraabdominal.

b) ***Infecciones de sintomatología preferentemente respiratoria.***

- Neumonía y broncomonía.
- Difteria.
- Tuberculosis pulmonar.
- Micosis respiratorias.
- Infecciones respiratorias virales.

c) ***Infecciones de sintomatología preferentemente linfática.***

- Mononucleosis infecciosa.
- Linfadenitis estreptocócico y estafilocócica.
- Peste bubónica.
- Tularemia.
- Linfogranuloma venéreo.
- Enfermedad por rasguño de gato.

d) ***Infecciones de sintomatología principalmente nerviosa.***

- Meningitis cerebroespinal.
- Encefalitis.
- Poliomielitis.
- Rabia.
- Tétanos.

e) ***Infecciones de sintomatología principalmente exantemático o dérmica.***

- Fiebres eruptivas.
- Tifo exantemático.
- Fiebre punteada de las montañas Rocosas.
- Dengue.
- Erisipela.

- Pústula maligna o ántrax.
- Herpes zóster.
- Actinomicosis.

f) ***Infecciones de sintomatología principalmente articular.***

- Reumatismo poliarticular agudo.
- Artritis aguda bacteriana.
- Artritis micóticas, sifilíticas, virales, tuberculosis.

Infecciones en las que el diagnóstico se hace a partir de la fiebre. Se dividen en varios subgrupos:

a) Fiebres fugaces.

- Infecciones fugaces de ciclo conocido: gripa, resfriado común.
- Formas fugaces de infecciones raves: neumonía, tifoidea, paratifoidea, etc.
- Fiebres fugaces indiagnosticables.

b) Fiebres en accesos. La fiebre se presenta en forma de accesos, con escalofríos intensos, seguido de hipertermia y diaforesis ulterior.

- Paludismo.
- Fiebre recurrente.
- Fiebre de las trincheras.
- Focos sépticos.

c) Fiebres altas y prolongadas.

- Fiebre tifoidea.
- Fiebres paratifoideas.
- Septicemias.
- Tuberculosis.
- Brucelosis.
- Kala-azar.
- Psitacosis.

- Tularemia.
- Infecciones profundas por hongos.
- Infecciones localizadas (colecistitis, colangitis, abscesos renales y perinefríticos).
- Abscesos hepático amebiano.

d) Hipertermias prolongadas de tipo ondulatorio.

- Fiebre de malta.
- Linfoma de Hodking.

e) Infecciones con febrícula.

- Tuberculosis.
- Focos sépticos.
- Infecciones generales de forma febricular.
- Febrículas no infecciosas.

f) Fiebres no infecciosas.

- Neoplasias malignas. En órganos como riñón, pulmón, páncreas e hígado.
- Enfermedades del tejido conjuntivo. Fiebre reumática, lupus eritematoso diseminado, artritis reumatoide y polimialgía reumática.
- Diversas. Embolias pulmonares múltiples, estados hemolíticos y fiebre mediterránea familiar.
- Hipertermias falsas. Hipertermia habitual, fiebre ficticia y fiebre facticia.

3.3.6) Pruebas de laboratorio

Las pruebas de laboratorio son muy importantes para un buen diagnóstico, entre las diferentes pruebas de laboratorio encontramos.

a) ***Cultivos de sangre***, médula ósea y otros fluidos corporales.

b) ***Enzimas séricas***, particularmente las que reflejan daño hepatocelular.

c) ***Frotis sanguíneos*** son para buscar cuentas y morfologías anormales y parásitos.

d) ***Examen de la medula ósea,*** buscan células neoplásicas, granulomas, glóbulos blancos y rojos anormales.

e) ***Pruebas inmunológicas***, Antiestreptolísimas, proteínas C reactiva, anticuerpos antinucleares, prueba de fijación de látex y reacciones de aglutinación.

f) **Reacciones "febriles" de aglutinación,** su utilidad se ha exagerado. Las reglas de interpretación correcta son:

- No solicitarlas antes de una semana iniciada la fiebre.
- El título de aglutinación en una sola muestra de sangre tiene poco valor diagnóstico.
- Sólo un incremento del título de aglutinación de 4 o más veces, entre muestras obtenidas en fechas diferentes, es evidencia inequívoca de infección reciente.
- Si no se detectan anticuerpos IgM o IgG el paciente no está infectado y está desarrollando una respuesta inmune.
- Si sólo se detectan anticuerpos IgG y no IgM, el paciente tiene inmunidad para el agente etiológico, pero no necesariamente sufre la infección.
- En algunas personas (especialmente portadoras de anticuerpos adquiridos por infecciones previas o que no fueron vacunadas) ocurren reacciones cruzadas que dificultan la interpretación de resultados.
- Un 70% de las reacciones tífico-paratíficas practicadas con la técnica de aglutinación en placa son falsas positivas. Por ello, sus resultados no son dignos de crédito y es aconsejable confirmarlas y cuantificarlas mediante la técnica de aglutinación en tubo.
- Los resultados y las variaciones en los títulos de aglutinación carecen de valor para vigilar la evolución de una infección.

3.3.7) Radiografías

a) Tórax.

b) Huesos (osteomielitis).

c) Urografía excretora.

d) Aorgrafía abdominal (tumores renales, retroperitonales, hepáticos, pancreáticos e intestinales).

e) Linfangiografía (linfomas abdominales y retroperitoneales).

f) Colangiografía intravenosa.

g) Tomografía axial computarizada.

3.3.8) Ultrasonografías y Resonancia magnética

a) Tórax.

b) Abdomen.

c) Pelvis.

3.3.9) Gammagrafías

a) Hepáticas.

b) Pulmonar.

c) Ósea.

d) Galio radiactivo.

e) Leucocitos marcados (radiactivos).

3.3.10) Biopsia

a) Medula ósea.

b) Hígado (cáncer, linfomas, tuberculosis, brucelosis, sarcoidosis y linfomas).

c) Ganglio linfático (linfomas, cáncer, tuberculosis y micosis).

d) Músculo (dermatomiositis, periarteritis nodosa, sarcoidosis y triquinosis).

e) Pulmón.

f) Riñón.

g) Pleura.

h) Artería temporal (arteritis temporal).

3.3.11) Fiebre de origen oscuro (FOO)

Proceso febril de duración superior a tres semanas, con elevaciones de temperatura de 38 (° C) o más, no diagnosticado a pesar de estudios clínicos y de un número habitualmente adecuado de estudios paraclínicos.

Las causas más frecuentes de FOO son enfermedades raras y exóticas; son las presentaciones raras de las enfermedades comunes como la tuberculosis, endocarditis, micosis, brucelosis, salmonelosis, malaria, toxoplasmosis, infecciones por citomegalovirus o el virus de Epstein-Barr, e infecciones por el virus de inmunodeficiencia humana.

3.3.12) Debilidad o Astenia

Sensación de cansancio, laxitud, falta de energía, languidez o no sentirse bien. El término se aplica también a la disminución de la fuerza muscular requerida o esperada.

La debilidad, tal como ha sido definido, es un síntoma que puede presentarse en una gran diversidad de situaciones clínicas. Las más importantes son las siguientes:

a) ***Exceso de trabajo:*** Existen en la sociedad, particularmente en los grandes centros de población, numerosas personas que sufren las consecuencias físicas y mentales de un trabajo excesivo de cuya magnitud no se dan cuenta.

b) Ansiedad y tensión nerviosa clásica: Se asocia frecuentemente de debilidad, síntoma que, en estos casos, se asocia al nerviosismo, irritabilidad, ansiedad, depresión, insomnio, dolores de cabeza, dificultad de concentración mental y trastornos mentales.

c) Depresión: Este gran síndrome psiquiátrico, de enorme frecuencia, de muchas facetas y diversas causas, suele incluir entre sus síntomas cardinales, la debilidad y el cansancio, que tienen la peculiaridad de ser más acentuados en las mañanas qua al final del día.

d) Aburrimiento: Hay muchas personas en la sociedad contemporánea que carecen de metas e ideales y cuentan con mucho tiempo libre. Pertenecen a este grupo muchas mujeres cuyos hijos, ya crecidos, han abandonado el hogar, y muchos hombres han alcanzado la edad de jubilación.

e) Infección aguda y crónica: Debe sospecharse en todo paciente en quien el síntoma aparece de manera más o menos repentina o cuando se presenta en ausencia de síntomas neuropsiquiátricos. Las enfermedades infecciosas con más frecuencia provocan debilidad y fatiga como la hepatitis aguda y crónica, tuberculosis, brucelosis, endocarditis bacteriana y mononucleosis infecciosa.

f) Enfermedades metabólicas y endocrinas: La astenia es uno de los síntomas principales de la insuficiencia suprarrenal crónica, insuficiencia hipofisaria, hipotiroidismo, algunos casos de hipertiroidismo, diabetes mellitus descontrolada, hipoparatiroidismo, hipogonadismo y síndrome de Cushing.

g) Anemia: Cuando la anemia es de magnitud moderada o intensa produce astenia.

h) Deficiencia nutricional: Esta es una causa importante de debilidad, que por desgracia todavía es muy frecuente en nuestro país.

i) Parasitosis crónica: El paludismo, la uncinariasis y otras parasitosis intestinales pueden causar astenia.

j) Intoxicaciones crónicas: El consumo frecuente de alcohol, barbitúricos y otros medicamentos tranquilizantes, propanol, bloqueadores β adrenérgicos, así como relajantes musculares y otros fármacos, son causa de astenia.

k) Neoplasias malignas: Se presentan en el cáncer de páncreas, estómago, colon, hígado, riñón, pulmón, etc.

l) Síndrome de fatiga crónica: Fatiga persistente, carente de explicación, no causada por actividad física actual ni aliviada por el descenso. Cuatro o más de los siguientes síntomas siguientes, que se hayan presentado de manera persistente durante 6 meses consecutivos del padecimiento y no lo hayan precedido.

- Dolor faríngeo.
- Ganglios linfáticos cervicales o axilares dolorosas.
- Dolor muscular.
- Poliartralgias sin signos inflamatorios.
- Sueño que no es reparador.
- Cefalalgias de carácter o intensidad.
- Malestar que no es consecutivo al ejercicio, con duración de 24 o más.

El síndrome se ha sido atribuido a causas de infección, inmunitarias y neuropsicológicas, pero hasta la fecha no se ha logrado comprobar ninguna de las numerosas hipótesis propuestas.

3.3.13) Agudeza visual

Es todo síntoma relacionado con la función visual, lo que se busca es la disminución visual o ambliopía. La ***amaurosis*** es la pérdida total de la vista. ***Escotoma*** es un área ciega del campo visual, ***Hemianopsia*** es ceguera del medio campo visual.

La disminución de la agudeza visual puede deberse a anormalidades de los medios transparentes del ojo o a las lesiones de la retina, del nervio óptico o de las partes del cerebro con que se conectan.

Los rayos luminosos que entran en el ojo son enfocados hacia la capa externa de la retina, en donde se encuentran los bastoncillos y los conos. Los conos y los bastoncillos contienen el pigmento visual. Los bastoncillos tienen mayor sensibilidad a la luz, y los conos mayor capacidad de discriminación.

Los pigmentos son derivados de la vitamina A y, al ser excitados por los rayos luminosos, sufren modificaciones en su estructura fisicoquímica; que dan lugar a la descarga de impulsos nerviosos aferentes. El color es percibido por los conos, de los cuales hay tres tipos que se distinguen uno del otro por contener pigmentos responsables de la percepción de uno de los tres colores (azul, verde o rojo). Los impulsos procedentes de los fotorreceptores son transmitidos por neuronas secundarias, las células bipolares, a la capa de células ganglionares más profundas. Los axones de estas células conducen los impulsos a los nervios ópticos para seguirse por el quiasma, pasar allí a la cintilla óptica y terminar en el cuerpo geniculado externo. De ahí parten los axones que constituyen las radiaciones ópticas para terminar en el lóbulo occipital, que es centro de la visión.

a) La pérdida o disminución súbita y unilateral puede deberse a:

- Obstrucción de la vena central de la retina.
- Obstrucción de la artería central de la retina.
- Hemorragia del vítreo o la retina.
- Neuritis óptica, papilitis o neuritis retrobulbar.
- Ambliopía tóxica.

b) En la oftalmitis de origen embólico:

- Trombosis de la artería carótida interna.
- Traumatismo craneano con hemorragia en el conducto óptico.
- Amaurosis urémica.

c) Pérdida o disminución gradual y unilateral puede deberse a:

- Errores de refacción: miopía, hiperopía y astigmatismo.
- Catarata.
- Keratoconus.
- Dislocación o subluxión del cristalino.
- Diabetes mellitus.
- Lesiones orbitarias.

- Lesiones de la córnea: queratitis, distrofia, alergia y edema.
- Lesiones del tracto uveal: iritis, uveítis, coroiditis, degeneración muscular y tumores.
- Glaucoma.

d) La pérdida o disminución súbita y bilateral pueden deberse a:

- Neuritis óptica.
- Amaurosis urémica.
- Traumatismo craneano.
- Histeria.
- Migraña.
- Lesiones del humor vítreo: apacificación y hemorragias.
- Lesiones retinianas: vasculares, degenerativas maculares, tóxicas, inflamatorias, tumores y desprendimiento.
- Lesiones del nervio óptico: lesiones quiasmáticas. neuritis óptica, neuritis retrobulbar, papiledema, atrofia del nervio óptico, tumor o comprensión tumoral.

e) La pérdida visual puede ser transitoria y fluctuante. Las causas son las siguientes:

- Xeroftalmía, es decir secreción lagrimal disminuida.
- Hiperglucemia repentina.
- Presbiopía.
- Amaurosis fugaz. El paciente experimenta la sensación de una cortina o nube que momentáneamente obstaculiza la visión.

3.3.14) Hipoacusia

Es la disminución de la agudeza auditiva. Puede ser relativa o absoluta, unilateral o bilateral.

La función auditiva se realiza en dos fases: La primera es la de la conducción, consiste en el paso de las vibraciones sonoras desde el medio aéreo al medio líquido del oído interno, con la membrana del tímpano y los huesecillos del oído como importante eslabón intermedio. Las alteraciones de los elementos de está fase disminuye la intensidad de los sonidos con mínima distorsión de sus otras cualidades físicas.

La segunda fase, o neurosensorial o de percepción, inicia en la cóclea, dónde se encuentran las células del órgano de Corti que traducen la energía vibratoria a potenciales eléctricos y en donde tiene lugar la codificación de la intensidad y el tono de los sonidos. La información es transmitida a lo largo del nervio auditivo y el tallo encefálico hasta la corteza auditiva, en la que se realiza de decodificación y la compresión. La lesión de algún elemento de la segunda fase no sólo causa reducción en la intensidad de los sonidos, sino la distorsión de los mismos.

Es conveniente clasificar las hipoacusias en aquellas que se deben a defectos de conducción y las que se producen por defectos de percepción.

a) Las hipoacusias de conducción más importantes son: por obstrucción del conducto auditivo externo (tapón de cerumen, cuerpos extraños, forunculosis y tumores), por alteraciones de la membrana del tímpano (perforación e infección), por alteraciones de los huesecillos del oído (fibrosis, atrofia y necrosis), otras alteraciones.

b) La hipoacusia de percepción se clasifica en:

- Congénita: endógena (hereditaria), exógena (lesiones intrauterinas o perinatales como rubiola, anoxia e incompatibilidad de factor Rh).
- Infecciosa: sarampión, influenza, neumonía, sifilitis, otros virus.
- Medicamentosa: estreptomicina, neomecina, kanamicina y gentamicina.
- Degenerativas: Insuficiencia vascular (envejecimiento) y alteraciones bioquímicas.
- Hereditaria.
- Traumática: Lesiones del hueso temporal o del nervio acústico y lesiones producidas por ruidos fuertes.
- Tumoral: Del hueso temporal, del nervio acústico y del ángulo pontocerebeloso.
- Por hidropesía endolinfática: enfermedad del Méniere.
- Por enfermedades vasculares: insuficiencia vascular aguda y vasculitis.
- Por lesiones neurológicas: inflamación del nervio acústico, esclerosis múltiple, tumores, insuficiencia vascular y otras neuropatías.
- Psicogénicas: Histeria.

3.3.15) Acúfenos

Se trata de la percepción de sonidos en ausencia de estímulos auditivos externos. Los acufenos también reciben el nombre de tinnitus.

Los acufenos pueden resultar de diversos procesos que afectan el epitelio auditivo, membrana basilar, endolinfa o la vía acústica.

Como ya se menciono las alteraciones que pueden ocasionar acufenos son las siguientes:

a) Vasculares.

- Soplo cervical venoso.
- Soplos carotideos o cardiacos.
- Malformaciones arteriovenosas.
- Circulación hiperdinámica.

b) Auditivas.

- Oído externo: cerumen impactado, otitis externa, perforación del tímpano, miringitis y cuerpos extraños.
- Oído medio: otitis media, otosclerosis, ruptura osicular traumática, barotrauma, exposición a presiones excepcionalmente elevadas (como el buceo) o bajas (como aeroplanos sin cabina), tumores, tics neuromusculares de la cadena osicular y obstrucciones en la trompa de Eustaquio.

c) Neurológicas.

- Cóclea: otosclerosis, enfermedad del Méniere, laberintitis, contusión coclear, presbiacusia y exposición al ruido.
- Vías centrales: neuroma acústico, tumores del ángulo pontocerebeloso, confusión, tumores corticales y trastornos convulsivos.
- Fármacos: Alcohol, café, té, salicilatos, ácido acetilsalicílico, antibióticos aminoglucósidos, quinina y furasimida.

d) Psicogénicos.

3.3.16) Otorrea y otorragía

Otorrea *es la salida de flujo no hemorrágico por el meato auditivo externo;* ***otorragía*** es la salida de sangre por el mismo lugar.

Cualquier proceso inflamatorio del conducto auditivo externo puede ocasionar salida de flujo seroso o purulento. Así mismo, las infecciones del oído medio pueden provocar otorrea u otorragía cuando se perfora la membrana timpánica.

Las causas más importantes de otorrea y otorragía son:

a) Salida de líquido cefalorraquídeo: se debe a fractura de la base del cráneo.

b) Secreción serosa o seropurulenta: infecciones del conducto auditivo externo (furúnculo, infecciones generales como las de origen gripal o los producidos por estreptococos.

c) Secreción purulenta: infecciones del conducto auditivo externo y otitis media tuberculosa.

3.3.17) Otalgia

Es el dolor de oído y puede ser producida por las siguientes causas:

a) Lesiones del oído externo:

- Dolor del pabellón de la oreja, generalmente producido por traumatismo.
- Lesiones del conducto auditivo externo: eczema, inflamaciones a veces úlceras en el curso de diversas infecciones generales y herpes zóster.

b) Lesiones del oído medio:

- La otitis media ocasiona dolor intenso, hipoacusia, fiebre y mareo ligero, suele ocurrir después de infecciones respiratorias altas.
- Mastoiditis: complicación de la otis media.
- Miringitis: Inflamación aguda de la membrana del tímpano causada por virus, bacterias y micoplasmas.
- Tumores del oído medio.

c) Lesiones de órganos ajenos al sistema auditivos: gran número de lesiones de la boca, faringe y cuello pueden producir dolor auricular referido, todos los procesos laríngeos, inflamatorios o tumorales, neuralgias del facial y procesos inflamatorios de la glándula tiroides.

3.3.18) Vértigo

Es la sensación de desorientación en el espacio asociado a sensación de movimiento. El vértigo suele acompañarse de otros síntomas, como palidez, sudoración y náuseas.

El vértigo se debe a disfunción del sistema vestibular. Las causas de vértigo son múltiples, algunos casos son benignos y otros son graves. Los más importantes son:

a) Periféricas.

- Aparato vestibular del oído (síndrome de Méniere, combinación de vértigo con hipoacusia y acufenos.
- Traumatismo (fractura del hueso temporal).
- Trastornos vasculares (obstrucción de la artería auditiva).
- Trastornos oculares.

b) Centrales.

- Vascular: insuficiencia vertebrobasilar, hipotensión ortostática. Estenosis aórtica, bradicardia y arritmia.
- Migraña: puede manifestarse por vértigo paroxístico episódico como equivalente del ataque migrañoso clásico.
- Tumores: tumores del ángulo cerebelopóntico y tumores de la fosa tumoral.
- Convulsiones: epilepsia del lóbulo temporal.
- Esclerosis múltiple: puede empezar con vértigo como síntoma inicial.
- Traumatismo: sacudimiento cervical en latigazo.
- Infecciones: meningitis, encefalitis y neurosifilis.

c) Por drogas.

- Alcohol: barbitúricos, estreptomicina y kanamicina.

d) Metabólicas.

- Hipotiroidismo e hipoglucemia.

3.3.19) Rinorrea

Rinorrea es el flujo nasal. Conviene clasificar la Rinorrea en cuatro grupos.

a) Expulsión nasal de sangre.

b) Expulsión de mucosidad clara.

- En las rinitis o corizas alérgicas, se presenta en forma estacional (fiebre de heno y polinosis) o permanente (rinitis vasomotora).
- En ciertas intoxicaciones, como las de yodo, bromo y arsénico.
- Por la acción de gases o atmósferas irritantes: amoniaco, formol y ácido clorhídrico.

c) Expulsión de mucosidad nasal espesa, amarillenta y mucopurulente.

- En todos los estados catarrales de la mucosa nasal, agudos o crónicas.
- En la difteria nasal.
- En las sinusitis crónicas, ya sean maxilares, frontales o etmoidales.
- En los casos de cuerpos extraños en la nariz.

d) Eliminación nasal de líquido cefalorraquídeo.

- Se presenta en casos de fractura de la base del cráneo y tiene gran valor diagnóstico.

3.3.20) Epistaxis

Epistaxis es la hemorragia de las fosas nasales. La hemorragia puede originarse directamente en la nariz o en estructuras cercanas, como los senos paranasales, nasofaringe y otros tejidos vecinos.

La nariz tiene una rica irrigación, procedentes de las arterias carótidas externa e interna. Desde el punto de vista etiológico, las epistaxis pueden clasificarse en causas locales y causas generales.

a) Epistaxis por causas locales.

- Inflamación: infección aguda y reacciones alérgicas.
- Reacciones parasimpáticas, enfermedad granulomatosa y vasculitis.
- Traumatismo.

- Resequedad excesiva: mucosa atrófica y anomalías anatómicas.
- Tumores.
- Cuerpos extraños.
- Telangiectasias e insuficiencia vascular.

b) Epistaxis por causas generales.

- Hipertensión arterial.
- Enfermedades hemorragíparas: anemia aplásica, leucemia, trombocitopenia y hepatopatías.
- Enfermedades renales crónicas.
- Enfermedad de Rendu-Osler-Weber, también llamada Telangiectasias hemorrágica hereditaria: anomalía vascular caracterizada por la presencia de telangiectasis en la piel y membranas mucosas. Estas lesiones están constituidos por vasos sanguíneos pequeños, dilatados que tienden a sangrar espontáneamente o por efecto de traumatismos mínimos.

3.3.21) Alteraciones del gusto

Se habla de ***disgusía*** cuando se trata de la identificación anormal de sabores; ***hipogeusia*** cuando existe disminución en la percepción del sabor; ***ageusia*** o ***ageustia*** cuando falta el sentido del mismo; ***hipergeusia*** cuando se trata de un estado exagerado del sabor; ***cacogensia*** cuando existe perversión del sentido por identificación en forma equivocada y desagradable de un sabor determinado.
Las papilas gustativas son el órgano especializado en percibir el sabor. Son de diversos tipos: fungiformes, caliciformes, palatinas y epiglóticas. Las perturbaciones del gusto dependen del trayecto de los nervios o de la lengua misma, alteraciones de saliva, trastornos psíquicos y finalmente alteraciones del olfato.

a) Lesiones del sistema nervioso. Cuando afectan al gusto se traduce por su pérdida. Las principales causas nerviosas de la ageusia son:

- Lesiones de la cuerda del tímpano: las cuales se acompañan generalmente de parálisis facial periférica. La ageusia afecta los dos tercios anteriores de la lengua en el lado de la lesión, la causa más frecuente es una lesión del oído y trompa de Eustaquio.
- Lesión del nervio lingual: la ageusia afecta también los dos tercios anteriores de la lengua en el mismo lado; casi siempre la lesión lingual es parte de una lesión del trigémino y entonces se añaden trastornos de la sensibilidad de la cara y, si está afectada la raíz motora; pueden existir lesiones aisladas de la naturaleza tumoral en el nervio lingual.

- Lesión del nervio glosofaríngeo: causa ageusia en la parte posterior del dorso lingual del lado afectado, puede haber a la vez paresía del paladar y la faringe y se debe a causas tumorales o traumáticas.

- Lesiones del sistema nervioso central: parálisis bulbar, tumores cerebrales, cuando son de localización occipital puede haber ageusia o disgusía. En los tumores de la circunvolución del hipocampo se producen las llamadas crisis uniformes caracterizadas por sensación gustativa y olfativa desagradable, y estado crepuscular o pérdida rápida de la conciencia.

b) Neurosis y psicosis: la ageusia, hipergeusia o disgusía se observan en el histerismo y en diversas psicosis.

c) Lesiones nasales: la sinusitis crónicas y agudas, la rinitis atrófica y la adenoiditis se pueden acompañar de ageusia o disgusía.

d) Lesiones de la boca: puede haber disgeusia o ageusia por estomatitis, glositis, lesiones dentarias, síndrome Sjögrey, radiación, dentadura artificial y tumores.

e) Ciertos estados generales: como embarazo, pelagra e insuficiencia suprarrenal, causan disgeusia.

f) Algunas comidas o bebidas: como ajo, cebolla y vino.

g) Intoxicación por medicamentos: anfetaminas, anestésicos locales, clofibrato, griseofulvina, insulina, carbonato de litio, fenidiona, fenitoina, oxifedrina, metimazol, metiltiouracilo, metronidazol, biguanidas, ácido quenodesoxicólico, mercurio, arsénico, bromuros, yoduros, bismuto y oro.

3.4) Tipos de exploración complementaria

3.4.1) Alimentación

Uno de los problemas más frecuentes y graves a que se encuentra el médico en nuestro país está constituido por la alimentación insuficiente y sus trágicas consecuencias, en una proporción importante de personas de ambos sexos y de todas las edades, pero, especialmente en los niños.

Los principales componentes de los alimentos son carbohidratos, grasa y proteínas, suministran lo necesario para satisfacer las necesidades energéticas del organismo, para la síntesis de los tejidos, para la realización de las funciones excretoras y para el mantenimiento del equilibrio térmico. En México, aproximadamente el 10% de las colorías derivan de proteínas, 50% de carbohidratos y el 40% restantes de grasa. El organismo humano tiene una notable capacidad para adaptarse a proporciones diversas de los componentes alimenticios.

Muchos habitantes de nuestro país parecen encontrarse en buenas condiciones de salud a pesar de que su dieta no contiene más de 30 o 40 g de proteína y cantidades igualmente pequeñas de grasa. Sin embargo, cuando a estas cifras mínimas de proteínas se añaden padecimientos infecciosos y parasitarios, las consecuencias para el desarrollo físico e intelectual, así como para la predisposición a sufrir estados patológicos, son muy importantes.

Por lo que respecta en calorías, se considera que el adulto joven de sexo masculino requiere aproximadamente 2,800 y el sexo femenino 2000. Durante el embarazo la mujer requiere 200 calorías diarias extras y 1000 calorías diarias durante la lactancia.
Los carbohidratos no son esenciales en la dieta humana, pero el organismo los necesita como fuente de energía para las neuronas y para otros fines especializados. La dieta rica en sucrosa, particularmente en forma de azúcar y caramelos, favorece el desarrollo de caries dentales y también la elevación de la concentración de triglicéridos en el suero sanguíneo.

3.4.2) Sodio y cloro

El cloruro de sodio es ingerido diariamente en cantidades que fluctúan entre 7 y 15 g, cantidad que excede en gran medida los requerimientos del organismo, Debido a que los mecanismo de conservación del sodio son extraordinariamente eficientes, bastaría una ingestión de sodio de 50 a 100 mg al día para llenar las necesidades de un individuo.

Las necesidades de cloro y sodio aumentan si las condiciones climatológicas determinan una pérdida excesiva por transpiración y sudor o si existen condiciones patológicas que aumentan las pérdidas de estas sustancias por el tubo digestivo, riñón o glándulas sudoríparas. La ingestión excesiva de cloruro de sodio puede ser factor etiológico en el desarrollo de la hipertensión arterial.

3.4.3) Ocupación

La ocupación del paciente constituye uno de sus más importantes antecedentes personales, y su indagación no ha de prescindir en toda historia clínica. La mayor parte de las enfermedades ocupacionales no son específicas, sino que pueden ser causadas por factores no ocupacionales.

3.4.4) Tabaquismo

El tabaquismo es el hábito de consumir tabaco, la nicotina es el alcaloide obtenido del tabaco; su nombre químico es β-piridil-k-n-metilpirrolina. Los efectos del humo del tabaco y los de la contaminación atmosférica se potencian, dando lugar a un mayor daño a las estructuras respiratorias.

3.4.5) Alcoholismo e ingestión de bebidas alcohólicas

Definición de la Organización de la salud. El alcoholismo es un trastorno de conducta manifestado por la ingestión excesiva de bebidas alcohólicas y por dependencia del alcohol, de magnitud tal que muestra pródromos o manifestaciones francas de alteración mental, del comportamiento social y de la productividad económica.

Las manifestaciones clínicas del alcoholismo son tantas que nos limitaremos a enumerarlas:

a) Efectos sobre órganos digestivos.

- Náuseas y vómitos digestivos.
- Trastornos digestivos como distensión abdominal, malestar epigástrico, eructos, síntomas ulceriformes y hematemesis.
- Gastritis superficial.
- Aumento de la frecuencia de la úlcera péptica.
- Síndrome de Mallory-Weiss.
- Esteatosis hepática.
- Hepatitis alcohólica y cirrosis alcohólica.
- Pancreatitis recidivante.

b) Efectos sobre el sistema endocrino.

- Atrofia testicular.
- Ginecomastia.

c) Efectos sobre el sistema nervioso.

- Intoxicación alcohólica.
- Síndrome de abstinencia.
- Síndrome de Wernicke-korsakoff.
- Polineuropatías.
- Neuropatía retrobulbar.
- Pelagra.
- Degeneración cerebelosa.

- Enfermedad de Marchiafava-Bignani.
- Atrofia cerebral.
- Coma hepáticos.
- Degeneración crónica hepatocerebral.

d) Otros efectos.

- Miopía alcohólica.
- Cardiomiopatía alcohólica.

3.4.6) Fármacodependencia

Es el estado psíquico, y en algunas ocasiones también físicos, caracterizado por la compulsión por tomar un fármaco en forma continua o periódica con el fin de experimentar sus efectos y algunas veces para evitar el malestar producido al privarse de tomarlo. Se distinguen las siguientes tipos de farmacodependencia:

a) Tipo morfínico. Se caracteriza por:

- Dependencia psíquica muy intensa.
- Dependencia física.
- Síndrome de abstinencia.

b) Tipo alcohol-barbitúrico. Se caracteriza por:

- Dependencia psíquica que puede conducir al abuso periódico y continúo.
- Síndrome de abstinencia.

c) Tipo cocaínico. Se caracteriza por.

- Dependencia psíquica variable.
- No hay dependencia física.
- No hay síndrome de abstinencia característico.

d) Tipo cannábico. Se caracteriza por:

- Dependencia psíquica variable.
- No hay dependencia física.
- No hay síndrome de abstinencia.

- No hay tolerancia.

e) Tipo alucinógeno. Se caracteriza por:

- Dependencia psíquica generalmente reducida.
- No hay dependencia física.
- No hay síndrome de abstinencia característico.

3.5) Errores en el diagnóstico

Las principales causas de errores diagnosticas se presentan a continuación:

- Falta de especialización del médico.
- Descuido del personal médico al realizar pruebas de laboratorio.
- Falta de sinceridad del paciente al contestar las preguntas realizadas por el médico.
- Falta de equipo médico.

Algoritmo para diagnosticar Vértigo

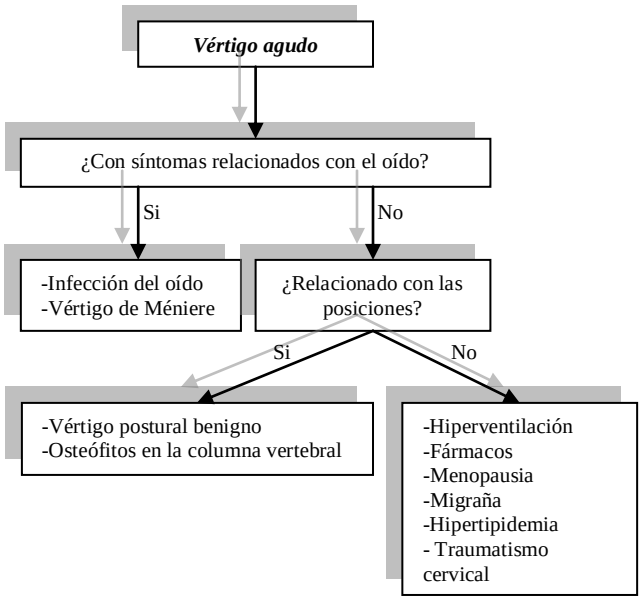


Figura 3.3 Algoritmo para Diagnosticar vértigo Agudo

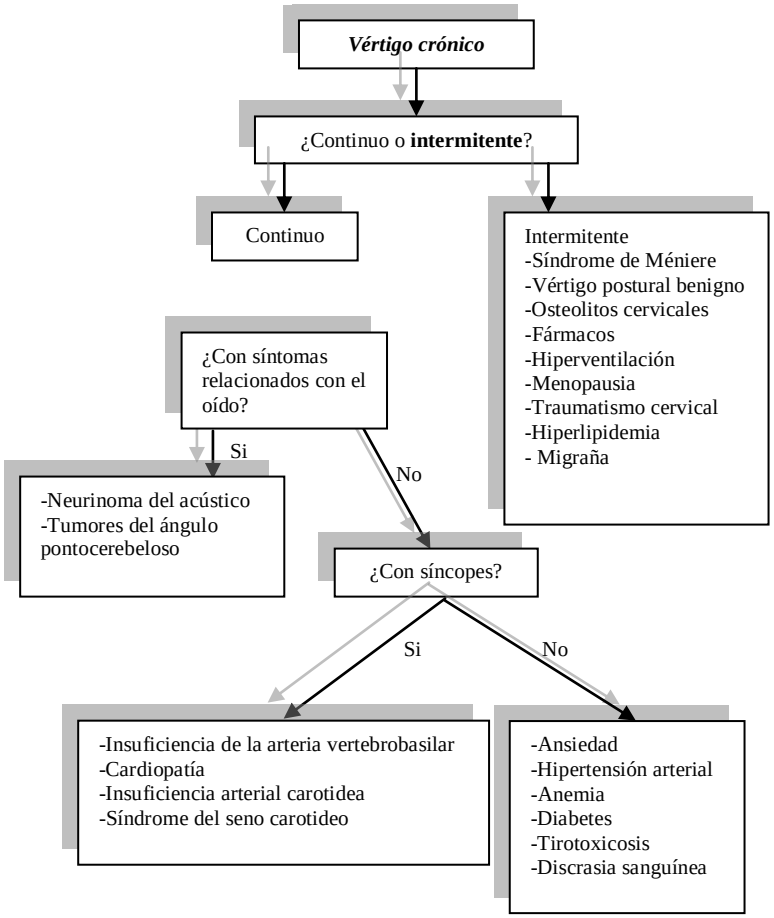


Figura 3.4 Algoritmo para diagnosticar vértigo crónico

Algoritmo para diagnosticar Hipertensión

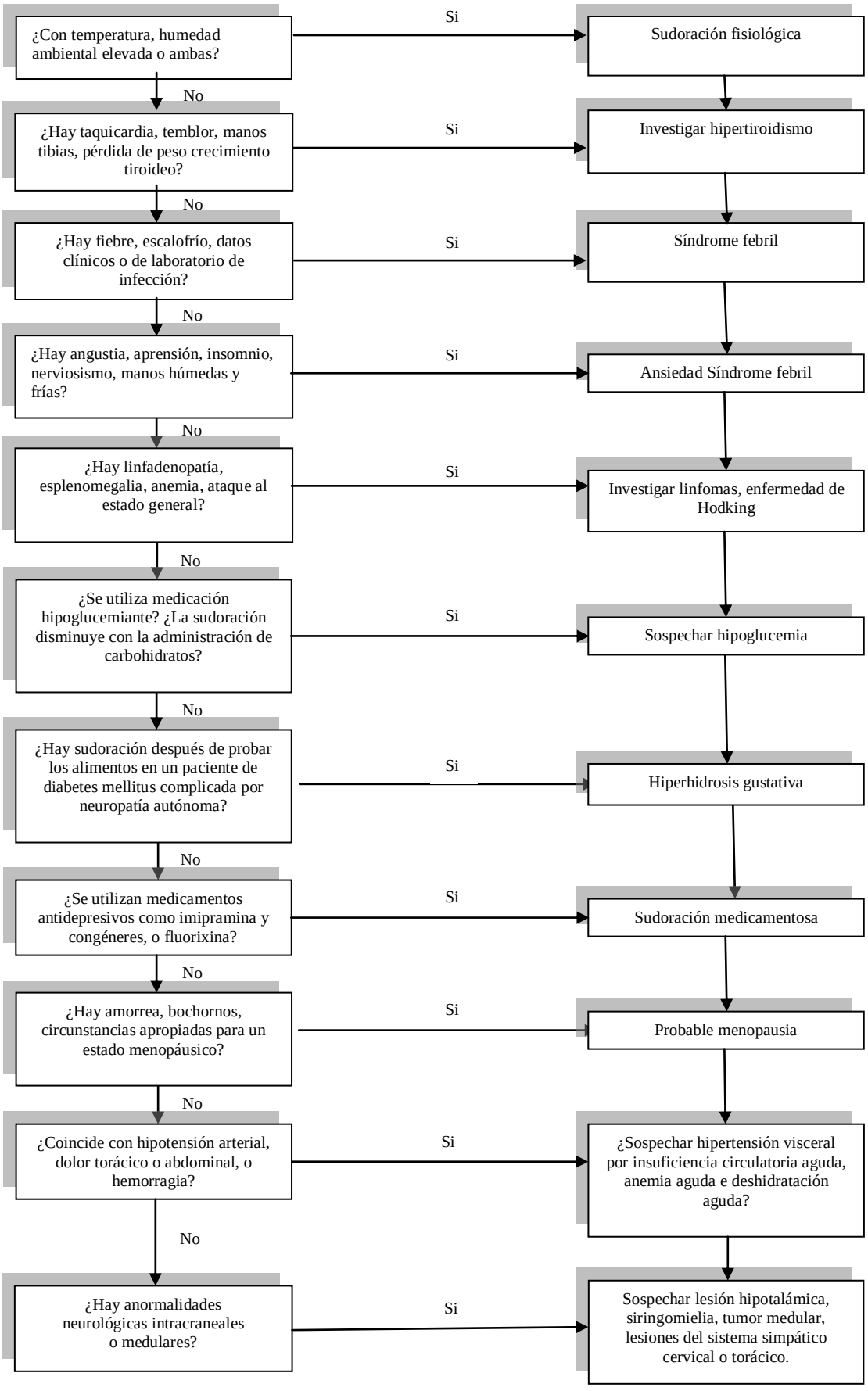


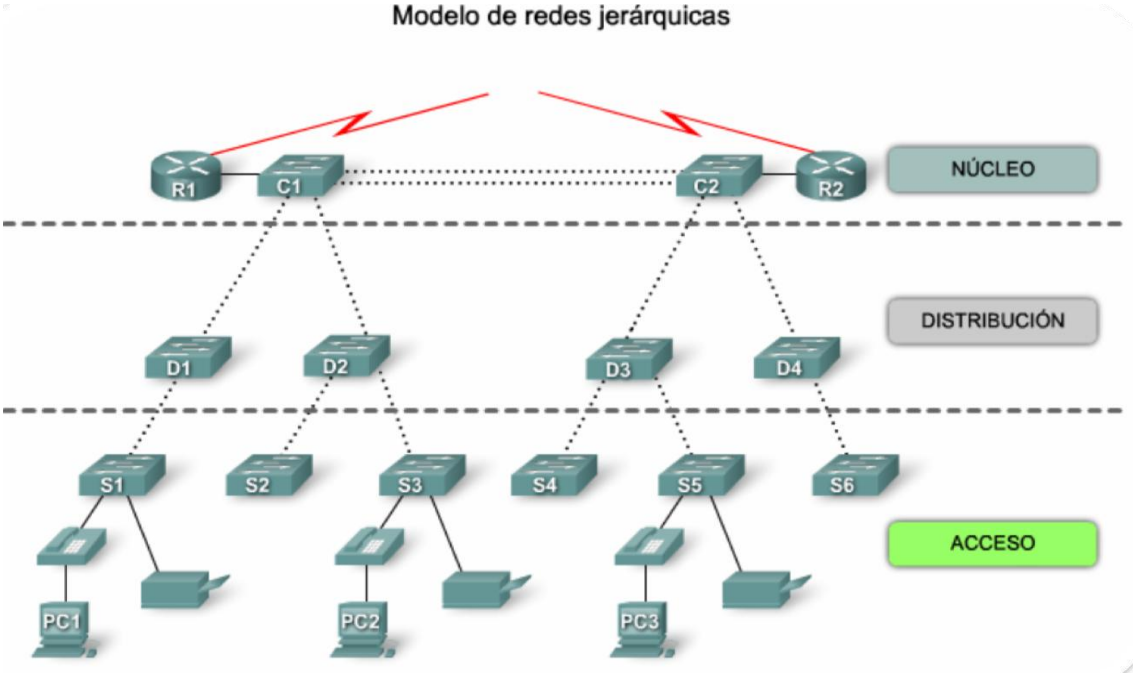
Figura 3.5 Algoritmo para diagnosticar hipertensión

4) Diseño de la red Wi-Fi

En este capitulo diseñaremos la red Wi-Fi utilizando el programa Cisco Packet Trace con las características descritas en este capitulo y realizaré el costo del proyecto para una estimación aproximada.

El diseño de la red Wi-Fi debe cumplir el modelo de redes jerárquicas que está compuesta por la capa de acceso, capa de distribución y capa núcleo.

- ***Capa de acceso:*** Interactúa con dispositivos finales, como computadoras personales, laptops, impresoras y teléfonos IP, para proporcionar acceso al resto de la red.
- ***Capa de distribución:*** Agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final.
- ***Capa núcleo:*** Interconecta los dispositivos de la capa de distribución con el ***backbone*** *(*principales conexiones troncales de internet).



4.1 Modelo de red jerárquica

Los beneficios que se tendrá al diseñar una red con el modelo de redes jerárquicas son:

- ***Escalabilidad***
- ***Redundancia***
- ***Seguridad***
- ***Facilidad de administración***
- ***Facilidad de mantenimiento***

4.1) Diámetro de una red

El diámetro de una red es el número de switches en la ruta de tráfico entre dos puntos finales.

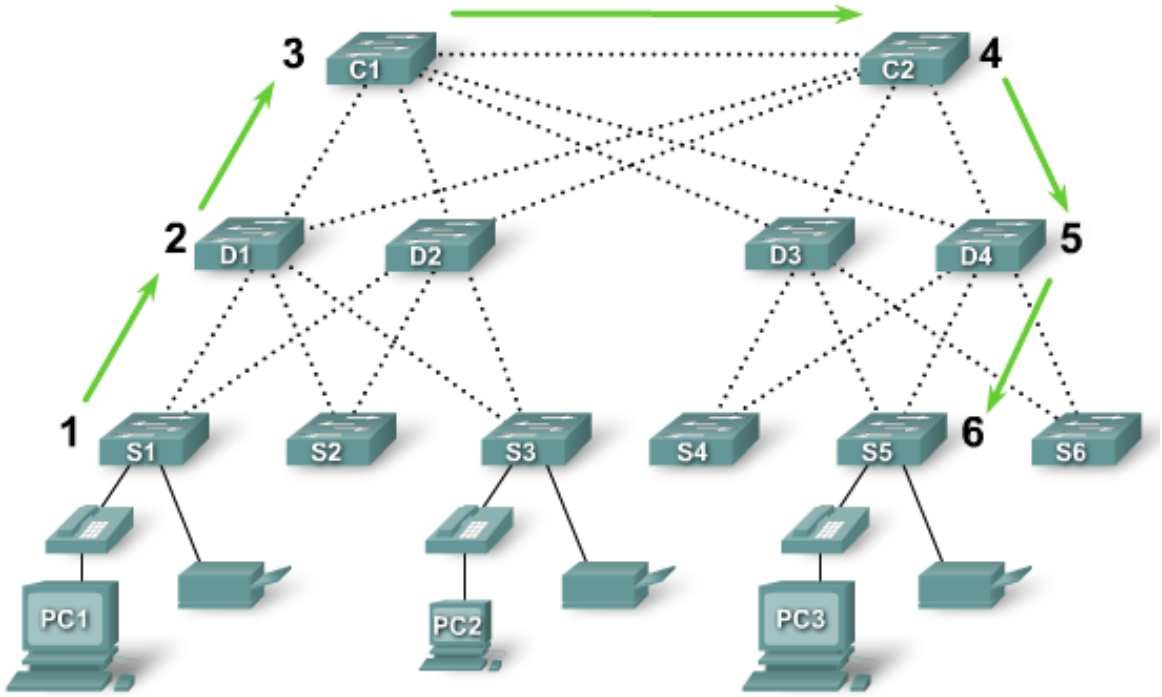


Figura 4.2 Diámetro de una red

4.2) Redundancia de una red

Son todos los enlaces entre las capas de redes jerárquicas a fin de asegurar la disponibilidad de la red.

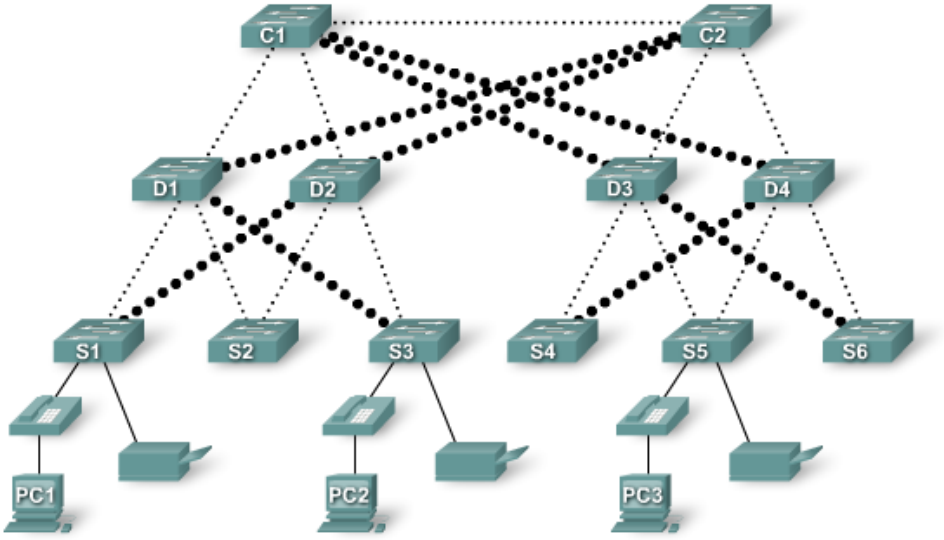


Figura 4.3 Redundancia de una red

4.3) Tecnología PoE (Power over Ethernet)

Es una tecnología que incorpora alimentación eléctrica a una infraestructura de red a través del cable Ethernet, está diseñada para no disminuir el rendimiento de comunicación de los datos en la red o reducir el alcance de la red.

PoE en una red que no dispone de dispositivos que la soporten directamente se usa una unidad base con un adaptador de alimentación para recoger la electricidad y una unidad terminal con un cable de alimentación para que el dispositivo final obtenga la energía necesaria para su funcionamiento, en el mercado existen varios dispositivos de red como ***switches, access point o hubs*** que soportan esta tecnología.

Ventajas:

- Los dispositivos se pueden apagar o reiniciar desde un lugar remoto usando los protocolos existentes.
- Simplifica y abarata la creación de un suministro eléctrico altamente robusto para los sistemas.
- Los dispositivos se instalan fácilmente.

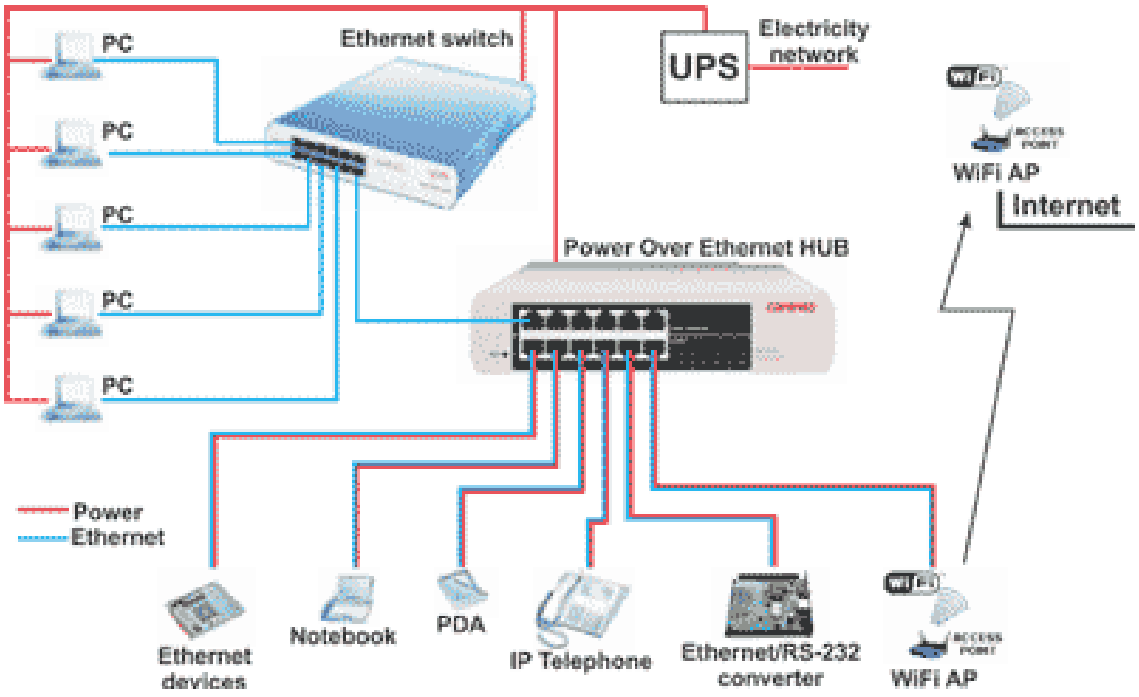


Figura 4.4 Tecnología PoE

4.4) Consideraciones para la elección del switch para la red Wi-Fi

a. **Configuración fija:** Es aquella en la que no se pueden agregar características u opciones más allá de las que vienen en el producto.

Figura 4.5 Switch con configuración fija

b. **Configuración modular:** Contiene chasis de diferente tamaño para la instalación de tarjetas de línea.

Figura 4.6 Switch con figuración modular

c. **Configuración apilable:** Pueden interconectarse con el uso de un cable especial del backplane que otorga rendimiento de ancho de banda alto entre los switches, operan con efectividad como un switch único más grande.

Figura 4.7 Configuración de switch apilable

4.5) Switch con Tecnología PoE (Power over Ethernet)

Usa la tecnología PoE que permite que el switch suministre energía a un dispositivo por el cable Ethernet, en la figura 4.8 se puede observar cómo se suministra energía a un teléfono IP y a un punto de acceso inalámbrico.

PoE permite mayor flexibilidad al instalar los puntos de accesos inalámbricos y los teléfonos IP porque se les puede instalar en cualquier lugar donde se puede tender un cable de Ethernet.

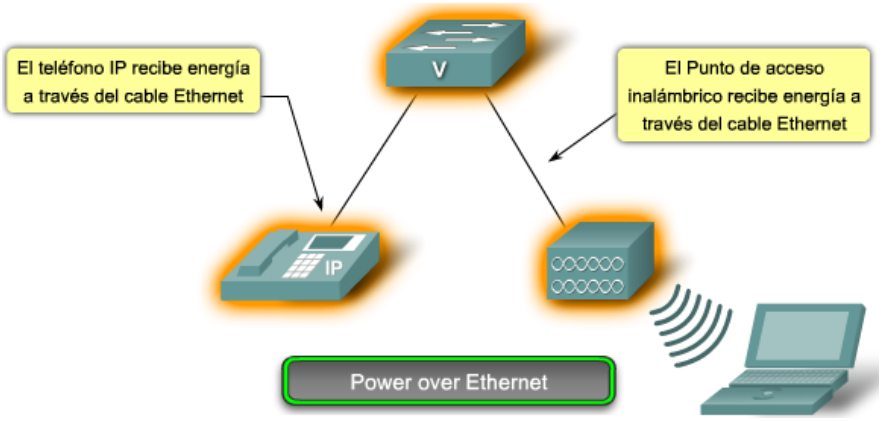


Figura 4.8 Switch con tecnología PoE

En los switch con tecnología PoE existen dos maneras para transmitir energía:

a) En el modo A los hilos 1-2 (par #2 en el ponchado 568B) llevan un lado de los 48 V DC, y los hilos 3-6 (par #3 en 568B) llevan el otro lado. Estos son los mismos pares que transportan datos en 10Base-T y 100Base-T.

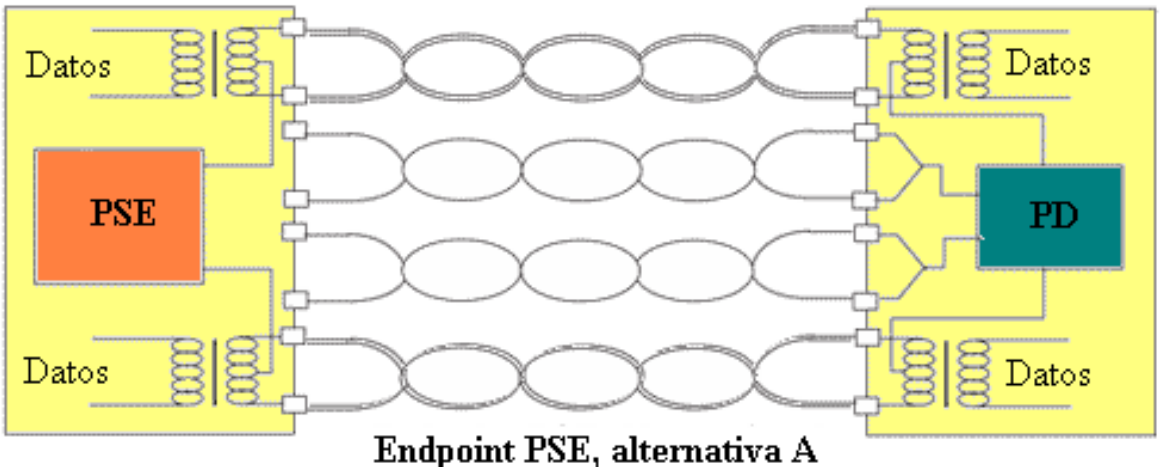


Figura 4.9 Switch PoE funcionando en modo A

b) En el modo B los hilos 4-5 (par #1 en ambos ponchados: 568A y 5678B) llevan un lado de la fuente DC y los hilos 7-8 (par #4 en 568A y 568B) proporcionan el retorno, estos son los pares ociosos en 10BASE-T y 100BASE-TX,el modo B usa los 4 pares del cable.

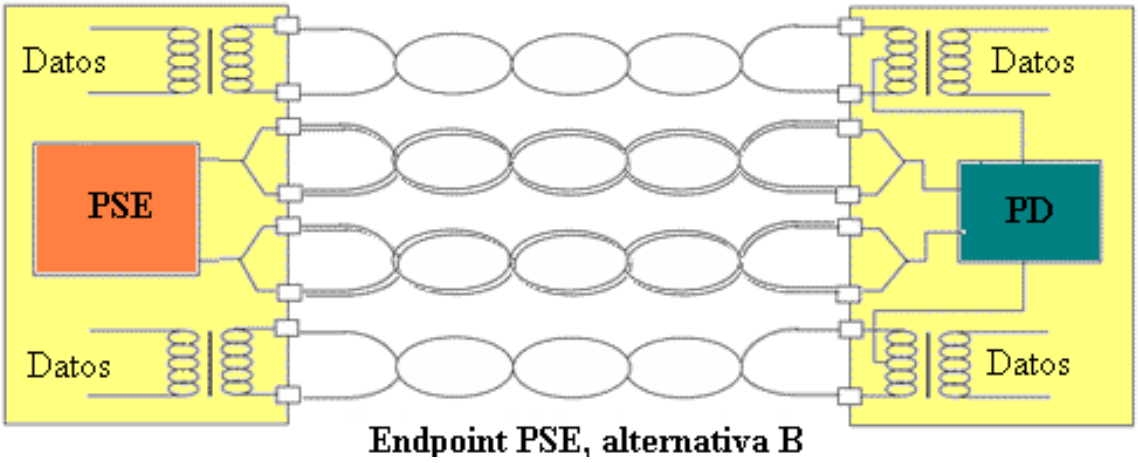


Figura 4.10 Switch PoE funcionando en modo B

4.6) RJ45

Es una interfaz física comúnmente usada para conectar redes de cableado estructurado (categorías 4, 5, 5e, 6 y 6a), se usan en cables de red Ethernet, donde suelen usarse 8 pines (4 pares).

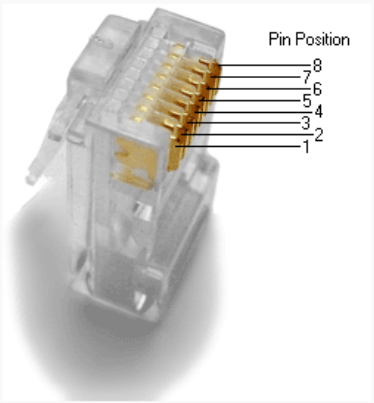
Pin	Color T568A	Color T568B	Pines en conector macho (en conector hembra se invierten)
1	Blanco/Verde (W-G)	Blanco/Naranja (W-O)	
2	Verde (G)	Naranja (O)	
3	Blanco/Naranja (W-O)	Blanco/Verde (W-G)	
4	Azul (BL)	Azul (BL)	
5	Blanco/Azul (W-BL)	Blanco/Azul (W-BL)	
6	Naranja (O)	Verde (G)	
7	Blanco/Marrón (W-BR)	Blanco/Marrón (W-BR)	
8	Marrón (BR)	Marrón (BR)	

Figura 4.11 RJ45 tipo A y B

4.7) Protocolos de enrutamiento

Los protocolos de enrutamiento proporcionan mecanismos distintos para elaborar y mantener las tablas de enrutamiento de los diferentes routers de la red, así como determinar la mejor ruta para llegar a cualquier host remoto.

Es muy importante saber qué tipo de protocolo de enrutamiento se está utilizando en la red, ya que los protocolos de Cisco no son compatibles con ningún otro.

Existen dos tipos de protocolos de enrutamiento:

a) **Enrutamiento Estático:** Las tablas de enrutamiento se introducen de manera manual y el principal problema es que no puede adaptarse por sí solo a los cambios que puedan producirse en la topología de la red.
b) **Enrutamiento dinámico:** Mantienen las tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia.

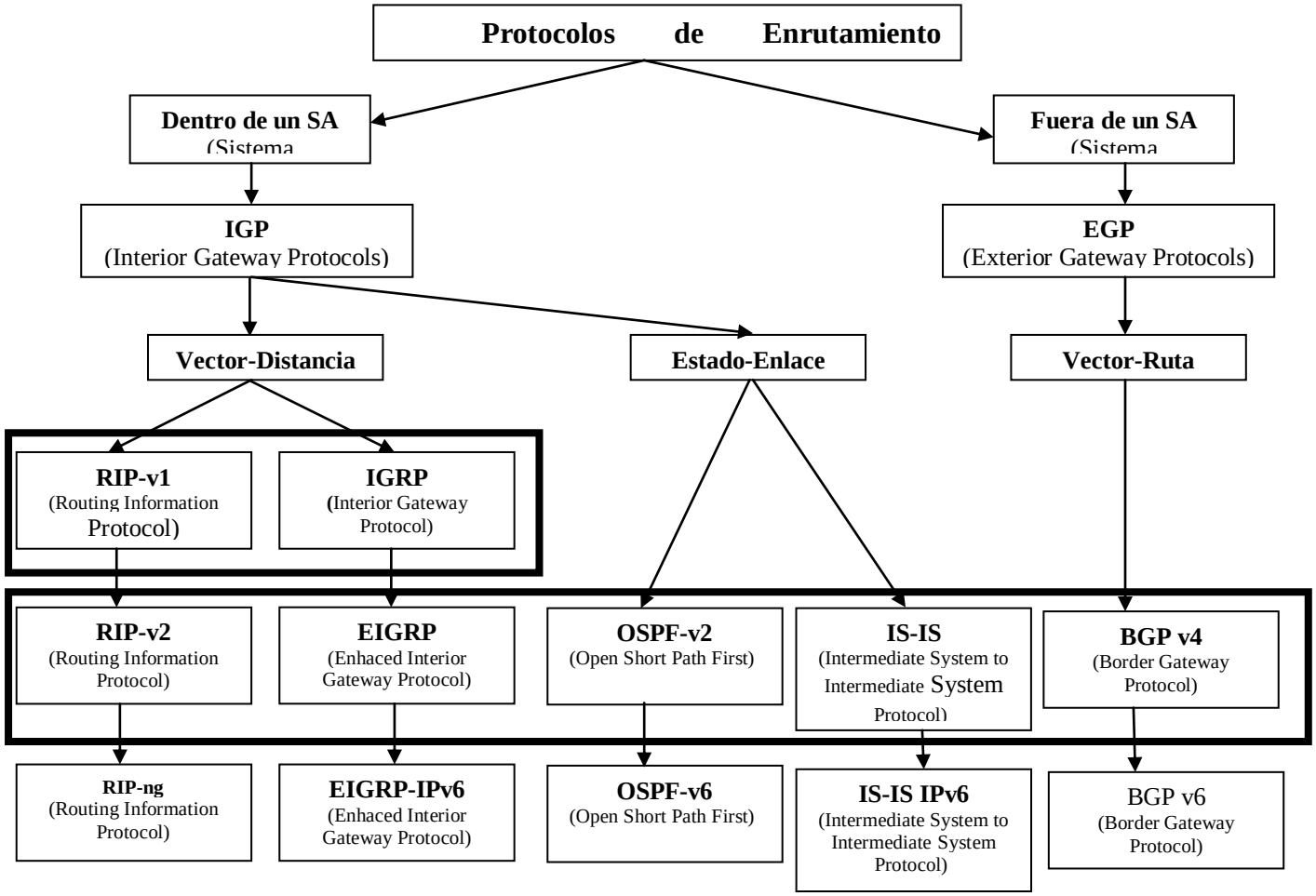


Figura 4.12 Protocolos de enrutamiento dinámicos

- ***Un Sistema Autónomo (SA)***: Es un conjunto de redes, o de routers, que tienen una única política de enrutamiento y que se ejecuta bajo una administración común, utilizando habitualmente un único IGP, para el mundo exterior, el SA es visto como una única entidad.
- ***Routing Information Protocol (RIP):*** Es un protocolo universal de enrutamiento por vector de distancia que utiliza el número de saltos como único sistema métrico, un salto es el paso de los paquetes de una red a otra.

  Si existen dos rutas posibles para alcanzar el mismo destino, RIP elegirá la ruta que presente un menor número de saltos. RIP no tiene en cuenta la velocidad ni la fiabilidad de las líneas a la hora de seleccionar la mejor ruta, RIP envía un mensaje de actualización del enrutamiento cada 30 segundos, en el que se incluye toda la tabla de enrutamiento del router, utilizando el protocolo UDP para el envío de los avisos.

  RIP-1 está limitado a un número máximo de saltos de 15, no soporta VLSM y CIDR, y no soporta actualizaciones desencadenadas, puede realizar equilibrado de la carga en un máximo de seis rutas de igual coste.

  RIP-2 es un protocolo sin clase que admite CIDR, VLSM, resumen de rutas y seguridad mediante texto simple y autenticación MD5, RIP publica sus rutas sólo a los routers vecinos.
- ***Interior Gateway Protocol (IGRP***): Fue diseñado por Cisco a mediados de los ochenta, para corregir algunos de los defectos de RIP y para proporcionar un mejor soporte para redes grandes con enlaces de diferentes anchos de banda, siendo un protocolo propietario de Cisco. IGRP es un protocolo de enrutamiento por vector de distancia capaz de utilizar hasta 5 métricas distintas (ancho de banda K1, retraso K3, carga, fiabilidad, MTU), utilizándose por defecto únicamente el ancho de banda y el retraso.
- ***Enhaced IGRP – EIGRP****:* Basado en IGRP y como mejora de este, es un protocolo híbrido que pretende ofrecer las ventajas de los protocolos por vector de distancia y las ventajas de los protocolos de estado de enlace.

  EIGRP soporta VLSM y soporta una convergencia muy rápida, EIGRP publica sus rutas sólo a los routers vecinos. Para la configuración de OSPF se requiere un número de proceso, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers.
- ***Open Short Path First (OSPF):*** Es un protocolo universal basado en el algoritmo de estado de enlace, desarrollado por el IETF para sustituir a RIP.

  OSPF utiliza un algoritmo que le permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes, soporta VLSM, ofrece convergencia rápida, autenticación de origen de ruta, y publicación de ruta mediante multidifusión.

  Publica sus rutas a todos los routers de la misma área. En la RFC 2328 se describe el concepto y operatividad del estado de enlace en OSPF, mientras que la implementación de OSPF versión 2 se muestra en la RFC 1583.
- ***Intermediate System to Intermediate System Protocol (IS-IS):*** Es un protocolo de estado enlace, que permite la convergencia muy rápida con gran

escalabilidad, es un protocolo muy flexible y se ha ampliado para incorporar características de vanguardia tales como la ingeniería de tráfico MPLS.

- ***Exterior Gateway Protocol (EGP):*** Los protocolos de enrutamiento exterior fueron creados para controlar la expansión de las tablas de enrutamiento y para proporcionar una vista más estructurada de Internet mediante la división de dominios de enrutamiento en administraciones separadas, llamadas Sistemas Autónomos (SA), los cuales tienen cada uno sus propias políticas de enrutamiento.
- ***Border Gateway Protocol (BGP):*** Es un protocolo de enrutamiento por vector de distancia usado comúnmente para enrutar paquetes entre dominios, estándar en Internet, gestiona el enrutamiento entre dos o más routers que sirven como routers fronterizos para determinados Sistemas Autónomos.
- ***BGP versión 4 (BGP-4):*** Es el protocolo de enrutamiento entre dominios elegido en Internet, en parte porque administra eficientemente la agregación y la propagación de rutas entre dominios, es un protocolo de enrutamiento exterior, también puede utilizarse dentro de un SA como un conducto para intercambiar actualizaciones BGP.

  Las conexiones BGP dentro de un SA son denominadas BGP interno (IBGP), mientras que las conexiones BGP entre routers fronterizos (distintos SA) son denominadas BGP externo (EBGP).

  Los routers BGP se configuran con la información del vecino a fin de que puedan formar una conexión TCP fiable sobre la que transportar información de la ruta de acceso del sistema autónomo y la ruta de la red. Tras establecer una sesión BGP entre vecinos, ésta sigue abierta a menos que se cierre específicamente o que haya un fallo en el enlace. Si dos routers vecinos intercambian información de ruta y sesiones BGP, se dice que son iguales BGP. En principio, los iguales BGP intercambian todo el contenido de las tablas de enrutamiento BGP. Posteriormente, sólo se envían actualizaciones incrementales entre los iguales para avisarles de las rutas nuevas o eliminadas.

4.8) Simulación de la red

Para el diseño de la red será necesario tomar en cuenta un hospital del segundo nivel de atención que deberá contar con especialidades troncales: Ginecología, pediatría, medicina interna y cirugía.

Suponiendo que la dirección de red para todos los hospitales de la zona rural es: 10.20.0.0/21

Para la asignación de las direcciones se hizo el cálculo de las reparticiones por VLSM (mascaras de subred de longitud variable) y tomando en cuenta que se está utilizando Ipv4 que utiliza cuatro octetos para el cálculo.

En esta tesis estudie los esquemas de direccionamiento de clases de IPs, pero en la vida real no se sigue este procedimiento por que existiría un gran desperdicio de IPs.

Hay que tomar en cuenta que necesito trabajar con IP privadas dentro de la red, ya que los enrutadores hacen el servicio NAT (Network Address Translation - Traducción de Dirección de Red) para convertir una red privada en una red pública y poder comunicarse a internet.

En este diseño de red supondré una red que tiene los dos protocolos de enrutamiento más utilizados en la vida real que son el OSPF y el EIGRP (CISCO), ya que un diseñador de redes sabe que EIGRP no es compatible con ningún otro protocolo de enrutamiento, y es factible comprar enrutadores CISCO porque son compatibles con ambos protocolos de enrutamiento.

Para simular la red utilicé el programa ***Cisco Packet Trace*** que fue proporcionado por el laboratorio de redes de la Facultad de Ingeniería de la UNAM.

En el primer segmento de red trabaje con 104 computadoras, un enrutador para un sistema autónomo y el enrutador de borde, distribuidas en tres subredes.

Este segmento de red se trabajará con protocolo OSPF y con la siguiente dirección de red: 10.20.1.0/24

No de host	**Cálculo**	**Mascara**	**Brocast**
64	$2^7 = 128 - 2 = 126$	10.20.1.0/25	10.20.1.127
30	$2^5 = 32 - 2 = 30$	10.20.1.128/27	10.20.1.159
10	$2^4 = 16 - 2 = 14$	10.20.1.160/28	10.20.1.175
2	$2^2 = 4 - 2 = 2$	10.20.1.176/30	10.20.1.179

Tabla 4.1 Calculo de red con protocolo OSPF

En el segundo segmento de red trabaje con 100 computadoras, un enrutador para un sistema autónomo y el enrutador de borde, distribuidas en cuatro subredes.

En el segmento de red se trabajará con protocolo EIGRP para tener una red con dispositivos Cisco en la implementación de la red con la siguiente dirección de red: 10.20.2.0/24

No de host	***Cálculo***	***Mascara***	***Brocast***
60	$2^6 = 64 - 2 = 62$	***10.20.2.0/26***	***10.20.2.63***
20	$2^5 = 32 - 2 = 30$	***10.20.2.64/27***	***10.20.1.95***
20	$2^4 = 16 - 2 = 14$	***10.20.2.96/27***	***10.20.1.127***
2	$2^2 = 4 - 2 = 2$	***10.20.2.128/30***	***10.20.1.131***

Tabla 4.2 Calculo de red con protocolo EIGRP

En la figura 4.13 están las mascaras de red para comprobar el número de host que se deben de colocar en cada subred calculada en cada uno de los protocolos incluidos.

Binario	Decimal	CIDR	Nº HOSTs	Clase
11111111.11111111.11111111.11111111	255.255.255.255	/32	1	
11111111.11111111.11111111.11111110	255.255.255.254	/31	2	
11111111.11111111.11111111.11111100	255.255.255.252	/30	4	
11111111.11111111.11111111.11111000	255.255.255.248	/29	8	
11111111.11111111.11111111.11110000	255.255.255.240	/28	16	
11111111.11111111.11111111.11100000	255.255.255.224	/27	32	
11111111.11111111.11111111.11000000	255.255.255.192	/26	64	
11111111.11111111.11111111.10000000	255.255.255.128	/25	128	
11111111.11111111.11111111.00000000	255.255.255.0	/24	256	C
11111111.11111111.11111110.00000000	255.255.254.0	/23	512	
11111111.11111111.11111100.00000000	255.255.252.0	/22	1024	
11111111.11111111.11111000.00000000	255.255.248.0	/21	2048	
11111111.11111111.11110000.00000000	255.255.240.0	/20	4096	
11111111.11111111.11100000.00000000	255.255.224.0	/19	8192	
11111111.11111111.11000000.00000000	255.255.192.0	/18	16384	
11111111.11111111.10000000.00000000	255.255.128.0	/17	32768	
11111111.11111111.00000000.00000000	255.255.0.0	/16	65536	B
11111111.11111110.00000000.00000000	255.254.0.0	/15	131072	
11111111.11111100.00000000.00000000	255.252.0.0	/14	262144	
11111111.11111000.00000000.00000000	255.248.0.0	/13	524288	
11111111.11110000.00000000.00000000	255.240.0.0	/12	1048576	
11111111.11100000.00000000.00000000	255.224.0.0	/11	2097152	
11111111.11000000.00000000.00000000	255.192.0.0	/10	4194304	
11111111.10000000.00000000.00000000	255.128.0.0	/9	8388608	
11111111.00000000.00000000.00000000	255.0.0.0	/8	16777216	A
11111110.00000000.00000000.00000000	254.0.0.0	/7	33554432	
11111100.00000000.00000000.00000000	252.0.0.0	/6	67108864	
11111000.00000000.00000000.00000000	248.0.0.0	/5	134217728	
11110000.00000000.00000000.00000000	240.0.0.0	/4	268435456	
11100000.00000000.00000000.00000000	224.0.0.0	/3	536870912	
11000000.00000000.00000000.00000000	192.0.0.0	/2	1073741824	
10000000.00000000.00000000.00000000	128.0.0.0	/1	2147483648	
00000000.00000000.00000000.00000000	0.	/0	4294967296	

Tabla 4.3 Máscaras de red

En la figura 4.13 se ve la distribución de la red que calculé con anterioridad.

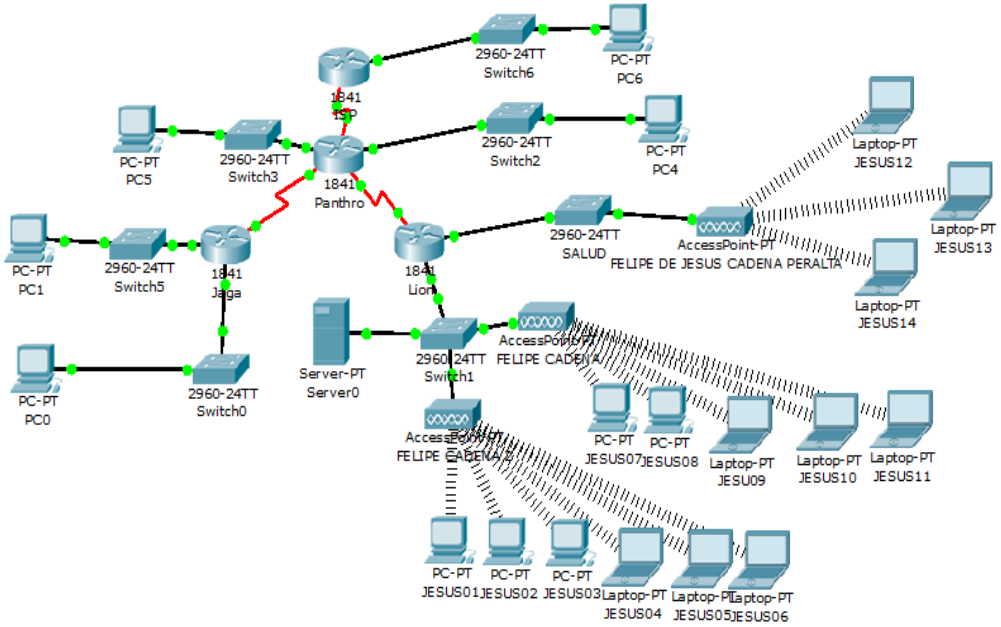


Figura 4.13 Diseño de la red

En la figura 4.14 se observa la programación del enrutador Panthro con protocolo de enrutamiento ***BGP*** (***Protocol Gateway Protocol).***

BGP se programan los dos protocolos de enrutamiento de los sistemas autónomos (SA) el ***OPSF*** y el ***EIGRP*** en el enrutador con nombre Panthro.

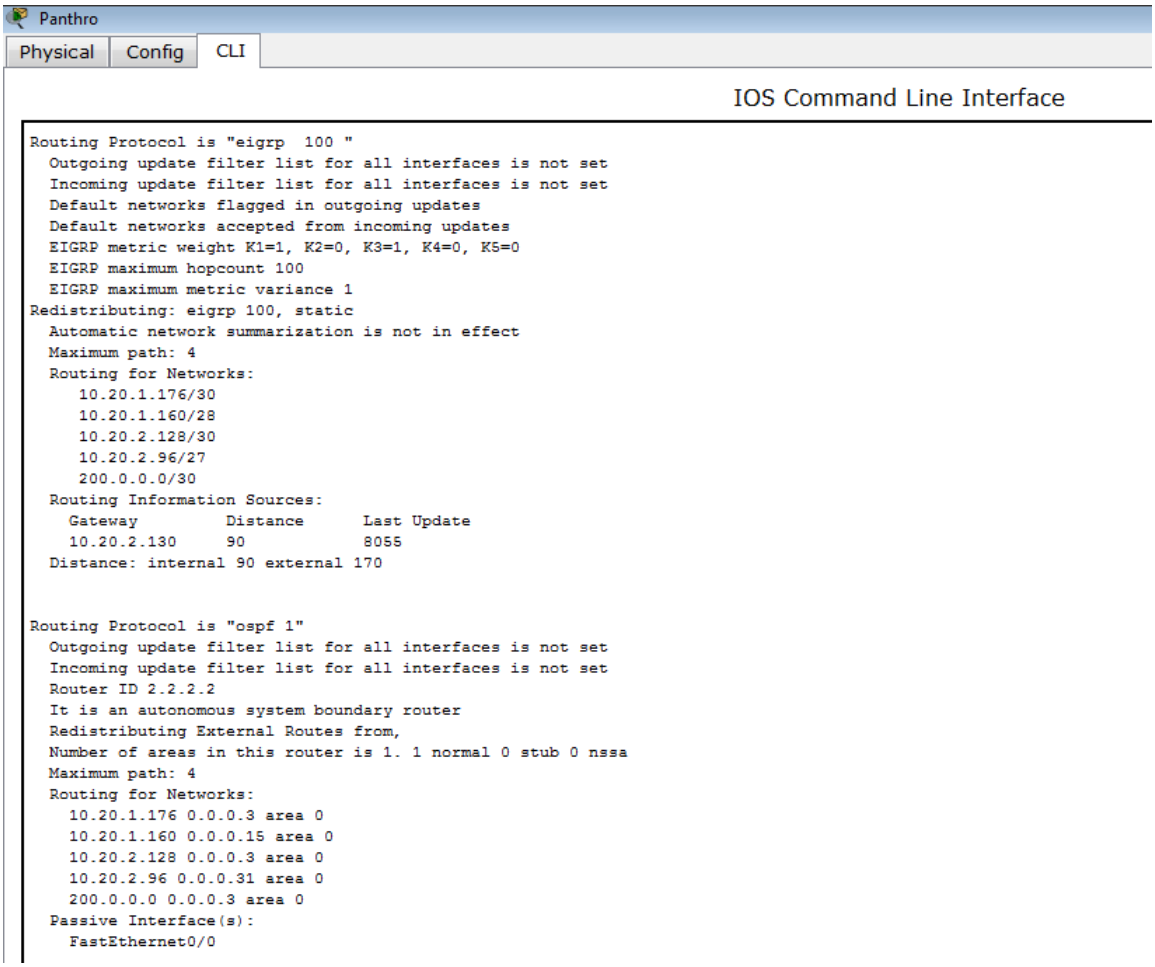


Figura 4.14 Enrutador de borde

En la figura 4.15 se observa la programación del enrutador Jaga con el protocolo ***OSPF*** (***Open Short Path First).***

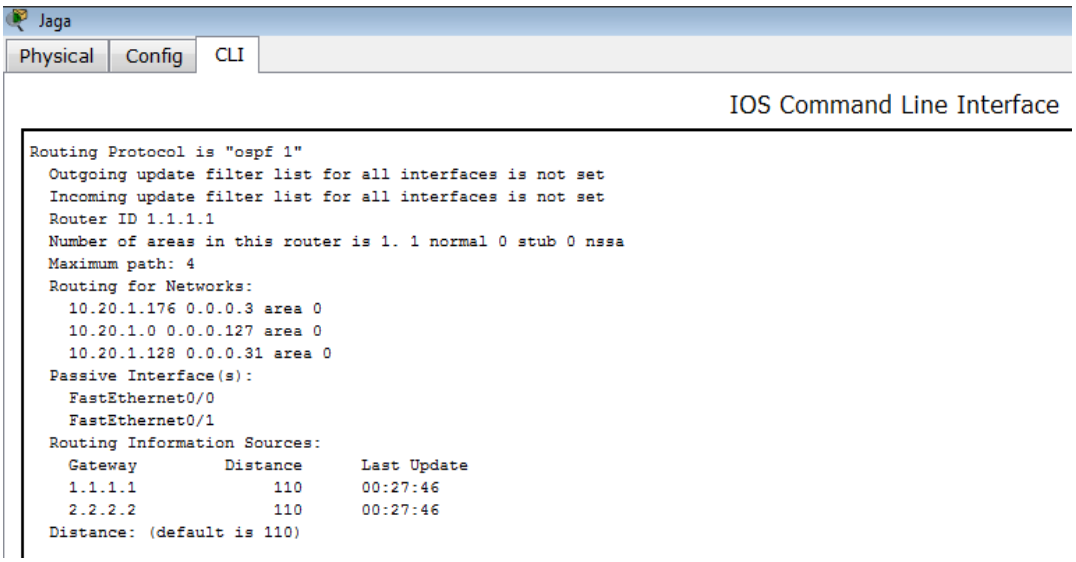


Figura 4.15 protocolo OSPF

En la figura 4.16 se observa la programación del enrutador Lion con el protocolo ***Enhaced Interior Gateway Protocol (EIGRP).***

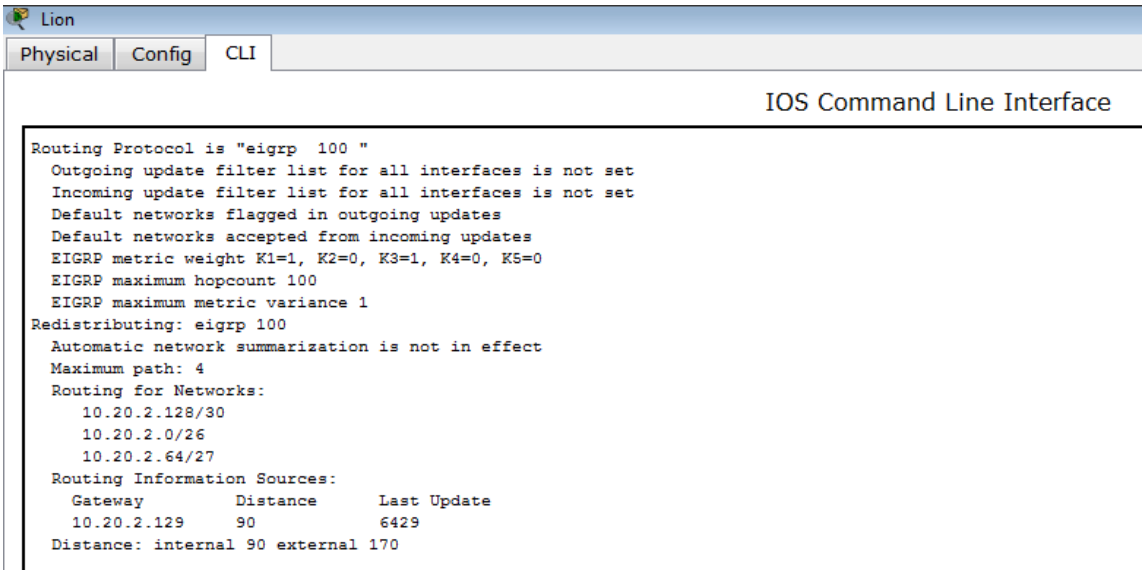


Figura 4.16 protocolo EIGRP

En la figura 4.17 se observa cómo se realiza la prueba de entrega de paquetes de información y comprobar que la red esta bien configurada.

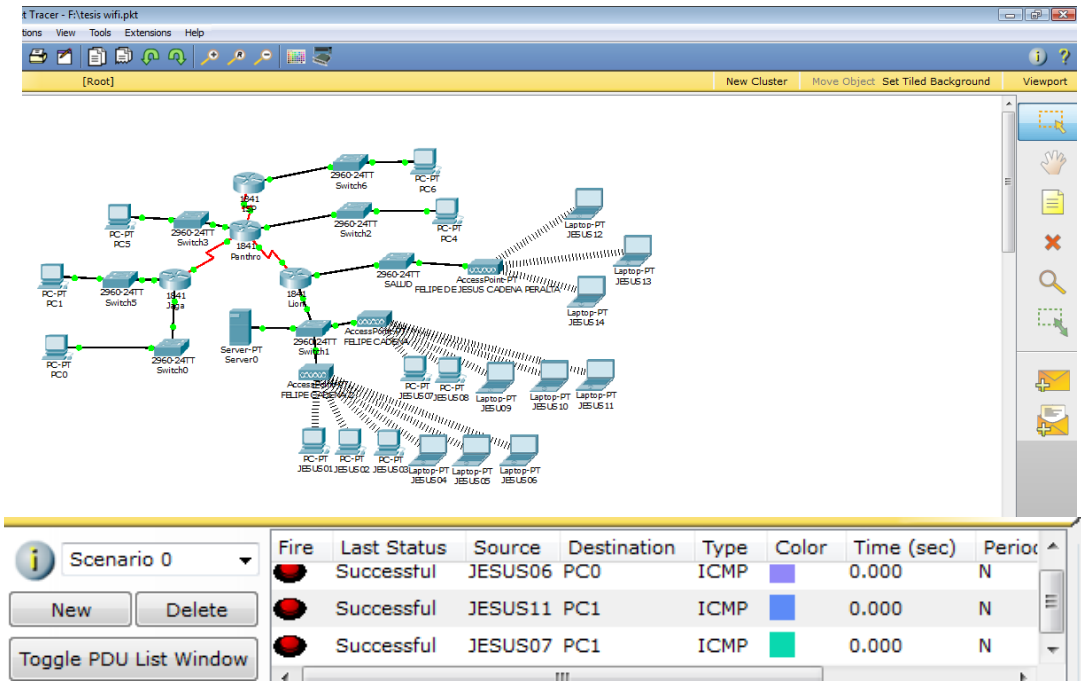


Figura 4.17 Simulación de la red

- Se observa la entrega de paquetes exitoso entre el host JESUS06 y el host PCO
- Se observa la entrega de paquetes exitoso entre el host JESUS11 y el host PC1
- Se observa la entrega de paquetes exitoso entre el host JESUS07 y el host PC1

- El acces point elegido es el cisco ap 541n que admite la tecnología EoP (Power over Ethernet) y que tiene un gran alcance.

  La configuración de este dispositivo se hace por medio de una página web.

  El costo del dispositivo es de $**4,369.40**.

Figura 4.18 AP Cisco

  Si necesita más características técnicas consultar la siguiente página web http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10492/ps10597/cisco_ap541n_wap_datasheet_spanish.pdf

- El host utilizado tiene que tener navegador web con Internet Explorer 6.0 o más reciente, o Firefox 3.0 o más reciente.

  El costo de una laptop Dell Alienware M14X Intel Core i5-2430M 2.4 GHz 4096 MB 250 GB es de $**20,999 c/u.**

Figura 4.19 Laptop Dell

- El switch elegido es el Switch Gigabit de 24 puertos Cisco SGE2000P, ya que incluye la tecnología EoP (Power over Ethernet).

  El costo es de $**19,950 c/u**

Figura 4.20 Switch Cisco

  Si necesitas más características técnicas consultar la siguiente página web: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9967/ps9983/data_sheet_c78-502070_es.pdf

	Cantidad	Precio	total
Acces point	3	$4369.40	$13108.2
Host	14	$20,999	$293986
Switch	3	$19,950	$59850
----------	----------	----------	$366,944.20

Tabla 4.4 Costo de la red

5) CONCLUSIONES

Para el diseño de este tipo de red, se analizaron diferentes tecnologías y protocolos de comunicación, buscando siempre la mejor eficiencia en la transmisión de la información tanto en la emisión como en la recepción, así como en la seguridad de la misma.

Es importante mencionar que el diseño de la red se hace siempre buscando la máxima eficiencia de está, sin embargo, existen parámetros ajenos al diseño que pueden inferir en la transmisión de los datos, ocasionando que está no trabaje al máximo de su capacidad, esto es, que la velocidad de transmisión disminuya.

Hacer un diseño eficiente de seguridad de la red Wi-Fi nos garantiza que ningún usuario no autorizado tenga acceso a la transmisión de la información y tener una adecuada atención de consulta con el paciente de una forma confiable.

La implementación de una red Wi-Fi en comunidades rurales puede llegar hacer de gran utilidad, permitiendo la comunicación para realizar diagnósticos eficientes de segundo nivel de salud a distancia, y poder ofrecer el servicio médico con un mejor diagnóstico.

Finalmente, se puede decir que la tesis ofrece un panorama general de las redes inalámbricas, así como algunos conceptos generales sobre la telemedicina que pueden ser de utilidad para la comunidad rural.

Sobre las aportaciones que está tesis me aporta, puedo decir que en el aspecto profesional seguí desarrollando mi capacidad de análisis y evaluación, así mismo la necesidad de tomar en cuenta la población y su cultura, pues será sustantivo reconocer sus necesidades para plantear soluciones, en este caso, sobre la salud.

Por otro lado, la formación que recibí durante mi trayectoria estudiantil fue fundamental, ya que se aprovecharon las diferentes temáticas abordadas durante la licenciatura, desde aspectos técnicos y tecnológicos, hasta aspectos culturales, sociales, económicos, etc.

GLOSARIO

CCMP- Counter Mode with Cipher Chainig Message Authentication Code Protocol: Es un protocolo de cifrado creado para sustituir al TKIP.

CCMP, parte del estándar 802.11i, que utiliza el Advanced Encryption Standard (AES). A diferencia de TKIP , gestión de claves y la integridad del mensaje es manejado por un solo componente construido en torno a AES con una clave de 128 bits, un bloque de 128 bits y 10 rondas de codificación por la FIPS 197 estándar.

CCMP utiliza MCP con los siguientes parámetros:

- M = 8 - lo que indica que el MIC es de 8 octetos,
- L = 2 - indica que el campo de longitud de 2 octetos.

El encabezado CCMP es de 8 octetos y consta de los siguientes campos:

- Número de paquete (número de código) (NP)
- Ext. IV
- Key ID

CHAP-Challenge Handshake Authentication Protocol: Es un método de autentificación usado por servidores accesibles vía PPP.

CHAP verifica periódicamente la identidad del cliente remoto usando un intercambio de información de tres etapas. Esto ocurre cuando se establece el enlace inicial y puede pasar de nuevo en cualquier momento de la comunicación. La verificación se basa en un secreto compartido (como una contraseña).

1. Después del establecimiento del enlace, el agente autentificador manda un mensaje que ***desafía*** al usuario.
2. El usuario responde con un valor calculado usando una función hash de un sólo sentido, como la suma de comprobación MD5.
3. El autentificador verifica la respuesta con el resultado de su propio cálculo de la función hash. Si el valor coincide, el autentificador informa de la autentificación, de lo contrario terminaría la conexión.
4. A intervalos aleatorios el autentificador manda un nuevo ***desafío*** con lo que se repite el proceso.

CHAP protege contra los ataques de REPLAY mediante el uso de un identificador que se va incrementando y un valor de desafío variable.

CHAP requiere que el cliente mantenga el secreto disponible en texto plano.

Concentrador o Hub*:* Es en dispositivo que recibe una señal y la repite emitiéndola por varios puertos.

CRC32-Cyclic Redundancy Check- Código de Redundancia Cíclica: Es un método

utilizado por los radio módems Freewave para verificar la integridad de los datos de transmisión, en acorde con el estándar internacional IEEE-802 para redes locales.
El CRC de 32 bits tiene actualmente un uso muy extendido, incluso hasta en el Departamento de los EU. Se considera hoy en día como el método más eficiente de comunicación digital en materia de detección y corrección de errores. Se puede implementar ya sea mediante un circuito cableado (hardware) o empleando un un algoritmo de procesamiento digital (software).

Este código se basa en el principio de que *n* bits de datos se pueden considerar como los coeficientes de un polinomio de orden *n-1*. Por ejemplo, los datos *1101* pueden tratarse como el polinomio $x^3+ x^2+1$.

$$\mathbf{1}x^3+ \mathbf{1}x^2+\mathbf{0}x^1+\mathbf{1} = x^3+ x^2+1$$

A estos bits de datos se le agregan 32 ***ceros*** a la derecha llamados ***bits de redundancia***

11010000000000000000000000000000000

posteriormente se obtiene el residuo de dividir el polinomio resultante de *32+n* bits entre un polinomio llamado ***generador polinomial*** de 32 bits.

$$\text{Generador polinomial}\overline{)11010000000000000000000000000000000}\ \text{cociente}$$

residuo

El resultado de la sustracción binaria en módulo 2 del polinomio de *32+n* bits y el residuo de la división representará la cadena de bits que habrá de ser transmitida.

11010000000000000000000000000000000-*residuo = cadena a transmitir*

El proceso de detección de errores, es equivalente a matemáticamente dividir la cadena de bits transmitida por un determinado binomio.

$$\text{Binomio comprobador}\overline{)cadena\_transmitida}\ \text{cociente}$$

residuo

Sólo si el residuo de esta nueva división es cero, la comunicación estará libre de errores.

Datagrama*:* Es un fragmento de paquete que es enviado con la suficiente información para que la red pueda simplemente encaminar el fragmento hacia el Equipo Terminal de Datos (ETD) receptor, de manera independiente a los fragmentos restantes. Esto no garantiza que los paquetes lleguen en el orden adecuado o que todos lleguen a su destino.

DHCP-Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host: Es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa

IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Encriptación AES.- Advanced Encryption Standard -Estándar de Encriptación Avanzada: Es una técnica de cifrado de clave simétrica que remplazará el Estándar de Encriptación de Datos (DES) utilizado habitualmente.

Hash: Es una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una ***función hash o algoritmo hash.*** Una función de hash es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor (un subconjunto de los números naturales por ejemplo). Varían en los conjuntos de partida y de llegada y en cómo afectan a la salida similitudes o patrones de la entrada. Una propiedad fundamental del hashing es que si dos resultados de una misma función son diferentes, entonces las dos entradas que generaron dichos resultados también lo son.

Es posible que existan claves resultantes iguales para objetos diferentes, ya que el rango de posibles claves es mucho menor que el de posibles objetos a resumir (las claves suelen tener en torno al centenar de bits, pero los ficheros no tienen un tamaño límite).

Son usadas en múltiples aplicaciones, como los arrays asociativos, criptografía, procesamiento de datos y firmas digitales, entre otros.

Una buena función de hash es aquella que experimenta pocas colisiones en el conjunto esperado de entrada; es decir que se podrán identificar unívocamente las entradas.

Hotspot: Es la zona de cobertura Wi-Fi, en el que un punto de acceso (*Access Point*) o varios proveen servicios de red a través de un Proveedor de Servicios de Internet Inalámbrico (WISP). Los hotspots se encuentran en lugares públicos, como aeropuertos, bibliotecas, centros de convenciones, cafeterías, hoteles, etcétera. Este servicio permite mantenerse conectado a Internet en lugares públicos.

IPsec-Internet Protocol security: Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando o cifrando cada paquete IP en un flujo de datos.

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan en la capa de transporte (capas OSI 4 a 7). Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados.

IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar

su código.

ISM Band - Industrial, Scientific and Medical Band: Las bandas reservadas internacionalmente para uso no comercial de radio frecuencia electromagnética en áreas industrial, científica y médica. En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones Wi-Fi o WPAN (Bluetooth).

Las bandas ISM fueron definidas por la Unión Internacional de Telecomunicaciones en el artículo 5 de las Regularizaciones de Radio (RR), concretamente 5.138 y 5.150

El uso de estas bandas de frecuencia está abierto a todo el mundo sin necesidad de licencia, respetando a las regulaciones que limitan los niveles de potencia transmitida. Este hecho fuerza a que este tipo de comunicaciones tengan cierta tolerancia frente a errores y que utilicen mecanismos de protección contra interferencias, como técnicas de ensanchado de espectro.

L2TP -Layer 2 Tunneling Protocol*:* Fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF (RFC 2661).

L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

Al utilizar PPP para el establecimiento telefónico de enlaces, L2TP incluye los mecanismos de autenticación de PPP, PAP y CHAP. De forma similar a PPTP, soporta la utilización de estos protocolos de autenticación, como RADIUS.

A pesar de que L2TP ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas. Por ejemplo:

- Sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.
- Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por acabado el túnel L2TP o la conexión PPP subyacente.
- L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos.
- A pesar de que la información contenida en los paquetes PPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

A causa de estos inconvenientes, el grupo del IETF que trabaja en el desarrollo de PPP

consideró la forma de solventarlos. Ante la opción de crear un nuevo conjunto de protocolos para L2TP del mismo estilo de los que se están realizando para IPSec, y dado la duplicación del trabajo respecto al propio grupo de desarrollo de IPSec que supondría, se tomó la decisión de utilizar los propios protocolos IPSec para proteger los datos que viajan por un túnel L2TP.

L2TP es en realidad una variación de un protocolo de encapsulamiento IP. Un túnel L2TP se crea encapsulando una trama L2TP en un paquete UDP, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Siendo el protocolo de encapsulamiento más externo IP, los protocolos IPSec pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.

Latencia: Es la suma de retardos temporales que se presentan dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.

LDAP.-Lightweight Directory Access Protocol-Protocolo Ligero de Acceso a Directorios: *Es* un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. El ejemplo más común es el directorio telefónico, que consiste en una serie de nombres (personas u organizaciones) que están ordenados alfabéticamente, con cada nombre teniendo una dirección y un número de teléfono adjuntos.

Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos u organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol.

Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.).

LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Loops ó Bucle: Es una sentencia que se realiza repetidas veces a un trozo aislado de código, hasta que la condición asignada a dicho bucle deje de cumplirse.

MAC address-Media Access Control address o Dirección de Control de Acceso al Medio: Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una Ethernet de red. Se conoce también como la dirección física en cuanto a identificar dispositivos de red. Cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el OUI. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64 las cuales han sido diseñadas para ser identificadores globalmente únicos.

Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en el hardware en su momento de fabricación. Debido a esto, las direcciones MAC son a veces llamadas ***Direcciones Quemadas Dentro (BIA-Burned-in Address).***

Si nos fijamos en la definición como cada bloque hexadecimal son 8 dígitos binarios (bits), tendríamos:

6*8=48 bits únicos

En la mayoría de los casos no es necesario conocer la dirección MAC, ni para montar una red doméstica, ni para configurar la conexión a internet. Pero si queremos configurar una red Wi-Fi y habilitar en el punto de acceso un sistema de filtrado basado en MAC (a veces denominado filtrado por hardware), el cual solo permitirá el acceso a la red a adaptadores de red concretos, identificados con su MAC, entonces necesitamos conocer dicha dirección. Dicho medio de seguridad se puede considerar como un refuerzo de otros sistemas de seguridad, ya que teóricamente se trata de una dirección única y permanente, aunque en todos los sistemas operativos hay métodos que permiten a las tarjetas de red identificarse con direcciones MAC distintas de la real.

MAC opera en la capa 2 del modelo OSI, encargada de hacer fluir la información libre de errores entre dos máquinas conectadas directamente. Para ello se generan tramas, pequeños bloques de información que contienen en su cabecera las direcciones MAC correspondiente al emisor y receptor de la información.

La dirección MAC original IEEE 802, ahora oficialmente llamada ***MAC-48***, viene con la especificación Ethernet. Desde que los diseñadores originales de Ethernet tuvieran la visión de usar una dirección de 48-bits de espacio, hay potencialmente 2^48 o 281,474,976,710,656 direcciones MAC posibles.

Cada uno de los tres sistemas numéricos usa el mismo formato y difieren solo en el tamaño del identificador. Las direcciones pueden ser "direcciones universalmente administradas" o "localmente administradas".

Una dirección universalmente administrada es únicamente asignada a un dispositivo por su fabricante, estas algunas veces son llamadas ***burned-in addresses***. Los tres primeros octetos (en orden de transmisión) identifican a la organización que publicó el identificador y son conocidas como ***Identificador de Organización Único (OUI).***

Los siguientes tres (MAC-48 y EUI-48) o cinco (EUI-64) octetos son asignados por

esta organización a su discreción, conforme al principio de la unicidad. La IEEE espera que el espacio de la MAC-48 se acabe no antes del año 2100 y de las EUI-64 no se espera que se agoten en un futuro previsible.
Con esto podemos determinar como si fuera una huella digital, desde que dispositivo de red se emitió el paquete de datos aunque este cambie de dirección IP, ya que este código se ha acordado por cada fabricante de dispositivos.

PAP-Password Authentication Protocol: Un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet. PAP es un subprotocolo usado por la autenticación del protocolo PPP (Point to Point Protocol), validando a un usuario que accede a ciertos recursos.

PAP transmite contraseñas o password en ASCII sin cifrar, por lo que se considera inseguro. PAP se usa como último recurso cuando el servidor de acceso remoto no soporta un protocolo de autenticación más fuerte.

Puerto: El campo de puerto tiene una longitud de 16 bits, por lo que el rango de valores válidos va de 0 a 65,535.
El puerto 0 está reservado, pero es un valor permitido como puerto origen si el proceso emisor no espera recibir mensajes como respuesta.

Los puertos 1 a 1023 se llaman puertos ***bien conocidos*** y en sistemas operativos tipo Unix enlazar con uno de estos puertos requiere acceso como superusuario.

Los puertos 1024 a 49,151 son puertos registrados.

Los puertos 49,152 a 65,535 son puertos efímeros y son utilizados como puertos temporales, sobre todo por los clientes al comunicarse con los servidores.

RC4 o ARC4: Es el sistema de cifrado de flujo ***Stream Cipher*** más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas). RC4 fue excluido enseguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.

El algoritmo de criptografía RC4 fue diseñado por Ron Rivest de la RSA Security en el año 1987; su nombre completo es Rivest Cipher 4, teniendo el acrónimo RC un significado alternativo al de ***Ron's Code*** utilizado para los algoritmos de cifrado RC2, RC5 y RC6.

RC4 es parte de los protocolos de cifrado más comunes como WEP, WPA para tarjetas Wireless y TLS. Entre los factores principales que han ayudado a que RC4 esté en un rango tan amplio de aplicaciones son su increíble velocidad y simplicidad. La implementación tanto en software como en hardware es muy sencilla de desarrollar y

son muy pocos los recursos necesarios para obtener un rendimiento eficiente de ARC4.

RC4 es un algoritmo sorprendentemente simple. Este consiste en 2 algoritmos: 1-Key Scheduling Algorithm (KSA) y 2- Pseudo-Random Generation Algorithm (PRGA). Ambos de estos algoritmos usan 8-by-8 S-box, el cual es solo un array de 256 números en el cual ambos son únicos en cuanto a rango y su valor va desde 0 hasta 255. Todos los números de 0 a 255 existen dentro del array, pero están solo mezclados de diferentes maneras, el KSA se encarga de realizar la primera mezcla en el S-Box, basado en el valor de la semilla dada dentro de él, y esta "semilla" puede ser de 256 bits de largo.

Primero, el S-box array es llenado con valores secuenciales desde 0-255. Este array será llamado simplemente S. Entonces, el otro array de 256-bits es llenado con el valor de la ***semilla,*** repitiendo como sea necesario hasta que todo el array es llenado. Este array será llamado K, entonces el array S es mezclado usando el siguiente Pseudo-Código.

Pseudo-Code es utilizado para programación como un desarrollo en ***sucio*** del cual se va perfeccionando el código.

Switch: Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

UDP- User Datagram Protocol: 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.

Warchalking: Es un lenguaje de símbolos normalmente escritos con gis en las paredes que informa a los posibles interesados de la existencia de una red inalámbrica en ese punto.

Inspirado en el lenguaje de símbolos que utilizan los vagabundos, su sencillez ha sido uno de los factores que han hecho posible su proliferación por las grandes ciudades. Además otras características como la no perdurabilidad de las marcas durante grandes períodos hacen que sea muy dinámico y se va adaptando constantemente a las características cambiantes de las redes sobre cuya existencia informan.

Los símbolos más usados son:

- SSID
-)(Nodo abierto ,() Nodo cerrado, (W) Nodo con WEP
- 1.5 Ancho de banda

WEP-Wired Equivalent Privacy-Privacidad Equivalente a Cableado: Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.

Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

BIBLIOGRAFÍA

1. Vargas Grajeda Andrea Guadalupe y Méndez Tierri Luis Antonio, "**Sistema de Teleimagenologia Clínica",** tesis, Ciudad Universitaria 2003.
2. Rojas García Francisco, **"Seguridad en redes Inalámbricas Wi-Fi (802.11)"**, tesina, Acatlán 2006.
3. Blanchard B. S, and Fabricky W. J**." System Engineering and Analysis"**, editorial Prentice-Hall, USA 1981.
4. Tsai Alice Y. H**.," Sistemas de base de datos (administración y uso)"**, editorial Prentice-Hall Hispanoamericana, México 1990.
5. Stewart, M., **"Seguridad en Wi-Fi"**, Mc Graw Hill, México 2003.
6. Reid y Seide, **"802.11 (Wi-Fi) Manual de Redes Inalámbricas",** Mc Graw Hill, México 2003.
7. Klander, L**.,"Hacker Proof The Ultimate Guide to Network Security",** Jamsa Press, USA 2005.
8. Scott, et al., **"Virtual Private Networks",** O´Relly. USA 1999.
9. Scambray, et al, **"Hacking Exposed"**, Osborne / Mc Graw Hill, USA 2001.
10. Hunt, R., **"TCP /IP Network Administration"**, O´Relly & Associates, Inc., USA 1994.
11. Stevens, R., "**TCP / IP Illustrated: The Protocols Volume I"**, Addison – Wesley Publishing Company, USA 1994.

MESOGRAFÍA

1. http://www.virusprot.com/cursos/Redes-Inalámbricas-Curso-gratis.htm#Introducción
2. http://www.ampere.com.mx/freewave/crc.php#ch
3. http://dctrl.fi-b.unam.mx/~capituloestudiantil/boletin/Boletin02.pdf
4. http://www.wi-fi.org/
5. http://www.cdi.gob.mx/
6. http://www.aulaclic.es/articulos/wifi.html
7. http://www.howstuffworks.com/wireless-network.htm
8. http://www.webopedia.com/TERM/W/Wi_Fi.html
9. http://www.elhacker.net/manual_hacking_wireless.html
10. http://es.scribd.com/doc/56290077/36/Switches-de-configuracion-fija
11. http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx#TiposEnrutamiento
12. http://www.programas-hack.com/category/hackear-wireless/