Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

ANÁLISIS DE LOS DISPOSITIVOS DE RED EN AMBIENTE VIRTUAL

Sergio Romeo Santos Revolorio
Asesorado por el Ing. Oscar Alejandro Paz Campos

Guatemala, agosto de 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ANÁLISIS DE LOS DISPOSITIVOS DE RED EN AMBIENTE VIRTUAL

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

SERGIO ROMEO SANTOS REVOLORIO
ASESORADO POR EL ING. OSCAR ALEJANDRO PAZ CAMPOS

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, AGOSTO DE 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Jurgen Andoni Ramírez Ramírez
VOCAL V	Br. Oscar Humberto Galicia Nuñez
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Sergio Arnaldo Méndez Aguilar
EXAMINADOR	Ing. José Alfredo González Diaz
EXAMINADOR	Ing. Oscar Alejandro Paz Campos
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

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

ANÁLISIS DE LOS DISPOSITIVOS DE RED EN AMBIENTE VIRTUAL

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha enero de 2017.

Sergio Romeo Santos Revolorio

Guatemala, 25 de mayo de 2,017

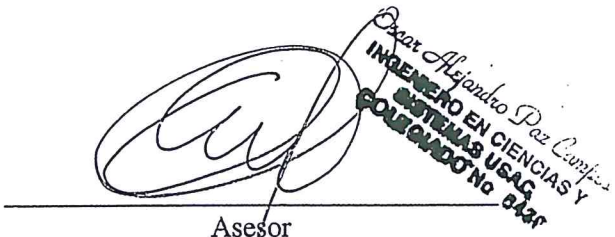
Ingeniero
Marlon Antonio Perez Turk
Director de la Escuela de ingeniería
Ciencias y Sistemas

Respetable Ingeniero Perez

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **SERGIO ROMEO SANTOS REVOLORIO**, identificado con el número de carné **200219393**, titulado: **"ANALISIS DE LOS DISPOSITIVOS DE RED EN AMBIENTE VIRTUAL"**, y a mi criterio el mismo cumple con los objetivos propuestos para su elaboración de acuerdo al protocolo presentado.

Sin otro particular, me suscribo de usted,

Atentamente,



Asesor
Oscar Alejandro Paz Campos
Ingeniero en Ciencias y Sistemas
Colegiado 6430

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 7 de Junio de 2017

Ingeniero
Marlon Antonio Pérez Türk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **SERGIO ROMEO SANTOS REVOLORIO** con carné **200219393** y **CUI 1884 34399 0101**, titulado **"ANALISIS DE LOS DISPOSITIVOS DE RED EN AMBIENTE VIRTUAL"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
INGENIERIA EN CIENCIAS Y SISTEMAS
COORDINACION TESIS

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"ANÁLISIS DE LOS DISPOSITIVOS DE RED EN AMBIENTE VIRTUAL"****, realizado por el estudiante SERGIO ROMEO SANTOS REVOLORIO aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

Ing. Marlon Antonio Pérez Turk
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 03 de agosto de 2017

ersidad de San Carlos
de Guatemala

cultad de Ingeniería
Decanato

Ref.DTG.D.344.2017

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **ANÁLISIS DE LOS DISPOSITIVOS DE RED EN AMBIENTE VIRTUAL,** presentado por el estudiante universitario: **Sergio Romeo Santos Revolorio,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, agosto de 2017

/cc

ACTO QUE DEDICO A

Dios	Por haber estado conmigo todo el tiempo.
Mis padres	Por su apoyo incondicional durante toda la vida. Romeo Victalino Santos De León, Elvia del Carmen Revolorio.
Mi familia	Por haberme apoyado en todo momento.
Mi esposa	Nidia Roxana Pinto.
Mis amigos	Por su guía y apoyo cuando se les necesitaba.

AGRADECIMIENTOS A

Dios	Por guiar mis pasos y ayudarme en todo momento.
Escuela Politécnica	Por inculcar el espíritu de superación.
Mis padres	Por su apoyo incondicional durante toda la vida. Romeo Victalino Santos De Leon, Elvia Del Carmen Revolorio.
Mi familia	Por haberme apoyado en todo momento.
Mis amigos	Por su guía y apoyo cuando se les necesitaba.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES VII
LISTA DE SÍMBOLOS IX
GLOSARIO XI
RESUMEN XIII
OBJETIVOS XV
INTRODUCCIÓN XVII

1. ¿QUÉ ES UNA RED DE COMPUTADORA? 1
   1.1. Red de computadoras 1
   1.2. Red de computadora 1
   1.3. Clasificación de redes 2
   1.4. Protocolo de redes 5
   1.5. Componentes básicos de las redes de ordenadores 6
   1.6. Tipos de sitios de trabajo 8
   1.7. Tipos de servidores 8
   1.8. Tipos de redes 11
      1.8.1. Red interna 14
      1.8.2. Intranet 15
      1.8.3. Internet 15
   1.9. Construcción de una red de computadoras 15
      1.9.1. Una red simple 15
      1.9.2. Redes prácticas 16
   1.10. Componentes básicos de una red 17
      1.10.1. Software 17

1.10.1.1. Definición de software 19
1.10.1.2. Extraído del estándar729 del IEEE 19
1.10.2. Clasificación del software 20

2. TIPOS DE RED 25
2.1. Tipos de redes 25
2.1.1. Diferentes tipos de redes 25
2.1.1.1. Redes LAN 25
2.1.2. Redes MAN 26
2.1.2.1. Redes WAN 26
2.1.3. Redes inalámbricas vrs alámbricas 27
2.1.4. Redes inalámbricas 28
2.1.4.1. La velocidad de las redes inalámbricas 28
2.1.4.2. Ventajas de las redes inalámbricas 29
2.1.4.3. Inconvenientes de las redes inalámbricas 30
2.1.4.4. Desventajas de las redes inalámbricas 31
2.2. Incertidumbre tecnológica 33
2.2.1. Tecnologías inalámbricas 34
2.3. Parámetros que definen una red 35
2.3.1. ¿Qué aporta una red inalámbrica? 35
2.4. Red alámbrica 37
2.4.1. Ventajas de una red alámbrica 38
2.4.2. Las desventajas de una red alámbrica 38
2.4.3. Velocidades de una red alámbrica 38
2.4.4. Instalación y configuración 39

2.4.5. Tarjeta de red alámbrica y tarjeta de red inalámbrica 39

3. DISPOSITIVOS DE RED 41
3.1. Router 41
3.1.1. Funcionamiento 43
3.1.2. Arquitectura física 44
3.2. Tipos de encaminadores 45
3.2.1. Conectividad *small office, home office* (SOHO) 45
3.2.2. Encaminador de empresa 46
3.2.3. Acceso 46
3.2.4. Distribución 47
3.2.5. Núcleo 47
3.2.6. Borde 48
3.2.7. Encaminadores inalámbricos 48
3.2.8. Enrutador sin módem, conexiones 49
3.2.9. Enrutadores y conmutadores en el modelo OSI 50
3.2.10. Interfaces encaminadas 50
3.2.11. Interfaces conmutadas 51
3.2.12. Conmutadores frente a enrutadores 51
3.3. Switch 52
3.3.1. Introducción al funcionamiento de conmutadores 53
3.3.2. Cut-Through 55
3.3.3. Adaptative Cut-Through 55
3.3.4. Conmutadores de capa 2 56
3.3.5. Conmutadores de capa 3 57
3.3.6. Conmutadores de capa 4 58
3.3.7. Conmutadores de capa 5 58
3.3.7.1. Paquete por paquete 58

3.4. Módem 58
3.4.1. Cómo funciona 60
3.5. Módems para PC 60
3.5.1. Internos 61
3.5.2. Externos 62
3.6. Tipos de conexión 62
3.7. Módems telefónicos 63
3.7.1. Velocidad de transmisión 64
3.8. Primeros módem 65
3.8.1. Módems de segunda generación 65
3.8.2. Lista de velocidades de acceso telefónico 67
3.8.3. Tipos de modulación 68
3.8.4. Órdenes de comunicación 69
3.8.5. Registros 69
3.8.6. Pasos o procesos para establecer comunicación a través del módem 72
3.8.7. Test en módems *Hayes* 75
3.8.8. Protocolos de comprobación de errores 76
3.8.9. Protocolos de transferencia de archivos 77
3.8.10. Servidor 80
3.8.10.1. ¿Qué es un servidor? 80
3.8.10.2. Plataformas de servidor (*server platforms*) 82
3.8.10.3. Servidores de aplicaciones (*application servers*) 82
3.8.11. Servidores de audio/video (*audio/video servers*) 82
3.9. Firewall 84
3.10. Hub 87
3.10.1. ¿Qué es un hub y cómo funciona? 87

3.10.2. Existen tres tipos de hub diferentes 89

4. DISPOSITIVOS DE RED EN AMBIENTE VIRTUAL 91
4.1. ¿Qué es virtual router? 91
4.1.1. ¿Dónde se puede utilizar virtual router? 91
4.1.2. Los fundamentos de virtual wifi router 93
4.2. Primeros pasos de configuración 93
4.2.1. Creando el punto de acceso 96
4.3. Switch virtual 98
4.4. Servidor virtual 100
4.5. Firewall virtual 103
4.5.1. Virtual hub (hub virtual) 115
4.5.2. Detalles del hub virtual (VHub) VH4000/VH2000 . 116
4.5.3. Aprovisionamiento de enlace largo 117
4.5.4. VHub de RFoG 118
4.5.5. VHub de transmisión/difusión restringida 118
4.5.6. VHub para servicios comerciales 118
4.5.7. VHub de nodo recolector 119

5. DISPOSITIVOS DE RED VERSUS DISPOSITIVOS DE RED EN AMBIENTE VIRTUAL 121
5.1. Ventajas y desventajas de la virtualización 121
5.1.1. La importancia de la gestión de la virtualización ... 121
5.2. Virtualización y negocio 123
5.3. VirtualWiFiRouter 124
5.3.1. Implementación 125
5.4. Swicht virtual 127
5.5. Firewall virtual 129
5.5.1. Firewalls virtuales 130

5.5.1.1. Tipos de firewalls: ventajas y desventajas 131
5.6. Virtual modem PRO 133
5.6.1. Software de módem virtual 133
5.6.1.1. Modem virtual 134
5.7. Hub virtual 144

CONCLUSIONES 147
RECOMENDACIONES 149
BIBLIOGRAFÍA 151

ÍNDICE DE ILUSTRACIONES

FIGURAS

1. Red de computadoras 2
2. Clasificación de redes 3
3. Protocolos de redes 5
4. Ejemplos de redes 14
5. Buscador de programas en ubuntu 13.10 18
6. Hardware típico de una computadora personal 22
7. Redes 27
8. Redes inalámbricas 29
9. Red alámbrica 37
10. Tarjetas de red alámbrica e inalámbrica 40
11. Encaminador 45
12. Captura de pantalla de la interfaz web de LuCI OpenWrt 46
13. Equipos domésticos 49
14. Router wifi 49
15. Enrutadores en el modelo OSI 50
16. Conexiones en un conmutador Ethernet 52
17. Conmutadores de red Juniper (arriba) y Netgear (abajo) 53
18. Módem por software PCI (izquierda) y módem hardware ISA (derecha) 59
19. Firewall 85
20. Hub y cómo funciona 88
21. Virtual router sin publicidad, sin molestias 92
22. Activar o desactivar características de Windows 94

23. Centro de redes y recursos compartidos 95
24. Conexión de área local 96
25. Virtual Router 97
26. Configuración de red 98
27. Cómo funciona 111
28. Ubicación independiente 112
29. Solución de software verdadera 113
30. Funciona como servicio del sistema 113
31. Ejemplo de uso 114
32. Switch virtual 127
33. Tipos de firewall 131
34. Ventajas 137
35. Menor costo de equipo. 137
36. Red formal de comunicaciones 138
37. Menos interrupciones en el trabajo. 138
38. Contribución social 139
39. Aislamiento 140
40. Temor a perder el trabajo 140
41. Principales ventajas de los servidores virtuales 141

TABLAS

I. Lista de velocidades de acceso telefónico 67

LISTA DE SÍMBOLOS

Símbolo	Significado
GB	Gigabyte
GHz	Gigahertz
MB	Megabyte
MHz	Megahertz

GLOSARIO

Internet Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP que garantiza que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

Intranet Es una red de ordenadores privados que utiliza tecnología Internet para compartir de forma segura cualquier información o programa del sistema operativo para evitar que cualquier usuario de Internet pueda ingresar.

Red irregular Es un sistema de cables y buses que se conectan a través de un módem y que da como resultado la conexión de una o más computadoras.

Servidor Proxy: realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones.

RESUMEN

Una red de ordenadores la integran elementos o componentes que necesitan la comunicación entre ellos; en esta tesis plantea lo necesario para la comunicación o conexión la cual se logra por medio de los dispositivos de red que permiten que fluya la información entre los diferentes dispositivos.

Generalmente se dice que existen tres categorías de redes: red de área local (LAN), red de área metropolitana (MAN) y red de área extensa (WAN).

Acceso a Internet o conexión a Internet es el sistema de enlace con que el computador, dispositivo móvil o red de computadoras cuenta para conectarse a Internet, lo que les permite visualizar las páginas web desde un navegador y acceder a otros servicios que ofrece Internet, como correo-e, mensajería instantánea, protocolo de transferencia de archivos (FTP), etcétera. Se puede acceder a Internet desde una conexión por línea conmutada, banda ancha fija (a través de cable coaxial, cables de fibra óptica o cobre), WiFi, vía satélite, banda ancha móvil y teléfonos celulares o móviles con tecnología 2G/3G/4G. Las empresas que otorgan acceso a Internet reciben el nombre de proveedores de servicios de Internet (*Internet Service Provider*, ISP).

Para la conexión de los ordenadores es necesario de los dispositivos tanto físicos y virtuales así como el conocimiento de los mismos: sus capacidades y propiedades para su mejor funcionamiento.

OBJETIVOS

General

Dar a conocer los diferentes dispositivos de red utilizados en un ambiente virtual, así como la interconexión de un ordenador a otro, el uso de dichos dispositivos haciendo un análisis y demostrar las ventajas y desventajas de este tipo de dispositivos dentro de la infraestructura de una red; también, se verá la importancia de los dispositivos para el manejo de la información en una empresa determinada ya que dicha empresa requiere de que la información llegue segura y poder dar el soporte a dicha información y así asegurar el transporte y portabilidad de los dispositivos físicos y virtuales.

Específicos

1. Describir los dispositivos de red en ambientes virtual y físico para mejorar la implementación de una red en un proyecto de infraestructura de red.

2. Describir la conexión de los diferentes dispositivos con los ordenadores en ambiente virtual así como los requisitos necesarios en cada uno de los componentes para agilizar el proceso de diseño de redes.

3. Dar a conocer las ventajas y desventajas del uso de los dispositivos en ambiente virtual sobre su contraparte física para contribuir así a la toma de decisiones de infraestructura de red.

4. Asegurar la portabilidad y uso de los dispositivos de red (físicos como virtuales) y asegurar la implementación de los diferentes dispositivos.

5. Promover el uso de los dispositivos de red físicos y virtuales indicando cual es su comportamiento con los ordenadores y el uso de la memoria.

INTRODUCCIÓN

Los dispositivos de redes son los componentes que ayudan a la conectividad de varios elementos o bien ordenadores para compartir información entre sí; en pocas palabras, no son más que la posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios; un componente vital de la era de la información.

La generalización del ordenador o computadora personal (PC) y de la red de área local (LAN) durante la década de los ochenta ha dado lugar a la posibilidad de acceder a información en bases de datos remotas, cargar aplicaciones desde puntos de ultramar, enviar mensajes a otros países y compartir archivos; todo desde un ordenador personal.

Las redes que permiten todo esto son equipos avanzados y complejos. Su eficacia se basa en la confluencia de muy diversos componentes. El diseño e implantación de una red mundial de ordenadores es uno de los grandes milagros tecnológicos de las últimas décadas sin hacer de menos los dispositivos de red en un ambiente virtual lo cual se considera esencial en esta tesis.

1. ¿QUÉ ES UNA RED DE COMPUTADORA?

1.1. Red de computadoras

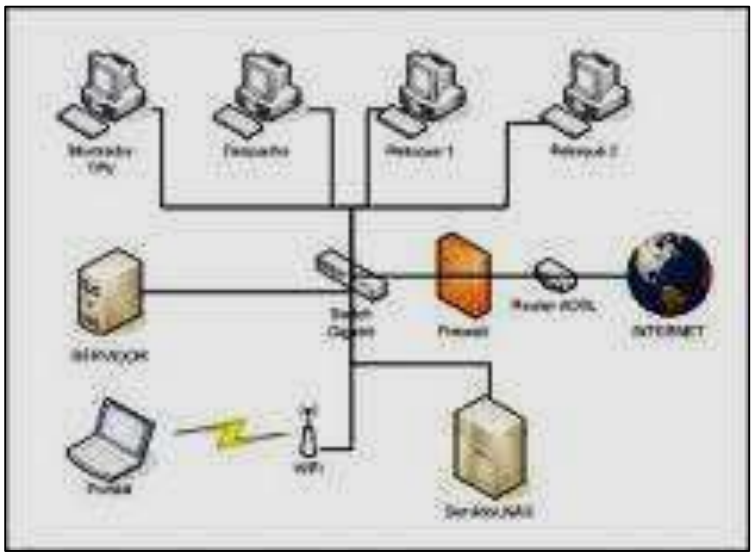
Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras), servicios (acceso a internet, e-mail, chat, juegos).

Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos (no jerárquica -master/slave-). Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios de transmisión (aire, vacío, cable de cobre, cable de fibra óptica).

1.2. Red de computadora

Es un conjunto de equipos (computadoras y o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información

Figura 1. **Red de computadoras**

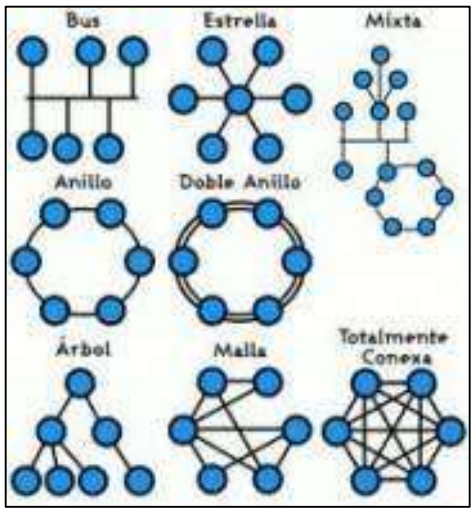


Fuente*: Red de computadoras*. https://www.ecured.cu/Red_de_computadoras. Consulta: 10 de enero de 2017.

1.3. Clasificación de redes

Para simplificar la comunicación entre programas (aplicaciones) de distintos equipos, se definió el modelo OSI por la ISO que especifica 7 distintas capas de abstracción. Con ello, cada capa desarrolla una función específica con un alcance definido.

Figura 2. **Clasificación de redes**



Fuente: *Clasificación de redes*. https://redesadsi.files.wordpress.com/2008/06/topologia-de-la-red.png. Consulta: 10 de enero de 2017.

- Por alcance:
  - Red de área personal (PAN)
  - Red de área local (LAN)
  - Red de área de campus (CAN)
  - Red de área metropolitana (MAN)
  - Red de área amplia (WAN)
  - Red de área simple (SPL)
  - Red de área de almacenamiento (SAN)

- Por método de la conexión
  - Medios guiados: cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables.
  - Medios no guiados: radio, infrarrojos, microondas, láser y otras redes inalámbricas.

- Por relación funcional
  - Cliente-servidor
  - Igual-a-igual (P2p)

- Por topología de red
  - Red en bus
  - Red en estrella
  - Red en anillo (o doble anillo)
  - Red en malla (o totalmente conexa)
  - Red en árbol
  - Red mixta (cualquier combinación de las anteriores)

- Por la direccionalidad de los datos (tipos de transmisión)
  - Simplex (unidireccionales): un equipo terminal de datos transmite y otro recibe. (p. ej. streaming)

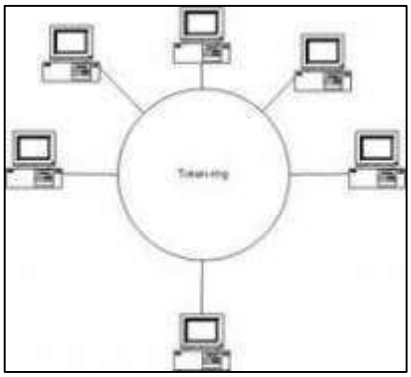
  - Half-duplex (bidireccionales): solo un equipo transmite a la vez. También se llama semi-duplex (p. ej. una comunicación por equipos de radio, si los equipos no son *full dúplex*, uno no podría transmitir (hablar) si la otra persona está también transmitiendo (hablando) porque su equipo estaría recibiendo (escuchando) en ese momento).

  - *Full-duplex* (bidireccionales): ambos pueden transmitir y recibir a la vez una misma información. (p. ej. videoconferencia).

1.4. Protocolo de redes

El protocolo de red o también protocolo de comunicación es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red.

Figura 3. **Protocolos de redes**



Fuente: *Protocolo de redes.*
https://sites.google.com/site/fundamentosderedesuteztic1h/protocolos-pop-imap-y-smtp.
Consulta: 10 de enero de 2017.

- Estándares de redes:

- IEEE 802.3, estándar para Ethernet
- IEEE 802.5, estándar para Token Ring
- IEEE 802.11, estándar para Wi-Fi
- IEEE 802.15, estándar para Bluetooth

Algunas tecnologías relacionadas: AppleTalk, ATM, Bluetooth, DECnet, FDDI, Frame Relay, HIPPI, PPP, HDLC, BGAN.

Para la disciplina científica y la ingeniería que estudia las redes de ordenadores, una red de ordenadores es el conjunto de ordenadores conectados junto con un sistema de telecomunicaciones con el fin de comunicarse y compartir recursos e información.

Expertos en la materia de discusión del establecimiento de una red dicen que si dos ordenadores están conectados entre sí en forma de medio de comunicaciones constituyen una red. Sin embargo, unos afirman que una red se constituye de tres ordenadores conectados o más.

Por ejemplo, telecommunications: glossary of telecommunication terms (traducido al español, *Telecomunicaciones: glosario de términos de telecomunicación)* explica que una red de ordenadores "es *una red de los* nodos de procesamiento de datos que se interconectan con el fin de la comunicación *de datos*, del término *red* que se define en el mismo documento como *una* interconexión *de tres entidades o más que se comunican"*.

Un ordenador conectado a un dispositivo (conectado a una impresora vía Ethernet, por ejemplo) también puede representar una red de ordenadores, aunque este artículo no trata de dicha configuración.

Este artículo define que se requiere por lo menos de dos ordenadores para formar una red. Las mismas funciones básicas de este caso se pueden aplicar a redes más grandes.

1.5. Componentes básicos de las redes de ordenadores

- El ordenador

La mayoría de los componentes de una red media son los ordenadores individuales, también denominados host; generalmente son sitios de trabajo o servidores.

- Tarjetas de red

Para lograr el enlace entre las computadoras y los medios de transmisión (cables de red o medios físicos para redes alámbricas e infrarojos ó radiofrecuencias para redes inalámbricas), es necesaria la intervención de una tarjeta de red o NIC (*network card interface*) con la cual se puedan enviar y recibir paquetes de datos desde y hacia otras computadoras, empleando un protocolo para su comunicación y convirtiendo esos datos a un formato que pueda ser transmitido por el medio (bits 0's/1's). Cabe señalar que a cada tarjeta de red le es asignado un identificador único por su fabricante, conocido como dirección MAC (m*edia access control*), que consta de 48 Bits (6 Bytes). Dicho identificador permite direccionar el tráfico de datos de la red del emisor al receptor adecuados.

El trabajo del adaptador de red es el de convertir las señales eléctricas que viajan por el cable (ej: red Ethernet) o las ondas de radio (ej: red wifi) en una señal que pueda interpretar el ordenador.

Estos adaptadores son unas tarjetas PCI que se conectan en las ranuras de expansión del ordenador. En el caso de ordenadores portátiles, estas tarjetas vienen en formato PCMCIA. En algunos ordenadores modernos, tanto de sobremesa como portátiles, estas tarjetas ya vienen integradas en la placa base.

Adaptador de red es el nombre genérico que reciben los dispositivos encargados de realizar dicha conversión. Esto significa que estos adaptadores pueden ser tanto Ethernet, como Wireless, así como de otros tipos como fibra

óptica, coaxial, etc. También las velocidades disponibles varían según el tipo de adaptador; estas pueden ser, en Ethernet, de 10, 100 o 1000 Mbps, y en los inalámbricos de 11 o 55 Mbps.

1.6. Tipos de sitios de trabajo

Hay muchos tipos de sitios de trabajo que se pueden incorporar en una red particular, algo de la cual tiene exhibiciones *high-end*, sistemas con varios CPU, las grandes cantidades de RAM, las grandes cantidades de espacio de almacenamiento en disco duro, u otros componentes requeridos para las tareas de proceso de datos especiales, los gráficos u otros usos intensivos del recurso.

1.7. Tipos de servidores

En las siguientes listas hay algunos tipos comunes de servidores y sus propósitos.

- Servidor de archivos: almacena varios tipos de archivo y los distribuye a otros clientes en la red.

- Servidor de impresiones: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada directamente con el puerto de impresora del sitio de trabajo.

- Servidor de correo: almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con *e-mail* para los clientes de la red.

- Servidor de fax: almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.

- Servidor de la telefonía: realiza funciones relacionadas con la telefonía, como la de contestador automático, realiza las funciones de un sistema interactivo para la respuesta de la voz, almacena los mensajes de voz, encamina las llamadas y controla también la red o el Internet; p. ej., la entrada excesiva del IP de la voz (VoIP).

- Servidor proxy: realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones (p. ej., *prefetching* y depositar documentos u otros datos que se soliciten muy frecuentemente). También sirve seguridad; esto es, tiene un firewall (cortafuegos). Permite administrar el acceso a internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios web.

- Servidor del acceso remoto (RAS): controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responden llamadas telefónicas entrantes o reconocen la petición de la red y realizan los chequeos necesarios de seguridad y otros procedimientos necesarios para registrar a un usuario en la red.

- Servidor de uso: realiza la parte lógica de la informática o del negocio de un uso del cliente; acepta las instrucciones para que se realicen las

operaciones de un sitio de trabajo y sirve los resultados a su vez al sitio de trabajo, mientras que el sitio de trabajo realiza el interfaz operador o la porción del GUI del proceso (es decir, la lógica de la presentación) que se requiere para trabajar correctamente.

- Servidor web: almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido) y distribuye este contenido a clientes que la piden en la red.

- Servidor de reserva: tiene el software de reserva de la red instalado y tiene cantidades grandes de almacenamiento de la red en discos duros u otras formas del almacenamiento (cinta) disponibles para que se utilice con el fin de asegurarse de que la pérdida de un servidor principal no afecte a la red. Esta técnica también es denominada *clustering*.

- Impresoras: muchas impresoras son capaces de actuar como parte de una red de ordenadores sin ningún otro dispositivo, como un *print server*, a actuar como intermediario entre la impresora y el dispositivo que está solicitando un trabajo de impresión de ser terminado.

- Terminal: muchas redes utilizan este tipo de equipo en lugar de puestos de trabajo para la entrada de datos. En estos solo se exhiben datos o se introducen. Este tipo de terminales, trabajan contra un servidor el que realmente procesa los datos y envía pantallas de datos a los terminales.

- Otros dispositivos: hay muchos otros tipos de dispositivos que se pueden utilizar para construir una red, muchos de los cuales requieren una comprensión de conceptos más avanzados del establecimiento de una red

de la computadora antes de que puedan ser entendidos fácilmente (los cubos, las rebajadoras, los puentes, los interruptores, los cortafuegos del hardware). En las redes caseras y móviles, que conecta la electrónica del consumidor con los dispositivos, como consolas de vídeo juegos, está llegando a ser cada vez más comunes.

- Servidor de autenticación: es el encargado de verificar que un usuario pueda conectarse a la red en cualquier punto de acceso, ya sea inalámbrico o por cable, basado en el estándar 802.1x; puede ser un servidor de tipo RADIUS.

- Servidor DNS: este tipo de servidor resuelve nombres de dominio sin necesidad de conocer su dirección IP.

1.8. Tipos de redes

- Red pública: una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectados capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

- Red privada: una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.

- Red de área personal (PAN): (*personal área network*) es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las ayudantes digitales personales)

cerca de una persona. Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. El alcance de una PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación entre los dispositivos personales de ellos mismos (comunicación del intrapersonal), o para conectar con una red de alto nivel y el Internet (un *up link*). Las redes personales del área se pueden conectar con cables con los buses de la computadora tales como USB y FireWire. Una red personal sin hilos del área (WPAN) se puede también hacer posible con tecnologías de red como IrDA y Bluetooth.

- Red de área local (LAN): una red que se limita a un área especial relativamente pequeña como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de la localización. Nota: para los propósitos administrativos, una LAN grande se divide generalmente en segmentos lógicos más pequeños llamados Workgroups. Un Workgroups es un grupo de las computadoras que comparten un sistema común de recursos dentro de un LAN.

- Red de área local virtual (VLAN): una Virtual LAN o comúnmente conocida como VLAN, es un grupo de computadoras, con un conjunto común de recursos a compartir y de requerimientos, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos los nodos pueden alcanzar a los otros por medio de Broadcast en la capa de enlace de datos, a pesar de su diversa localización física. Con esto, se pueden lógicamente agrupar computadoras para que la localización de la red ya no sea tan asociada y restringida a la localización física de cada computadora, como sucede con una LAN, otorgando además seguridad, flexibilidad y ahorro de recursos. Para lograrlo, se ha establecido la especificación IEEE 802.1Q como un estándar diseñado

para dar dirección al problema de cómo separar redes físicamente muy largas en partes pequeñas, así como proveer un alto nivel de seguridad entre segmentos de redes internas teniendo la libertad de administrarlas sin importar su ubicación física.

- Red del área del campus (CAN): se deriva a una red que conecta dos o más LAN que deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.

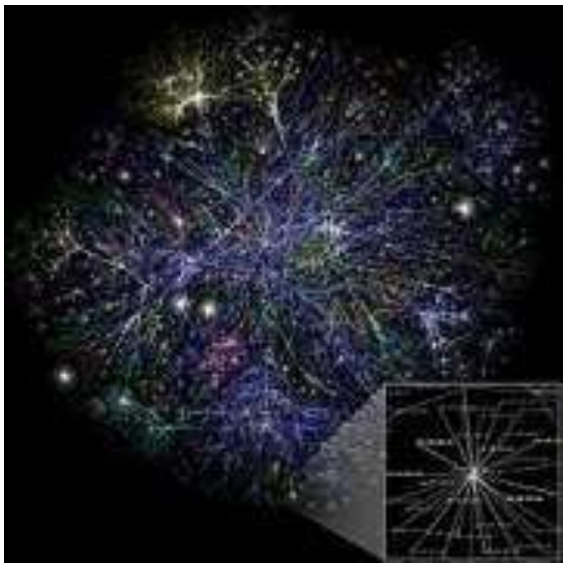
- Red de área metropolitana (MAN): una red que conecta las redes de un área de dos o más locales juntos pero no extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Los enrutadores (routers) múltiples, los interruptores (switch) y los cubos están conectados para crear a una MAN.

- Red de área amplia (WAN): es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, como compañías del teléfono. Las tecnologías WAN funcionan generalmente en las tres capas más bajas del modelo de referencia OSI: la capa física, la capa de enlace de datos y la capa de red.

- Red de área de almacenamiento (SAN): Es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología de fibra o iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos de almacenamiento que la conforman.

- Red irregular: es un sistema de cables y buses que se conectan a través de un módem, y que da como resultado la conexión de una o más computadoras. Esta red es parecida a la mixta, solo que no sigue con los parámetros presentados en ella. Muchos de estos casos son muy usados en la mayoría de las redes.

Figura 4. **Ejemplos de redes**



Fuente: *Ejemplo de redes.* https://www.ecured.cu/Red_de_computadoras. Consulta: 11 de enero de 2017.

1.8.1. Red interna

Dos o más redes o segmentos de la red conectados con los dispositivos que funcionan en la capa 3 (la capa de la red) del modelo de la referencia básica de la OSI, tal como un router. Nota: cualquier interconexión entre las redes del público, privadas, comerciales, industriales, o gubernamentales se puede también definir como red interna.

1.8.2. Intranet

Una Intranet es una red de ordenadores privados que utiliza tecnología Internet para compartir de forma segura cualquier información o programa del sistema operativo para evitar que cualquier usuario de Internet pueda ingresar. En la arquitectura que el software servidor se ejecuta en una Intranet anfitriona. No es necesario que estos dos software, el cliente y el servidor, sean ejecutados en el mismo sistema operativo. Podría proporcionar una comunicación privada y exitosa en una organización.

1.8.3. Internet

Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

1.9. Construcción de una red de computadoras

1.9.1. Una red simple

Una red de computadoras sencilla se puede construir de dos ordenadores agregando un adaptador de la red (controlador de interfaz de red (NIC)) a cada ordenador y conectándolos mediante un cable especial llamado cable cruzado (el cual es un cable de red con algunos cables invertidos, para evitar el uso de un *router* o *switch*). Este tipo de red es útil para transferir información entre dos

ordenadores que normalmente no se conectan entre sí por una conexión de red permanente o para usos caseros básicos del establecimiento de red.

Alternativamente, una red entre dos computadoras se puede establecer sin aparato dedicado adicional, usando una conexión estándar, tal como el puerto serial RS-232 en ambos ordenadores, conectándolos entre sí vía un cable especial cruzado nulo del módem.

En este tipo de red solo es necesario configurar una dirección IP, pues no existe un servidor que les asigne IP automáticamente.

En el caso de querer conectar más de dos ordenadores, o con vista a una posible ampliación de la red, es necesario el uso de un concentrador que se encargará de repartir la señal y el ancho de banda disponible entre los equipos conectados a él.

Simplemente le llega el paquete de datos al concentrador, el cual lo reenvía a todos los equipos conectados a él; el equipo destinatario del paquete lo recoge, mientras que los demás simplemente lo descartan.

Esto afecta negativamente al rendimiento de la red, ya que solo se puede enviar un paquete a la vez, por lo que mientras ese paquete se encuentra en circulación ningún otro paquete será enviado.

1.9.2. Redes prácticas

Redes prácticas constan generalmente de más de dos ordenadores interconectados y generalmente requieren dispositivos especiales además del controlador de interfaz de red con el cual cada ordenador se debe equipar.

Ejemplos de algunos de estos dispositivos especiales son los concentrador (hubs), multiplexor (switches) y enrutador (routers).

Las características más importantes que se utilizan para describir una red son: velocidad, seguridad, disponibilidad, escalabilidad y confiabilidad. La consideración de estas características permite dimensionar de manera adecuada una red de computadoras solucionando las necesidades de los usuarios.

- Velocidad: es una medida de la rapidez con que los datos son transmitidos sobre la red.
- Seguridad: indica el grado de seguridad de la red incluyendo los datos que son transmitidos por ella.
- Disponibilidad: es una medida de la probabilidad de que la red va a estar disponible para su uso.
- Escalabilidad: indica la capacidad de la red de permitir más usuarios y requerimientos de transmisión de datos.
- Confiabilidad: es una medida de la probabilidad de falla.

1.10. Componentes básicos de una red

Es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos que utilizan distintas tecnologías de hardware/software.

1.10.1. Software

Dentro de la categoría de software de aplicación están incluidos los procesadores de texto como LibreOffice Writer (arriba) y los editores gráficos rasterizados como Krita (abajo).

Figura 5. **Buscador de Programas en Ubuntu 13.10**

Fuente: *Buscador de Programas en Ubuntu 13.10.* https://es.wikipedia.org/wiki/Archivo:Buscador_de_Programas_en_Ubuntu_13.10.png. Consulta: 11 de enero de 2017.

Se conoce como software al equipo lógico o soporte lógico de un sistema informático que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

Los componentes lógicos incluyen, entre muchos otros, las aplicaciones informáticas, tales como el procesador de texto, que permite al usuario realizar todas las tareas concernientes a la edición de textos; el llamado software de sistema, tal como el sistema operativo, que básicamente, permite al resto de los programas funcionar adecuadamente, facilitando también la interacción entre los componentes físicos y el resto de las aplicaciones, y proporcionando una interfaz con el usuario.

El anglicismo software es el más ampliamente difundido al referirse a este concepto, especialmente en la jerga técnica; en tanto que el término sinónimo

logicial, derivado del término francés *logiciel*, es utilizado mayormente en países y zonas de influencia francesa. Su abreviatura es Sw.

1.10.1.1. Definición de software

Existen varias definiciones similares aceptadas para software, pero probablemente la más formal sea la siguiente:

Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación.

1.10.1.2. Extraído del estándar 729 del IEEE

Considerando esta definición, el concepto de software va más allá de los programas de computación en sus distintos estados: código fuente, binario o ejecutable; también su documentación, los datos a procesar e incluso la información de usuario forman parte del software: es decir, abarca todo lo intangible, todo lo no físico relacionado.

El término software fue usado por primera vez en este sentido por John W. Tukey en 1957. En la ingeniería de software y las ciencias de la computación, el software es toda la información procesada por los sistemas informáticos: programas y datos.

El concepto de leer diferentes secuencias de instrucciones (programa) desde la memoria de un dispositivo para controlar los cálculos fue introducido por Charles Babbage como parte de su máquina diferencial. La teoría que forma la base de la mayor parte del software moderno fue propuesta por Alan Turing en

su ensayo de 1936, Los números computables, con una aplicación al problema de decisión.

1.10.2. Clasificación del software

Si bien esta distinción es, en cierto modo, arbitraria, y a veces confusa, a los fines prácticos se puede clasificar al software en tres tipos:

- Software de sistema: su objetivo es desvincular adecuadamente al usuario y al programador de los detalles del sistema informático en particular que se use, aislándolo especialmente del procesamiento referido a las características internas de: memoria, discos, puertos y dispositivos de comunicaciones, impresoras, pantallas, teclados, etc. El software de sistema le procura al usuario y programador adecuadas interfaces de alto nivel, controladores, herramientas y utilidades de apoyo que permiten el mantenimiento del sistema global. Incluye entre otros:

    - Sistemas operativos
    - Controladores de dispositivos
    - Herramientas de diagnóstico
    - Herramientas de corrección y optimización
    - Servidores
    - Utilidades

- Software de programación: es el conjunto de herramientas que permiten al programador desarrollar programas de informática, usando diferentes alternativas y lenguajes de programación, de una manera práctica. Incluyen en forma básica:

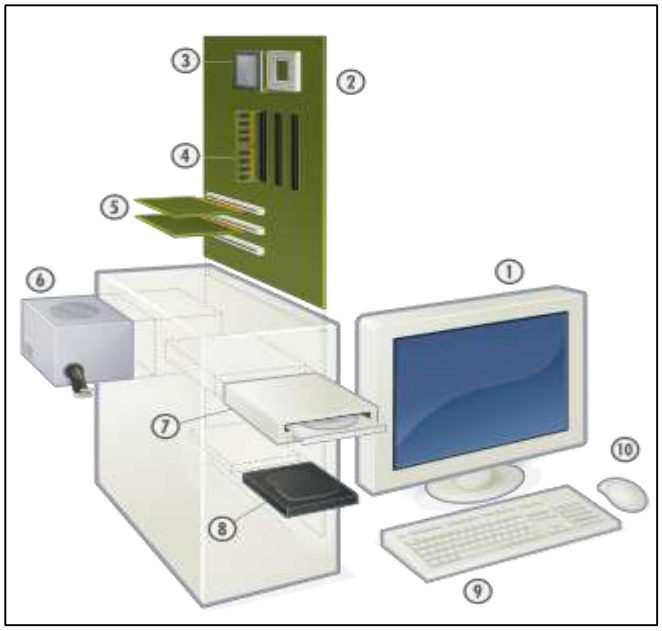
- Editores de texto.
- Compiladores.
- Intérpretes.
- Enlazadores.
- Depuradores.
- Entornos de desarrollo integrados (IDE): agrupan las anteriores herramientas, usualmente en un entorno visual, de forma tal que el programador no necesite introducir múltiples comandos para compilar, interpretar, depurar, etc. Habitualmente cuentan con una avanzada interfaz gráfica de usuario (GUI).

- Software de aplicación: es aquel que permite a los usuarios llevar a cabo una o varias tareas específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido, con especial énfasis en los negocios. Incluye entre muchos otros:

  - Aplicaciones para Control de sistemas y automatización industrial.
  - Aplicaciones ofimáticas.
  - Software educativo.
  - Software empresarial.
  - Bases de datos.
  - Telecomunicaciones (por ejemplo Internet y toda su estructura lógica).
  - Videojuegos.
  - Software médico.
  - Software de cálculo numérico y simbólico.
  - Software de diseño asistido (CAD).
  - Software de control numérico (CAM).

- Hardware
  - Monitor.
  - Placa principal.
  - Microprocesador (CPU) y zócalo.
  - Un módulo de RAM y tres ranuras.
  - Dos tarjetas de expansión y tres ranuras.
  - Fuente de alimentación.
  - Unidad de disco óptico (CD; DVD; BD).
  - Unidad de disco duro ó unidad de estado sólido.
  - Teclado.
  - Ratón.

Figura 6. **Hardware típico de una computadora personal**



Fuente: *Hardware típico de una computadora personal.* https://es.wikipedia.org/wiki/Hardware. Consulta: 12 de enero de 2017.

La palabra hardware en informática se refiere a las partes físicas tangibles de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos. Cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado componen el hardware; contrariamente, el soporte lógico e intangible es el llamado software.

El término es propio del idioma inglés, su traducción al español no tiene un significado acorde, por tal motivo se lo ha adoptado tal cual es y suena. La Real Academia Española lo define como “Conjunto de los componentes que integran la parte material de una computadora”. El término, aunque sea lo más común, no solamente se aplica a las computadoras, también es a menudo utilizado en otras áreas de la vida diaria y la tecnología. Por ejemplo, hardware también se refiere a herramientas y máquinas, y en electrónica hardware se refiere a todos los componentes electrónicos, eléctricos, electromecánicos, mecánicos, cableados y tarjetas de circuito impreso o PCB. También, se considera al hardware como uno de tres pilares fundamentales en diseño electrónico. Otros ejemplos donde se aplica el término hardware son: un robot , un teléfono móvil, una cámara fotográfica, un reproductor multimedia o cualquier otro dispositivo electrónico. Cuando dichos dispositivos procesan datos poseen además de hardware, firmware y/o software.

La historia del hardware de computador se puede clasificar en cuatro generaciones, cada una caracterizada por un cambio tecnológico de importancia. Una primera delimitación podría hacerse entre hardware principal, como el estrictamente necesario para el funcionamiento normal del equipo, y el complementario, como el que realiza funciones específicas.

Un sistema informático se compone de una unidad central de procesamiento (UCP o CPU), encargada de procesar los datos, uno o varios

periféricos de entrada, los que permiten el ingreso de la información y uno o varios periféricos de salida, que posibilitan dar salida (normalmente en forma visual o auditiva) a los datos procesados. Su abreviatura es Hw.

2. TIPOS DE RED

2.1. Tipos de redes

Diferentes tipos de redes

- Redes LAN
- Redes MAN
- Redes WAN

2.1.1. Diferentes tipos de redes

Se distinguen diferentes tipos de redes (privadas) según su tamaño (en cuanto a la cantidad de equipos), su velocidad de transferencia de datos y su alcance. Las redes privadas pertenecen a una misma organización. Generalmente, se dice que existen tres categorías de redes: red de área local (LAN), red de área metropolitana (MAN) y red de área extensa (WAN).

Existen otros dos tipos de redes: TAN (red de área diminuta), igual que la LAN pero más pequeña (de 2 a 3 equipos); y CAN (red de campus), igual que la MAN (con ancho de banda limitado entre cada una de las LAN de la red).

2.1.1.1. Redes LAN

LAN significa red de área local. Es un conjunto de equipos que pertenecen a la misma organización y, además, están conectados dentro de un área geográfica pequeña mediante algún tipo de cableado de red, generalmente con la misma tecnología (la más utilizada es Ethernet).

La versión más simple de una red es una red de área local. La transferencia de información en una red de área local puede alcanzar hasta 10 Mbps de velocidad (por ejemplo, en una red tipo Ethernet) y 1 Gbps (por ejemplo, en redes FDDI o Gigabit Ethernet). Una red de área local puede soportar 100 o incluso 1000 usuarios.

Al extender la definición de una red LAN con los servicios que ofrece, se pueden definir dos modos operativos diferentes: de igual a igual y cliente/servidor. En una red de igual a igual, la comunicación se realiza de un equipo a otro, sin un equipo central y en el que cada equipo tiene la misma función, mientras que en un entorno cliente/servidor, un equipo central brinda servicios de red para los usuarios.

2.1.2. Redes MAN

Una MAN (red de área metropolitana) interconecta diversas LAN cercanas geográficamente (en un área de unos cincuenta kilómetros) a alta velocidad. Por tanto, una MAN permite que dos nodos remotos se comuniquen como si formaran parte de la misma red de área local.

Una MAN está conformada por conmutadores o *routers* conectados entre sí mediante conexiones de alta velocidad (generalmente cables de fibra óptica).

2.1.2.1. Redes WAN

Una WAN (red de área extensa) conecta múltiples LAN entre sí a través de grandes distancias geográficas. La velocidad disponible en una red WAN varía según el costo de las conexiones (que se incrementa con la distancia) y puede ser más reducida. Este tipo de red funciona con *routers*, que pueden elegir la ruta

más apropiada para que los datos lleguen a un nodo (punto) de la red. La WAN más conocida es Internet.

2.1.3. Redes inalámbricas vrs alámbricas

Se entiende por red al conjunto interconectado de computadoras autónomas. Es decir, es un sistema de comunicaciones que conecta a varias unidades y que les permite intercambiar información. La red permite comunicarse con otros usuarios y compartir archivos y periféricos.

Figura 7. **Redes**

Fuente: *Redes.* http://redesinaalam.blogspot.com/. Consulta: 12 de enero de 2017.

La conexión no necesita hacerse a través de un hilo de cobre, también puede hacerse mediante el uso de láser, microondas y satélites de comunicación.

2.1.4. Redes inalámbricas

Las redes inalámbricas no son más que un conjunto de computadoras, o de cualquier dispositivo informático comunicados entre sí mediante soluciones que no requieran el uso de cables de interconexión.

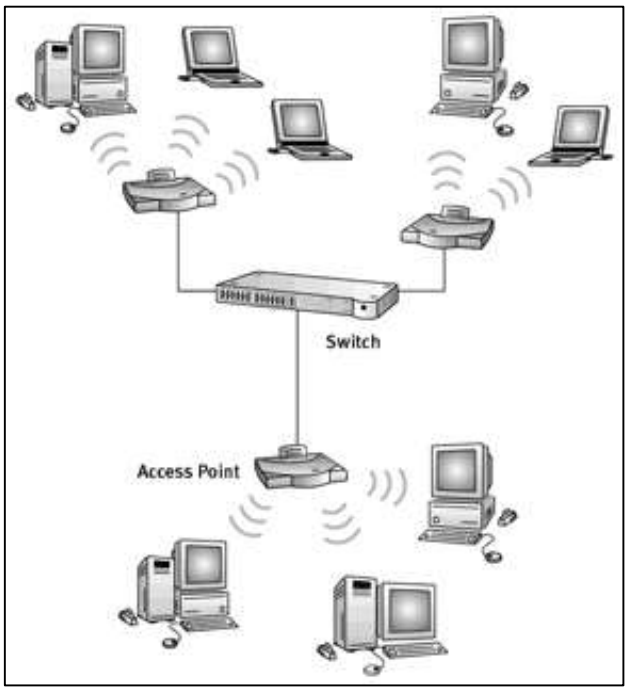
En el caso de las redes locales inalámbricas, el sistema que se está imponiendo es el normalizado por IEEE con el nombre 802.11b. A esta norma se la conoce más habitualmente como WI-FI (Wiriless Fidelity).

Con el sistema WI-FI se pueden establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzándose distancia de hasta cientos de metros. No obstante, versiones más recientes de esta tecnología permiten alcanzar los 22, 54 y hasta los 100 Mbps.

2.1.4.1. La velocidad de las redes inalámbricas

La velocidad máxima de transmisión inalámbrica de la tecnología 802.11b es de 11 Mbps. Pero la velocidad típica es solo la mitad: entre 1,5 y 5 Mbps dependiendo de si se transmiten muchos archivos pequeños o unos pocos archivos grandes. La velocidad máxima de la tecnología 802.11g es de 54 Mbps. Pero la velocidad típica de esta última tecnología es solo unas 3 veces más rápida que la de 802.11b: entre 5 y 15 Mbps.

Figura 8. **Redes inalámbricas**



Fuente: *Redes inalámbricas.* http://redesinaalam.blogspot.com/. Consulta: 12 de enero de 2017.

2.1.4.2. Ventajas de las redes inalámbricas

- Flexibilidad

Dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar y no estarán atados a un cable para poder estar comunicados por el mundo. Por ejemplo, para hacer esta presentación se podría haber colgado la presentación de la web y haber traído simplemente el portátil y abrirla desde Internet incluso aunque la oficina en la que estuviésemos no tuviese rosetas de acceso a la red cableada.

- Poca planificación

Con respecto a las redes cableadas. Antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas, mientras que con una red inalámbrica solo se tiene que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.

- Diseño

Los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, entre otros.

- Robustez

Ante eventos inesperados que pueden ir desde un usuario que se tropieza con un cable o lo desenchufa hasta un pequeño terremoto o algo similar. Una red cableada podría llegar a quedar completamente inutilizada, mientras que una red inalámbrica puede aguantar bastante mejor este tipo de percances inesperados.

2.1.4.3. Inconvenientes de las redes inalámbricas

- Calidad de servicio

Las redes inalámbricas ofrecen una peor calidad de servicio que las redes cableadas. Velocidades que no superan habitualmente los 10 Mbps, frente a los 100 que puede alcanzar una red normal y corriente. Por otra parte, hay que tener en cuenta también la tasa de error debida a las interferencias. Esta se puede situar alrededor de 10-4 frente a las 10-10 de las redes cableadas. Esto significa que hay 6 órdenes de magnitud de diferencia y eso es mucho. Se refiere a 1 bit

erróneo cada 10.000 bits o lo que es lo mismo, aproximadamente de cada Megabit transmitido, 1 Kbit será erróneo. Esto puede llegar a ser imposible de implantar en algunos entornos industriales con fuertes campos electromagnéticos y ciertos requisitos de calidad.

- Coste

Aunque cada vez se está abaratando bastante, aún sale bastante más caro. Recientemente en una revista comentaban que puede llegar a salir más barato montar una red inalámbrica de 4 ordenadores que una cableada si se tiene en cuenta costes de cablear una casa. El ejemplo era para una casa, aunque, todo hay que decirlo, estaba un poco forzado. Aún no merece la pena debido a la poca calidad de servicio, falta de estandarización y coste.

- Soluciones propietarias

Como la estandarización está siendo bastante lenta, ciertos fabricantes han sacado al mercado algunas soluciones propietarias que sólo funcionan en un entorno homogéneo y, por lo tanto, estando atado a ese fabricante. Esto supone un gran problema ante el mantenimiento del sistema, tanto para ampliaciones del sistema como para la recuperación ante posibles fallos. Cualquier empresa o particular que desee mantener su sistema funcionando se verá obligado a acudir de nuevo al mismo fabricante para comprar otra tarjeta, punto de enlace, entre otros.

2.1.4.4. Desventajas de las redes inalámbricas

Evidentemente, como todo en la vida, no todo son ventajas, las redes inalámbricas también tiene unos puntos negativos en su comparativa con las

redes de cable. Los principales inconvenientes de las redes inalámbricas son los siguientes:

- Menor ancho de banda

Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas wi-fi lo hacen a 11 Mbps. Es cierto que existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tiene un precio superior al de los actuales equipos wi-fi.

- Mayor inversión inicial

Para la mayoría de las configuraciones de la red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.

- Seguridad

Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Esto fundamentalmente es una ventaja, pero se convierte en una desventaja cuando se piensa que cualquier persona con una computadora portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes wi-fi no es de lo más fiables. A pesar de esto también es cierto que ofrece una seguridad válida para la inmensa mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (WPA) que hace a wi-fi mucho más confiable.

- Interferencias

Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 GAZ. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes wi-fi funcionan en la misma banda de frecuencias incluida la de los vecinos. Este hecho hace que no se tenga la garantía de nuestro entorno radioelectrónico este completamente limpio para que nuestra red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

2.2. Incertidumbre tecnológica

La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como wi-fi (IEEE 802.11B). Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad, es posible que, cuando se popularice esta nueva tecnología, se deje de comenzar la actual o, simplemente se deje de prestar tanto apoyo a la actual. Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades del cliente y, aunque existe una incógnita, los fabricantes no querrán perder el tirón que ha supuesto wi-fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales. La historia nos ha dado muchos ejemplos similares.

2.2.1. Tecnologías inalámbricas

Actualmente, las tecnologías de LAN inalámbricas comprenden de infrarrojo (IR), radio de UHF, spread spectrum y radio microondas, que van desde frecuencias en Ghz en la región de Europa (900 Mhz en los EE.UU.) a frecuencias infrarrojas. La red de comunicación personal (PCN) puede usar una banda CDMA (*code-division multiple access*) compartida, y el servicio celular digital una banda TDMA (*time-division multiple access*). Hay una controversia considerable entre los expertos en el campo, con respecto a los méritos relativos al spread spectrum (CDMA) y la banda-angosta (TDMA) para la red de comunicación privada (PCN). La técnica preferida realmente puede variar con el escenario PCN especifico hacia quien va dirigido.

- *Spread spectrum (*CDMA*):* Este término define una clase de sistemas de radios digitales en los que el ancho de banda ocupado es considerablemente mayor que la proporción de información. La técnica se propuso inicialmente para uso del ejército, donde las dificultades de descubrir o bloquear semejante signo le hicieron una opción atractiva para comunicación. El término CDMA se usa a menudo en referencia a sistemas que tienen la posibilidad de transmitir varias señales en la misma porción de espectro usando códigos pseudo-aleatorios para cada uno. Esto puede ser logrado por una serie de pulsos de frecuencias diferentes, en un modelo predeterminado o a la sucesión directa de una onda binaria pseudo-aleatoria cuya tasa de símbolos es un múltiplo mayor a la tasa de bit de la trama original.

- Time division multiple access *(*TDMA*):* El principio de TDMA es básicamente simple. Tradicionalmente, los canales de voz han sido creados dividiendo el espectro de la radio en portadores de frecuencia RF

(canales), con una conversación que ocupa un canal (dúplex). Esta técnica es conocida como FDMA (frecuency division multiple access). TDMA divide a los portadores de la radio en una sucesión repetida de pequeñas ranuras de tiempo (canales). Cada conversación ocupa justo una de estas ranuras de tiempo. Así en lugar de sólo una conversación, cada portador de la radio lleva varias conversaciones a la vez.

2.3. Parámetros que definen una red

- Topología: arreglo físico en el cual el dispositivo de red se conecta al medio.

- Medio físico: cable físico (o frecuencia del espectro electromagnético) para interconectar los dispositivos a la red.

- Protocolo de acceso al medio: reglas que determinan como los dispositivos se identifican entre sí y como accesan al medio de comunicación para envíar y recibir la información.

2.3.1. ¿Qué aporta una red inalámbrica?

El auge que actualmente vive esta tecnología se debe fundamentalmente a que es capaz de ofrecer la movilidad de la que se carece con el equipamiento tradicional, manteniendo unas prestaciones, coste y complejidad de conexión razonables; así, a efectos prácticos de aplicación, se puede considerar que una tasa de transferencia teórica que parte de los 11 Mbps permite toda una serie de aplicaciones de los entornos de trabajo más habituales, que no son grandes consumidoras de ancho de banda, tales como por ejemplo:

- Acceso a la información y la navegación web
- Consulta de correo electrónico
- Acceso a herramientas de trabajo colaborativo

El aporte de la movilidad significará un beneficio para los usuarios que, dependiendo del perfil de cada uno, podrán ganar en eficiencia, productividad o, simplemente, en la oportunidad de realizar una consulta dada en un momento dado.

En un entorno como el de la Universidad Politécnica de Valencia, en el que se dispone de una red cableada de alta densidad de puntos de conexión, se presentan a menudo diversas situaciones con una problemática especial, la cual se puede ver solucionada mediante este tipo de soluciones:

- En las áreas destinadas a la realización de convenciones, suele ser imprescindible ofertar a los asistentes de los medios de conexión adecuados.

- En salas de reunión, a menudo es necesario desplazar equipos y conexiones de red para realizar una conexión determinada.

- En las bibliotecas y salas de estudio existe una demanda creciente de puntos de conexión para equipos portátiles.

- En laboratorios y zonas dedicadas a la investigación y de acogida de profesores visitantes.

- En diferentes zonas de servicios, de encuentros e incluso de espera no es extraño echar de menos un punto de conexión.

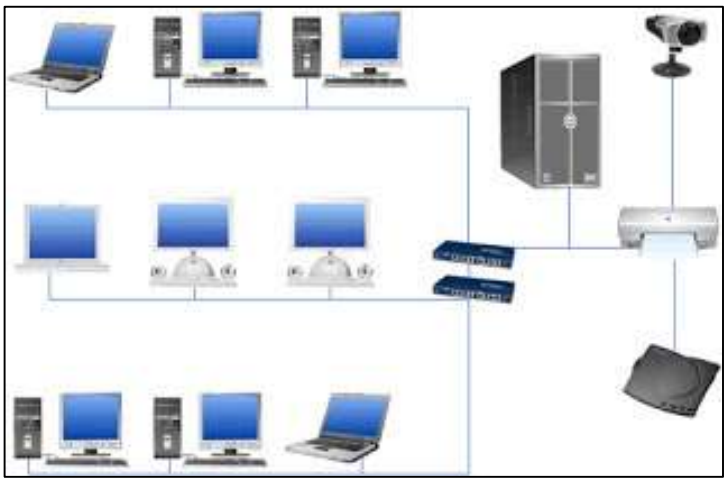
- Zonas de movilidad de estudiantes, como aulas, cafeterías e incluso jardines.

De todo ello se deduce el gran aporte que esta tecnología puede desempeñar como complemento a la red cableada tradicional.

2.4. Red alámbrica

Se comunica a través de cables de datos (generalmente basada en Ethernet). Los cables de datos, conocidos como cables de red de Ethernet o cables con hilos conductores (CAT5), conectan computadoras y otros dispositivos que forman las redes. Las redes alámbricas son mejores cuando se necesita mover grandes cantidades de datos a altas velocidades, como medios multimedia de calidad profesional.

Figura 9. **Red alámbrica**



Fuente: *Red alámbrica*. https://www.google.com.gt/search?q=red+alámbrica. Consulta: 13 de enero de 2017.

2.4.1. Ventajas de una red alámbrica

- Costos relativamente bajos
- Ofrece el máximo rendimiento posible
- Mayor velocidad – cable de Ethernet estándar hasta 100 Mbps.

2.4.2. Las desventajas de una red alámbrica

- El costo de instalación siempre ha sido un problema muy común en este tipo de tecnología, ya que el estudio de instalación, las canaletas, conectores, cables y otros no mencionados suman costos muy elevados en algunas ocasiones.

- El acceso físico es uno de los problemas más comunes dentro de las redes alámbricas. Ya que para llegar a ciertos lugares dentro de la empresa, es muy complicado el paso de los cables a través de las paredes de concreto u otros obstáculos.

- Dificultad y expectativas de expansión es otro de los problemas más comunes, ya que cuando se piensa en tener un número definidos de nodos en una oficina, la mayoría del tiempo hay necesidades de construir uno nuevo y ya no se tiene espacio en los switches instalados.

2.4.3. Velocidades de una red alámbrica

Existen diferentes estándares. Los más comunes son 802.11b y 802.11g, los cuales tienen la mayoría de los equipos (generalmente laptops) y transmite a una frecuencia de 2.4 GHz, está disponible casi universalmente con una velocidad de hasta 11 Mbps y 54 Mbps, respectivamente (de un 20 % a un 50 %

de la velocidad de las redes cableadas). Todavía está en prueba el estándar 802.11n que trabaja a 2.4 GHz a una velocidad de 108 Mbps (imagínese la misma velocidad de red cableada, pero inalámbrica).

2.4.4. Instalación y configuración

Una vez que se tiene todo el equipo, lo siguiente es instalarlo y configurar las computadoras para que se comuniquen entre ellas. Lo que se necesita hacer exactamente depende del tipo hardware que tengas.

Por ejemplo, si las computadoras ya cuentan con conexión para red, lo único que se necesitará es comprar un switch o un ruteador, los cables necesarios y configurar las computadoras para poder usarlas en las redes cableadas.

Independientemente del tipo y marca de hardware que se elija, el ruteador, switch, tarjetas de red, etc., que se compre deberá venir acompañados de las instrucciones de configuración.

Los pasos necesarios para configurar las computadoras en la red, dependerán también del sistema operativo que se utilice en las redes cableadas.

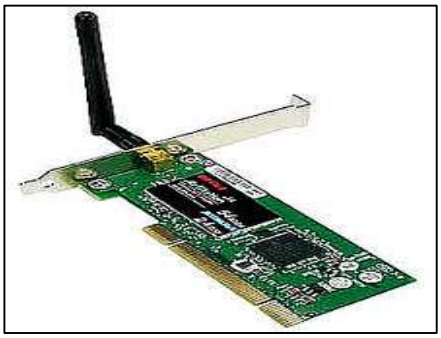
2.4.5. Tarjetas de red alámbrica y tarjeta de red inalámbrica

Las tarjetas inalámbricas funcionan sin cables, se conectan mediante señales de frecuencia específicas a otro dispositivo que sirva como concentrador de estas conexiones, en general puede ser un Access Point; estas tarjetas tienen la ventaja de poder reconocer sin necesidad de previa configuración a muchas redes siempre y cuando estén en el rango especificado. Permiten a los usuarios

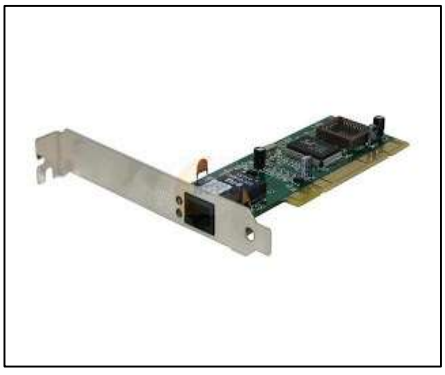
acceder a información y recursos sin necesidad de estar físicamente conectados a un determinado lugar. Las tarjetas de red alámbrica, como su nombre lo indica, tienen conexión a la red por medio de cables, antes de ser utilizadas, ocupan que las configuren, proporcionan mayor seguridad y una mayor velocidad.

Una red (en general) es un conjunto de dispositivos (de red) interconectados físicamente (ya sea vía alámbrica o vía inalámbrica) que comparten recursos y que se comunican entre sí a través de reglas (protocolos) de comunicación.

Figura 10. **Tarjetas de red alámbrica e inalámbrica**



Tarjeta de red inalámbrica



Tarjeta de red alámbrica

Fuente*: Tarjetas de red alámbrica e inalámbrica.*
https://www.google.com.gt/search?q=tarjeta+de+red+alambrica+e+inalambrica.
Consulta: 13 de enero de 2017.

3. DISPOSITIVOS DE RED

3.1. Router

También conocido como enrutador, encaminador o rúter, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red) y que, por tanto, tienen prefijos de red distintos.

- Historia

El primer dispositivo que tenía fundamentalmente la misma funcionalidad que lo que el día de hoy se entiende por encaminador, era el interface message processor o IMP. Los IMP eran los dispositivos que formaban la ARPANET, la primera red de conmutación de paquetes. La idea de un encaminador (llamado por aquel entonces puerta de enlace) vino inicialmente de un grupo internacional de investigadores en redes de computadoras llamado el International Network Working Group (INWG). Creado en 1972 como un grupo informal para considerar las cuestiones técnicas que abarcaban la interconexión de redes diferentes, se convirtió ese mismo año en un subcomité del International Federation for Information Processing.

Esos dispositivos se diferenciaban de los conmutadores de paquetes que existían previamente en dos características. Por una parte, conectaban tipos de redes diferentes, mientras que por otra parte, eran dispositivos sin conexión, que

no aseguraban fiabilidad en la entrega de datos, dejando este rol enteramente a los anfitriones. Esta última idea había sido ya planteada en la red CYCLADES.

La idea fue investigada con más detalle con la intención de crear un sistema prototipo como parte de dos programas. Uno era el promovido por DARPA, programa que creó la arquitectura TCP/IP que se usa actualmente, y el otro era un programa en Xerox PARC para explorar nuevas tecnologías de redes, que produjo el sistema llamado PARC Universal Packet. Debido a la propiedad intelectual que concernía al proyecto, recibió poca atención fuera de Xerox durante muchos años.

Un tiempo después de 1974, Xerox consiguió el primer encaminador funcional, aunque el primer y verdadero enrutador IP fue desarrollado por Virginia Stazisar en BBN, como parte de ese esfuerzo promovido por DARPA, durante 1975-76. A finales de 1976, tres encaminadores basados en PDP-11 entraron en servicio en el prototipo experimental de Internet.

El primer encaminador multiprotocolo fue desarrollado simultáneamente por un grupo de investigadores del MIT y otro de Stanford en 1981. El encaminador de Stanford se le atribuye a William Yeager y el del MIT a Noel Chiappa. Ambos estaban basados en PDP-11. Como ahora prácticamente todos los trabajos en redes usan IP en la capa de red, los encaminadores multiprotocolo son en gran medida obsoletos, a pesar de que fueron importantes en las primeras etapas del crecimiento de las redes de ordenadores, cuando varios protocolos distintos de TCP/IP eran de uso generalizado. Los encaminadores que manejan IPv4 e IPv6 son multiprotocolo, pero en un sentido mucho menos variable que un encaminador que procesaba AppleTalk, DECnet, IP, y protocolos de XeroX. Desde mediados de los años 1970 y en los años 1980, los miniordenadores de propósito general servían como enrutadores.

Actualmente, los encaminadores de alta velocidad están altamente especializados, ya que se emplea un hardware específico para acelerar las funciones de encaminamiento más específicas, como son el encaminamiento de paquetes y funciones especiales como la encriptación IPsec.

3.1.1. Funcionamiento

El funcionamiento básico de un enrutador o encaminador, como se deduce de su nombre, consiste en enviar los paquetes de red por el camino o ruta más adecuada en cada momento. Para ello almacena los paquetes recibidos y procesa la información de origen y destino que poseen. Con arreglo a esta información reenvía los paquetes a otro encaminador o bien al anfitrión final, en una actividad que se denomina 'encaminamiento'. Cada encaminador se encarga de decidir el siguiente salto en función de su tabla de reenvío o tabla de encaminamiento, la cual se genera mediante protocolos que deciden cuál es el camino más adecuado o corto, como protocolos basado en el algoritmo de Dijkstra.

Por ser los elementos que forman la capa de red, tienen que encargarse de cumplir las dos tareas principales asignadas a la misma:

- Reenvío de paquetes: cuando un paquete llega al enlace de entrada de un encaminador, éste tiene que pasar el paquete al enlace de salida apropiado. Una característica importante de los encaminadores es que no difunden tráfico difusivo.

- Encaminamiento de paquetes: mediante el uso de algoritmos de encaminamiento tiene que ser capaz de determinar la ruta que deben seguir los paquetes a medida que fluyen de un emisor a un receptor.

Por tanto, se debe distinguir entre reenvío y encaminamiento. Reenvío consiste en coger un paquete en la entrada y enviarlo por la salida que indica la tabla, mientras que por encaminamiento se entiende el proceso de hacer esa tabla.

3.1.2. Arquitectura física

En un enrutador se pueden identificar cuatro componentes:

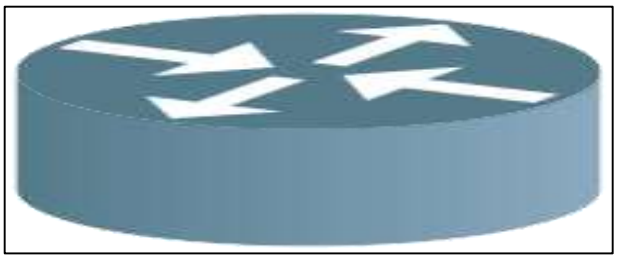
- Puertos de entrada: realiza las funciones de la capa física consistentes en la terminación de un enlace físico de entrada a un encaminador; realiza las funciones de la capa de enlace de datos necesarias para interoperar con las funciones de la capa de enlace de datos en el lado remoto del enlace de entrada; realiza también una función de búsqueda y reenvío de modo que un paquete reenviado dentro del entramado de conmutación del encaminador emerge en el puerto de salida apropiado.

- Entramado de conmutación: conecta los puertos de entrada del enrutador a sus puertos de salida.

- Puertos de salida: almacena los paquetes que le han sido reenviados a través del entramado de conmutación y los transmite al enlace de salida. Realiza entonces la función inversa de la capa física y de la capa de enlace que el puerto de entrada.

- Procesador de encaminamiento: ejecuta los protocolos de encaminamiento, mantiene la información de encaminamiento y las tablas de reenvío y realiza funciones de gestión de red dentro del enrutador.

Figura 11. **Encaminador**



Fuente: *Encaminador*. https://www.google.com.gt/search?q=encaminador. Consulta: 13 de enero de 2017.

3.2. Tipos de encaminadores

Los encaminadores pueden proporcionar conectividad dentro de las empresas, entre las empresas e Internet, y en el interior de proveedores de servicios de Internet (ISP). Los encaminadores más grandes (por ejemplo, el Alcatel-Lucent 7750 SR) interconectan ISP, se suelen llamar metro encaminador, o pueden ser utilizados en grandes redes de empresas

3.2.1. Conectividad Small Office, Home Office (SOHO)

Los encaminadores se utilizan con frecuencia en los hogares para conectar a un servicio de banda ancha, tales como IP sobre cable o ADSL. Un encaminador usado en una casa puede permitir la conectividad a una empresa a través de una red privada virtual.

Si bien son funcionalmente similares a los encaminadores, los encaminadores residenciales usan traducción de dirección de red en lugar de direccionamiento.

En lugar de conectar ordenadores locales a la red directamente, un encaminador residencial debe hacer que los ordenadores locales parezcan ser un solo equipo.

3.2.2. Encaminador de empresa

En las empresas se pueden encontrar encaminadores de todos los tamaños. Si bien los más poderosos tienden a ser encontrados en ISP, instalaciones académicas y de investigación, pero también en grandes empresas.

El modelo de tres capas es de uso común, no todos de ellos necesitan estar presentes en otras redes más pequeñas.

3.2.3. Acceso

Los encaminadores de acceso, incluyendo SOHO, se encuentran en sitios de clientes como sucursales que no necesitan de encaminamiento jerárquico de los propios. Normalmente, son optimizados para un bajo costo.

Figura 12. **Captura de pantalla de la interfaz web de LuCI OpenWrt**

Fuente: *Captura de pantalla de la interfaz web de LuCI OpenWrt.* http://tombatossals.github.io/openwrt-repetidor-wireless/. Consulta: 14 de enero de 2017.

3.2.4. Distribución

Los encaminadores de distribución agregan tráfico desde encaminadores de acceso múltiple, ya sea en el mismo lugar, o de la obtención de los flujos de datos procedentes de múltiples sitios a la ubicación de una importante empresa. Los encaminadores de distribución son a menudo responsables de la aplicación de la calidad del servicio a través de una WAN; por lo tanto, deben tener una memoria considerable, múltiples interfaces WAN y transformación sustancial de inteligencia.

También, pueden proporcionar conectividad a los grupos de servidores o redes externas. En la última solicitud, el sistema de funcionamiento del encaminador debe ser cuidadoso como parte de la seguridad de la arquitectura global. Separado del encaminador puede estar un VPN concentrador o el encaminador puede incluir estas y otras funciones de seguridad. Cuando una empresa se basa principalmente en un campus, podría no haber una clara distribución de nivel, que no sea tal vez el acceso fuera del campus.

En tales casos, los encaminadores de acceso, conectados a una red de área local (LAN), se interconectan a través del enrutador de núcleo.

3.2.5. Núcleo

En las empresas, el enrutador de núcleo puede proporcionar una columna vertebral interconectando la distribución de los niveles de los encaminadores de múltiples edificios de un campus, o a las grandes empresas locales. Tienden a ser optimizados para ancho de banda alto.

Cuando una empresa está ampliamente distribuida sin ubicación central, la función del enrutador de núcleo puede ser asumido por el servicio de WAN al que se suscribe la empresa y la distribución de encaminadores se convierte en el nivel más alto.

3.2.6. Borde

Los encaminadores de borde enlazan sistemas autónomos con las redes troncales de Internet u otros sistemas autónomos, tienen que estar preparados para manejar el protocolo BGP y si quieren recibir las rutas BGP, deben poseer una gran cantidad de memoria.

3.2.7. Encaminadores inalámbricos

A pesar de que tradicionalmente los encaminadores solían tratar con redes fijas (Ethernet, ADSL, RDSI...), en los últimos tiempos han comenzado a aparecer encaminadores que permiten realizar una interfaz entre redes fijas y móviles (Wi-Fi, GPRS, Edge, UMTS, Fritz!Box, WiMAX). Un encaminador inalámbrico comparte el mismo principio que un encaminador tradicional. La diferencia es que este permite la conexión de dispositivos inalámbricos a las redes a las que el encaminador está conectado mediante conexiones por cable. La diferencia existente entre este tipo de encaminadores viene dada por la potencia que alcanzan, las frecuencias y los protocolos en los que trabajan.

En wi-fi estas distintas diferencias se dan en las denominaciones como clase a/b/g/ y n.

Figura 13. **Equipos domésticos**

Fuente: *Equipos domesticos*. https://commons.wikimedia.org/wiki/File:Routeur-wifi.jpg. Consulta 15 de enero de 2017.

Figura 14. **Router wifi**

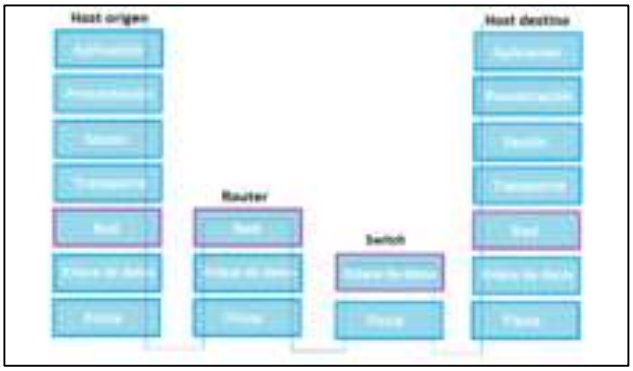
Fuente: *Router wifi.* https://commons.wikimedia.org/wiki/File:Enrutador_banda_ancha_conexiones.jpeg. Consulta: 15 de enero de 2017.

3.2.8. Enrutador sin módem, conexiones

Los equipos que actualmente se le suelen vender al consumidor de a pie como enrutadores no son simplemente eso, sino que son los llamados equipos locales del cliente (CPE). Los CPE están formados por un módem, un enrutador, un conmutador y opcionalmente un punto de acceso wifi.

Mediante este equipo se cubren las funcionalidades básicas requeridas en las 3 capas inferiores del modelo OSI.

Figura 15. **Enrutadores en el modelo OSI**



Fuente. *Enrutadores en el modelo OSI.* https://commons.wikimedia.org/wiki/File:Router_switch_in_OSI_model.png. Consulta: 15 de enero de 2017.

3.2.9. Enrutadores y conmutadores en el modelo OSI

En el modelo OSI se distinguen diferentes niveles o capas en los que las máquinas pueden trabajar y comunicarse para entenderse entre ellas. En el caso de los enrutadores hay dos tipos de interfaces:

3.2.10. Interfaces encaminadas

Son interfaces de nivel 3, accesibles por IP. Cada una se corresponde con una dirección subred distinta. En IOS se denominan IP interface. Se distinguen a su vez dos subtipos:

- Interfaces físicas: aquellas accesibles directamente por IP.
- Interfaces virtuales: aquellas que se corresponden con una VLAN o un CV. Si dicha interfaz se corresponde con una única VLAN se denomina s*witch virtual interfaz* (SVI), mientras que si se corresponde con un enlace trunk o con un CV, actúan como subinterfaces.

3.2.11. Interfaces conmutadas

Se trata de interfaces de nivel 2 accesibles solo por el módulo de conmutamiento. En IOS reciben el nombre de puertos de conmutador. Las hay de dos tipos:

- Puertos de acceso: soportan únicamente tráfico de una VLAN
- Puertos trunk: soportan tráfico de varias VLAN distintas

Estas posibilidades de configuración están únicamente disponibles en los equipos modulares, ya que en los de configuración fija, los puertos de un enrutador actúan siempre como interfaces encaminadas, mientras que los puertos de un conmutador como interfaces conmutadas. Además, la única posible ambigüedad en los equipos configurables se da en los módulos de conmutamiento, donde los puertos pueden actuar de las dos maneras, dependiendo de los intereses del usuario.

3.2.12. Conmutadores frente a enrutadores

Un conmutador, al igual que un encaminador es también un dispositivo de conmutación de paquetes de almacenamiento y reenvío. La diferencia fundamental es que el conmutador opera en la capa 2 (capa de enlace) del

modelo OSI, por lo que para enviar un paquete se basa en una dirección MAC, al contrario de un encaminador que emplea la dirección IP.

3.3. Switch

Un switch (en castellano, conmutador) es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*open systems interconnection*). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Al igual que los puentes, dado que funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local (LAN).

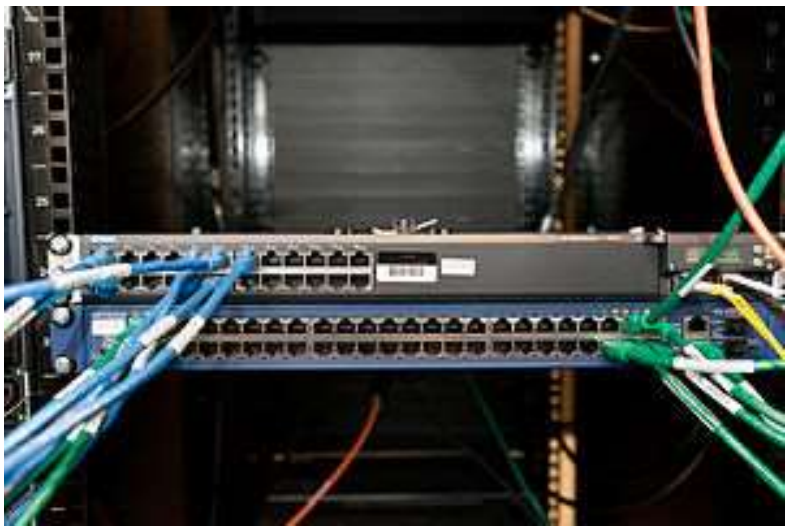
Figura 16. **Conexiones en un conmutador Ethernet**

Fuente: *Conexiones en un conmutador Ethernet.* Consulta: 18 de enero de 2017.

3.3.1. Introducción al funcionamiento de conmutadores

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de la capa 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores, la información dirigida a un dispositivo vaya desde el puerto origen al puerto de destino.

Figura 17. **Conmutadores de red Juniper (arriba) y Netgear (abajo)**



Fuente. *Conmutadores de red Juniper (arriba) y Netgear (abajo).* https://commons.wikimedia.org/wiki/File:Wikimedia_Servers-0001_42.jpg. Consulta 18 de enero de 2017.

En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los

dispositivos accesibles por sus puertos, por lo tanto, en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

- Bucles de red e inundaciones de tráfico

Como anteriormente se comentaba, uno de los puntos críticos de estos equipos son los bucles, que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de conmutadores. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten alcanzar el equipo. Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones.

- Clasificación

Atendiendo al método de direccionamiento de las tramas utilizadas *store-and-forward.*

Artículo principal: almacenamiento y reenvío.

Los conmutadores s*tore-and-forward* guardan cada trama en un búfer antes del intercambio de información hacia el puerto de salida. Mientras la trama está en el búfer, el switch calcula el CRC y mide el tamaño de la misma. Si el CRC falla, o el tamaño es muy pequeño o muy grande (una trama Ethernet tiene entre 64 bytes y 1518 bytes) la trama es descartada. Si todo se encuentra en orden es encaminada hacia el puerto de salida.

Este método asegura operaciones sin error y aumenta la confianza de la red. Pero el tiempo utilizado para guardar y chequear cada trama añade un tiempo de demora importante al procesamiento de las mismas. La demora o delay total es proporcional al tamaño de las tramas: cuanto mayor es la trama, más tiempo toma este proceso.

3.3.2. Cut-through

Artículo principal: *Conmutación cut-through.*

Los conmutadores *cut-through* fueron diseñados para reducir esta latencia. Esos switches minimizan el delay leyendo solo los 6 primeros bytes de datos de la trama, que contiene la dirección de destino MAC, e inmediatamente la encaminan.

El problema de este tipo de switch es que no detecta tramas corruptas causadas por colisiones (conocidos como *runts*), ni errores de CRC. Cuanto mayor sea el número de colisiones en la red, mayor será el ancho de banda que consume al encaminar tramas corruptas.

Existe un segundo tipo de switch *cut-through*, los denominados *fragment free*, fue proyectado para eliminar este problema. El switch siempre lee los primeros 64 bytes de cada trama, asegurando que tenga por lo menos el tamaño mínimo, y evitando el encaminamiento de runts por la red.

3.3.3. Adaptative cut-through

Son los conmutadores que procesan tramas en el modo adaptativo y son compatibles tanto con *store-and-forward* como con *cut-through*. Cualquiera de los

modos puede ser activado por el administrador de la red, o el *switch* puede ser lo bastante inteligente como para escoger entre los dos métodos, basado en el número de tramas con error que pasan por los puertos.

Cuando el número de tramas corruptas alcanza un cierto nivel, el conmutador puede cambiar del modo *cut-through* a *store-and-forward*, volviendo al modo anterior cuando la red se normalice.

Los conmutadores *cut-through* son más utilizados en pequeños grupos de trabajo y pequeños departamentos. En esas aplicaciones es necesario un buen volumen de trabajo o *throughput*, ya que los errores potenciales de red quedan en el nivel del segmento, sin impactar la red corporativa.

Los conmutadores *store-and-forward* son utilizados en redes corporativas, donde es necesario un control de errores.

Atendiendo a la forma de segmentación de las subredes.

3.3.4. Conmutadores de capa 2

Son los conmutadores tradicionales, que funcionan como puentes multi-puertos. Su principal finalidad es dividir una LAN en múltiples dominios de colisión, o en los casos de las redes en anillo, segmentar la LAN en diversos anillos. Basan su decisión de envío en la dirección MAC destino que contiene cada trama.

Los conmutadores de la capa 2 posibilitan múltiples transmisiones simultáneas sin interferir en otras subredes. Los switches de capa 2 no consiguen, sin embargo, filtrar difusiones o broadcasts, multicasts (en el caso en

que más de una subred contenga las estaciones pertenecientes al grupo multicast de destino), ni tramas cuyo destino aún no haya sido incluido en la tabla de direccionamiento.

3.3.5. Conmutadores de capa 3

Son los conmutadores que, además de las funciones tradicionales de la capa 2, incorporan algunas funciones de enrutamiento o *routing*, como por ejemplo la determinación del camino basado en informaciones de capa de red (capa 3 del modelo OSI), validación de la integridad del cableado de la capa 3 por *checksum* y soporte a los protocolos de *routing* tradicionales (RIP, OSPF, etc).

Los conmutadores de capa 3 soportan también la definición de redes virtuales (VLAN), y según modelos posibilitan la comunicación entre las diversas VLAN sin la necesidad de utilizar un router externo.

Por permitir la unión de segmentos de diferentes dominios de difusión o broadcast, los switches de capa 3 son particularmente recomendados para la segmentación de redes LAN muy grandes, donde la simple utilización de switches de capa 2 provocaría una pérdida de rendimiento y eficiencia de la ADSL, debido a la cantidad excesiva de broadcasts.

Se puede afirmar que la implementación típica de un switch de capa 3 es más escalable que un enrutador, pues este último utiliza las técnicas de enrutamiento a nivel 3 y enrutamiento a nivel 2 como complementos, mientras que los switches sobreponen la función de enrutamiento encima del encaminamiento, aplicando el primero donde sea necesario.

3.3.6. Conmutadores de capa 4

Están en el mercado hace poco tiempo y hay una controversia en relación con la clasificación adecuada de estos equipos. Muchas veces son llamados de l*ayer 3*+ (l*ayer 3 plus*).

Básicamente, incorporan a las funcionalidades de un conmutador de la capa 3; la habilidad de implementar la políticas y filtros a partir de informaciones de la capa 4 o superiores, como puertos TCP/UDP, SNMP, FTP, entre otros.

3.3.7. Conmutadores de capa 5

Dentro de los conmutadores de la capa 5 se tienen:

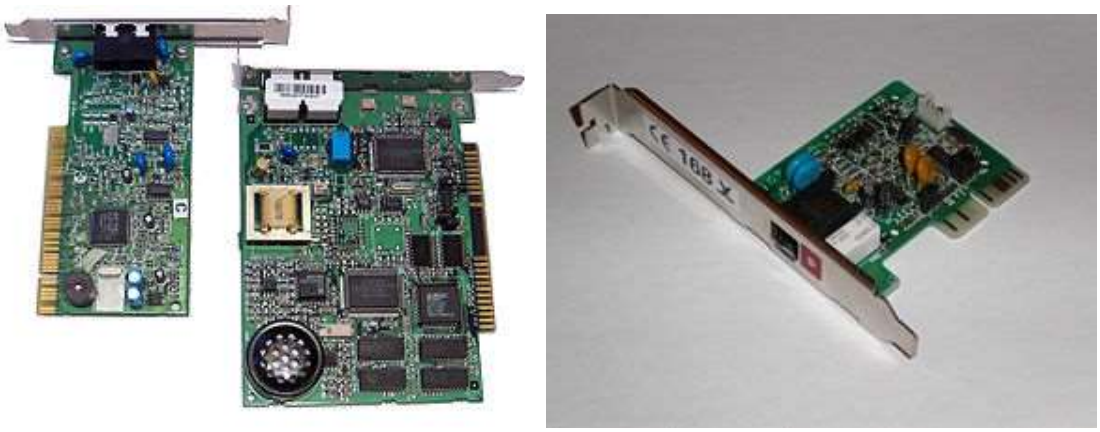
3.3.7.1. Paquete por paquete

Básicamente, un conmutador paquete por paquete (*packet by packet*) es un caso especial de un conmutador s*tore-and-forward* pues, al igual que este, almacena y examina el paquete, calculando el CRC y decodificando la cabecera de la capa de red para definir su ruta a través del protocolo de enrutamiento adoptado.

3.4. Módem

Fax módem externo U.S. Robotics 14.400 (1994)

Figura 18. **Módem por software PCI (izquierda) y módem hardware ISA (derecha)**



Fuente: *Módem por software PCI (izquierda) y módem hardware ISA (derecha)*. https://commons.wikimedia.org/wiki/File:WinmodemAndRegularModem.jpg. Consulta: 18 de enero 2017.

Un módem AMR, con hardware emulado por HSP.

Un módem (del inglés *modem*, acrónimo de modulator demodulator; pl. módems) es un dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (desmodulación), y permite así la comunicación entre computadoras a través de la línea telefónica o del cable módem. Sirve para enviar la señal *moduladora* mediante otra señal llamada *portadora*.

Se han usado módems desde la década de 1960, principalmente debido a que la transmisión directa de las señales electrónicas inteligibles, a largas distancias, no es eficiente; por ejemplo, para transmitir señales de audio por el aire se requerirían antenas de gran tamaño (del orden de cientos de metros) para su correcta recepción. Es habitual encontrar en muchos módems de red conmutada la facilidad de respuesta y marcación automática, que les permiten

conectarse cuando reciben una llamada de la RTPC (red telefónica pública conmutada) y proceder a la marcación de cualquier número previamente grabado por el usuario. Gracias a estas funciones se pueden realizar automáticamente todas las operaciones de establecimiento de la comunicación.

3.4.1. Cómo funciona

El modulador emite una señal denominada portadora. Generalmente, se trata de una simple señal eléctrica sinusoidal de mucha mayor frecuencia que la señal moduladora. La señal moduladora constituye la información que se prepara para una transmisión (un módem prepara la información para ser transmitida, pero no realiza la transmisión). La moduladora modifica alguna característica de la portadora (que es la acción de modular), de manera que se obtiene una señal, que incluye la información de la moduladora. Así el demodulador puede recuperar la señal moduladora original, quitando la portadora. Las características que se pueden modificar de la señal portadora son:

- amplitud, lo que da lugar a una modulación de la amplitud (AM/ASK)
- frecuencia, lo que da lugar a una modulación de la frecuencia (FM/FSK)
- fase, lo que da lugar a una modulación de la fase (PM/PSK)

También, es posible una combinación de modulaciones o modulaciones más complejas, como la modulación de amplitud en cuadratura.

3.5. Módems para PC

La distinción más común es la que suele hacerse entre módems internos y módems externos, aunque han aparecido módems llamados módems software, más conocidos como *winmódems* o *linuxmódems*, que han vuelto complejo el

panorama. También existen los módems para XDSL, RDSI, y los que se usan para conectarse a través de cable coaxial de 75 ohms (cablemódems).

3.5.1. Internos

Consisten en una tarjeta de expansión sobre la cual están dispuestos los diferentes componentes que forman el módem. Existen para diversos tipos de conector:

- Bus ISA: debido a las bajas velocidades que se manejan en estos aparatos, durante muchos años se utilizó en exclusiva este conector, hoy en día en desuso (obsoleto).

- Bus PCI: el formato más común en la actualidad, todavía en uso.

- AMR: en algunas placas; económicos pero poco recomendables por su bajo rendimiento. Hoy es una tecnología obsoleta.

La principal ventaja de estos módems reside en su mayor integración con el ordenador, ya que no ocupan espacio sobre la mesa y reciben energía eléctrica directamente del propio ordenador. Además, suelen ser algo más baratos debido a que carecen de carcasa y transformador, especialmente si son PCI (en este caso, son casi todos del tipo *módem software*). Por el contrario, son algo más complejos de instalar y la información sobre su estado solo puede obtenerse por software.

3.5.2. Externos

Semejantes a los anteriores, pero externos al ordenador o PDA. La ventaja de estos módems reside en su fácil portabilidad entre ordenadores previamente distintos entre ellos (algunos de ellos más fácilmente transportables y pequeños que otros), además de que es posible saber el estado del módem (marcando, con/sin línea, transmitiendo...) mediante los ledes de estado que incorporan. Por el contrario, ocupan más espacio que los internos.

3.6. Tipos de conexión

- La conexión de los módems telefónicos externos al computador se realiza generalmente mediante uno de los puertos serie tradicionales o RS-232 (COM), por lo que se usa la UART del ordenador, que deberá ser capaz de proporcionar la suficiente velocidad de comunicación. La UART debe ser de 16550 o superior para que el rendimiento de un módem de 28.800 bit/s o más sea el adecuado. Estos módems necesitan un enchufe para su transformador.

- Los módems PC Card (internos) tienen forma de tarjeta, que se utilizaban en portátiles, antes de la llegada del USB (PCMCIA). Su tamaño es similar al de una tarjeta de crédito algo más gruesa, pero sus capacidades son las mismas que los modelos estándares.

- Existen modelos para puerto USB (módem USB), de conexión y configuración aún más sencillas, que no necesitan toma de corriente. Hay modelos tanto para conexión mediante telefonía fija, como para telefonía móvil.

- Los módems por software HSP (*host signal processor*) o winmódems: son módems generalmente internos, en los cuales se han eliminado varias piezas electrónicas (por ejemplo, chips especializados), de manera que el microprocesador de la computadora debe suplir su función mediante un programa informático. Lo normal es que utilicen como conexión una ranura PCI (o una AMR), aunque no todos los módems PCI son de este tipo. El uso de la CPU entorpece el funcionamiento del resto de aplicaciones del usuario. Además, la necesidad de disponer del programa puede imposibilitar su uso con sistemas operativos no soportados por el fabricante, de manera que, por ejemplo, si el fabricante desaparece, el módem quedaría eventualmente inutilizado ante una futura actualización del sistema. A pesar de su bajo coste, resultan poco o nada recomendables.

- Módem completo: los módems clásicos no HSP, bien sean internos o externos. En ellos, el rendimiento depende casi exclusivamente de la velocidad del módem y de la UART del ordenador, no del microprocesador.

3.7. Módems telefónicos

Su uso más común y conocido es en transmisiones de datos por vía telefónica.

Las computadoras procesan datos de forma digital; sin embargo, las líneas telefónicas de la red básica sólo transmiten señales analógicas.

Los métodos de modulación y otras características de los módems telefónicos están estandarizados por el UIT-T (el antiguo CCITT) en la serie de

recomendaciones V. Estas recomendaciones también determinan la velocidad de transmisión. Destacan:

3.7.1. Velocidad de transmisión

- V.21. Comunicación Full Duplex entre dos módems analógicos realizando una variación en la frecuencia de la portadora de un rango de 300 baudios, logrando una transferencia de hasta 300 bit/s (bits por segundo).
- V.22. Comunicación *Full Duplex* entre dos módems analógicos utilizando una modulación PSK de 600 baudios para lograr una transferencia de datos de hasta 600 ó 1200 bit/s.
- V.32. Transmisión a 9.600 bit/s.
- V.32bis. Transmisión a 14.400 bit/s.
- V.34. Estándar de módem que permite hasta 28,8 kbit/s de transferencia de datos bidireccionales (full-duplex), utilizando modulación en PSK.
- V.34bis. Módem construido bajo el estándar V34, permite una transferencia de datos bidireccionales de 33,6 kbit/s, utilizando la misma modulación en PSK (estándar aprobado en febrero de 1998).
- V.90. Transmisión a 56,6 kbit/s de descarga y hasta 33.600 bit/s de subida.
- V.92. Mejora sobre V.90 con compresión de datos y llamada en espera. La velocidad de subida se incrementa, pero sigue sin igualar a la de descarga.

Existen, además, módems *DSL* (d*igital subscriber line*), que utilizan un espectro de frecuencias situado por encima de la banda vocal (300 - 3.400 Hz) en líneas telefónicas o por encima de los 80 kHz ocupados en las líneas RDSI, y permiten alcanzar velocidades mucho mayores que un módem telefónico convencional. También poseen otras cualidades, como la posibilidad de

establecer una comunicación telefónica por voz al mismo tiempo que se envían y reciben datos.

Ampliando un poco más esta evolución histórica, se puede marcar una diferencia importante si se toman como punto de partida los primeros módems que operaban de forma analógica, pudiendo transmitir en muy baja velocidad, llegando a través de la norma V.34 a unos 34 kbps como máximo y allí alcanza su límite.

Archivo:Primeros modem.jpg

3.8. Primeros modem

En muy poco tiempo comienzan a implantarse en determinados extremos, las primeras redes de conmutación de paquetes (universitarias, investigación, militares), con ello se gana muchísimo en la relación señal ruido y se evita una segunda conversión analógica digital, la norma V.92 fue su máximo exponente superando los 64 kbps.

Archivo:Modem segunda generacion.jpg

3.8.1. Modems de segunda generación

El hecho concreto que da inicio a este nuevo cambio, es la implantación de las Jerarquías digitales, inicialmente plesiócronas con PDH y hoy Sincrónicas con SDH, a través de estas nuevas tecnologías la voz, cumpliendo con los tres pasos (muestreo, cuantificación y codificación) pasa a transmitirse de forma digital, ocupando canales de 64 Kbps en accesos básicos (BRI = 128 kbps) y primarios (PRI = 2 Mbps con las tramas E1).

Archivo: arquitectura ADSL.jpg

Arquitectura ADSL

Aparece la tecnología RDSI (r*ed digital de servicios integrados*) que rápidamente es superada por xDSL (x digital subscriber line), sobre la que se profundisara. Estos servicios xDSL se basan sobre todo en nuevas formas de modulación (combinando sobre todo fase y amplitud) a través de constelaciones de bits, basados en la capacidad de varias portadoras asociadas a la relación señal ruido de esta última milla que se ha mencionado anteriormente; por esta razón es que xDSL es muy dependiente de la distancia y la calidad del par de cobre que llega hasta el domicilio, cuanto mejor sea la relación señal/ruido, mayor cantidad de bits podrá transmitirse por ese par de cobre y por lo tanto mayor ancho de banda se podrá ofrecer.

Estas tecnologías xDSL son una familia (HDSL, VDSL, ADSL, etc), de ellas, la que más empleo se termina haciendo en las redes de telefonía a nivel domiciliario es ADSL (*asynchronous DSL*). El concepto de asíncrono o asimétrico viene dado en virtud de emplearse dos canales para datos (y un tercero más, independiente para la voz). De los dos canales de datos uno se emplea para bajada de información que suele ser de mayor capacidad y otro para subida de información que suele ser sensiblemente menor. Las especificaciones técnicas de esta tecnología se encuentran en la recomendación G.992.1 (G.dmt) y G992.2 (G.lite) de la ITU-T y en el estándar T1.413-1998 de la ANSI. A continuación se presenta una imagen de su funcionamiento:

3.8.2. Lista de velocidades de acceso telefónico

Debe tenerse en cuenta que los valores indicados son valores máximos y los valores reales pueden ser más lento en ciertas condiciones (por ejemplo, las líneas telefónicas ruidosas). Un baudio es un símbolo por segundo, y cada símbolo puede codificar uno o más bits de datos.

Tabla I. **Lista de velocidades de acceso telefónico**

Conexión	**Modulación**	**Bitrate [kbit/s]**	**Año lanzamiento**
Módem de 110 baudios Bell 101	FSK	0.1	1958
Módem de 300 baudios (Bell 103 o V.21)	FSK	0.3	1962
Módem 1200 (1200 baudios) (Bell 202)	FSK	1.2	
Módem 1200 (600 baudios) (Bell 212A o V.22)	QPSK	1.2	1980?
Módem 2400 (600 baudios) (V.22bis)	QAM	2.4	1984
Módem 2400 (1200 baudios) (V.26bis)	PSK	2.4	
Módem 4800 (1600 baudios) (V.27ter)	PSK	4.8	
Módem 9600 (2400 baudios) (V.32)	QAM	9.6	1984
Módem 14.4k (2400 baudios) (V.32bis)	trellis	14.4	1991
Módem 28.8k (3200 baudios) (V.34)	trellis	28.8	1994
Módem 33.6k (3429 baudios) (V.34)	trellis	33.6	
Módem 56k (8000/3429 baudios) (V.90)	digital	56.0/33.6	1998
Módem 56k (8000/8000 baudios) (V.92)	digital	56.0/48.0	2000
Módem de enlace (dos módems 56k)) (V.92)[9]		112.0/96.0	
Compresión por hardware (variable) (V.90/V.42bis)		56.0-220.0	
Compresión por hardware (variable) (V.92/V.44)		56.0-320.0	
Compresión en el servidor web (variable) (Netscape ISP)		100.0-1,000.0	

Fuente: *Lista de velocidades de acceso telefónico*. https://es.wikipedia.org/wiki/M%C3%B3dem. Consulta: 18 de enero de 2017.

3.8.3. Tipos de modulación

Dependiendo de si el módem es digital o analógico se usa una modulación de la misma naturaleza. Para una modulación digital se tienen, por ejemplo, los siguientes tipos de modulación:

- ASK, (*Amplitude Shift Keying*, modulación por desplazamiento de amplitud): La amplitud de la portadora se modula a niveles correspondientes a los dígitos binarios de entrada 1 ó 0.

- FSK, (*Frecuency Shift Keying*, modulación por desplazamiento de frecuencia): La frecuencia portadora se modula sumándole o restándole una frecuencia de desplazamiento que representa los dígitos binarios 1 o 0. Es el tipo de modulación común en módems de baja velocidad en la que los dos estados de la señal binaria se transmiten como dos frecuencias distintas.

- PSK, (*Phase Shift Keying*, modulación por desplazamiento de fase): tipo de modulación donde la portadora transmitida se desplaza cierto número de grados en respuesta a la configuración de los datos. Los módems bifásicos por ejemplo, emplean desplazamientos de 180º para representar el dígito binario 0.

Sin embargo, en el canal telefónico también existen perturbaciones que el módem debe enfrentar para poder transmitir la información. Estos trastornos se pueden enumerar en: distorsiones, deformaciones y ecos; ruidos aleatorios e impulsivos y, por último, las interferencias.

Para una modulación analógica se tienen, por ejemplo, los siguientes tipos de modulación:

- AM amplitud modulada: La amplitud de la portadora se varía por medio de la amplitud de la moduladora.

- FM frecuencia modulada: La frecuencia de la portadora se varía por medio de la amplitud de la moduladora.

- PM *phase modulation*. Modulación de fase: en este caso el parámetro que se varía de la portadora es la fase de la señal, matemáticamente es casi idéntica a la modulación en frecuencia. Igualmente que en AM y FM, es la amplitud de la moduladora lo que se emplea para afectar a la portadora.

Órdenes AT

3.8.4. Órdenes de comunicación

- ATA: con esta orden el módem queda en espera de una llamada telefónica y se comporta como un receptor (*autoanswer*).

Cada módem utiliza una serie de órdenes AT comunes y otras específicas. Por ello, se deberá hacer uso de los manuales que acompañan al módem para configurarlo adecuadamente. Donde cada uno de los módems son aplicados.

3.8.5. Registros

Los registros o registros S son porciones de memoria donde se pueden guardar permanentemente parámetros que definen el perfil del módem (*profiles*).

Además de las órdenes AT, se dispone de esta serie de registros que permiten al usuario la modificación de otras características de su funcionamiento. Al igual que ocurre con las órdenes AT, existen registros comunes y otros específicos del módem. Se enumeraran los más comunes.

- Registro 0: número de llamadas que el módem espera antes de responder (*autoanswer*). Si su valor es 0, el módem nunca responderá a las llamadas.

- Registro 1: contabilizador de llamadas realizadas / recibidas.

- Registro 2: código del carácter que se utiliza para activar la secuencia de escape. Suele ser un +.

- Registro 3: código del carácter de fin de línea. Suele ser un 13 (enter).

- Registro 4: código de carácter de avance de línea, (*line feed*).

- Registro 5: código de carácter de borrado con retroceso (*backspace*).

- Registro 6: tiempo de espera antes de empezar a marcar (s).

- Registro 7: tiempo de espera para recibir portadora (s).

- Registro 8: tiempo asignado a la pausa del Hayes (la coma en s).

- Registro 9: tiempo de respuesta a la detección de portadora, para activar la DCD (en décimas de segundo).

- Registro 10: tiempo máximo de pérdida de portadora para cortar la línea. Aumentando su valor permite al remoto cortar temporalmente la conexión sin que el módem local inicie la secuencia de desconexión. Si es 255, se asume que siempre hay portadora. Este tiempo debe ser mayor que el del registro 9 (en décimas de segundo).

- Registro 12: determina el *guard time*; este es el tiempo mínimo que precede y sigue a un código de escape (+++), sin que se hayan transmitido o recibido datos. Si es 0, no hay límite de tiempo (S12 x 20 ms).

- Registro 18: contiene la duración de los tests.

- Registro 25: tiempo para que el módem considere que la señal de DTR ha cambiado.

- Registro 26: tiempo de respuesta de la señal CTS ante RTS.

Perfiles de funcionamiento

Existen 3 tipos de perfil para funcionamiento de los módems:

- el de fábrica (por defecto o predeterminado)
- el activo
- el del usuario

Estos perfiles están guardados en su NVRAM, y el perfil de fábrica está guardado en ROM.

Hay dos opciones o lugares de memoria donde se pueden grabar los perfiles:

- AT&Y0, (al encender se carga el perfil = 0)
- AT&Y1, (al encender se carga el perfil = 1)

Estas órdenes se envían antes de apagar el módem, para que los cargue en su próximo encendido.

Cuando se escriben las órdenes AT, en función del tamaño del buffer del módem, se pueden ir concatenando sin necesidad de escribir para cada uno de ellos el prefijo AT. De esta forma, por ejemplo, cuando en un programa se pide una secuencia de inicialización del módem, se pueden incluir conjuntamente en una sola línea todas las órdenes necesarias para configurar el módem.

3.8.6. Pasos o procesos para establecer comunicación a través del módem

- Detección del tono de línea. El módem dispone de un detector del tono de línea. Este se activa si dicho tono permanece por más de un segundo. De no ser así, sea por qué ha pasado un segundo sin detectar nada o no se ha mantenido activado ese tiempo el tono, envía a la computadora el mensaje No dialtone.

- Marcación del número. Si no se indica el modo de llamada, primero se intenta llamar con tonos y si el detector de tonos sigue activo, se pasa a llamar con pulsos. En el período entre cada dígito del número telefónico, el IDP (*interdigit pulse*), se continua atendiendo al detector de tono. Si en algún IDP el detector se activa, la llamada se termina y se retorna un

mensaje de Busy. Una vez terminada la marcación, se vuelve a atender al detector de tono para comprobar si hay conexión. En este caso pueden suceder varias cosas:

- Rings de espera. Se detectan y contabilizan los rings que se reciban, y se comparan con el registro S1 del módem. Si se excede del valor allí contenido, se retorna al mensaje No answer.

    - Si hay respuesta, se activa un detector de voz/señal, la detección de la respuesta del otro módem se realiza a través del filtro de banda alta (al menos debe estar activo 2 segundos).

- Si el detector de tono fluctúa en un período de 2 segundos se retorna el mensaje Voice. El mensaje No answer puede obtenerse si se produce un intervalo de silencio después de la llamada.

- Establecer el enlace. Implica una secuencia de procesos que dependen si se está llamando o si se recibe la llamada.

- Si se está llamando, será:

    - Fijar la recepción de datos a 1.
    - Seleccionar el modo de baja velocidad.
    - Activar 0'6 segundos el tono de llamada y esperar señal de línea.
    - Desactivar señal de tono.
    - Seleccionar modo de alta velocidad.
    - Esperar a recibir unos, después transmitir unos y activar la transmisión

- Analizar los datos recibidos para comprobar que hay conexión. Si ésta no se consigue en el tiempo límite fijado en el registro S7, se da el mensaje No carrier; en caso contrario, se dejan de enviar unos, se activa la señal de conexión, se desbloquea la recepción de datos y se da el mensaje Carrier.

- Si se está recibiendo, será:

  - Selección del modo respuesta.

  - Desactivar el scrambler.

  - Seleccionar el modo de baja velocidad y activar el tono de respuesta (p. ej. 2.400 Hz durante 3'3 s).

  - Desactivar el transmisor.

  - Esperar portadora, si no se recibe activar el transmisor, el modo de alta velocidad y el tono a 1.800 Hz.

  - Esperar el tiempo indicado en S7, si no hay conexión envía el mensaje No Carrier, si la hay, indica connect, se activa el transmisor, el detector de portadora y la señal de conexión.

En resumen, los pasos para el establecimiento de una conexión son:

- La terminal levanta la línea DTR.
- Se envía desde la terminal la orden ATDT 5551234 ("AT" -> atención, D -> marcar, T -> por tonos, 5551234 -> número a llamar.)

- El módem levanta la línea y marca el número.
- El módem realiza el hand shaking con el módem remoto.
- El programa de comunicación espera el código de resultado.
- Código de resultado CONNECT.

3.8.7. Test en módems h*ayes*

Los tests permiten verificar el módem local, la terminal local, el módem remoto y la línea de comunicaciones. Con el registro del módem S18 se indica el tiempo de duración de los tests. Si su contenido es 0, no hay límite de tiempo y es el usuario el que debe finalizar las pruebas con la orden AT&T0. El módem al encenderse realiza una serie de exámenes internos. En caso de surgir algún error, se le indicará al DTE oportunamente.

Los tests que pueden realizarse son:

- *Local analog loopback* (bucle local analógico): se ejecuta con &T1. Comprueba la conexión entre el módem y el terminal local. Tras introducir AT&T1, pasados unos segundos, se entra en modo *on line*. Para realizar el test debe estar activado el eco local. La ejecución correcta del test implica que todo carácter digitado por el usuario aparecerá duplicado. Para terminar el test, se pulsa la secuencia de escape y después AT&T0. Si el test se inicia estando ya conectado a un servicio, esta conexión se corta.

- *Local digital loopback* (bucle local digital): se ejecuta con &T3. Solo puede realizarse durante una conexión con un módem remoto. Comprueba la conexión entre el módem local y el remoto, y el circuito de línea. Envía al módem remoto las cadenas que reciba de él.

- *Remote digital loopback* (bucle digital remoto): se ejecuta con &T6. Comprueba el terminal local, el módem local, el módem remoto y el circuito de línea. Debe realizarse durante una conexión, y el módem remoto puede o debe aceptar la petición del test. Para finalizarlo se pasa a modo de órdenes con la secuencia de escape y se teclea AT&T0. El terminal local compara la cadena recibida con la transmitida por él previamente. Las cadenas son proporcionadas por el usuario.

- *Remote digital loopback with selftest* (bucle digital remoto con autotest): se ejecuta con &T7. Comprueba el módem local, el remoto, y el circuito de línea. Debe realizarse durante una conexión y para finalizarlo hay que indicar la secuencia de escape y AT&T0. Se genera un patrón binario, según la recomendación V.54 del CCITT, para comprobar la conexión. Al finalizar el test se indica el número de errores aparecidos, (de 000 a 255).

- *Local analog loopback with selftest* (bucle analógico local con autotest): se ejecuta con &T8. Comprueba el módem local. Tras iniciarse el test, pasados unos segundos, se retorna al modo de órdenes. Se finaliza con &T0 o si se alcanza el tiempo límite definido en S18. El test comprueba los circuitos de transmisión y recepción del módem. Se utiliza un patrón binario, según la recomendación CCITT V.54. Si está conectado con algún servicio, la conexión se corta. Al finalizar el test se retorna el número de errores, (000 a 255).

3.8.8. Protocolos de comprobación de errores

El control de errores son varias técnicas mediante las cuales se chequea la fiabilidad de los bloques de datos o de los caracteres.

- Paridad: función donde el transmisor añade otro bit a los que codifican un símbolo. Es paridad par, cuando el símbolo tenga un número par de bits y es impar en caso contrario. El receptor recalcula el número de par de bits con valor uno, y si el valor recalculado coincide con el bit de paridad enviado, acepta el paquete. De esta forma se detectan errores de un solo bit en los símbolos transmitidos, pero no errores múltiples.

- CRC (c*yclic redundancy check*, prueba de redundancia cíclica): esta técnica de detección de error consiste en un algoritmo cíclico en el cual cada bloque o trama de datos es chequeada por el módem que envía y por el que recibe. El módem que está enviando inserta el resultado de su cálculo en cada bloque en forma de código CRC. Por su parte, el módem que está recibiendo compara el resultado con el código CRC recibido y responde con un reconocimiento positivo o negativo dependiendo del resultado.

- MNP (m*icrocom networking protocol*, protocolo de red microcom): es un control de error desarrollado por microcom, Inc. Este protocolo asegura transmisiones libres de error por medio de una detección de error, (CRC) y retransmisión de tramas equivocadas.

3.8.9. Protocolos de transferencia de archivos

- Xmodem: es el protocolo más popular, pero lentamente está siendo reemplazado por protocolos más fiables y más rápidos. Xmodem envía archivos en bloques de 128 caracteres al mismo tiempo. Cuando el computador que está recibiendo comprueba que el bloque ha llegado intacto, lo señala así y espera el bloque siguiente. El chequeo de error es un checksum o un chequeo más sofisticado de redundancia cíclica.

Algunas comunicaciones por software soportan ambas y podrían automáticamente usar la más indicada para un momento dado. Durante una descarga, el software tiende a usar el CRC, pero se cambiará a checksum si se detecta que el host no soporta el CRC. El protocolo de Xmodem también necesita tener declarado en su configuración: no paridad, ocho bits de datos y un bit de parada.

- Xmodem-1k: es una pequeña variante del anterior que usa bloques que poseen un kilobyte (1.024 bytes) de tamaño. Este protocolo suele llamarse todavía Ymodem en algunos programas, lo cual es incorrecto.

- Xmodem-1k-g: es una variante del anterior para canales libres de error tales como corrección de errores por hardware o líneas de cable null-módem entre dos computadoras. Logra mayor velocidad enviando bloques uno tras otro sin tener que esperar el reconocimiento desde el receptor. Sin embargo, no puede retransmitir los bloques en caso de errores. En caso de que un error sea detectado en el receptor, la transferencia será abortada. Al igual que el anterior, muchas veces es mal llamado Ymodem-g.

- Zmodem: este avanzado protocolo es muy rápido al igual que garantiza una buena fiabilidad y ofrece varias características. Zmodem usa paquetes de 1 kb en una línea limpia, pero puede reducir el tamaño del paquete según si la calidad de la línea va deteriorándose. Una vez que la calidad de la línea es recuperada el tamaño del paquete se incrementa nuevamente. Zmodem puede transferir un grupo de archivos en un lote (*batch*) y guardar exactamente el tamaño y la fecha de los archivos. También puede detectar y recuperar rápidamente errores, y puede resumir

e interrumpir transferencias en un período más tarde. Igualmente es muy bueno para enlaces satelitales y redes de paquetes conmutadas.

- ASCII: en una transferencia ASCII, es como que si el que envía estuviera actualmente digitando los caracteres y el receptor grabándolos ahora. No se utiliza ninguna forma de detección de error. Usualmente, solo los archivos ASCII pueden ser enviados de esta forma, es decir, como archivos binarios que contienen caracteres.

- Ymodem: este protocolo es una variante del Xmodem, el cual permite que múltiples archivos sean enviados en una transferencia. A lo largo de ella, se guarda el nombre correcto, tamaño, y fecha del archivo. Puede usar 128 o (más comúnmente), 1,024 bytes para los bloques.

- Ymodem-g: este protocolo es una variante del anterior, el cual alcanza una tasa de transferencia muy alta, enviando bloques uno tras otro sin esperar por un reconocimiento. Esto, sin embargo, significa que si un error es detectado por el receptor, la transferencia será abortada.

- Telink: este protocolo se encuentra principalmente en Fido Bulletin Board Systems. Es básicamente el protocolo Xmodem usando CRC para chequear y un bloque extra enviado como cabecera del archivo que dice su nombre, tamaño y fecha. Por su parte, también permite que más de un archivo sea enviado al mismo tiempo (Fido es una BBS muy popular, que se utiliza en todo el mundo).

- Kermit: este protocolo fue desarrollado para facilitar el intercambio de archivos entre los diferentes tipos de computadoras. Casi ninguna computadora que usa Kermit puede ser configurada para enviar archivos

a otra computadora que también use Kermit. Kermit usa pequeños paquetes (usualmente de 94 bytes) y, aunque es fiable, es lento porque la relación del protocolo de datos para usarlos es más alta que en muchos otros protocolos.

3.8.10. Servidor

Un servidor en informática o computación es:

Una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor.

3.8.10.1. ¿Qué es un servidor?

- En Internet, un servidor es un ordenador remoto que provee los datos solicitados por parte de los navegadores de otras computadoras.

- En redes locales se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos.

- Los servidores almacenan información en forma de páginas web y a través del protocolo HTTP lo entregan a petición de los clientes (navegadores web) en formato HTML.

- En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

- Este uso dual puede llevar a confusión. Por ejemplo, en el caso de un servidor web, este término podría referirse a la máquina que almacena y maneja los sitios web, y en este sentido es utilizada por las compañías que ofrecen hosting o hospedaje. Alternativamente, el servidor web podría referirse al software, como el servidor de http de Apache, que funciona en la máquina y maneja la entrega de los componentes de los páginas web como respuesta a peticiones de los navegadores de los clientes.

- Los archivos para cada sitio de Internet se almacenan y se ejecutan en el servidor. Hay muchos servidores en Internet y muchos tipos de servidores, pero comparten la función común de proporcionar el acceso a los archivos y servicios.

- Un servidor sirve información a los ordenadores que se conecten a él. Cuando los usuarios se conectan a un servidor pueden acceder a programas, archivos y otra información del servidor.

- En la web, un servidor web es un ordenador que usa el protocolo http para enviar páginas web al ordenador de un usuario cuando el usuario las solicita.

- Los servidores web, servidores de correo y servidores de bases de datos son a lo que tiene acceso la mayoría de la gente al usar Internet.

- Algunos servidores manejan solamente correo o solamente archivos, mientras que otros hacen más de un trabajo, ya que un mismo ordenador puede tener diferentes programas de servidor funcionando al mismo tiempo.

Los servidores se conectan a la red mediante una interfaz que puede ser una red verdadera o mediante conexión vía línea telefónica o digital.

Esta lista categoriza los diversos tipos de servidores del mercado actual:

3.8.10.2. Plataformas de servidor (*server platforms*)

Un término usado a menudo como sinónimo de sistema operativo, la plataforma es el hardware o software subyacentes para un sistema, es decir, el motor que dirige el servidor.

3.8.10.3. Servidores de aplicaciones (*application servers*)

Designados a veces como un tipo de *middleware* (software que conecta dos aplicaciones), los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los conectan.

3.8.11. Servidores de audio/video (*audio/video servers*)

Los servidores de audio/video añaden capacidades multimedia a los sitios web permitiéndoles mostrar contenido multimedia en forma de flujo continuo (*streaming*) desde el servidor.

- Servidores de chat (*chat servers*)**:** los servidores de chat permiten intercambiar información a una gran cantidad de usuarios ofreciendo la posibilidad de llevar a cabo discusiones en tiempo real.

- Servidores de fax (*fax servers*): un servidor de fax es una solución ideal para organizaciones que tratan de reducir el uso del teléfono pero necesitan enviar documentos por fax.

- Servidores FTP (ftp *servers*): uno de los servicios más antiguos de internet, file transfer protocol permite mover uno o más archivos.

- Servidores groupware (g*roupware servers*): un servidor groupware es un software diseñado para permitir colaborar a los usuarios, sin importar la localización, vía Internet o vía Intranet corporativo y trabajar juntos en una atmósfera virtual.

- Servidores IRC (*irc servers*): otra opción para usuarios que buscan la discusión en tiempo real, *internet relay* chat consiste en varias redes de servidores separadas que permiten que los usuarios conecten el uno al otro vía una red IRC.

- Servidores de listas (*list servers*): los servidores de listas ofrecen una manera mejor de manejar listas de correo electrónico, bien sean discusiones interactivas abiertas al público o listas unidireccionales de anuncios, boletines de noticias o publicidad.

- Servidores de correo (m*ail servers*): casi tan ubicuos y cruciales como los servidores web, los servidores de correo mueven y almacenan el correo

electrónico a través de las redes corporativas (vía LANs y WANs) y a través de Internet.

- Servidores de noticias (*news servers*): los servidores de noticias actúan como fuente de distribución y entrega para los millares de grupos de noticias públicos actualmente accesibles a través de la red de noticias.

- Servidores proxy (p*roxy servers*): los servidores proxy se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones.

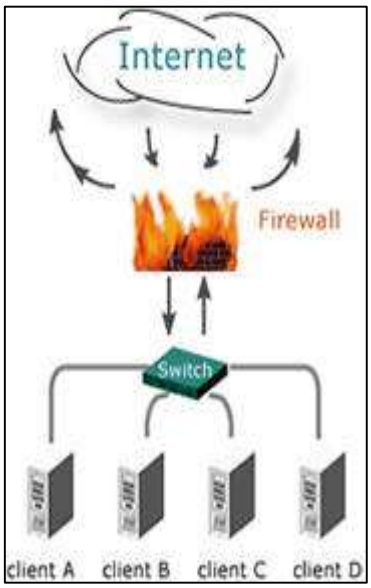
- Servidores telnet (t*elnet servers*): un servidor telnet permite a los usuarios entrar en un ordenador huésped y realizar tareas como si estuviera trabajando directamente en ese ordenador.

- Servidores web (w*eb servers*): básicamente, un servidor web sirve contenido estático a un navegador, carga un archivo y lo sirve a través de la red

3.9. Firewall

Cada computadora conectada a internet (y, hablando más genéricamente, a cualquier red informática) es susceptible a ser víctima de un ataque de un pirata informático. La metodología empleada generalmente por el pirata informático consiste en barrer la red (enviando paquetes de datos de manera aleatoria) en busca de una máquina conectada, y luego buscar un agujero de seguridad, el cual utilizará para acceder a los datos que allí se encuentren.

Figura 19. **Firewall**



Fuente: *Firewall*. http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Firewall-y-como-funciona.php. Consulta: 18 de enero de 2017.

Esta amenaza es todavía mayor si la computadora está permanentemente conectada a internet. Las razones son varias:

- La PC objeto puede estar conectada sin ser supervisada permanentemente.
- La PC objeto está conectada generalmente utilizando banda ancha.
- La PC objeto no cambia (o muy poco) la dirección IP.

Por lo tanto, es necesario que las redes de empresas y los usuarios de internet que posean una conexión con cable o ADSL, protegerse de las

intrusiones instalando un dispositivo de protección. En ese momento es que entra en acción el Firewall.

Qué es un *firewall*?

Un *firewall* (llamado también corta-fuego), es un sistema que permite proteger a una computadora o una red de computadoras de las intrusiones que provienen de una tercera red (expresamente de Internet). El *firewall* es un sistema que permite filtrar los paquetes de datos que andan por la red. Se trata de un puente angosto que filtra, al menos, el tráfico entre la red interna y externa.

Un *firewall* puede ser un programa (software) o un equipo (hardware) que actúa como intermediario entre la red local (o la computadora local) y una o varias redes externas.

Funcionamiento de un sistema *firewall*.

Un sistema firewall contiene un conjunto de reglas predefinidas que permiten:

- Autorizar una conexión (*allow*)
- Bloquear una conexión (*deny*)
- Redireccionar un pedido de conexión sin avisar al emisor (*drop*)

El conjunto de estas reglas permite instalar un método de filtración dependiente de la política de seguridad adoptada por la organización. Se distinguen habitualmente dos tipos de políticas de seguridad que permiten:

- Permitir únicamente las comunicaciones autorizadas explícitamente: Todo lo que no es autorizado explícitamente está prohibido.
- Impedir cualquier comunicación que fue explícitamente prohibida.

El primer método es el más seguro, pero requiere de una definición precisa de las necesidades de comunicación de toda la red.

3.10. *Hub*

En informática un *hub* o concentrador es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Los hubs han dejado de ser utilizados, debido al gran nivel de colisiones y tráfico de red que propician.

3.10.1. ¿Qué es un *hub* y cómo funciona?

Un *hub* de red o un repetidor *hub* es un dispositivo que sirve para conectar múltiples dispositivos mediante cables cruzados o fibra óptica, y haciéndolos funcionar como un único segmento de red. Los *hub* funcionan en la capa física (capa 1) del modelo OSI y funciona como una especie de repetidor multipuerto. Los *hub* repetidores también participan en la detección de colisiones, enviando una señal de congestión a todos los puertos si detecta una de estas colisiones. La disponibilidad de switches de red a precios muy bajos, han dejado a los hub bastante obsoletos, aunque todavía se pueden ver en algunas instalaciones antiguas o es ciertas situaciones donde se ha preferido poner uno de estos aparatos.

Lo cierto es que un *hub* es un dispositivo de red que no es sofisticado en absoluto. Los *hub* no gestionan nada del tráfico que pasa a través de él, y

cualquier paquete que entra por un puerto es difundido a todos los demás puertos. Al estar siendo enviado cada paquete por todos los demás puertos, hay como resultado colisiones, lo cual impide una afluencia fluida del tráfico. La necesidad de los dispositivos para detectar colisiones, limitan el número de hubs y el tamaño total de la red. Algunos hubs tienen puertos especializados que les permite combinarlos de una manera que pueden permitir más hubs simplemente uniéndolos mediante cables ethernet, aunque es probable que finalmente se tengan que utilizar switches para evitar ciertos problemas de red.

Algunos *hubs* inteligentes detectan problemas típicos, como colisiones excesivas en puertos individuales, y son capaces de particionar este puerto, desconectándolo del medio compartido. Un *hub* inteligente hace que encontrar un problema sea más sencillo porque las luces de indicación nos pueden dar el origen del problema. También tiene la ventaja de poder desconectar uno a uno cada dispositivo de red para ver donde está lo que no está afectando.

Figura 20. **Hub y cómo funciona**

Fuente: *Hub y cómo funciona*. http://www.ordenadores-y-portatiles.com/hub.html. Consulta: 20 de enero de 2017.

3.10.2. Tipos de *hub*

- Pasivos: es un *hub* que no necesita un fuente externa de energía porque no regenera la señal y por tanto es como si fuera una parte del cable, siempre teniendo en cuenta la longitud del cable.

- Activos: es un *hub* que regenera la señal y necesita una toma externa de alimentación.

- Inteligentes: el *hub* provee de detección de errores, como colisiones excesivas, y también hace lo que un *hub* activo.

Los *hubs* pasivos no amplifican las señales eléctricas de paquetes entrantes antes de difundirlos fuera de la red. Los activos por el contrario, si realizan esta amplificación, como lo podría hacer un repetidor. Como se ha comentado, los hubs inteligentes no proporcionan algunas funciones adicionales que son particularmente importantes para los negocios. Normalmente si fácilmente enracables, lo cual significa que se pueden poner uno encima de otro en un rack para tal función, de una manera muy fácil para conservar espacio. También, puede incluir funciones de gestión remota mediante SNMP.

En el pasado y cuando los *switches* estaban empezando a ser populares, los hubs eran la opción debido a su precio frente a lo que costaban los switches. Sin embargo, y como se ha dicho antes, la bajada de los precios en switches aunque los hubs todavía pueden ser útiles en algunas circunstancias. Por ejemplo, si se quiere usar un analizador de protocolos en una red, el *hub* puede servir de espejo para los puertos. También, es muy útil como conexión de emergencia en una reunión si hay varias personas en una habitación y una sola

toma de red. Se puede conectar un *hub* de varios puertos y así todos podrán conectar sus ordenadores portátiles para tener acceso a la red.

4. DISPOSITIVOS DE RED EN AMBIENTE VIRTUAL

4.1. ¿Qué es Virtual Router?

Virtual Router es un enrutador gratuito basado en software de código abierto para PCs que ejecutan Windows 8, Windows 7 o Windows Server 2008 R2. Usando el ranurador virtual, los usuarios pueden compartir sin hilos cualquier conexión de Internet (wifi, LAN, módem de cable, acceso telefónico, celular, etc.) con cualquier dispositivo de wifi (ordenador portátil, teléfono elegante, Impresora inalámbrica, etc.). Estos dispositivos se conectan a Virtual Router como cualquier otro punto de acceso, y la conexión está completamente protegida mediante WPA2 (el cifrado inalámbrico más seguro).

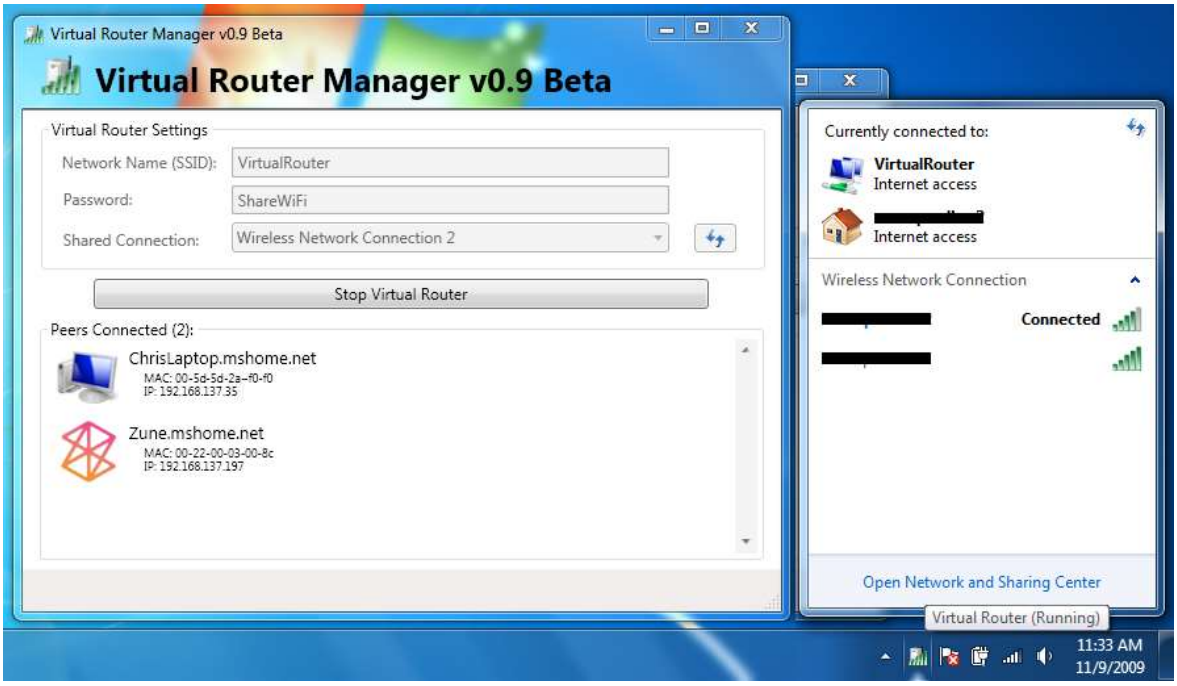
4.1.1. ¿Dónde se puede utilizar Virtual Router?

Dondequiera que se este

- Casa
- Oficina
- Universidad
- Aeropuerto
- Estación de autobuses
- El parque
- Casa de la abuela
- Los suegros
- ¡Absolutamente en cualquier lugar!

A diferencia de aplicaciones similares, Virtual Router no sólo es totalmente gratuito, pero no le molestará con cualquier anuncio. Además, dado que Virtual Router no es compatible con anuncios, no realiza un seguimiento de su tráfico web de la misma forma que otras aplicaciones publicitarias pueden / pueden hacer.

Figura 21. **Virtual Router Sin publicidad, sin molestias**



Fuente: *Virtual Router*. https://virtualrouter.codeplex.com/. Consulta: 25 de enero de 2017.

La Red Inalámbrica creada / compartida con Virtual Router usa Cifrado WPA2, y no hay forma de desactivar ese cifrado. Esto es en realidad una característica de la Wireless Hosted Network API integrada en Windows 7 y 2008 R2 para garantizar la mejor seguridad posible.

Usted puede dar a su red inalámbrica virtual cualquier nombre que desee, y también establecer la contraseña a cualquier cosa. Asegúrese de que la contraseña tenga al menos 8 caracteres.

4.1.2. Los fundamentos de Virtual WiFi Router

La principal función de Virtual wifi Router es crear un entorno personalizado mediante el cual convertimos nuestro ordenador en un *hotspot* o punto de acceso inalámbrico.

La señal que llega al ordenador y mediante la cual este puede conectarse a Internet es reenviada mediante un protocolo de Windows para compartir esta conexión; el programa se encarga pues de activar y desactivar el servicio, así como de proporcionarle un nombre y contraseña a la red para localizarla y protegerla respectivamente.

Como es lógico, para usar Virtual WiFi Router, tu ordenador deberá tener instalada una tarjeta de red inalámbrica.

4.2. Primeros pasos de configuración

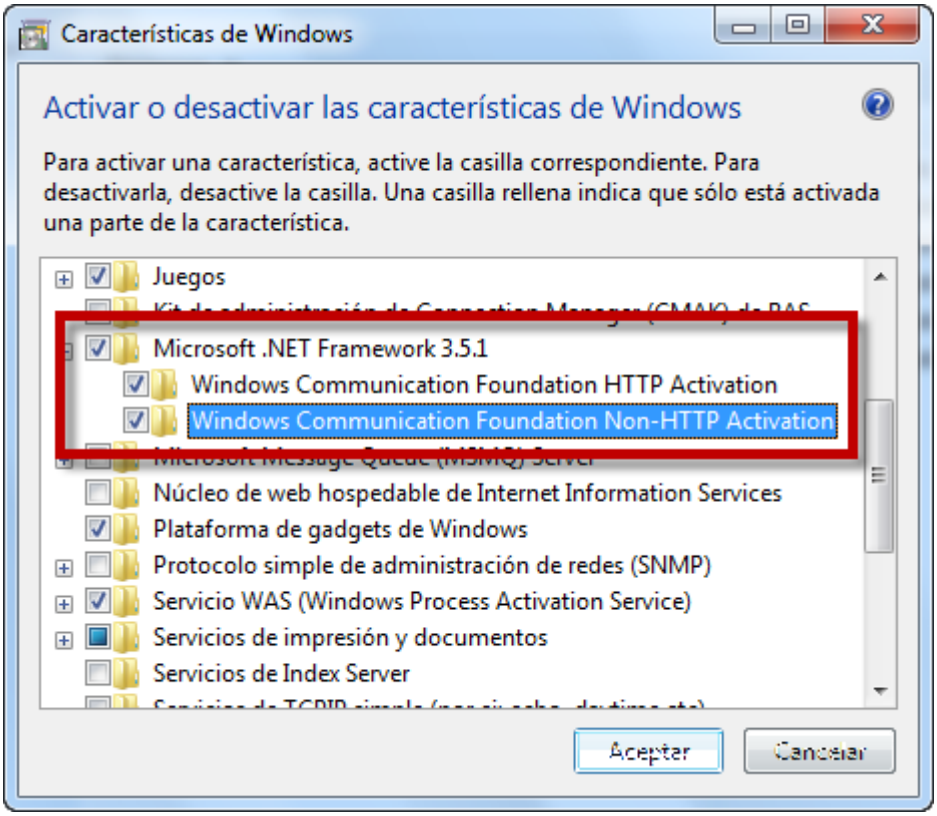
Antes de iniciar Virtual WiFi Router por primera vez es necesario configurar Windows para compartir la conexión entrante.

Lo primero que se tiene que hacer es activar una de las características de Microsoft .NET 3.5: los servicios de Windows Communication Foundation (WCF) que harán posible que el programa funcione y comparta la conexión. Esto se consigue desde la ruta Panel de control > Programas y características > Activar

o desactivar las características de Windows. La opción se encuentra en el lateral de esta ventana.

Si se busca en la ventana de características de Windows se verá estas opciones; deben quedar marcadas.

Figura 22. **Activar o desactivar características de Windows**

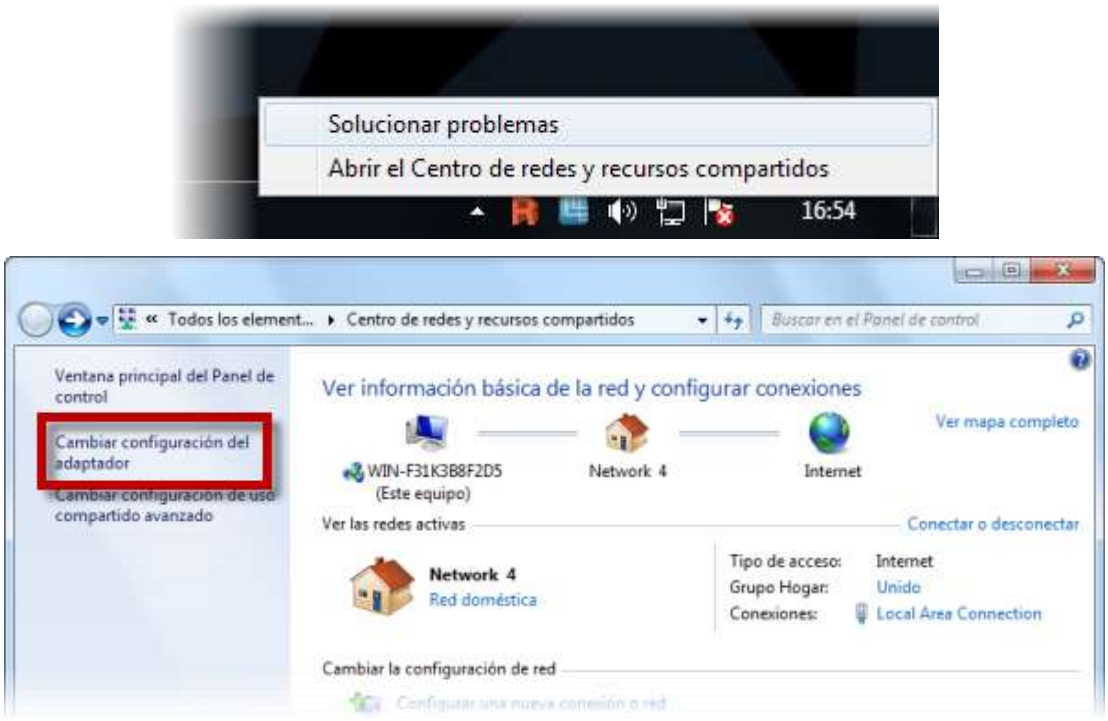


Fuente. *Activar o desactivar características de windows*. https://lecciones.batiburrillo.net/activar-o-desactivar-caracteristicas-de-windows-7/. Consulta: 25 de enero de 2017.

A continuación se tiene que activar la opción de uso compartido del adaptador de red desde el que recibes la conexión a Internet. Para ello dirige al

Centro de redes; el acceso más rápido está en el icono de acceso a internet en la barra de sistema.

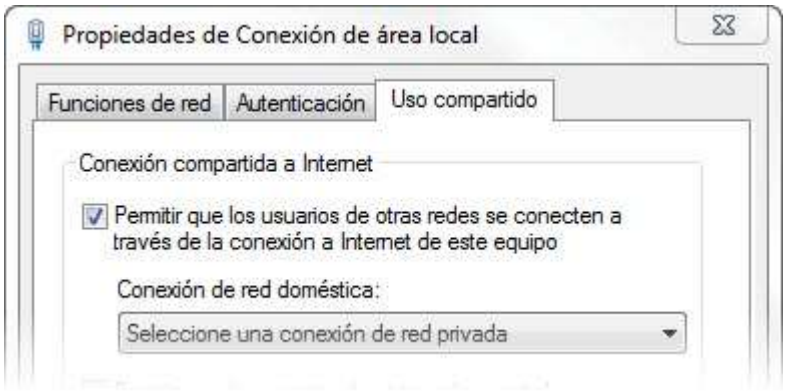
Figura 23. **Centro de redes y recursos compartidos**



Fuente:C*entro de redes y recursos compartidos*. https://lecciones.batiburrillo.net/activar-o-desactivar-caracteristicas-de-windows-7/. Consulta: 25 de enero de 2017.

La opción que has de activar se encuentra dentro del apartado Cambiar configuración del adaptador. Una vez dentro, haz clic derecho en el adaptador y elige Propiedades. La pestaña que te interesa es la de Uso compartido y la opción clave es la primera.

Figura 24. **Conexión de área local**



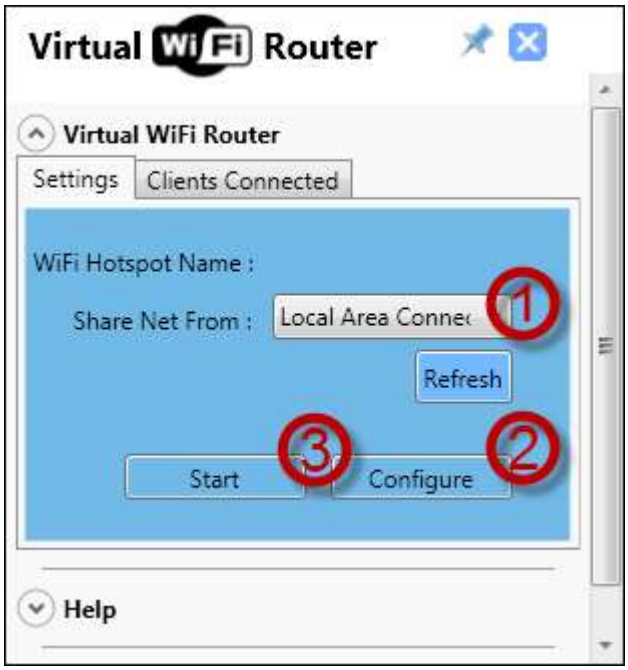
Fuente. *Conexión de área local*. https://lecciones.batiburrillo.net/activar-o-desactivar-caracteristicas-de-windows-7/. Consulta: 25 de enero de 2017.

Ya está todo listo para usar Virtual WiFi Router.

4.2.1. Creando el punto de acceso

Ahora que tienes todo a punto, es el momento de abrir el programa y acceder a su ventana haciendo clic en el icono que se instala en la barra de sistema. Cuando se abra la ventana verás dos pestañas; de momento la que te interesa es la primera, que define la conexión a compartir (1), los parámetros bajo los que se comparte (2) y arranca el servicio (3).

Figura 25. **Virtual Router**

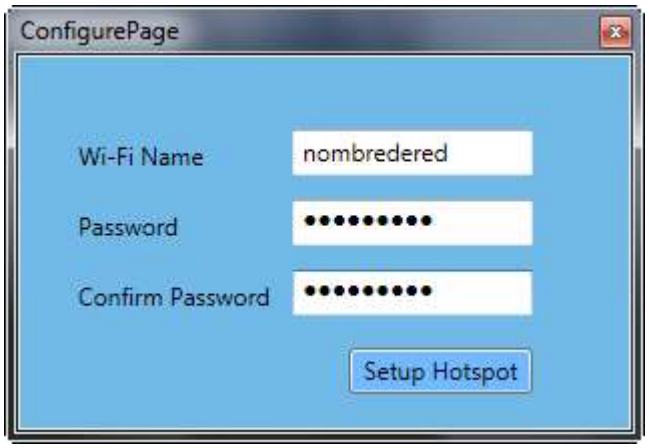


Fuente: *Virtual Router*. https://lecciones.batiburrillo.net/activar-o-desactivar-caracteristicas-de-windows-7/. Consulta 25 de enero 2017.

De la lista desplegable *Share Net From* has de elegir la conexión deseada. Si es una tarjeta normal y corriente, la mayoría de las veces será Local Area Connection**.**

En cuanto al apartado *Configure*, solo tienes que especificar un nombre para localizar la red con el resto de dispositivos y una contraseña de al menos 8 caracteres para acceder a ella. Para finalizar el proceso, pulsa en *Setup Hotspot* y luego *Start*.

Figura 26. **Configuración de red**



Fuente: *Configuración de red*. https://lecciones.batiburrillo.net/activar-o-desactivar-caracteristicas-de-windows-7/. Consulta: 25 de enero de 2017.

Y ya está. El resto del trabajo consiste en detectar la red con tus dispositivos y acceder mediante la contraseña. Ten en cuenta que si compartes una conexión de datos 3G, el límite dispuesto por la operadora puede agotarse rápidamente.

4.3. Switch Virtual

La funcionalidad de red en una infraestructura virtual es de suma importancia. Permite que las máquinas virtuales en un servidor VMware vSphere™ ESXi 5 puedan comunicarse con otras máquinas físicas o máquinas virtuales en otros servidores VMware vSphere™, mediante la configuración de los *virtual switches*.

También permite comunicarse con el *management network* de los servidores VMware vSphere™ 5 para poder gestionarlos y con el VMkernel para

poder configurar vMotion y cabinas de almacenamiento basadas en protocolos NFS o iSCSI.

Un *virtual switch* estándar (VSS) tiene tres funciones principales:

- Comunicar con máquinas virtuales dentro de un mismo servidor VMware ESXi o con otras máquinas físicas o virtuales en otro servidor VMware ESXi, para lo que se utiliza un v*irtual machine port group.*

- Comunicar con nuestro servidor ESXi vía SSH (puerto 22) o vSphere Client, para lo que se utiliza un *management network port.*

- Comunicar con el VMkernel y puertos IP de tipo VMotion, NFS e iSCSI, para lo que se utiliza un *VMkernel port*.

A diferencia de los switches físicos, no es posible conectar dos *virtual switch* juntos mediante un ISL (*interswitch link protocol*), ni se puede mapear la misma tarjeta de red a más de un *virtual switch* a la vez. Recuerdese que sí es posible configurar un *virtual switch* sin ninguna tarjeta de red, lo que es denominado como *internal switch only*.

Cuando se crea un *NIC teaming* (una o más tarjetas de red mapeadas a un *virtual switch* para incrementar el ancho de banda o dotar de alta disponibilidad a la capa de red), todas las tarjetas de red dentro del *teaming* pasan a ser activas por defecto. Para crear *virtual switches* se puede usar el vSphere Client o, desde la consola del servidor ESXi, puedes usar el comando: esxcfg-vswitch -a nombre vSwitch.

Si hay dos máquinas virtuales conectadas a dos virtual switches diferentes, el tráfico entre dichas máquinas fluirá a través de las tarjetas físicas mapeadas a los switches virtuales y entre los servidores ESXi. Por el contrario, si varias máquinas virtuales están conectadas al mismo VSS del mismo servidor ESXi, los paquetes no salen por la red, sino que son transmitidos internamente en el servidor ESXi por el VMkernel.

Para mejorar el rendimiento de red de las máquinas virtuales es posible mapear más de una tarjeta física (*uplink*) al VSS.

También es posible configurar switches distribuidos virtuales (*virtual distributed switch*). La configuración de los switches distribuidos (VDS) es almacenada en el servidor vCenter a diferencia de los switches estándar, los cuales almacenan la configuración en los servidores ESXi. Un v*irtual distributed switch* no es más que un VSS que es compartido entre múltiples servidores VMware vSphere™ ESXi.

4.4. Servidor virtual

Se conoce como servidor virtual a una partición dentro de un servidor que habilita varias máquinas virtuales dentro de dicha máquina por medio de varias tecnologías.

Los servidores dedicados virtuales (SDV) usan una avanzada tecnología de virtualización, que le permite proveer acceso [root] y la capacidad de reiniciarlo cuando desee, igual que un servidor dedicado. Con la posibilidad de instalar sus propias aplicaciones y controlar completamente la configuración de su servidor, los SDV representan una alternativa económica y eficiente para aquellos que

desean disfrutar los beneficios de un servidor dedicado pero aún no poseen el presupuesto para hacerlo.

Cada SDV tiene asignado un límite del uso de la CPU y la memoria RAM (entre otros) que es dedicado solo el de dentro del servidor. Así, cada uno de los SDV funcionan independientemente dentro del mismo servidor físico; es decir actúan como jaulas dentro de un mismo equipo. Por ejemplo, si uno de ellos está mal administrado y trabaja en forma sobrecargada, no afectará el funcionamiento del resto.

En cambio, en un hosting compartido (tanto reseller como individual) los recursos del servidor se comparten entre todas las cuentas de hosting que haya en él, y, si hay un problema de sobrecarga quizás generado por el uso abusivo de un sólo dominio, el rendimiento del hosting se verá sobrecargado en todo el equipo; es decir, en todas sus cuentas.

Se conoce como servidor virtual SPEC (Servidor élite en entorno Clúster) a una solución especialmente dirigida al sector profesional —y, en algún caso, al cliente final—, que permite gestionar virtualmente un servidor y optimizar recursos gracias a la utilización de una potente infraestructura redundada, clusterizada y con posibilidad de montar VPN. Permite configurar sistemas o aplicaciones, soportar cualquier tipo de servicio y determinar cómo desarrollarlo y definirlo.

Si se necesita alojar múltiples sitios web, un servidor virtual privado (VPS) es la opción más económica. Puede alojar numerosos sitios web en un VPS sin los gastos derivados de tener que adquirir su propio servidor físico independiente.

- Ventajas de un servidor VPS

Las ventajas de un servidor VPS respecto a un servidor compartido es que cada instalación es independiente. En un hosting compartido todos los usuarios comparten los recursos del servidor y hay algún problema todos los usuarios pueden ver afectado el rendimiento.

En un servidor VPS esto no es así. Los recursos asignados a un VPS los utiliza solo el propio VPS y es independiente del resto de instalaciones que existan en el mismo servidor.

Con esto se gana en estabilidad y rendimiento sin la necesidad de adquirir un servidor dedicado, los cuales tienen un precio mucho más elevado.

- ¿Cuándo se necesita un Hosting VPS?

La respuesta a esta pregunta es cuando el hosting compartido se queda pequeño. Si el hosting compartido que tienes contratado ya ha llegado a su límite lo mejor es pasar a un servidor VPS.

Si, por ejemplo, tienes un sitio web con más de 100 mil visitas al día, con picos de más de 60 personas conectadas al mismo tiempo, no hay hosting compartido que lo soporte y se tendrá que recurrir a un servidor VPS.

Servicios online, app para móviles, aplicaciones web, desarrolladores, etc. que necesiten de un mayor rendimiento también pueden optar por un servidor VPS ya que les proporcionará la potencia e individualidad que necesiten sin tener que adquirir un servidor dedicado.

Cada servidor VPS (servidor virtual) mantendrá un funcionamiento autónomo e independiente de los demás disponiendo de un servicio independiente de almacenamiento, teniendo su propia configuración de aplicaciones, sistemas, panel de control y acceso, su propia memoria RAM, procesadores.

Con los Servidores VPS de Hostinet se tendrá acceso a la potencia, privacidad y seguridad que otorga un servidor dedicado propio pero con el precio de un hosting compartido (más económico al compartir máquina con otras cuentas).

Si se necesita disponer de **t**odas las ventajas que te ofrece un servidor dedicado, pero no te hace falta un equipo para ti solo, un servidor VPS (servidor virtual) es el servicio que más se adecua a las necesidades. Solo se tiene que decidir el modelo de Server VPS que más se adecue a lo que el proyecto requiere y se conseguirá al mejor precio, el rendimiento de un servidor dedicado con todas las facilidades y flexibilidad del hosting compartido.

4.5. Firewall virtual

Un cortafuegos virtual VF es un servicio o dispositivo de firewall de red que se ejecuta completamente dentro de un entorno virtualizado y que proporciona el filtro de paquetes y la supervisión habituales proporcionados a través de un firewall de red físico. El VF se puede realizar como un firewall de software tradicional en una máquina virtual invitada que ya está en ejecución, un dispositivo de seguridad virtual diseñado específicamente con la seguridad de la red virtual, un conmutador virtual con capacidades de seguridad adicionales o un proceso de kernel administrado en el host Hipervisor

- 1 Antecedentes
  - 1.1 Cortafuegos virtuales

- 2 Operación

Mientras una red de computadoras se ejecute completamente sobre el hardware físico y el cableado, es una red física. Como tal, puede ser protegido por firewalls físicos y paredes de fuego por igual; la primera y más importante protección para una red física de computadoras siempre fue y sigue siendo una puerta física, cerrada, resistente a las llamas. Desde el inicio de Internet este fue el caso, y las paredes de fuego estructurales y firewalls de red fueron durante mucho tiempo tanto necesario como suficiente.

Desde 1998, ha habido un aumento explosivo en el uso de máquinas virtuales (VM) además de máquinas físicas, a veces en vez de físicas, para ofrecer muchos tipos de servicios informáticos y de comunicaciones en redes de área local y en el Internet más amplio. Las ventajas de las máquinas virtuales están bien exploradas en otros lugares.

Las máquinas virtuales pueden funcionar de forma aislada (por ejemplo, como un sistema operativo invitado en una computadora personal) o bajo un entorno virtualizado unificado supervisado por un supervisor de monitoreo de máquina virtual o un proceso de hipervisor. En el caso de que muchas máquinas virtuales funcionen bajo el mismo entorno virtualizado, podrían conectarse entre sí a través de una red virtual que consiste en conmutadores de red virtualizados entre máquinas e interfaces de red virtualizadas dentro de las máquinas. La red virtual resultante podría entonces implementar protocolos de red tradicionales (por ejemplo TCP) o aprovisionamiento de red virtual como VLAN o VPN ,

aunque estos últimos, útiles por sus propias razones, no son de ninguna manera requeridos.

Existe una percepción constante de que las máquinas virtuales son intrínsecamente seguras porque son vistas como sandbox dentro del sistema operativo host. A menudo se cree que el host, de igual manera, está protegido contra la explotación de la propia máquina virtual y que el host no es una amenaza para la máquina virtual porque es un activo físico Protegidos por la seguridad física y de red tradicional. Incluso cuando esto no se asume explícitamente, las pruebas tempranas de las infraestructuras virtuales a menudo se desarrollan en entornos de laboratorio aislados en los que la seguridad no es, por regla general, una preocupación inmediata, o la seguridad sólo puede aparecer cuando la misma solución está entrando en producción o en una nube de computadora, donde de repente máquinas virtuales de diferentes niveles de confianza pueden terminar en la misma red virtual que se ejecuta a través de cualquier número de hosts físicos.

Debido a que son verdaderas redes, las redes virtuales pueden terminar sufriendo los mismos tipos de vulnerabilidades asociadas con una red física, algunas de las cuales son:

- Los usuarios de las máquinas de la red virtual tienen acceso a todas las demás máquinas de la misma red virtual.

- Comprometer o apropiarse mal de una máquina virtual en una red virtual es suficiente para proporcionar una plataforma para ataques adicionales contra otras máquinas en el mismo segmento de red.

- Si una red virtual está interconectada a la red física de Internet más amplia, las máquinas de la red virtual podrían tener acceso a recursos externos (y explotaciones externas) que podrían dejarlos abiertos a la explotación.

- El tráfico de red que pasa directamente entre máquinas sin pasar por dispositivos de seguridad no se supervisa.

Los problemas creados por la casi invisibilidad del tráfico entre máquinas virtuales (VM a VM) en una red virtual son exactamente iguales a los encontrados en las redes físicas, complicado por el hecho de que los paquetes pueden estar moviéndose completamente dentro del hardware de un único anfitrión físico:

- Debido a que el tráfico de la red virtual nunca puede dejar el hardware físico del host, los administradores de seguridad no pueden observar el tráfico de VM a VM, no pueden interceptarlo y, por lo tanto, no pueden saber para qué sirve ese tráfico.

- El registro de la actividad de la red VM a VM en un solo host y la verificación del acceso a la máquina virtual para fines de cumplimiento normativo se vuelven difíciles.

- Los usos inadecuados de los recursos de la red virtual y el consumo de ancho de banda VM a VM son difíciles de descubrir o rectificar.

- Los servicios inusuales o inapropiados que se ejecutan en o dentro de la red virtual pueden pasar desapercibidos.

Hay problemas de seguridad que sólo se conocen en entornos virtualizados que causan estragos en las medidas y prácticas de seguridad física, y algunos

de ellos son vistos como ventajas reales de la tecnología de la máquina virtual sobre las máquinas físicas:

- Las VM se pueden migrar deliberadamente (o inesperadamente) entre entornos virtualizados de confianza y no confiables en los que la migración está habilitada.

- VMs y / o volúmenes de almacenamiento virtual pueden ser fácilmente clonados y el clon hecho funcionar en cualquier parte del ambiente virtualizado, incluyendo una DMZ .

- Muchas empresas utilizan sus departamentos de TI o de compras como la agencia líder de seguridad de TI, aplicando medidas de seguridad en el momento en que una máquina física se extrae de la caja y se inicializa. Dado que las máquinas virtuales pueden ser creadas en pocos minutos por cualquier usuario autorizado y ejecutarse sin un rastro de papel, pueden en estos casos evitar las prácticas establecidas de seguridad de primer arranque.

- Las máquinas virtuales no tienen una realidad física que deje una huella de su creación ni (en instalaciones virtualizadas más grandes) de su existencia continuada. Pueden ser destruidos tan fácilmente como bien, dejando casi ninguna firma digital y absolutamente ninguna evidencia física cualesquiera.

Además de los problemas de visibilidad del tráfico de la red y de la dispersión no coordinada de VM, una VM deshonesta que utiliza solo la red virtual, los *switches* y las interfaces (todos los cuales se ejecutan en un proceso en el hardware físico del host) Una red física, y de las formas habituales, aunque

ahora al consumir ciclos de CPU de host, puede además reducir todo el entorno virtualizado y todas las demás máquinas virtuales con él simplemente superando los recursos físicos del host que dependen del resto del entorno virtualizado.

Esto era probable que se convirtiera en un problema, pero se percibía dentro de la industria como un problema bien entendido y potencialmente abierto a las medidas y respuestas tradicionales.

- Firewalls virtuales

Un método para asegurar, registrar y supervisar el tráfico de VM a VM implicó el enrutamiento del tráfico de red virtualizado fuera de la red virtual y hacia la red física a través de VLAN y, por lo tanto, a un firewall físico ya presente para proporcionar servicios de seguridad y cumplimiento para la seguridad física red. El tráfico de la VLAN podría ser supervisado y filtrado por el cortafuegos físico y luego devuelto a la red virtual (si se considera legítimo para ese propósito) y en la máquina virtual de destino.

No es sorprendente que los administradores de LAN, los expertos en seguridad y los proveedores de seguridad de red comenzaran a preguntarse si sería más eficiente mantener el tráfico totalmente dentro del entorno virtualizado y asegurarlo desde allí.

Un cortafuegos virtual es, entonces, un servicio de firewall o un dispositivo que se ejecuta completamente dentro de un entorno virtualizado, incluso como otra máquina virtual, pero tan fácilmente dentro del propio hipervisor, que proporciona el filtro de paquetes y la supervisión habituales que proporciona un firewall físico. El VF se puede instalar como un firewall de software tradicional en una máquina virtual invitada que ya se está ejecutando en el entorno virtualizado;

o puede ser un dispositivo de seguridad virtual diseñado específicamente con la seguridad de la red virtual en mente; puede ser un conmutador virtual con capacidades adicionales de seguridad; puede ser un proceso de kernel administrado que se ejecuta dentro del hipervisor de host que se encuentra encima de toda la actividad de VM.

La dirección actual en la tecnología de cortafuegos virtual es una combinación de conmutadores virtuales con capacidad de seguridad, y dispositivos de seguridad virtual. Algunos cortafuegos virtuales integran funciones de red adicionales, como VPN de sitio a sitio y de acceso remoto, QoS, filtrado de URL y más.

- Operación

Los *firewalls* virtuales pueden operar en diferentes modos para proporcionar servicios de seguridad, dependiendo del punto de despliegue. Normalmente, estos son modos puente o hipervisor (hypervisor-based, hypervisor-resident). Ambos pueden venir envueltos como un dispositivo de seguridad virtual y pueden instalar una máquina virtual para fines de gestión.

Un *firewall* virtual que funciona en modo puente actúa como su análogo de firewall físico-mundial; Se encuentra en una parte estratégica de la infraestructura de red -normalmente en un switch o puente virtual inter-red- e intercepta el tráfico de red destinado a otros segmentos de red y que necesita viajar sobre el puente. Examinando el origen de la fuente, el destino, el tipo de paquete que es e incluso la carga útil, el VF puede decidir si el paquete debe permitir el paso, caer, rechazar o reenviar o reflejar a algún otro dispositivo. Los principiantes iniciales en el campo virtual del cortafuego eran en gran parte puente-modo y muchas ofertas conservan esta característica.

Por el contrario, un cortafuegos virtual que funciona en modo hipervisor no es en realidad parte de la red virtual en absoluto, y como tal no tiene dispositivo físico análogo del mundo. Un *firewall* virtual de modo hipervisor reside en el monitor de la máquina virtual o hipervisor donde está bien posicionado para capturar la actividad de la VM, incluidas las inyecciones de paquetes. Se puede examinar toda la VM supervisada y todo su hardware, software, servicios, memoria y almacenamiento virtuales, así como cambios en estos. Además, dado que un *firewall* virtual basado en hipervisor no es parte de la red adecuada y no es una máquina virtual, su funcionalidad no puede ser supervisada a su vez o alterada por usuarios y programas limitados a correr bajo una VM o tener acceso solo a la red virtualizada.

Los *firewalls* virtuales en puente se pueden instalar como cualquier otra máquina virtual en la infraestructura virtualizada. Dado que se trata de una máquina virtual, la relación de la VF con la otra VM puede complicarse con el tiempo debido a que las máquinas virtuales desaparecen y aparecen de forma aleatoria, migran entre diferentes hosts físicos u otros cambios no coordinados permitidos por la infraestructura virtualizada.

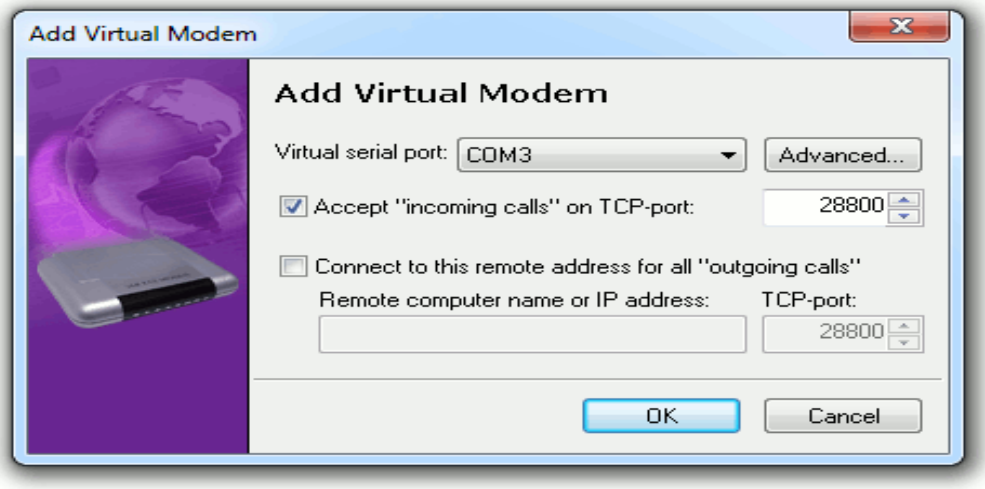
Los *firewalls* virtuales de modo hipervisor requieren una modificación en el kernel del hypervisor físico anfitrión para instalar ganchos de proceso o módulos que permitan al sistema de cortafuegos virtual acceder a información de VM y acceso directo a los conmutadores de red virtuales ya las interfaces de red virtualizadas que mueven el tráfico de paquetes entre VM o entre VM y la puerta de enlace de red. El *firewall* virtual residente en hypervisor puede usar los mismos ganchos para realizar todas las funciones de *firewall* habituales, como inspección, descarte y reenvío de paquetes, pero sin tocar la red virtual en ningún momento. Los *firewalls* virtuales de modo hipervisor pueden ser mucho más rápidos que la misma tecnología que se ejecuta en modo puente porque no están

haciendo inspección de paquetes en una máquina virtual, sino más bien dentro del kernel a velocidades de hardware nativas.

- Virtual Modem

Virtual Modem es una solución de software que reemplaza un par de módems de hardware con módems virtuales. Permite que dos aplicaciones de comunicaciones de módem interactúen a través de una red local o de Internet en lugar de marcar un número de teléfono. Olvídese de conexiones telefónicas no confiables, líneas ocupadas, cargadores de llamadas o cualquier equipo de hardware. El programa es un reemplazo absoluto de la solución de hardware.

Figura 27. **Cómo funciona**



Fuente: *Funcionamiento*. http://www.fabulatech.com/virtual-modem.html. Consulta: 3 de febrero de 2017.

Virtual Modem reemplaza completamente a los módems físicos en ambos lados. En el lado local crea un dispositivo de módem virtual que aparece en el

sistema operativo como el módem de hardware habitual. La principal diferencia es que el módem virtual marca una dirección IP remota a través de LAN o Internet en lugar de realizar una llamada telefónica real para conectarse a un lado remoto.

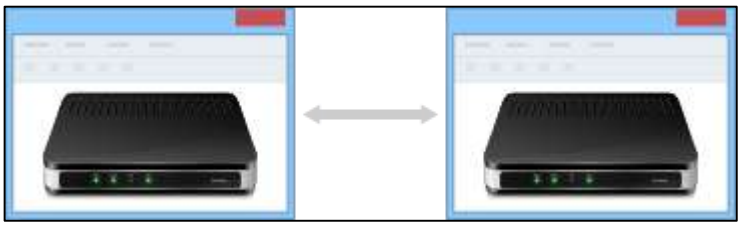
En el lado remoto, otro módem virtual detecta una conexión de red entrante y emula una llamada entrante para la aplicación de módem de escucha. Por lo tanto, las aplicaciones pueden conectarse ahora mediante una conexión de módem virtual a través de TCP / IP.

Figura 28. **Ubicación independiente**

Fuente: *Ubicación independiente*. http://www.fabulatech.com/virtual-modem.html. Consulta: 3 de febrero de 2017.

El módem virtual se puede utilizar en cualquier lugar donde la conexión a Internet o LAN esté disponible. Puede establecer una conexión de módem virtual en cualquier parte del mundo de forma gratuita.

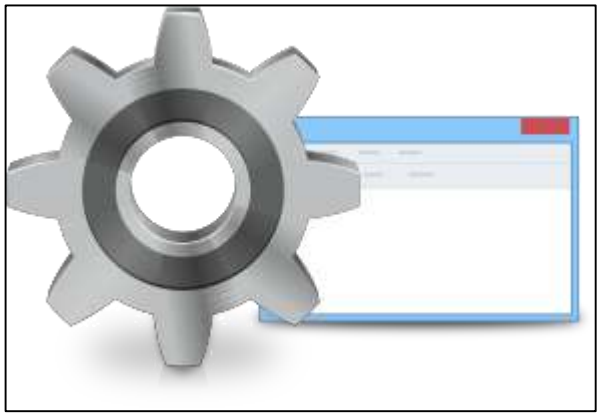
Figura 29. **Solución de software verdadera**



Fuente: *Solución de software verdadera*. http://www.fabulatech.com/virtual-modem.html. Consulta: 3 de febrero de 2017.

El módem virtual es una solución basada en software pura diseñada para reemplazar módems de hardware. El programa establece la conexión entre dos aplicaciones de comunicaciones a través de LAN o Internet. Virtual Modem emula completamente un módem de hardware en ambos equipos.

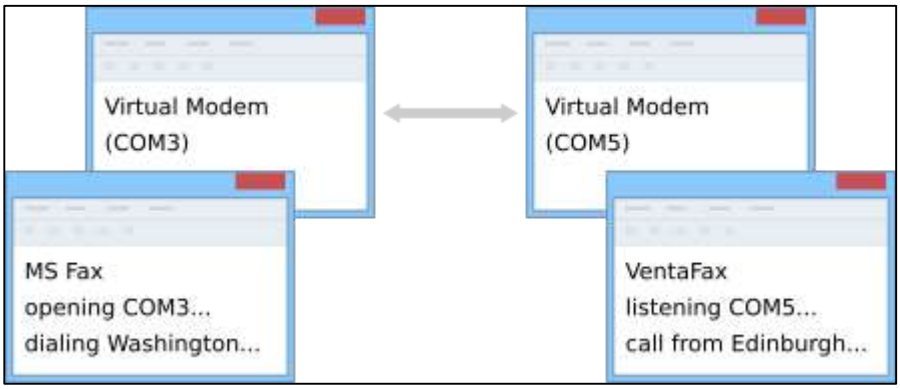
Figura 30. **Funciona como servicio del sistema**



Fuente: *Funciona como servicio del sistema*. http://www.fabulatech.com/virtual-modem.html. Consulta: 3 de febrero de 2017.

El programa hace que los módems virtuales sean accesibles en cada inicio del sistema incluso antes del inicio de sesión del usuario. Una vez configurados, los módems virtuales se crean automáticamente y no tiene que ajustar nada o incluso iniciar sesión en el sistema operativo.

Figura 31. **Ejemplo de uso**



Fuente: *Ejemplo de uso*. http://www.fabulatech.com/virtual-modem.html Consulta: 3 de febrero de 2017.

Se necesita enviar un mensaje de fax de Edimburgo a Washington DC. MS Fax se instala en una computadora en Edimburgo y Venta Fax se instala en una computadora en Washington.

Mediante el uso del software Virtual Modem, se crea un dispositivo de fax-módem virtual en ambos equipos. MS Fax en la computadora en Edimburgo "marca" la dirección IP remota en lugar de marcar un número de teléfono real y el lado remoto recibe la "llamada entrante".

Ahora puede enviar faxes de Edimburgo a Washington DC a través de Internet.

El módem virtual ofrece un método sencillo y práctico para usar Internet en lugar de llamadas telefónicas directas para software de fax, y puede ser manejado de forma transparente por cualquiera.

La solución está disponible en forma de licencia OEM de una sola vez. Esto significa que una vez comprado puede ser integrado en su propio proyecto y redistribuido sin regalías.

- Se pueden crear hasta 256 módems virtuales.
- Los módems virtuales funcionan con máquinas de fax IP.
- Las aplicaciones utilizan módems virtuales directamente desde puertos serie virtuales o a través de TAPI.
- Soporte de comandos AT principales.
- Apoyo de los principales S-registros.
- Interfaz de programa de uso fácil. Guía telefónica incluida.
- 64 bit y 32 bit compatible.
- Compatibilidad con tecnologías PnP y WMI.
- Funciona con cualquier máquina virtual.

4.5.1. Virtual *hub* (*hub* virtual)

Un conjunto de puertos conmutadores en el mismo entramado que se colocan en una agrupación lógica y usan un mecanismo de falsificación de dirección para emular un hub del ciclo arbitrado de Fibre Channel (FC-AL). Un hub virtual puede incluir todos los puertos en un único conmutador o varios puertos en uno o más conmutadores. Se usa principalmente para permitir que solo los dispositivos de ciclo más antiguos se asocien a un entramado y se pueda acceder a ellos como si contaran con capacidad de entramado.

El *hub* virtual (V*Hub*) VH4000/VH2000 de ARRIS reemplaza las instalaciones de hub típicas para 20000 clientes por un hub totalmente operativo en una carcasa de nodo estándar. Los operadores pueden iniciar soluciones completas de sistemas, como la amplificación y combinación de transmisión/difusión restringida (BC/NC), RFoG y EPON, a partir de un VHub único. Su diseño modular también asegura flexibilidad. Los operadores pueden ocupar el VHub con cualquier combinación de hasta 12 módulos para admitir aplicaciones residenciales y comerciales. El monitoreo y control remotos a través del software EMS Opti-Trace™ de ARRIS también simplifican la gestión.

Los VHubs ARRIS están disponibles en modelos de 6 y 12 ranuras. Ambos usan los mismos módulos y módulos enchufables, tienen equipos comunes de cabecera para su funcionamiento y comparten el mismo control y monitoreo integrados de estado. Con la continua incorporación de módulos enchufables cada vez más avanzados para satisfacer las necesidades en constante evolución de la industria, el VHub tiene un rol clave en las aplicaciones de hoy en día así como en las del futuro.

4.5.2. Detalles del Hub virtual (VHub) VH4000/VH2000

- Un hub totalmente operativo equivalente en una carcasa de nodo estándar.

- No es necesario tener instalaciones de hub u OTN (promedio de más de $30 mil cada una) por lo que se evitan los gastos inmobiliarios, de construcción de instalaciones, permisos adicionales, HVAC o generadores de respaldo.

- La característica compartida del módulo clave con los nodos ópticos NC4000 y NC2000 también reduce costos de repuestos e inventario.

- Admite hasta 6 (VH2000) o 12 (VH4000) módulos de ancho único, incluida cualquier combinación de EDFA, Light-Plex™ (módulo demultiplexor óptico de difusión restringida con combinadores BC/NC), interruptores ópticos, módulos e PON OLT y mucho más.

- La carcasa tiene montaje con pedestal o cable sin refrigeración externa (rango de temperatura de funcionamiento de 40 ºC a +65 ºC).

- Conexión mediante fuentes de alimentación estándar de línea coaxial de 45 - 90 VAC (consumo de energía inferior a 50 vatios).

- Capacidades de monitoreo y control de estado a través de EMS Opti-Trace.

- Admite aplicaciones residenciales y comerciales.

4.5.3. Aprovisionamiento de enlace largo

- Permite lograr el alcance máximo de los transmisores.

- Permite la colocación óptima de los amplificadores ópticos de etapa media.

- El compensador de dispersión opcional puede agregarse en la etapa media a los enlaces para incrementar aún más el rango.

- Admite el cambio a rutas alternativas.

4.5.4. VHub de RFoG

- Extiende el alcance de *down stream* y *up stream* RFoG más allá del límite tradicional P2P RFoG de 20 km con VHub.

- Crea un área de servicio de RFoG de 512 HHP en la ubicación de un nodo heredado con fibras existentes.

- Admite el cambio a rutas alternativas.

4.5.5. VHub de transmisión/difusión restringida

- Alimenta hasta 24 nodos, hasta 20 mil hogares, con una exclusiva lista de canales para cada nodo.

- El retorno digital elimina la necesidad de procesar *up stream* en el sitio del *hub*.

- Admite diversidad de rutas alternativas.

4.5.6. VHub para servicios comerciales

- Con el módulo PON OLT de nodo GE4404, los operadores pueden distribuir EPON y TURBO EPON a negocios en parques comerciales en áreas alejadas.

- Distribuye ancho de banda de 16 Gbps a hasta 1094 suscriptores de PON.

- Distribuye ancho de banda agregado de hasta 88 Gbps para acceso de punto a punto (GE, 10GE) y conexión *uplink*.

4.5.7. VHub de nodo recolector

- Extiende los desafíos de upstream y prolonga la vida útil de los láseres de DFB.

- Extiende el alcance de *upstream* a más de 100 km.

5. DISPOSITIVOS DE RED VERSUS DISPOSITIVOS DE RED EN AMBIENTE VIRTUAL

5.1. Ventajas y desventajas de la virtualización

Las soluciones óptimas para virtualizar los servidores críticos son las que se ejecutan en servidores de alta gama, por ejemplo HP Integrity Virtual Machines. Esta solución permite crear máquinas virtuales sobre servidores Itanium.

La arquitectura Itanium proporciona estupendas características de rendimiento: procesador 64 bits puro, con enormes cachés, entre otros.), fiabilidad y disponibilidad a la altura de los grandes ordenadores o mainframes. En HP Integrity Virtual Machines es posible ejecutar sistemas operativos estables como HP-UX.

La virtualización presenta múltiples ventajas para los centros de datos, principalmente desde el punto de vista de simplificación de la infraestructura física y conexiones. Pero al realizarse por software lo que antes se hacía por hardware, se introducen una nueva problemática que no existían en los entornos físicos.

5.1.1. La importancia de la gestión de la virtualización

En el apartado anterior se analizaba la importancia de elegir de la tecnología más adecuada para virtualizar correctamente el servidor que se desee; tanto o más importante es disponer de una buena herramienta de gestión.

La virtualización presenta múltiples ventajas para los centros de datos, principalmente desde el punto de vista de simplificación de la infraestructura física y conexiones**.** Pero al realizarse por software lo que antes se hacía por hardware, se introducen una nueva problemática que no existían en los entornos físicos.

Por ejemplo, si una máquina virtual puede ejecutarse en distintos servidores físicos, se debe saber en qué servidor físico se está ejecutando en cada momento. O si un servidor físico cuenta con varias máquinas virtuales que pueden estar arrancadas o no se, debe conocer en todo momento el estado de esas máquinas virtuales.

Normalmente, en un CPD convivirán servidores físicos y virtuales, por lo que la herramienta de gestión deberá permitir la administración de los dos tipos de plataformas, idealmente en una única consola**.** Además, si se utilizan diversas tecnologías de virtualización, desde esta consola deberán poderse invocar de manera transparente todas las herramientas de gestión específicas de cada plataforma.

Es idealmente, debería tratarse de una herramienta de gestión de la infraestructura con capacidad para integrarse con plataformas y soluciones de gestión empresarial**,** que nos avisen de la repercusión que un problema en una máquina virtual puede tener en el negocio.

Un ejemplo: si se detiene la máquina virtual que contiene la base de datos de clientes, se generaría una alerta en la herramienta de gestión de la infraestructura virtual; alerta que se redirigirá a la herramienta de gestión empresarial informando de que el servicio atención al cliente no está disponible.

5.2. Virtualización y negocio

Si además se quiere ligar totalmente nuestra infraestructura virtual con el negocio**,** no sólo a nivel de alertas, sino para asegurar que se satisfacen todos los compromisos de la compañía con sus clientes, se pueden utilizar las denominadas herramientas de automatización.

Las herramientas de automatización permiten definir una serie de métricas que deben cumplirse siempre en una máquina virtual, y si la herramienta detecta que se va a incumplir una métrica, es capaz de reconfigurar las máquinas virtuales para que esto no llegue a ocurrir. Esta métrica puede ser una medida de infraestructura (porcentaje consumo de CPU, MB de memoria libres) o una métrica de negocio (tiempo de respuesta, duración de un trabajo batch).

Supongamos una máquina física que alberga varias máquinas virtuales. Si una de estas máquinas virtuales contiene una aplicación cuyo tiempo de respuesta debe estar siempre por debajo de 2 segundos, pero la herramienta de automatización detecta que el tiempo de respuesta es de 1,9 segundos y es muy probable que en breve sobrepase los 2 segundos de máximo, la herramienta reconfigurará la máquina virtual asignándole, por ejemplo, más CPU.

Esta capacidad de CPU la puede obtener tomándola prestada de otra máquina virtual que se esté ejecutando en la misma máquina física (que no esté utilizando la CPU que tiene asignada), activando CPU presentes pero desactivadas de la máquina física o moviendo la máquina virtual a otra máquina física con más CPU libre disponibles, entre otras opciones.

Lo primero que hay que tener en cuenta es que la consolidación total es algo sólo teórico, que no es posible en el mundo real. La consolidación total

implicaría reutilizar todo el hardware existente, que no hubiera ningún tipo de traba política, de licenciamiento, ni de aislamiento entre aplicaciones, y lamentablemente esto no es así.

El término SLA (*servicelevelagreement* o acuerdo de nivel de servicio) se emplea mucho en las compañías, para referirse al contrato que tiene esa compañía con otras partes (normalmente clientes) de proporcionar un servicio con determinadas características de calidad.

Por ejemplo, una compañía de telefonía que ofrezca a sus clientes de línea ADSL un compromiso de sólo 30 minutos de indisponibilidad al año tendrá que vigilar una serie de métricas, que serán las que definirán si se cumple o no es SLA. Estas métricas se conocen con el nombre de SLOs (servicelevelobjectives).

Volviendo al ejemplo de la ADSL, un SLO podría ser que la aplicación que asigna dinámicamente direcciones IP a los routers domésticos de ADSL, debe proporcionar la IP en un tiempo de 5 segundos como máximo. Se podría decir que un SLA (contrato) está formado por SLOs (métricas).

Si en la herramienta de automatización se definen métricas que correspondan con los SLO, la compañía tendrá su infraestructura virtual totalmente ligada con los SLA, y por tanto, con el negocio.

5.3. Virtual WiFi router

Si utilizas un módem 3G/4G para acceder a Internet, pero tu PC está habilitada para wifi, puedes utilizar esta aplicación para permitir que otros dispositivos wifi accedan a tu conexión.

Virtual routerredundancyprotocol (VRRP) es un protocolo de penetración no propietario definido en el RFC 3768 diseñado para aumentar la disponibilidad de la puerta de enlace por defecto dando servicio a máquinas en la misma subred. El aumento de fiabilidad se consigue mediante el anuncio de un router virtual como una puerta de enlace por defecto en lugar de un router físico. Dos o más routers físicos se configuran representando al router virtual, con sólo uno de ellos realizando realmente el enrutamiento. Si el router físico actual que está realizando el enrutamiento falla, el otro router físico negocia para sustituirlo. Se denomina router maestro al router físico que realiza realmente el enrutamiento y routers de respaldo a los que están en espera de que el maestro falle.

VRRP se puede usar sobre redes Ethernet, MPLS y Token Ring. El protocolo VRRP ha sido implementado más que sus competidores. Fabricantes como Alcatel-Lucent, Extreme Networks, Dell, Nokia, Siemens-Ruggedcom, Nortel, Cisco Systems, Inc, AlliedTelesis, Juniper Networks, Huawei, Foundry Networks, Radware, Raisecom, Aethra y 3Com Corporation ofrecen routers y switches de nivel 3 que pueden utilizar el protocolo VRRP. También están disponibles implementaciones para Linux y BSD.

Hay que tener en cuenta que VRRP es un protocolo de router, no de routing. Cada instancia de VRRP se limita a una única subred. No anuncia rutas IP ni afecta a la tabla de encaminamiento.

5.3.1. Implementación

Un router virtual tiene que utilizar la siguiente dirección MAC: 00-00-5E-00-01-XX. El último byte de la dirección es el identificador de router virtual (v*irtual routerIdentifier* o VRID), que es diferente para cada router virtual en la red. Esta dirección sólo la utiliza un único router físico a la vez, y es la única forma de que

otros routers físicos puedan identificar el router maestro en un router virtual. Los routers físicos que actúan como router virtuales deben comunicarse entre ellos utilizando paquetes con dirección IP multicast 224.0.0.18 y número de protocolo IP 112.

Los routers maestros tienen una prioridad de 255 y los de respaldo entre 1 y 254. Cuando se realiza un cambio planificado de router maestro se cambia su prioridad a 0 lo que fuerza a que alguno de los routers de respaldo se convierta en maestro más rápidamente. De esta forma se reduce el periodo de agujero negro.

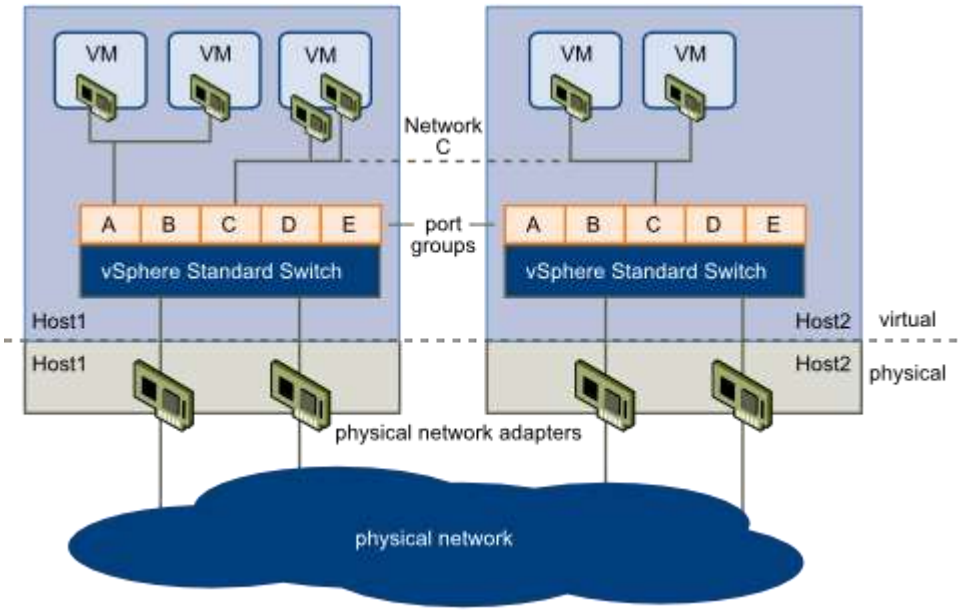
Un router virtual tiene que utilizar la siguiente dirección MAC: 00-00-5E-00-01-XX. El último byte de la dirección es el identificador de router virtual (*virtual routerIdentifier* o VRID), que es diferente para cada router virtual en la red. Esta dirección sólo la utiliza un único router físico a la vez, y es la única forma de que otros routers físicos puedan identificar el router maestro en un router virtual. Los routers físicos que actúan como router virtuales deben comunicarse entre ellos utilizando paquetes con dirección IP multicast 224.0.0.18 y número de protocolo IP 112.

Los routers maestros tienen una prioridad de 255 y los de respaldo entre 1 y 254. Cuando se realiza un cambio planificado de router maestro se cambia su prioridad a 0 lo que fuerza a que alguno de los routers de respaldo se convierta en maestro más rápidamente. De esta forma se reduce el periodo de agujero negro.

5.4. Switch virtual

En primer lugar hablaremos de los switches estándar, en este caso podemos decir que de las dos arquitecturas esta es la más limitada ya que sólo gestiona máquinas virtuales y redes a nivel host. Esta arquitectura está disponible en todas las versiones de VMWare.

Figura 32. **Switch virtual**



Fuente; switch virtuales. http://www.americagroupsrl.com/2014/11/switch-virtual-estandar-o-distribuido. Consulta:15 de febrero de 2017.

Switch estándar funciona de la misma manera que un switch físico de segundo orden, cuenta una tabla de desvío de puertos y tiene tres funciones importantes entre ellas buscar la MAC de destino de cada trama cuando estas llegan y dirigir estas tramas a uno o más puertos para que sean transmitidas y evitar envíos innecesarios .

Cada switch estándar tienen dos extremos los grupos de puertos, estos sirven para conectar las máquinas virtuales al switch virtual estándar. En el otro extremo están los puertos uplink que se encargan de conectar los switches virtuales con los adaptadores físicos de los host.

Se pueden crear hasta 127 switches estándar por host ESXI.

En cuanto a los switches distribuidos podemos diferenciarlo porque gestiona las máquinas virtuales y la red a nivel del centro de datos, esta arquitectura no está disponible en todas las versiones de VMWare, solo la podemos encontrar a partir de la versión Enterprise Plus 5.1 o posterior.

Está arquitectura cuenta con muchas más ventajas que la estándar, entre ellas tiene visibilidad del estado de toda la red tanto física como virtual. Cuenta con copias de seguridad y recuperación de configuraciones de red. Permite una recuperación rápida en caso de pérdida de conexión o configuración incorrecta.

En primer lugar hablaremos de los switches estándar, en este caso podemos decir que de las dos arquitecturas esta es la más limitada ya que sólo gestiona máquinas virtuales y redes a nivel host. Esta arquitectura está disponible en todas las versiones de VMWare.

switch estándar funciona de la misma manera que un switch físico de segundo orden, cuenta una tabla de desvío de puertos y tiene tres funciones importantes entre ellas buscar la MAC de destino de cada trama cuando estas llegan y dirigir estas tramas a uno o más puertos para que sean transmitidas y evitar envíos innecesarios .

Cada *switch* estándar tienen dos extremos los grupos de puertos, estos sirven para conectar las máquinas virtuales al *switch* virtual estándar. En el otro extremo están los puertos *uplink* que se encargan de conectar los *switches* virtuales con los adaptadores físicos de los host.

Se pueden crear hasta 127 *switches* estándar por host ESXI.

En cuanto a los *switches* distribuidos podemos diferenciarlo porque gestiona las máquinas virtuales y la red a nivel del centro de datos, esta arquitectura no está disponible en todas las versiones de VMWare, solo la podemos encontrar a partir de la versión Enterprise Plus 5.1 o posterior.

Está arquitectura cuenta con muchas más ventajas que la estándar, ente ellas tiene visibilidad del estado de toda la red tanto física como virtual. Cuenta con copias de seguridad y recuperación de configuraciones de red. Permite una recuperación rápida en caso de pérdida de conexión o configuración incorrecta.

5.5. Firewall virtual

Un cortafuegos virtual (VF) es un servicio o dispositivo de firewall de red que se ejecuta completamente dentro de un entorno virtualizado y que proporciona el filtro de paquetes y la supervisión habituales proporcionados a través de un *firewall* de red físico.El VF se puede realizar como un firewall de software tradicional en una máquina virtual invitada que ya está en ejecución, un dispositivo de seguridad virtual diseñado específicamente con la seguridad de la red virtual, un conmutador virtual con capacidades de seguridad adicionales o un proceso de kernel administrado en el host Hipervisor.

5.5.1. Firewalls virtuales

Un método para asegurar, registrar y supervisar el tráfico de VM a VM implicó el enrutamiento del tráfico de red virtualizado fuera de la red virtual y hacia la red física a través de VLANs y, por lo tanto, a un firewall físico ya presente para proporcionar servicios de seguridad y cumplimiento para la seguridad física red.El tráfico de la VLAN podría ser supervisado y filtrado por el cortafuegos físico y luego devuelto a la red virtual (si se considera legítimo para ese propósito) y en la máquina virtual de destino.

No es sorprendente que los administradores de LAN, los expertos en seguridad y los proveedores de seguridad de red comenzaran a preguntarse si sería más eficiente mantener el tráfico totalmente dentro del entorno virtualizado y asegurarlo desde allí.

Un cortafuegos virtual es entonces un servicio de *firewall* o un dispositivo que se ejecuta completamente dentro de un entorno virtualizado - incluso como otra máquina virtual, pero tan fácilmente dentro del propio hipervisor - que proporciona el filtro de paquetes y la supervisión habituales que proporciona un *firewall* físico. El VF se puede instalar como un firewall de software tradicional en una máquina virtual invitada que ya se está ejecutando en el entorno virtualizado; O puede ser un dispositivo de seguridad virtual diseñado específicamente con la seguridad de la red virtual en mente; o puede ser un conmutador virtual con capacidades adicionales de seguridad; o puede ser un proceso de kernel administrado que se ejecuta dentro del hipervisor de host que se encuentra encima de toda la actividad de VM.

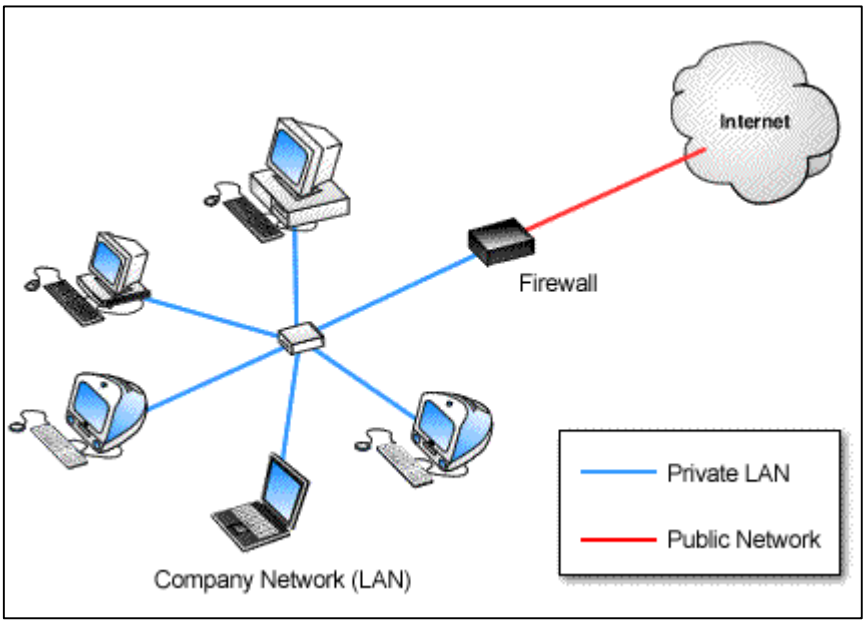
La dirección actual en la tecnología de cortafuegos virtual es una combinación de conmutadores virtuales con capacidad de seguridad, [18] y

dispositivos de seguridad virtual. Algunos cortafuegos virtuales integran funciones de red adicionales, como VPN de sitio a sitio y de acceso remoto, QoS, filtrado de URL y más.

5.5.1.1. Tipos de Firewalls: Ventajas y desventajas

Se conocen a los *firewall* de capa de red o filtrado de paquetes, es hora de conocer otro de los tipos de *firewalls*: los de capa de aplicación o Gateway. Son aquellos que como su mismo nombre indica, trabajan bajo en nivel 7 de la capa de aplicación del modelo OSI (*open systeminterconection*, el cual es un modelo creado por la International Standard Organization o ISO para la interconexión de redes de computadoras).

Figura 33. **Tipos de firewall**



Fuente; *Tipos de firewall*. http://www.informatica-hoy.com.ar/seguridad-informatica/Tipos-de-firewall.php.Consulta. 15 de marzo de 2017.

El nivel 7 se refiere al nivel que define, analiza e inspecciona los protocolos a utilizar para intercambiar datos, como correos electrónicos, ficheros FTP, páginas web (HTTP), entre otros. Es decir, regulan el tipo de protocolo a utilizarse. Por ejemplo, se podría restringir accesos a algunas páginas web mediante esta herramienta. Uno de los firewalls más destacados dentro de este sistema es el de *Sonicwall* y el de *iTinySoft*.

Se encuentran también a los *firewalls* personales, que son aquellos que se instalan en la computadora como un software, y filtra la información entre la computadora y el resto de la red.

Entre las ventajas y desventajas de contar con un *firewall* son las siguientes:

- Ventajas
    - Protección de información privada: define que usuarios de la red y que información va a obtener cada uno de ellos.
    - Optimización de acceso: define de manera directa los protocolos a utilizars
    - Protección de intrusos: protege de intrusos externos restringiendo los accesos a la red.
- Desventajas:
    - No protege de ataques que no pasen a través del *firewall*.
    - No protege amenazas y ataques de usuarios negligentes.

- No protege de la copia de datos importantes si se ha obtenido acceso a ellos.

- No protege de ataques de ingeniería social (ataques mediante medios legítimos. Por ejemplo el atacante contacta a la víctima haciéndose pasar por empleado de algún banco, y solicita información confidencial, por ejemplo, datos de la tarjeta de crédito, con el pretexto de la renovación de dicha tarjeta).

5.6. Virtual Modem PRO

5.6.1. Software de módem virtual

Virtual Modem PRO crea módems IP virtuales de software utilizando la tecnología de puertos serie virtual de Eltima. Todos los módems virtuales creados se asignan a puertos serie virtuales en su sistema operativo. Los módems virtuales emulan completamente los módems de hardware reales y duplican su funcionalidad. Sin embargo, los módems virtuales pueden hacer más, ya que utilizan la red Ethernet, incluyendo Internet, VLAN y VPN en lugar de línea telefónica convencional.

La conexión entre estos módems es mucho más rápida y más fiable que la conexión regular a través de la línea telefónica.Virtual Modem PRO es capaz de crear hasta 255 módems virtuales que funcionan exactamente como los reales (soportando los comandos Hayes AT) mediante el uso del protocolo TCP / IP para establecer la conexión con el *host* remoto.

5.6.1.1. Modem Virtual

Un módem es un dispositivo electrónico que posibilita transmitir y recepcionar datos binarios, o sea, datos computarizados, mediante un sistema telefónico. Existen dos categorías de módem en dependencia de su modo de instalación en la PC, los módems internos y los externos. Existen también los llamados cables módem que difieren en gran medida de los módems convencionales.

- Qué es un módem

Un módem (acrónimo de modulador-demodulador) no es más que un dispositivo electrónico que posibilita la transmisión y recepción de datos binarios, o sea, datos computarizados mediante un sistema telefónico.

Existen dos categorías de módem en dependencia de su modo de instalación en la PC, estos son:

Módem interno: estos son conectados en una ranura de expansión de la Motherboard y tienen dos puertos para la conexión telefónica in-out para la entrada de la señal y para la salido hacia un teléfono.

Módem externo: se ubica en un receptáculo o caja independiente. Este, a diferencia del interno, puede necesitar un suministro de energía eléctrica independiente. Se conecta a la PC a través de un puerto USB e igualmente tiene dos conectores telefónicos *in-out*.

- Ventajas y desventajas

Los módem tienen algunas ventajas para la conexión a Internet con respecto a otros métodos (vía satélite, etc.); también presentan desventajas. Antes de referirse a ellas, se detallan primero las ventajas respectivas entre los módems internos y externos.

- Módem interno

    - Al estar dentro de la PC no ocupan espacio adicional en el escritorio.
    - No utilizan ningún puerto de la PC.
    - Más económicos.

- Módem externo

    - No utilizan ninguna ranura de expansión
    - Podemos chequear permanentemente su estado a través de los led indicadores.
    - Son generalmente más resistentes y confiables que los módems internos.

Algunas ventajas y desventajas de la conexión vía a Internet.

- Ventajas

    - Servicio más barato
    - Sencillez de la conexión

- Desventajas

    - Imposibilidad de utilizar la línea telefónica para Internet y llamadas telefónicas simultáneamente.
    - Cortes de comunicación.
    - Líneas ocupadas.
    - Menor velocidad que muchas otras vías de acceso a Internet.

Ahora bien, todo lo referido anteriormente se refiere al clásico sistema de conexión de módem para internet telefónico (conocido como *dial-up*), pero existe otro modo de conexión más reciente denominado cable módem que es más ventajoso que el tradicional sistema *dual-up*:

- Ventajas del cable módem

    - Conexiones mucho más rápidas
    - No se necesitan líneas telefónicas
    - No sufre interrupciones

- Desventajas

    - Costo fijo y más elevado generalmente que el servicio dual-up
    - El servicio no existe en todos los lugares

Figura 34. **Ventajas**

Fuente: *Ventajas*. http://www.k-log.es/img/servicios-reduccion.jpg. Consulta: 16 de marzo de 2017.

- Menor costo de instalaciones. La compañía no tiene que contar con tanta capacidad de oficinas, debido a que algunos empleados están trabajando en otro lado. Esto permite reducir los costos en alquiler y expansión de oficinas.

Figura 35. **Menor costo de equipo.**

Fuente: *Menor costo del equipo*. http://oficinavirtual-sig.blogspot.com/p/ventajas-y-desventajas-de-la-oficina.html. Consulta: 16 de marzo de 2017.

- Menor costo de equipo. En lugar de proporcionar equipo de oficina a cada empleado, los trabajadores a distancia pueden compartir gran parte de equipo de forma similar como los usuarios de una LAN comparten sus recursos.

Figura 36. **Red formal de comunicaciones**

Fuente: *Red Formal de comunicaciones*. http://oficinavirtual-sig.blogspot.com/p/ventajas-y-desventajas-de-la-oficina.html. Consulta: 16 de marzo de 2017.

- Red formal de comunicaciones. Como los trabajadores a distancia deben mantenerse informados y recibir instrucciones específicas, deben prestar más atención a la red de comunicación. En la oficina tradicional mayor parte de la información se comunica a través de conversaciones casuales o por medio de la observación.
-

Figura 37. **Menos interrupciones en el trabajo.**

Fuente: *Menos interrupciones*. http://oficinavirtual-sig.blogspot.com/p/ventajas-y-desventajas-de-la-oficina.html. Consulta: 16 de marzo de 2017.

- Menos interrupciones en el trabajo. Cuando existen fenómenos naturales o se colapsan los medios de transporte esto impide a los empleados trasladarse, por ejemplo desde su hogar hasta la oficina interrumpiendo así o paralizándose las actividades de la organización.

Figura 38. **Contribución social**

Fuente: *Contribución social*. http://oficinavirtual-sig.blogspot.com/p/ventajas-y-desventajas-de-la-oficina.html. Consulta: 16 de marzo de 2017.

- *Contribución social.* Permite a la empresa contratar a personas que de otra manera no tendrían oportunidad de trabajar. Las personas con discapacidad, los adultos mayores y los padres con hijos pequeños son los más beneficiados ya que pueden trabajar desde la comodidad de su hogar.

- Sensación de aislamiento. Cuando los empleados no entran en contacto a diario con sus colegas, pierden la sensación de ser una parte importante en la organización.

Figura 39. **Aislamiento**

Desventajas

Fuente: *Aislamiento*. http://oficinavirtual-sig.blogspot.com/p/ventajas-y-desventajas-de-la-oficina.html. Consulta: 16 de marzo de 2017.

- Temor a perder el trabajo. Puesto que el trabajo del empleado se realiza con independencia de la operación de la compañía, los empleados fácilmente pueden comenzar a sentir que no son indispensables y que son reemplazables por cualquier persona que pueda utilizar una computadora y un módem.

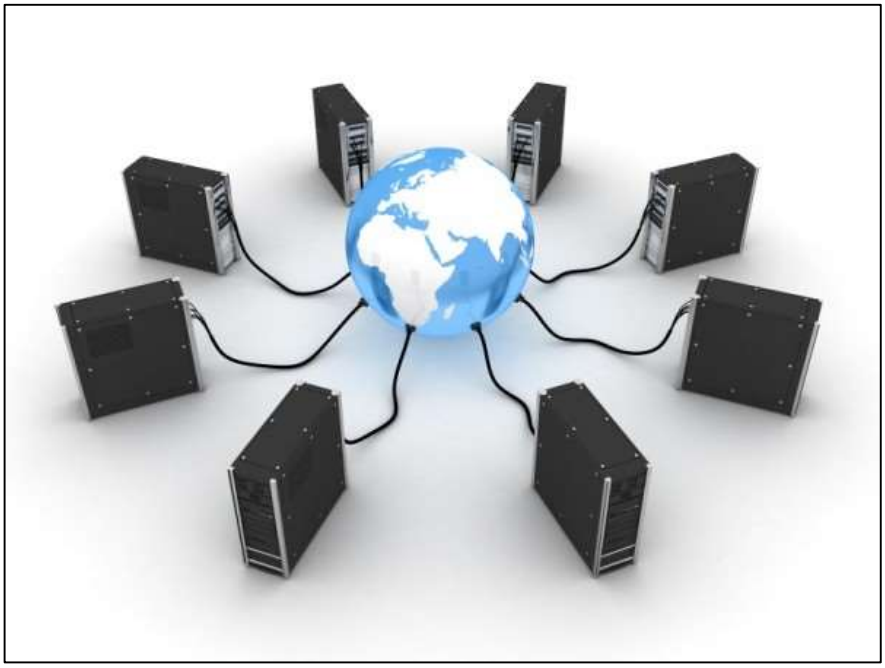
Figura 40. **Temor a perder el trabajo**

Fuente: *Temor a perder el trabajo*. http://oficinavirtual-sig.blogspot.com/p/ventajas-y-desventajas-de-la-oficina.html. Consulta: 16 de marzo de 2017.

- Decaimiento en el ánimo. La ausencia de retroalimentación positiva que se genera a través de una interacción a cara a cara con superiores o iguales. Otro factor es que los sueldos de los trabajadores a distancia suelen ser menores que los que trabajan en oficinas fijas.

- Tensión familiar. Si hay tensiones en la casa el trabajador no puede escapar de ellas, aumentando así la tensión y no puede concentrarse en el trabajo.

Figura 41. **Principales ventajas de los servidores virtuales**



Fuente*: Principales ventajas de los servidores virtuales*.
http://www.muycomputerpro.com/2014/01/29/servidor-virtual. Consulta: 16 de marzo de 2017.

Un servidor virtual es aquel que tiene una partición dentro de otro servidor que habilita varias máquinas virtuales por medio de varias tecnologías. Es una

solución muy utilizada por empresas de hosting y de dominios ya que ofrecen varias ventajas respecto a los servidores tradicionales. Alguna de sus ventajas son las siguientes.

- Personalizables**.** Los servidores virtuales pueden ser configurados según la capacidad que cada cliente considere oportuna para ofrecer sus servicios. De esta forma, se pueden delimitar los recursos físicos que se van a consumir, como por ejemplo el disco duro y la memoria RAM.

- Seguros. Estas máquinas virtuales están redundadas, de forma que no están vinculadas a un único servidor físico. Esto permite que si un componente utilizado por el cliente se detiene por alguna razón, hay otro recorrido válido, por lo tanto el servicio sigue siempre activo y no hay ningún fallo.

- Escalables. Debido a que los servidores virtuales no son una máquina física, el cliente puede ampliar su capacidad en cualquier momento y pasar a utilizar más recursos. De esta forma, el cliente puede adaptar su servidor en caso de que pase a alojar más webs o de que su tráfico aumente.

- Economías de escala**.** De cara a los proveedores de alojamiento para webs, los servidores virtuales tienen la ventaja de que, aunque haya que hacer un desembolso inicial significativo, el retorno de la inversión es muy alto cuantos más clientes se tiene. De lo contrario, los revendedores tendrían que comprar un servicio de hosting compartido para cada uno de sus clientes.

- IP única. Los servidores virtuales cuentan con una dirección IP única, aunque compartan espacio físico con otros servidores virtuales en una

misma máquina física. Con esto se evitan los problemas del hosting compartido que, al concurrir cientos de miles de clientes en un servidor, puede dar problemas por motivos de búsqueda o puede provocar que una página termine en una lista negra, en el caso de que un cliente esté haciendo un uso fraudulento. De forma complementaria, los revendedores pueden contratar varias direcciones IP y asignarlas a cada uno de los dominios que alojan.

- Más baratos que el cloud. En caso de que sea una PYME la que esté interesada en contratar un servicio de hosting dedicado, la ventaja del servidor compartido sobre los servidores cloud es el ahorro. Los servidores cloud establecen unos parámetros de tráfico que, de ser sobrepasados, suponen un sobrecoste para el cliente; sin embargo, las empresas pueden tener picos de actividad y tener tráfico en todo momento, por lo que los virtuales ofrecen una solución más adecuada.

- Servicio de *backup*. Nominalia dispone de un servicio de backup que mejora las condiciones de seguridad de sus productos. Con espacio *Backup*, el cliente puede contratar un espacio de 500 gigabytes para almacenar una copia de seguridad de la información que tiene en su servidor virtual o dedicado. Al tratarse de un almacenamiento que se efectúa en una máquina diferente del servidor del cliente, los datos quedan protegidos ante cualquier contratiempo que surja en estos dispositivos.

Los servidores virtuales de Nominalia se basan en un clúster; detrás del hardware virtual hay una máquina física, pero siempre está redundada, por lo que es mucho más seguro, asegura Marco Gori, SeniorProduct Manager del grupo multinacional europeo Dada, al que pertenece Nominalia. *En comparación con el servidor dedicado, el virtual supone un ahorro, especialmente en la configuración*

que utiliza Nominalia, ya que la plataforma está aprovechada al máximo. De esta forma, además, la huella de carbono es mínima", concluye.

5.7. Hub Virtual

Concentrador (*hub*) es el dispositivo que permite centralizar el cableado de una red de computadoras, para luego poder ampliarla.

Trabaja en la capa física (capa 1) del modelo OSI o la capa de acceso al medio en el modelo TCP/IP. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos (repetidor).

En la actualidad, la tarea de los concentradores la realizan, con frecuencia, los conmutadores (*switches*).

Un conjunto de puertos conmutadores en el mismo entramado que se colocan en una agrupación lógica y usan un mecanismo de falsificación de dirección para emular un hub del ciclo arbitrado de FibreChannel (FC-AL). Un hub virtual puede incluir todos los puertos en un único conmutador o varios puertos en uno o más conmutadores. Se usa principalmente para permitir que solo los dispositivos de ciclo más antiguos se asocien a un entramado y se pueda acceder a ellos como si contaran con capacidad de entramado.

- Ventajas

    - Dejan pasar paquetes de cualquier protocolo
    - Pueden instalarse en diferentes tipos de cable
    - Se usan para extender al máximo posible la distancia entre nodos de un segmento

- Desventajas

    - Dejan pasar paquetes con errore
    - No permiten filtrado de paquetes.
    - Incrementan el tráfico congestionando todos los segmentos de la LAN.
    - Limitación del número de repetidores a utilizar.

CONCLUSIONES

1. Se logró mejorar los dispositivos de red en ambientes virtual y físico y se implementó una red en un proyecto de infraestructura de red.

2. Se logró describir adecuadamente la conexión de los diferentes dispositivos con los ordenadores en ambiente virtual así como los requisitos necesarios en cada uno de los componentes logrando agilizar el proceso de diseño de las redes.

3. Se establecieron las ventajas y desventajas del uso de los dispositivos en ambiente virtual sobre su contraparte física contribuyendo así a la toma de decisiones de infraestructura de red.

4. De una manera adecuada se logró asegurar la portabilidad y uso de los dispositivos de red (físicos como virtuales), y además se aseguró la implementación de los diferentes dispositivos.

5. Con una adecuada capacitación y demostraciones se logró promover el uso de los dispositivos de red físicos como virtuales indicando cual es el comportamiento de los mismos con los ordenadores y el uso de la memoria.

RECOMENDACIONES

1. Para que la red tenga un funcionamiento optimó es necesario revisar las líneas, los *routers*, *switches,* servidores, *firewall*, *hubs,* entre otros, un tiempo no mayor de seis meses, esto ayudará a que no halla colapsos en dicha red cuando hallan varios dispositivos funcionando al mismo tiempo.

2. Capacitar al personal que este encargado de dicha red, para que estén informados y sepan cómo solventar situaciones que se puedan presentar al momento que hallan colapsos o deficiencias en el sistema que se este implementando o utilizando.

3. Comprar, *routers, switches, servidores, firewall, hubs,* de mayor capacidad para que no hallan deficiencias cuando se desee implementar o conectar más dispositivos en dicha red y con esto se estará previendo un gasto innecesario.

BIBLIOGRAFÍA

1. *Análisis de tráfico de red en ambiente virtualizado*. [en línea]. <http://searchdatacenter.techtarget.com/es/consejo/Analisis-de-trafico-de-red-en-ambiente-virtualizado>.[Consulta: 10 de enero de 2017].

2. *Aspectos básicos de redes*. [en línea]. <http://itpn.mx/recursosisc/6semestre/redesdecomputadoras/Unidad%20III.pdf> [Consulta: 11 de enero de 2017].

3. *Cómo crear modem virtual.* [en línea].< http://www.taringa.net/post/hazlo tu-mismo/17002409/Crear-Modem-Virtual-Sin-Programas-Paso-A-Paso.html>. [Consulta: 10 de enero de 2017].

4. *Conmutador dispositivo de red* [en línea]. <https://es.wikipedia.org/wiki/Conmutador_(dispositivo_de_red)>. [Consulta: 12 de enero de 2017].

5. *Crear un modem virtual*. [en línea] <http://www.taringa.net/post/hazlo-tu-mismo/17002409/Crear-Modem-Virtual-Sin-Programas-Paso-A-Paso.html>.[Consulta: 11 de enero de 2017].

6. *Definición de las 7 capas del modelo osi*. [en línea]. <https://support.microsoft.com/es-gt/kb/103884>. [Consulta: 10 de enero de 2017].

7. *Diferentes tipos de dispositivos de redes*. [en línea]. <https://darkub.wordpress.com/2008/01/19/diferentes-tipos-de-dispositivos-de-redes/>.[Consulta: 10 de enero de 2017].

8. *Dispositivos Activos y pasivos*. [en línea]. <https://es.slideshare.net/wwwgooglecomco/dispositivos-activos-y-pasivos1-1> [Consulta: 12 de enero de 2017].

9. *Dispositivos de red*. [en línea]. <http://es.slideshare.net/tati-pineda/dispositivos-de-red-10078566?next_slideshow=3> [Consulta: 12 de enero de 2017].

10. *Dispositivos de red virtual.* [en línea]. <http://docs.oracle.com/cd/E24621_01/html/E23598/virtualnetworkdevice.html> [Consulta: 12 de enero de 2017].

11. *Entorno virtual de aprendizaje*. [en línea]. <https://es.wikipedia.org/wiki/Entorno_Virtual_de_Aprendizaje>. [Consulta: 10 de enero de 2017].

12. *Modem*. [en línea].<https://es.wikipedia.org/wiki/Modem> [Consulta: 11 de enero de 2017].

13. Principales ventajas de servidores virtuales. [en línea] <http://www.muycomputerpro.com/2014/01/29/servidor-virtual> [Consulta: 28 de febrero de 2017].

14. *Que es un firewall y c*omo funciona. [en línea] <http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Firewall-y-como-funciona.php>.[Consulta:12 de febrero de 2017].

15. *Que es un hub virtual*. [en línea] <http://es.arris.com/productos/acceso/hub-virtual-vhub-para-planta-exterior-64j/>. [Consulta: 12 de febrero de 2017].

16. *Que es un servidor.* [en línea].<http://www.masadelante.com/faqs/servidor>. [Consulta: 12 de enero de 2017].

17. *Que es un servidor virtual*. [en línea] <https://www.hostinet.com/servidores-vps/que-es-un-servidor-virtual-que-es-un-servidor-vps/>.[Consulta:12 de febrero de 2017].

18. *Red de computadora.* [en línea]. <https://es.wikipedia.org/wiki/Red_de_computadoras#Dispositivos_de_red>. [Consulta: 12 de enero de 2017].

19. Reglas fundamentales para la administración del firewall. [en línea].<http://www.dell.com/learn/co/es/cobsdt1/sb360/sb-newsletter-3-2012-2>.[Consulta: 10 de enero de 2017].

20. *Switch virtual y cómo funciona la red en vmware.* [en línea]. <https://www.josemariagonzalez.es/2012/02/16/que-es-un-switch-virtual-y-como-funciona-red-vmware.html> [Consulta: 10 de enero de 2017].

21. *Servidor vps*. [en línea].<https://www.hostinet.com/servidores-vps/que-es-un-servidor-virtual-que-es-un-servidor-vps/>[Consulta: 11 de enero de 2017].

22. *Softether vpn*. [en línea]. <https://www.softether.org/4-docs/1-manual/3._SoftEther_VPN_Server_Manual/3.4_Virtual_Hub_Functions> [Consulta: 11 de enero de 2017].

23. *Switch virtual* [en línea] <https://www.josemariagonzalez.es/2012/02/16/que-es-un-switch-virtual-y-como-funciona-red-vmware.html> [Consulta: 12 de febrero de 2017].

24. *Tipos de firewall Ventajas y desventajas*. [en línea] <https://www.actualidadgadget.com/tipos-de-firewalls-ventajas-y-desventajas/>.[Consulta:18 de febrero de 2017].

25. *Ventajas y desventajas de la conexión vía módem*. [en línea] <http://isbelg.over-blog.com/article-internet-via-modem-ventajas-desventajas-conexion-86799580.html>.[Consulta:18 de febrero de 2017].

26. *Ventajas y desventajas de la oficina virtual.* [en línea] <http://oficinavirtual-sig.blogspot.com/p/ventajas-y-desventajas-de-la-oficina.html> [Consulta: 18 de febrero de 2017].

27. *Ventajas y desventajas del switch.* [en línea]. <http://alexis-pe.blogspot.com/2011/08/ventajas-y-desventajas-del-switch.html.> [Consulta: 11 de enero de 2017].

28. *Ventajas y desventajas de la tecnología en la sociedad*. [en línea] https://julyvelez.wordpress.com/2012/06/01/ventajas-y-desventajas-de-la-tecnologia-en-la-sociedad/ [Consulta: 12 de febrero de 2017].

29. *Virtual firewall*. [en línea]. <https://en.wikipedia.org/wiki/Virtual_firewall.> [Consulta: 11 de enero de 2017].

30. *Virtual hub* [en línea] <https://www.symantec.com/es/mx/security_response/glossary/define.jsp?letter=v&word=virtual-hub> [Consulta: 28 de febrero de 2017].

31. *Virtual router*. [en línea].<https://virtualrouter.codeplex.com/>.[Consulta: 11 de enero de 2017].