

**UNIVERSIDAD NACIONAL DEL CALLAO
ESCUELA DE POSGRADO
UNIDAD DE POSGRADO DE LA FACULTAD DE
INGENIERÍA
ELÉCTRICA Y ELECTRÓNICA**



**“VIRTUALIZACIÓN COMO HERRAMIENTA PARA LA
ENSEÑANZA DE REDES DE COMPUTADORAS”**

**TESIS PARA OPTAR EL GRADO ACADÉMICO DE
DOCTOR EN INGENIERÍA ELÉCTRICA**

Autor: M. Sc. JORGE GUSTAVO BUTLER BLACKER

**Callao – 2018
PERÚ**

HOJA DE REFERENCIA DEL JURADO

MIEMBROS DEL JURADO

Dr.	: FERNANDO JOSÉ OYANGUREN RAMÍREZ	PRESIDENTE
Dr.	: JUAN HERBER GRADOS GAMARRA	SECRETARIO
Dr.	: NICANOR RAÚL BENITES SARAIVA	MIEMBRO
Dr.	: NOÉ MANUEL JESÚS CHÁVEZ TEMOCHE	MIEMBRO
Dr.	: MARCELO NEMESIO DAMAS NIÑO	ASESOR

Nº DE LIBRO : 01

FOLIO : 076

FECHA DE APROBACIÓN : octubre 05, 2018

RESOLUCIÓN DIRECTORAL : 050-2018-DUPFIEE

DEDICATORIA

A Dios y la Virgen Santísima por
darme siempre fuerzas para
seguir.

INDICE

RESUMEN	6
ABSTRACT	8
I. PLANTEAMIENTO INICIAL DE LA INVESTIGACIÓN	10
1.1 Identificación del problema.....	10
1.2 Formulación del problema.....	15
1.3 Objetivos de la investigación.....	16
1.3.1 General.....	16
1.3.2 Específicos.....	16
1.4 Justificación de la investigación.....	16
II. MARCO TEÓRICO	19
2.1 Antecedentes del estudio.....	19
2.2 Marco Teórico conceptual.....	44
2.2.1 Fundamento ontológico.....	48
2.2.2 Fundamento epistemológico.....	53
2.2.3 Fundamento metodológico.....	64
2.3 Definiciones de términos básicos.....	67
III. VARIABLES E HIPOTESIS	70
3.1 Definición de las variables.....	70
3.2 Operacionalización de las variables.....	70
3.3 Hipótesis general e hipótesis específicas.....	71
IV. METODOLOGIA	73
4.1 Tipo de Investigación.....	73
4.2 Diseño de la Investigación.....	73
4.2.1 Conceptos básicos de sistemas de virtualización.....	74
4.2.2 Velnet.....	76
4.2.3 Software de Virtualización.....	89
4.2.4 Laboratorios de Redes Virtuales.....	91
4.2.5 Implementación de laboratorios Virtuales.....	97
4.2.6 Ejemplos de los ejercicios en los laboratorios de redes virtuales.....	98
4.2.7 Experiencias en laboratorio virtuales.....	100
4.3 Población y muestra.....	161
4.4 Técnicas e instrumentos de recolección de datos.....	161
4.5 Procedimiento de recolección de datos.....	162

V. RESULTADOS	163
5.1 Análisis de las características técnicas.....	163
5.2 Investigación de la opinión de los alumnos	165
VI. DISCUSIÓN DE RESULTADOS	168
6.1 Contrastación de la hipótesis con los resultados	168
6.2 Contrastación de resultados con otros estudios similares	170
VII. CONCLUSIONES	173
VIII. RECOMENDACIONES	175
IX. REFERENCIAS BIBLIOGRAFICAS	176
ANEXOS	179
✓ Matriz de consistencia.....	179
✓ Constancia de la FIEE-UNI del uso del laboratorio par la implementación de la tesis.	
✓ Formato de Encuesta	
✓ Estadística de Encuesta	

INDICE DE FIGURAS

<i>Fig. 2.1 Ilustración de un ambiente de red virtual</i>	<i>20</i>
<i>Fig. 2.2 Aplicaciones corriendo en máquina virtual.....</i>	<i>23</i>
<i>Fig. 2.3 Sistemas operativos operando en máquinas virtuales.....</i>	<i>25</i>
<i>Fig. 2.4 Proceso de virtualización</i>	<i>26</i>
<i>Fig. 2.5 IBM AS/400 (Fuente IBM del Perú).....</i>	<i>30</i>
<i>Fig. 2.6 Ordenamiento de las páginas en la estrategia del reloj</i>	<i>38</i>
<i>Fig. 2.7 El hipervisor.....</i>	<i>40</i>
<i>Fig. 2.8 Categorías de VMM</i>	<i>43</i>
<i>Fig. 2.9 Modelo de virtualización con Spice.....</i>	<i>46</i>
<i>Fig. 2.10 El Campus virtual y sus espacios virtuales</i>	<i>57</i>
<i>Fig. 4.1 Los componentes de Velnet.....</i>	<i>77</i>
<i>Fig. 4.2 Windows 2000 con 5 VM</i>	<i>79</i>
<i>Fig. 4.3 Topología de laboratorios de redes</i>	<i>85</i>
<i>Fig. 4.4 Arquitectura general de Virtualización sobre un servidor con cuatro máquinas virtuales.....</i>	<i>95</i>

<i>Fig. 4.5 Arquitectura general de un servidor sin virtualización</i>	<i>95</i>
<i>Fig. 4.6 Red física</i>	<i>96</i>
<i>Fig. 4.7 Topología física de partida (inicio)</i>	<i>101</i>
<i>Fig. 4.8 Topología básica para el ejercicio 1</i>	<i>102</i>
<i>Fig. 4.9 Topología inicial para el ejercicio 2</i>	<i>105</i>
<i>Fig. 4.10 Direccionamiento público y privado</i>	<i>115</i>
<i>Fig. 4.11 Ventana de configuración de parámetros en Windows 7</i>	<i>118</i>
<i>Fig. 4.12 Configuración de DHCP</i>	<i>119</i>
<i>Fig. 4.13 Conexiones Switch – Router – Pc (CISCO)</i>	<i>124</i>
<i>Fig. 4.14 Ejercicio de configuración de Router</i>	<i>126</i>
<i>Fig. 4.15 Algoritmo de DIJKSTRA</i>	<i>137</i>
<i>Fig. 4.16 Modelo FTP</i>	<i>138</i>
<i>Fig. 4.17 Modo activo de conexión</i>	<i>147</i>
<i>Fig. 4.18 Modo pasivo de conexión</i>	<i>149</i>
<i>Fig. 4.19 Esquema de localización de un cortafuego en una red</i>	<i>152</i>
<i>Fig. 4.20 Interfaz de usuario para un cortafuego</i>	<i>152</i>

INDICE DE TABLAS

<i>Tabla 2.1 Estrategias para el reemplazo de páginas</i>	36
<i>Tabla 2.2 Funciones de la gestión del conocimiento</i>	55
<i>Tabla 4.1 Algunas herramientas para virtualización</i>	90
<i>Tabla 4.2 Características de software para virtualización</i>	92
<i>Tabla 4.3 Laboratorios básicos de redes</i>	99
<i>Tabla 4.4 Clases de direcciones IP</i>	120
<i>Tabla 5.1 Resultados técnicos los componentes</i>	164
<i>Tabla 5.2 Resultado da encuesta a los alumnos</i>	167

RESUMEN

El uso de la tecnología de la Virtualización no es una simple especulación del futuro de las computadoras. Los montos en inversiones y ganancias de parte de compañías líderes en el diseño y producción de software y hardware de cómputo lo demuestran de forma contundente. VMware es una empresa que ha logrado diseñar que en un mismo servidor corran distintos sistemas operativos y distintas aplicaciones. Las expectativas puestas en la Virtualización se reflejaron perfectamente en la salida a bolsa de VMware cuando superó al estreno en el parque de Google y se situó entre las cuatro empresas de mayor capitalización bursátil del Nasdaq. VMware aprovechó bien su temprana participación en el mercado, logrando un crecimiento interanual del 90% y una facturación de 9,139'000,000 de pesos (703'000,000 de dólares) en lo que llevaba de ejercicio en esa fecha. La compañía asegura que su software de Virtualización supone un ahorro no menor a los 120'000,000 de pesos anuales (6,000 euros) por aplicación en cada servidor. De este ahorro 25,440 pesos corresponden a un recorte en el gasto energético y de refrigeración, sin contar con el ahorro de espacio pues con menos máquinas se necesitan menos metros cuadrados para instalar equipos. El gran impulso de la utilización de la Virtualización va a venir marcado por la entrada en el mercado de Microsoft, quien a partir de febrero incorporó de serie en su Windows Server 2008 su software de Virtualización Hyper-V. Microsoft ya había incursionado en la Virtualización con su Virtual Server

2005 R2 en el que cuatro servidores físicos hospedaban cada uno de 10 a 13 máquinas virtuales y cada una de ellas corría una aplicación. Este año el equipo IT de la compañía planea migrar este ambiente a Hiper-V para mover de 10 a 15 nuevas aplicaciones directamente a las máquinas virtuales en el ambiente de producción. La consultora IDC calcula que sólo el 15% de los servidores están virtualizados, por lo que queda el 85%; eso sin tener en cuenta las nuevas áreas de expansión como las soluciones Gris. Microsoft en su visión de esta tecnología incorporará la virtualización de escritorios, de aplicaciones, y la administración de ambientes virtualizados, lo que señala el rumbo de los productos del mayor fabricante de software a nivel mundial.

ABSTRACT

The use of virtualization technology is not a simple speculation of the future of computers. The amounts in investments and profits on the part of leading companies in the design and production of software and computer hardware show this in a convincing way. VMware is a company that has managed to design different operating systems and different applications on the same server. The virtualization expectations were perfectly reflected in the VMware IPO when it surpassed the premiere in the Google park and ranked among the four companies with the highest market capitalization of the Nasdaq. VMware made good use of its early market share, achieving an inter-annual growth of 90% and a turnover of 9 thousand 139 million pesos (703 million dollars) in what it took exercise on that date. The company claims that its virtualization software means savings of no less than 120 million pesos per year (6,000 euros) per application on each server. Of this saving 25 thousand 440 pesos correspond to a cut in energy expenditure and cooling, without saving space because with fewer machines less square meters are needed to install equipment. The great impetus for the use of virtualization will come marked by the entry into the market of Microsoft, who from February incorporated as standard in his Windows Server 2008 his virtualization software Hyper-V Microsoft had already ventured into virtualization with its Virtual Server 2005 R2 in which four physical servers each hosted 10 to 13

virtual machines and each of them ran an application. This year the company's IT team plans to migrate this environment to Hyper-V to move 10 to 15 new applications directly to the virtual machines in the production environment. The IDC consultant estimates that only 15% of the servers are virtualized, so 85% remains; that without taking into account the new areas of expansion such as the Gray solutions. Microsoft in its vision of this technology will incorporate the virtualization of desktops, applications, and the administration of virtualized environments, which indicates the direction of the products of the largest software manufacturer in the world.

CAPITULO I

PLANTEAMIENTO INICIAL DE LA INVESTIGACIÓN

1.1 Identificación del problema.

La problemática que afronta la capacitación y el entrenamiento, en especial en las instituciones públicas y/o privadas que preparan especialistas en Ingeniería de todas las ramas y en particular la Eléctrica, no solo en nuestro país, sino en muchas otras sociedades, es principalmente la falta de infraestructura adecuada necesaria para realizar las experiencias que permitan una capacitación de calidad, por los altos costos que representa la implementación de laboratorios. Por otro lado, el equipamiento actual de los Centros de Control y de Despacho de requiere que los profesionales que laboran en ellos tengan capacitación en redes de computadoras, la cual se realiza en la mayor parte de las instituciones de nivel superior o técnica, en grupos conformados por un gran número de alumnos, imposibilitando de esta forma que todos tengan la posibilidad de realizar las experiencias sino que son simples espectadores de la persona que la realiza, disminuyendo su posibilidad de adquirir la experiencia requerida para afrontar posteriores retos.

Como una forma de plantear una posible solución a dicho problema, nos permitimos presentar al uso de la Virtualización como una de las mejores alternativas que permita mejorar la capacitación en diferentes áreas del

conocimiento, en especial a lo referente a redes de computadoras.

El uso de la Virtualización permitirá resolver problemas de interés, tales como:

- 1) Un mejor entendimiento, por parte de los estudiantes, de los conceptos teóricos, que plasmados en una experiencia vivencial mejore la captación de los mismos.
- 2) El tener que invertir gran cantidad de dinero, por el alto costo de los mismos, para implementar laboratorios físicos y en especial de redes de computadoras.
- 3) La poca flexibilidad para la adecuación de las redes tanto en la parte física, (topología), como en el software, (sistema operativo).
- 4) Resolver el problema referido a que los laboratorios puedan ser utilizados por un pequeño número de estudiantes por vez, debido a la estricta limitación física.

Algunas opiniones en torno al uso de la Virtualización.

Recientemente, el concepto de Virtualización de redes ha tenido atención significativa en el debate de como modelar el paradigma de redes de la próxima generación que pueda reemplazar a la actual Internet.

Existen dos corrientes, los favorables a los cambios a la arquitectura como medio para la evaluación de nuevas arquitecturas, y los pluralistas como Cisco, líder mundial en redes para Internet, que conciben la

Virtualización como un atributo fundamental para la arquitectura de la próxima generación.

Un memorando del Presidente de Estados Unidos de América, publicado en junio de 2013, reconoce que ampliar la disponibilidad del espectro para uso comercial innovador y flexible, incluidos los servicios de banda ancha, ayudará a promover el desarrollo económico proporcionando a los ciudadanos y empresarios una mayor velocidad de transmisión y disponibilidad de cobertura, impulsará el desarrollo de tecnologías, aplicaciones y servicios inalámbricos avanzados y ayudará a disminuir las tasas por su utilización en hogares y empresas. De forma similar, la Agenda Digital para Europa reconoce que el espectro radioeléctrico es un recurso natural esencial para las conexiones inalámbricas y la innovación. La idea de esta investigación es visualizar los conceptos de Virtualización de redes y proporcionar un mejor entendimiento de los desafíos resultantes de la aplicación de esta tecnología en la capacitación de los Ingenieros y Técnicos.

Con la utilización de la Virtualización en la enseñanza de redes, es posible que ayude a mejorar la parte práctica de dicha capacitación, permitiendo que más participantes tengan la posibilidad de realizar experiencias, y que las entidades puedan contar con una infraestructura para tal fin a un menor costo.

Sobre la viabilidad del uso de la Virtualización. El uso de las VMs para proporcionar una abstracción al host físico, es un método históricamente común y hoy evoluciona y encuentra aplicación en la mayoría de campos. En el mundo de los juegos, el uso de Virtualización de aplicaciones no es nuevo. Muchos juegos modernos incluyen scripting de comportamiento de personajes que no son jugadores y de otros aspectos del juego, usando lenguajes que ejecutan códigos de bytes, pero el concepto de Virtualización de aplicaciones en los juegos en realidad va mucho más atrás.

Así como la Virtualización de plataforma (o sistema) ha cambiado la forma en la que aprovisionamos y administramos tanto servidores como PCs de escritorio, la Virtualización de aplicaciones continúa proporcionando mecanismos eficientes para abstraer una aplicación de su sistema host. Dada la popularidad de este enfoque, es interesante ver la evolución del software y del hardware para hacer aún más flexible y eficiente la Virtualización de aplicaciones.

El concepto de Virtualización no se ha detenido con el paso de los años, esto se demuestra con los avances obtenidos en los últimos años:

- ✓ 2008: Microsoft lanza la versión final de Hyper-V.
- ✓ 2010: Virtual Box pasa a llamarse Oracle VM VirtualBox.
- ✓ 2011: Se empiezan a incluir ciertas partes en la rama oficial del kernel de Linux 2.6.37. Integración completa en la versión 3.0.

Hoy, gracias a la tecnología, una persona puede trabajar desde su casa, comprar bienes y servicios por internet y hacer pagos electrónicos desde sus cuentas bancarias. Las tecnologías de la información y la comunicación han variado notablemente las actividades humanas y desde esa premisa, proponemos investigar la viabilidad del uso de la Virtualización, en aras de mejorar la capacitación en redes de los ingenieros y técnicos.

En el futuro, aparece la Virtualización como una de las claves en la explotación óptima de las actuales tendencias tecnológicas en informática. Tendencias actuales como por ejemplo el direccionamiento de 64 bits, CPUs multicore (más de 16 cores/CPU por servidor), el tratamiento de manera importante de la refrigeración y ahorro de energía en los servidores, la convergencia de las interfaces de E/S mediante el uso de interfaces de red y almacenamiento de alta velocidad compartidas, o el almacenamiento virtualizado basado en red, hacen ver que la Virtualización en un futuro juegue sin duda un papel de suma importancia en el aprovechamiento de todos estos avances tecnológicos. Todo ello hace presagiar que vamos encaminados a la implantación de datacenters completamente virtuales.

Con este trabajo, se espera conocer la opinión de los usuarios (profesores y alumnos) referente al uso de la Virtualización en la capacitación en el diseño y manejo de redes. De tener una respuesta positiva, su implementación permitiría cumplir varios objetivos, entre ellos, una mejor

capacitación de los estudiantes, el evitar los gastos requeridos para contar con gran cantidad de equipos físicos y brindar una mejor calidad de servicio educativo.

1.2 Formulación del problema.

El principal problema por solucionar es el de mejorar la calidad de la capacitación de los profesionales en Ingeniería y de los Técnicos, en el área de tele informática en general y de redes de computadoras en particular.

Problema general:

¿Cómo se puede utilizar la Virtualización como herramienta para la enseñanza de redes de computadoras que mejoren la capacitación en las áreas de ingeniería?

Problemas específicos

- a) ¿Se pueden crear laboratorios virtuales, que permita mejorar la calidad de servicio en la obtención de conocimientos, sobre la configuración y el manejo de redes de computadoras como herramienta de Ingeniería?
- b) ¿Es posible disminuir los gastos relacionados con la implementación de laboratorios especializados, que permitan la enseñanza práctica de redes de computadoras como herramienta de Ingeniería?
- c) ¿Qué ventajas se obtendrían con la implementación de laboratorios utilizando Virtualización?

1.3 Objetivos de la investigación.

1.3.1 General

Haciendo uso de lo que nos ofrece la tecnología en el campo de la electrónica y las telecomunicaciones, emplear la Virtualización como herramienta económica y práctica que permita la enseñanza de redes de computadoras como herramienta de Ingeniería.

1.3.2 Específicos

- a) Mejorar la calidad de servicio que se brinda a los estudiantes de Ingeniería, haciendo uso de la Virtualización como herramienta para la enseñanza del diseño de topologías de redes de computadoras.
- b) Hacer uso de la Virtualización como herramienta que permita la reducción de costos, en la implementación de laboratorios para la enseñanza de redes de computadoras de Ingeniería.
- c) Utilizar la Virtualización como herramienta de enseñanza, que reduzcan los tiempos necesarios en el diseño de topologías y manejo de redes de computadoras, de forma, que una mayor cantidad de alumnos tengan acceso directo a la capacitación práctica.

1.4 Justificación de la investigación.

Según la Ley de Educación Nro. 28044, en su artículo 2º dice:

“La educación es un proceso de enseñanza y aprendizaje, que se desarrolla a lo largo de toda la vida, y que contribuye a la formación

integral de las personas, al pleno desarrollo de sus potencialidades, a la creación de cultura, y al desarrollo de la familia y de la comunidad nacional, latinoamericana y mundial. Se desarrolla en instituciones educativas y en diferentes ámbitos de la sociedad”.

En su Artículo 3° dice:

“La educación es un derecho fundamental de la persona y de la sociedad. El Estado garantiza el ejercicio del derecho a una educación integral y de calidad para todos, buscando la universalización de la Educación. La sociedad tiene la responsabilidad de contribuir a la educación y el derecho a participar en su desarrollo.”

La utilización de la Virtualización, como una herramienta para la capacitación de los estudiantes de las Universidades y de los Institutos Superiores Tecnológicos propuesto, permitirá el diseño de redes utilizando esta tecnología de punta, cumpliendo de esta forma con una de las metas de la Ley de Educación.

Su utilización servirá para cambiar la forma de enseñanza de los conceptos de redes, proporcionando una mejor calidad de enseñanza, con la finalidad de que los egresados de estas instituciones adquieran una mayor experiencia práctica.

El tema de la utilización de la Virtualización está en pleno proceso de desarrollo en los países avanzados, pero su empleo en educación está en fase de diseño de prototipos, la realización del presente trabajo de tesis nos

permitirá dar un paso adelante en beneficio de los estudiantes que es la razón de ser de la educación.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes del estudio.

El concepto de Virtualización se viene usando desde los años 60 en las computadoras IBM 370, y ha sido aplicado a diferentes aspectos y ámbitos de la informática, desde sistemas computacionales completos, hasta capacidades o componente individuales.

En informática, Virtualización es la creación a través de software de una versión virtual de algún recurso tecnológico, como una plataforma de hardware, sistema operativo, un dispositivo de almacenamiento o cualquier elemento de una red.

La Virtualización es referida a la abstracción de los recursos de una red llamada Virtual Machine Monitor (VMM). Crea una capa de abstracción entre la máquina real (física) y el sistema operativo de la máquina virtual (virtual machine, guest), dividiéndose el recurso en uno o más entornos de ejecución.

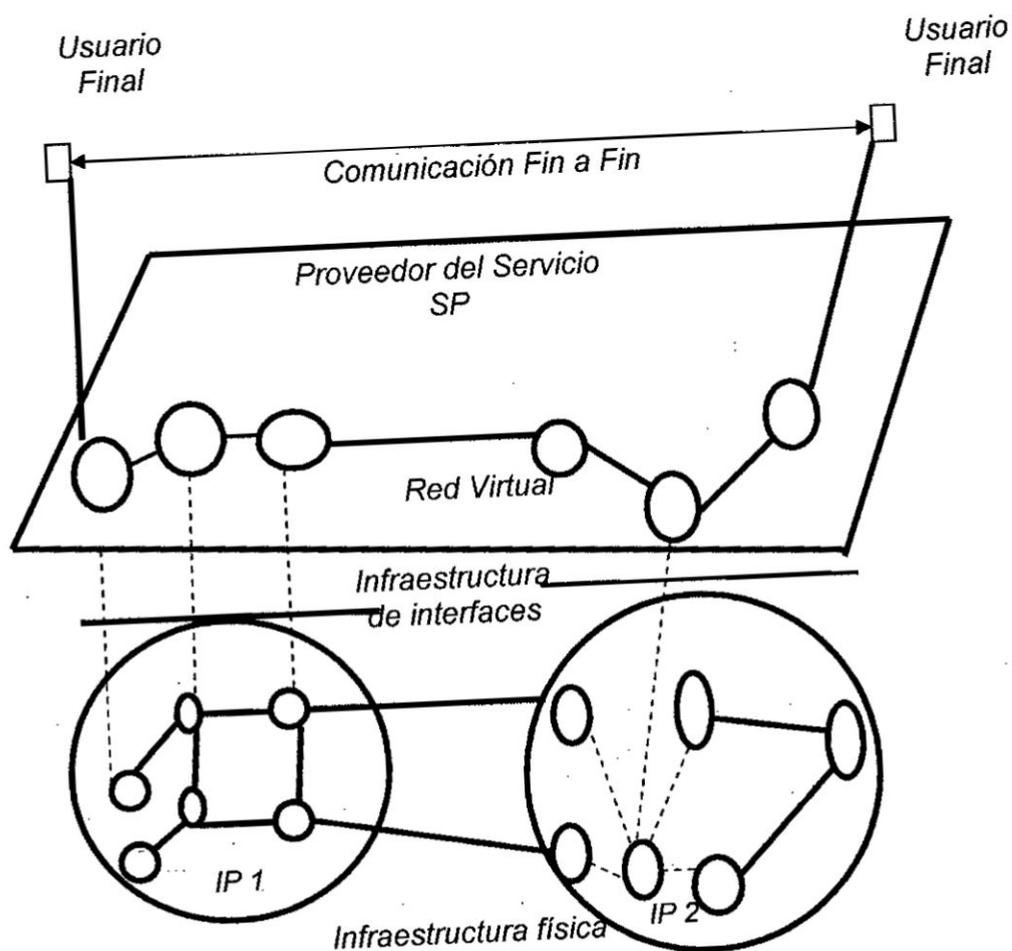
¿Qué es una red Virtual?

Una red virtual es una colección de nodos virtuales conectados por medio de un conjunto de links virtuales para formar una topología virtual la cual es esencialmente un subconjunto de la actual topología física. Cada nodo

virtual puede ser hospedero en un nodo físico particular o puede ser una abstracción lógica de un sistema de red. Un enlace virtual se extiende sobre un camino en la red física e incluye una porción de los recursos de red a lo largo del camino.

La fig.2.1 ilustra un ambiente de Virtualización de red en la cual un SP construye una red virtual acesando recursos de red de dos proveedores de infraestructura IP 1 y IP 2.

Fig. 2.1 Ilustración de un ambiente de red virtual
(Fuente propia)



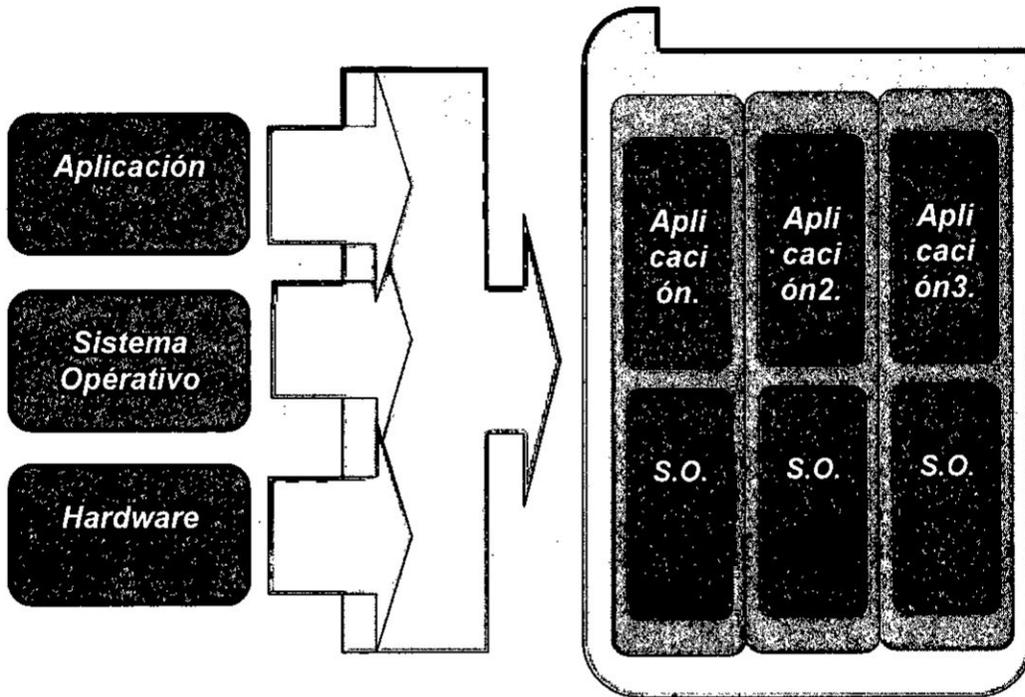
En este punto es conveniente aclarar una tradicional confusión en la utilización informática de los términos emulación y Virtualización. La emulación es una técnica más limitada en prestaciones y en rendimientos; su finalidad es traducir todas las instrucciones del código original (el que queremos emular) al lenguaje que utiliza nuestra plataforma; un trabajo que una máquina virtual no tiene que hacer. La Virtualización hace, y siempre ha hecho, uso de la emulación y de la simulación para tratar correctamente las instrucciones generadas en otros sistemas con arquitecturas distintas, un simulador es un "**emulador de precisión**", que imita el comportamiento exacto de un sistema real, incluso a nivel interno. Una máquina virtual, además de la Virtualización, realiza y maneja la abstracción de la capa del hardware y de los mecanismos específicos de control de estos recursos y periféricos, como son los críticos de entrada/salida.

En la actualidad, las máquinas virtuales pueden resolver una infinidad de problemas tanto en entornos personales como corporativos. En nuestro caso, la mejora de la calidad de servicio en la capacitación en redes de computadoras, lo mismo, el reducir los altos costos de implementación de laboratorios para tal fin. Por ejemplo, si tenemos un equipo con sistema operativo XP, y queremos utilizar periféricos que sólo funcionan con Win98, se arranca el equipo con el sistema operativo XP, y cuando esté listo, se lanza un proceso de máquina virtual con el sistema operativo Win98.

Con relación a la seguridad, se puede tener el sistema anfitrión (el que arranca inicialmente con el equipo) protegido, pues las operaciones de navegación, descargas o simplemente instalaciones comprometidas, se realizan sobre una máquina virtual que incluso puede ser una copia del propio sistema anfitrión. Simultáneamente, se puede ejecutar aquella versión de NT necesaria para que corra una aplicación "congelada" y siga funcionando sin cambios; simultáneamente se puede tener otra máquina virtual con un sistema operativo Win2000 Server, y otra con labores de Linux. También es posible conseguir que en un servidor corran distintos sistemas operativos o que incluso, sobre el sistema anfitrión, operen diversas instancias del mismo en las que se puedan ejecutar concurrentemente entornos de desarrollo, de preproducción, de pruebas para actualización de parches, etc. Ello supone un remedio a muchas dolencias que afectan a servidores empresariales y sobre todo, la apertura a nuevos modos de ver la gestión de sistemas, y para nuestro caso, la capacitación.

Fig. 2.2 Aplicaciones corriendo en máquina virtual
(Fuente propia)

Máquina Virtual



Las soluciones que brinda la Virtualización nos permite contar con las ventajas de creación de espacios o particiones independientes de proceso, con todos los recursos hardware necesarios. Se genera un entorno de trabajo funcionalmente real que, aunque cuente con base virtual, nos ofrece la memoria, el disco y el resto de dispositivos que queramos predefinir. Se comporta como un sistema "a la carta", en el que podemos instalar y aprender cuánto se quiera, y si no nos gusta lo eliminamos. El estado del arte nos permite disponer de un catálogo de máquinas listas para usar o bien definir y añadir nuevas máquinas a nuestro gusto; se puede tener un control específico sobre los recursos de

cada equipo virtual, con una variedad de sistemas operativos compatibles, y una fácil exportación e importación de copias "congeladas" del estado de cada VM. Puede tener una consola central de gestión de todas las máquinas virtuales activas, monitorizando sus procesos y rendimientos, e incluso cambiar o asignar nuevos dispositivos virtuales "en caliente", o ampliar la memoria virtual asignada. Este último punto es importante, ya que las máquinas físicas donde se implanten sistemas virtuales requerirán mucha memoria. Los avances en tecnología a nivel hardware y especialmente en procesadores tipo Intel y AMD nos lleva a un hecho constatable: la actual infrautilización de procesadores.

La Virtualización será la tecnología más disruptiva hasta bien entrada la siguiente década. La consultora Gartner¹ ve la Virtualización como una tendencia que redefinirá esquemas de licenciamiento de productos, y revolucionará el uso de los equipos personales y corporativos mediante la separación del hardware y del software, permitiendo que múltiples sistemas operativos corran simultáneamente en un solo equipo. Gartner estima que la Virtualización permitirá, a los departamentos de TI, implementar políticas de soporte de una forma más eficiente, lográndose contratos de outsourcing con mayor rentabilidad. También estima que la Virtualización redefinirá dramáticamente la industria de micros computadores y servidores, atenuándose la diferenciación de productos y forzando a los vendedores a competir puramente en servicio y precio;

¹ *Gartner Inc., empresa consultora especializada en Tecnología Informática. EEUU.*

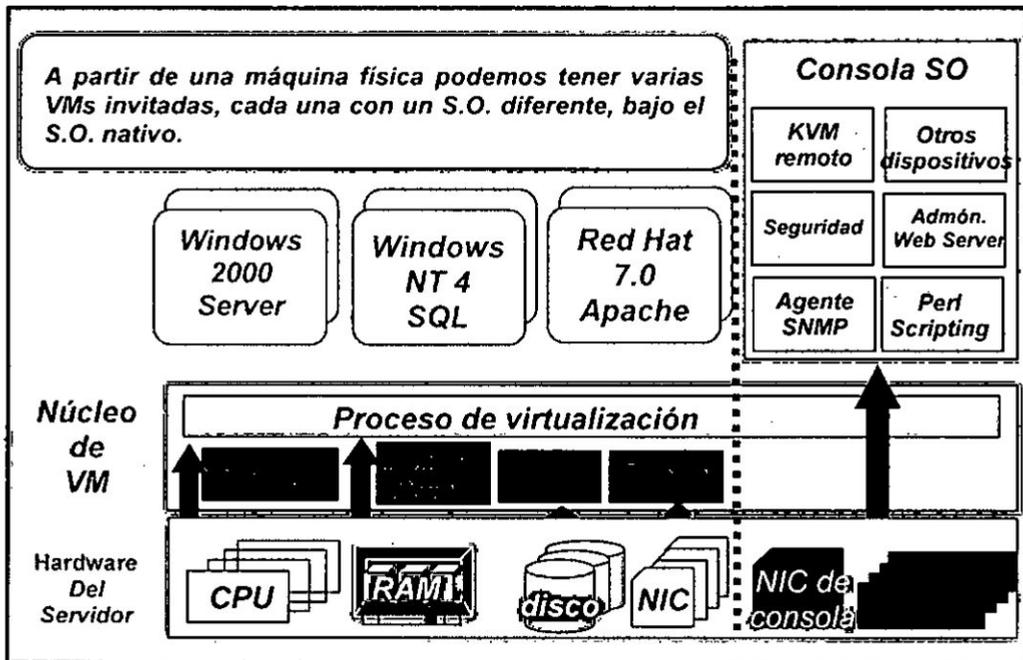
también afirma que el software de Virtualización de PCs necesita, a corto plazo, de futuros desarrollos que mejoren aspectos de seguridad y facilidad de uso. De acuerdo a Brian Gammage, vicepresidente de Gartner, la Virtualización de equipos logrará una amplia aceptación en un corto tiempo. La actual tecnología de Virtualización está siendo potenciada, con prioridad en el negocio, por empresas tan importantes como Intel y Microsoft.

Fig. 2.3 Sistemas operativos operando en máquinas virtuales.
(Fuente propia)



Las nuevas arquitecturas de los procesadores de Intel y AMD, llevan incorporadas instrucciones específicas de Virtualización, capaces de dar respuesta en gran medida a las excepciones de protección, y su manejo pasa de software a **firmware**. Intel incorpora la nueva arquitectura llamada VMCS (Virtual Machin Control Structure), que cuenta con 10 nuevas instrucciones VT-x. Hoy los procesadores de 64-bit, Dual-Core Intel® Xeon® para servidores, así como las memorías DDR2 están optimizados para los entornos de servicios virtualizados. Intel, además, trabaja con los desarrolladores de software de Virtualización VMware, Microsoft, XenSource, así como con la comunidad open-source Xen, para asegurar que las futuras plataformas no solo cumplan las expectativas de estos desarrolladores, sino también las necesidades de los clientes corporativos.

Fig. 2.4 Proceso de Virtualización
(Fuente Virtualization for Dummies)



La Virtualización crea una interfaz externa que encapsula una implementación interior mediante la combinación de recursos en localizaciones físicas diferentes, o por la simplificación del sistema de control.

Un avanzado desarrollo de nuevas plataformas y tecnologías de Virtualización han producido que en los últimos años se vuelva a prestar atención a esta tecnología.

Una máquina virtual simula una plataforma de hardware autónoma incluyendo un sistema operativo que se ejecuta como si estuviera instalado.

Existen varias formas de realizar Virtualización: de hardware, de software, de sesiones de usuario, de aplicaciones, etc.

Los proveedores de software, como VMware y Microsoft, han desarrollado tecnologías de Virtualización integrales tales como VMware Server y Windows Server 2008 Hyper-V para servidores.

La Virtualización puede permitir reducir el número de servidores necesarios para garantizar la viabilidad del Centro de Proceso de Datos (CPD), ello puede proporcionar las siguientes ventajas:

- ✓ Ahorros en inversión, espacio y costos de mantenimiento.
- ✓ Mayor seguridad a un menor costo.
- ✓ Mejora de la disponibilidad de la información.
- ✓ Reducción y simplificación de infraestructuras.
- ✓ Tipificación y estandarización de plataformas y configuraciones.

- ✓ Mejora en la fiabilidad.
- ✓ Reducción de los costes de administración y soporte del servicio.
- ✓ Mejora en la utilización de los recursos.
- ✓ Mejora en la integración y simplificación de procesos.
- ✓ Mejor control y utilización de los recursos TI.

En lo que se refiere a la enseñanza de los conceptos de redes de computadoras, es muy difícil de realizarla sin disponer de laboratorios especializados de redes, u otras herramientas adecuadas para tal fin. Todas las tentativas realizadas han tenido por objetivo suprimir, cuanto sea posible, las muchas desventajas de los laboratorios especializados.

¿Cuáles son esas principales desventajas? En primer lugar, el precio es bastante alto, y en segundo lugar, ellos no son tan flexibles como para atender a las necesidades de una variedad de topologías de red. Además de esto, estos tipos de laboratorios pueden ser usados solamente por un número pequeño de estudiantes al mismo tiempo debido principalmente a la limitación física. Existen algunas formas alternativas como el uso de software de simulación, que permite la "simulación" de pequeñas y grandes redes con diferentes tecnologías y topologías.

¿A pesar de esto existen otras alternativas? Recientemente cuando se tienen muchas tecnologías emergentes, una en particular parece ser muy adecuada para la simulación de redes de computadores: **La Virtualización.**

Es posible el uso de la tecnología de Virtualización en la enseñanza de

las redes de computadoras. Esta puede ser utilizada como una herramienta adecuada para la creación de laboratorios de redes virtuales, que complementen los laboratorios reales en la enseñanza de los conceptos de redes.

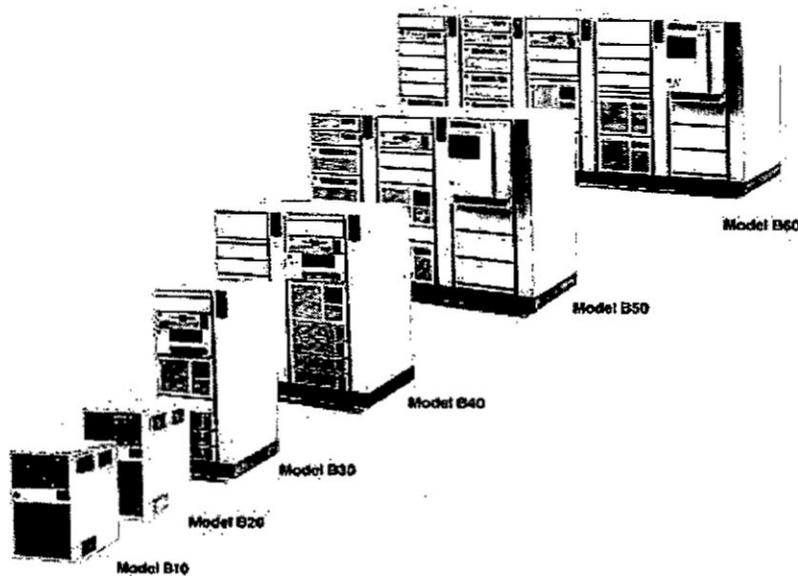
Los problemas para la implementación de laboratorios físicos reales especializados para la enseñanza de redes de computadoras, tales como, la falta de financiamiento de los equipos requeridos, el espacio físico, los riesgos y amenazas para el entorno de red e infraestructura, se pueden resolver mediante el uso de un entorno de aprendizaje virtual. Una iniciativa en fase de evaluación es **Velnet AE** (Virtual Environment for Learning), que es un ejemplo de aprendizaje virtual que está siendo desarrollado por la University of Western Sydney, Australia, para máquinas virtuales y sus sistemas operativos. Es una red virtual que conecta las máquinas virtuales con sus estaciones remotas. Esta infraestructura de realidad virtual, permitiría a los estudiantes construir topologías de redes y experiencias relacionadas en un laboratorio virtual.

La Virtualización es un término que se refiere a la abstracción de los recursos de una computadora llamada Hypervisor o VMM (Virtual Machine Monitor).

Con la entrada en uso de los computadores personales, el concepto de acceso al mismo tiempo a los recursos de un único supercomputador fue desapareciendo, y con él se vio eclipsada la Virtualización. Lo importante era el rendimiento más que la seguridad y fiabilidad. Al ocaso de la

Virtualización también contribuyó el que no fuera una buena idea la partición de los recursos de los miniordenadores, o computadores personales, debido a su escasez; los mainframes quedaron reducidos a lugares críticos y puntuales. La evolución con los años siguió la misma línea, hasta llegar a la situación que conocemos, en la que prácticamente existe un computador por persona. Afortunadamente, la Virtualización junto a tecnologías como, los sistemas operativos multiusuario y multitarea, sobrevivieron en las Universidades y en sectores en los que su uso y fiabilidad eran críticos: grandes empresas, bancos, sistemas militares, etc. Estos sistemas fueron evolucionando y ya no eran los mainframes usados antiguamente, sino que eran sistemas que usaban hardware de miniordenador con arquitectura mainframe, como la familia IBM AS/400, cuyo primer modelo vio la luz en 1988.

Fig. 2.5 IBM AS/400
(Fuente IBM del Perú)



En la actualidad asistimos a su eclosión, gracias al fuerte descenso del costo total de propiedad (TCO) atribuible a tecnologías vía hardware como Intel VT, AMD-V Pacifica, NPIV y vía software VMWare, RedHat-V, Microsoft Hyper-V, XEN, etc.

En el año 1962, la IBM utilizó la Virtualización para su modelo IBM 7044, en el que la máquina física era la M44, que albergaba varias máquinas lógicas 44X para los procesos, y el CTSS (Compatible Time Sharing System) desarrollado por el MIT (Massachusetts Institute of Technology).

El IBM 7044, y el proyecto Atlas de la Manchester University (uno de los primeros supercomputadores del mundo, operativo en 1962), fue el pionero en el uso de paginación bajo demanda y llamadas en modo supervisor. Así es como nació la Virtualización, con la necesidad de particionar recursos de disco, memoria y capacidad de proceso.

Otro de los primeros usos de la Virtualización es el uso del procesador simulado P-Code (Pseudo-Code). El P-Code es un lenguaje máquina que es ejecutado en una máquina virtual más que en el hardware real, lo que permitió a los programas codificados en P-Code ser altamente portables y correr en cualquier lugar en el que esté disponible la máquina virtual P-Code.

El mismo concepto en el que se fundamentó el P-Code, fue usado en los años setenta por el Basic Combined Programming Language BCPL, predecesor del lenguaje C.

virtual" difiere completamente de la memoria física o la memoria de acceso aleatorio (RAM) instalada en la computadora. La memoria virtual, es el espacio libre en el disco duro que emplea un sistema operativo como fuente adicional de memoria, cuando la cantidad de memoria física disponible es insuficiente para ejecutar una aplicación. Sin embargo, la memoria virtual es demasiado lenta para funcionar como un sustituto directo para la memoria física, así que sólo debería usarse cuando sea necesario.

Un sistema operativo usa el espacio del disco duro como memoria virtual cuando se queda sin RAM. Esto incrementa las posibilidades de ejecutar múltiples aplicaciones de manera bastante cómoda, sin tener que instalar tarjetas de memoria adicionales en la computadora. Cuando un sistema operativo emplea la memoria virtual, la guarda en un tipo de archivo que se conoce como "archivo de paginación" en la raíz de la partición del disco duro. La memoria virtual puede incrementarse hasta tres veces la cantidad de la memoria física disponible, aunque Microsoft recomienda 1,5 veces como la cantidad ideal de memoria virtual que debe asignarse a un sistema operativo.

Memoria Virtual: Paginamiento en Demanda.

Cuando la memoria real de un computador se hace insuficiente, el núcleo del sistema operativo puede emular una memoria de mayor tamaño que la

memoria real, haciendo que parte de los procesos se mantengan en disco. A este tipo de memoria se le denomina memoria virtual, pues es una memoria inexistente, pero que para cualquier proceso es indistinguible de la memoria real.

El mecanismo que implementa la memoria virtual se denomina paginamiento en demanda. Consiste en que el núcleo lleva a disco las páginas virtuales de un proceso que tienen poca probabilidad de ser referenciadas en el futuro cercano. Un proceso puede continuar ejecutándose con parte de sus páginas en disco, pero con la condición de no acceder a esas páginas.

La realización de un sistema de memoria virtual se hace posible gracias al principio de localidad de las referencias, un proceso tiende a concentrar el 90% de sus accesos a la memoria en sólo el 10% de sus páginas. Sin embargo, para que un proceso pueda acceder una "palabra", es necesario que la página que contiene esa "palabra" deba estar completamente residente en memoria real. Aun así, empíricamente se observa, que un proceso puede pasar períodos prolongados en los que accesa sólo entre un 20% al 50% de sus páginas. El resto de las páginas pueden llevarse a disco mientras no son usadas.

Page-fault.

Las páginas residentes en disco se marcan en la tabla de páginas del proceso con el bit V en cero, de modo que si el proceso la referencia se

Para hacer este análisis se consideran los siguientes parámetros:

Tabla 2.1 Estrategias para el reemplazo de páginas
(Fuente propia)

Parámetro	Significado	Valor aproximado
TM	Tiempo de acceso a la memoria real.	60 nanosegundos
Tp	Tiempo de lectura de una página.	12 milisegundos
r	Tasa de page - fault	

El tiempo promedio de acceso a una palabra en memoria es:

$$t = (1 - r) TM + r * Tp$$

La estrategia FIFO.

Por medio de esta estrategia, entre las páginas virtuales residentes, se

elige como la página a reemplazar a la primera que fue cargada en memoria.

La estrategia LRU.

LRU significa Least-Recently-Used. La estrategia consiste en llevar a disco la página que ha permanecido por más tiempo sin ser accesada. El fundamento de esta estrategia es que estadísticamente se observa que mientras más tiempo permanece una página sin ser accesada, menos probable es que se accese en el futuro inmediato.

La estrategia del reloj.

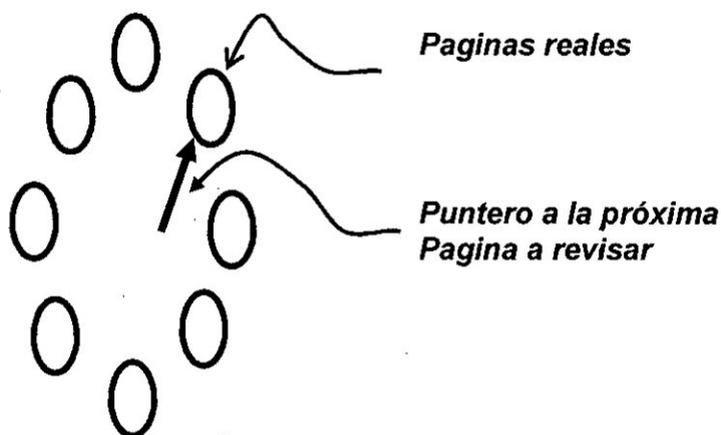
Esta estrategia es una aproximación al LRU. El fundamento es que no es necesario escoger exactamente la página LRU, sino que es suficiente elegir una página que lleva más tiempo sin ser accesada.

La estrategia usa el bit R de la tabla de página y que el hardware coloca en 1 cuando la página es accesada. El scheduler de páginas, coloca en 0 este bit, y lo consulta cuando estima que ha transcurrido el tiempo suficiente como para que aquella página sea reemplazada si no ha sido accesada, es decir si el bit R continúa en 0.

La estrategia del reloj ordena las páginas reales circularmente como si fueran los minutos de un reloj (ver figura 2.6). Un puntero señala en cada instante una de las páginas. Inicialmente todas las páginas parten con R

en 0. Luego de cierto tiempo algunas páginas han sido accedidas y por lo tanto su bit R pasa a 1.

Fig. 2.6 Ordenamiento de las páginas en la estrategia del reloj
(Fuente propia)



Cuando ocurre un page-fault se ejecuta el siguiente procedimiento:

1. Mientras el bit R de la página apuntada sea 1:
 - a. Colocar el bit R en 0.
 - b. Avanzar el puntero en una página.
2. La página apuntada tiene su bit R en 0. Se elige esa página para ser reemplazada, es decir que esa página virtual se lleva a disco, lo que libera una página real. Esa página real se usa para cargar la página que causó el page-fault.

3. Avanza el puntero en una página.

La idea es que la página elegida para ser reemplazada no ha sido accesada por una vuelta completa del reloj. La estrategia considera que este tiempo es suficiente como para suponer que la página no será accesada en el futuro inmediato.

El tiempo que demora el puntero en dar una vuelta depende de la tasa de page-faults. Mientras mayor sea esta tasa, menor será el tiempo en dar la vuelta y por lo tanto el scheduler reemplazará páginas que llevan menos tiempo sin ser accesadas. Al contrario, si la localidad de los accesos a memoria es buena, la tasa de page-faults será baja y el tiempo de una revolución del puntero aumentará. Esto quiere decir que el scheduler tendrá que reemplazar páginas que llevan más tiempo sin ser accesadas.

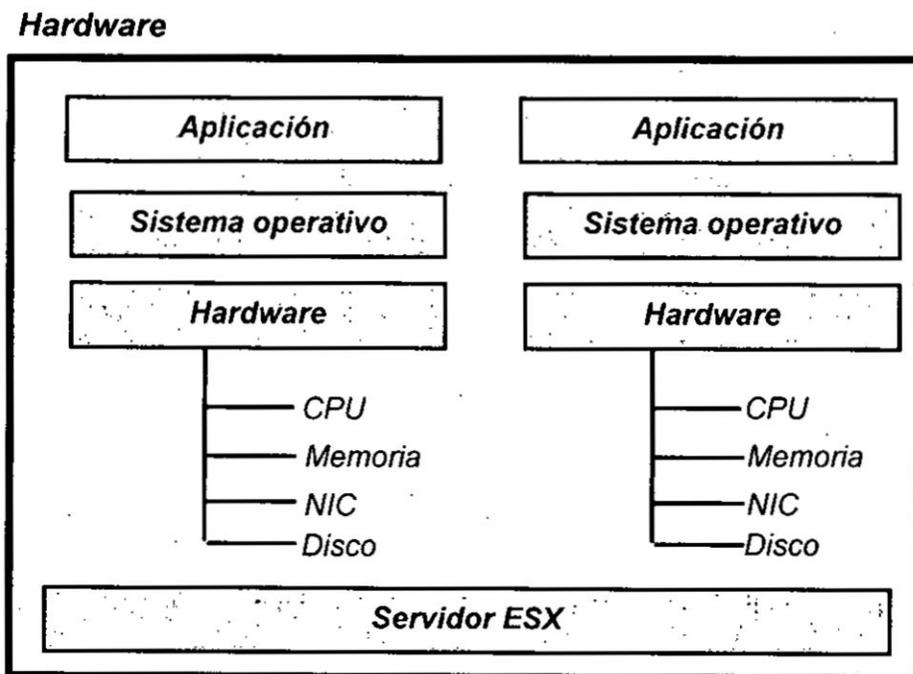
Esta estrategia es fácil de implementar eficientemente con el hardware disponible y funciona muy bien con un solo proceso. En caso de varios procesos, la estrategia se comporta razonablemente en condiciones de carga moderada.

El VMware. -

La base de la tecnología de Virtualización es el llamado "monitor de máquina virtual (VMM)". VMM es una capa de software que emula el hardware de un sistema completo de computación. VMware se basó en un concepto existente, pero logró algo absolutamente impensado,

aplicarlo sobre una plataforma que no fue creada específicamente para ello, con un nivel de estabilidad tal, que permitió su adopción en el mercado de tecnología en forma masiva y sorprendentemente rápido. Cuando en el año 2006 VMware lanza el concepto de Virtual Infrastructure comienza la era de la infraestructura virtual. Este producto basado en un hipervisor muy robusto, ofrecía funcionalidades avanzadas de administración, alta disponibilidad y balanceo de carga, que permitía "correr" aplicaciones críticas con una estabilidad de la que era difícil dar crédito si no se veía con los propios ojos. El llamado hipervisor es un componente de software que permite que varios sistemas operativos puedan acceder a un equipo en forma concurrente, como si cada uno de ellos fuera el dueño, coordinando el acceso y uso de sus recursos.

Fig. 2.7 El hipervisor.
(Fuente *Virtualization for Dummies*)



con AMD-V, logrando una mejor captura de instrucciones, ocultamiento de la memoria al hipervisor o VMM, o como se está viendo con el desarrollo de las MMUs (Memory Management Units) de E/S lo mismo que dispositivos de E/S que aceleran la Virtualización.

Las máquinas virtuales de hardware o de sistema, que son las que conforman el corazón del modelo de Virtualización que es aplicado en el desarrollo del proyecto (Virtualización de plataforma), son las que corren paralelamente sobre una máquina física anfitrión o host, de manera que tienen acceso y hacen uso de los recursos hardware que son abstraídos de él. Cada máquina virtual es "engañada" ya que cree que posee de forma exclusiva los recursos hardware de los que dispone, cuando en realidad lo hace de manera virtual, ejecuta una instancia de sistema operativo sobre el que corren determinados servicios o aplicaciones.

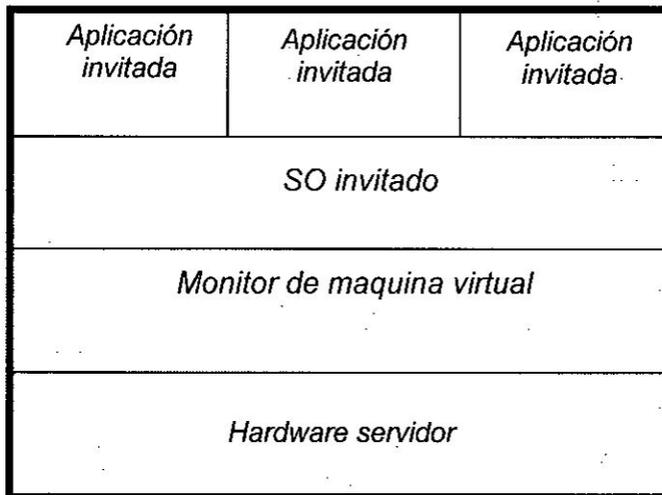
La virtualización se desarrolló inicialmente para habilitar la emulación de varias máquinas virtuales en un único equipo físico. El computador emulado, en términos generales, puede ser instalado en cualquier otro sistema operativo y actuar como un nodo independiente. Un equipo virtual utiliza el hardware existente de una máquina física, puede ser capaz de emular varias tarjetas de red en una tarjeta de red física. Computadoras emuladas pueden utilizarse para establecer comunicaciones de red virtual y simular redes virtuales.

Todos los "paquetes de software" en el campo de la tecnología de Virtualización, pueden dividirse en tres categorías según su estructura o la

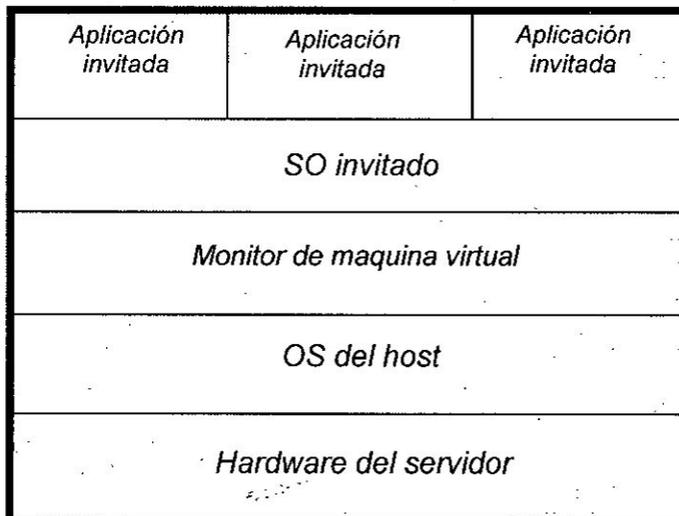
plataforma en la cual se construyen (Fig. 2.8):

Fig. 2.8 Categorías de VMM
(Fuente *Virtualization for Dummies*)

VMM Tipo I



VMM Tipo II



1) VMM tipo I (stand-alone), son implementados directamente en el

- hardware físico, por ejemplo, **IBMVM/370**, **VMwareESXServer**.
- 2) VMM tipo II (hosted), construido completamente sobre el sistema operativo del host, por ejemplo, Linuxuser-mode.
 - 3) VMM tipo III, híbrido entre tipo I e II. Ellos operan básicamente en el hardware físico, sin embargo, usan el sistema operativo del host para efectuar las operaciones de entrada y salida, por ejemplo, VMwareWorkstation, MicrosoftVirtualPC y VirtualServer 2005.

En cuanto al software de Virtualización, puede dividirse en dos categorías según su uso:

- 1) Software del tipo servidor de acceso remoto y control de las máquinas virtuales, como el Microsoft Virtual Server 2005 y VMwareServerGSX.
- 2) Software del tipo de usuario único, diseñado para ser usado en un solo equipo por separado, como por ejemplo Microsoft Virtual pc 2004, VMwareWorkstation 5.5 y Xen.

El software de Virtualización es adecuado para crear laboratorios de redes virtuales.

2.2 Marco Teórico conceptual

Por marco teórico se entiende, en términos generales, al sistema de conceptos básicos, que constituyen el fundamento y conjunto de los

procesos epistemológicos que buscan plantear los problemas específicos y propios de un área, en este caso la Virtualización, según la problemática que ésta presenta, y resolverlos a través del desarrollo de las bases metodológicas, que usualmente lo complementan, proporcionando los métodos y procedimientos correspondientes. Como un ejemplo podemos citar el método para la implementación de laboratorios virtuales de la Technical Faculty "Mihajlo Pupin" de Zrenjanin (Universidad de Novi Sad, Serbia & Montenegro). El laboratorio está diseñado para utilizarse en un curso sobre redes de ordenadores, para enseñar IP, enrutamiento estático y dinámico, (RIP e OSPF), conceptos de Firewall y servicios de red (Web e FTP). Para tener bajo costo, la solución debió ser fácil de usar y ser basada en la plataforma **Windows XP**, debido a que el mismo laboratorio pueda ser utilizado para otros cursos basados en la plataforma Windows.

Las herramientas de software para la realización del proyecto se limitaron a la utilización de **VMWare** y **PC Virtual**, debido a los requisitos anteriores, y sin probar otra opción Microsoft VirtualPC 2004 fue elegido por ser una versión con licencia. Los sistemas operativos (**OS**) invitados deben instalarse en cada una de las máquinas virtuales por separado, y pueden ser diferentes a los sistemas operativos básicos.

Considerando que el plan básico era desarrollar un ambiente de bajo costo, la opción más lógica es **Linux** u otro sistema operativo. Existen varias versiones de **Linux** conveniente para el uso. Uno de los sistemas

Las asignaturas relacionadas con redes de computadoras poseen una extensa base teórica de la que se abreva según la orientación de la carrera en la que se dictan. En particular, en las carreras de ingeniería se espera que el estudiante adquiera competencias en diseño, implementación y administración de redes por lo que tiene especial importancia la interrelación de la práctica. Se plantea la dificultad de mantener actualizados los laboratorios en cuanto a equipos, ya que rápidamente se vuelven obsoletos y cada vez son más costosos sumada a la necesidad de sostener personal suficiente para mantener las prácticas.

A medida que pasa el tiempo, la Virtualización va teniendo más repercusión en todos los ámbitos universitarios, institutos superiores y empresariales dada su gran evolución y constante mejora. Los laboratorios de redes virtuales le acercan a los estudiantes a una nueva alternativa para poner en práctica los conocimientos teóricos adquiridos y experimentar todas las funcionalidades de los Sistemas Operativos y del diseño de redes.

Una red virtual es una red de computadoras que se compone, al menos en parte, de enlaces de red virtuales. Un enlace de red virtual no se implementa mediante una conexión física (por cable o inalámbrica) entre dos dispositivos de computación, sino que se lleva a cabo utilizando

incluyendo restricciones además de los conceptos y las propiedades.

Otra alternativa es la definición por medio de un conjunto de fórmulas de lógica de primer orden. En este caso las instancias de la ontología son todas aquellas estructuras que respetan el conjunto de fórmulas (restricciones). Esta última alternativa dificulta que la ontología sea computable. Esta es precisamente una de las razones por las que surgieron las lógicas descriptivas, en un afán por consensuar capacidad de procesamiento y riqueza expresiva del conocimiento.

Su uso más extendido es el de representar conocimiento sin mayor pretensión que ayudar a su comprensión de cara a las personas, sin que sea procesado computacionalmente. La formalización de ontologías es el primer paso para hacerla computable y, en consecuencia, tener las herramientas para aprovechar todo su potencial. Cuando definimos ontologías para aplicaciones ideadas para ambientes inteligentes, tal como representa en el presente trabajo de tesis, debemos tener en mente todas sus capacidades. Por tanto, una lista de características, funcionalidades, ventajas y usos, se describe a continuación:

- Mejorar la comunicación tanto entre humanos, como entre sistemas y humanos y entre los propios sistemas computacionales. El objetivo es consensuar el conocimiento de nuestra porción de realidad modelada.

- Además de la comunicación entre sistemas computacionales, las ontologías favorecen la interoperabilidad entre sistemas heterogéneos al dar significado a los conceptos que deben compartir, aunque cada uno los implemente de forma distinta.
- Las ontologías permiten la organización y reutilización del conocimiento. La estructura jerárquica de las ontologías ayuda a los desarrolladores a reutilizar ontologías de dominios concretos.
- Proporcionan mecanismos para aumentar la independencia de los sistemas y servicios respecto a la tecnología y las peculiaridades de cada contexto de aplicación. Esto conlleva una mayor posibilidad de reutilización y adaptación.
- Permiten reducir costos, evitando la necesidad de disponer de gran cantidad de equipos.

El diseño y generación de ontologías debe seguir un proceso que permita guiar y evaluar la tecnología propuesta. No existen metodologías ampliamente aceptadas, pero podemos encontrar estudios que ayuden en esta tarea. Un ejemplo son los criterios identificados por Gruber (T. R. Gruber, 1995):

- Claridad: El objetivo es comunicar de manera efectiva el significado de la tecnología a utilizar.
- Coherencia: Debe soportar inferencias consistentes con las definiciones.

El espacio natural, artificial y cibernético. -

El espacio natural es el primer entorno, es donde habita el hombre. El segundo entorno es la ciudad, espacio artificial correspondiente a distintas dimensiones territoriales, urbanísticas y arquitectónicas donde desarrolla sus actividades.

El tercer entorno corresponde a los espacios cibernéticos que involucran a los procesos de la Virtualización, procesos mediatizadores de un nuevo espacio social generado por las tecnologías de la información, de las comunicaciones, de los hipermedias y de la realidad virtual. Espacio que no está conformado por dimensiones espaciales, sino que está inscripto en la temporalidad singular de una difusión instantánea. Espacio telemático, caracterizado como espacio ni físico ni presencial sino electrónico y representacional, un no lugar digital fuera de los límites que establece el territorio físico.

En el mundo virtual, el espacio deja de ser una forma a priori y se convierte en una imagen que hay que formalizar y modelar. Esto implica una recomposición y una redefinición permanente de las relaciones espaciales entre los objetos. Los objetos no sólo habitan un espacio, lo constituyen tanto como son constituidos por él. El espacio deja de ser un sustrato intangible y se vuelve objeto de modelaje en interacción constante con los otros objetos modelados. Para entender su naturaleza es fundamental entender su capacidad de mediación entre los sentidos y la inteligencia.

Estos mundos virtuales no están en ninguna parte. No son necesariamente coherentes en sus correspondencias con la realidad (coherencia espacial, invariabilidad en cualquier transformación y estabilidad en el tiempo) y pueden ser modelados para simular la realidad pero también pueden ser modelados en forma arbitraria para crear otras realidades.

En los procesos de Virtualización del cuerpo, los cuerpos visibles, audibles y sensibles proliferan y se dispersan hacia el exterior como nuestros propios simulacros. El cuerpo sale de sí mismo, es permeable, adquiere nuevas velocidades y espacios, crea y reconoce otras formas y transforma la exterioridad técnica o la alteridad biológica en subjetividad concreta.

Cuando una persona, información o cosa se virtualiza, se coloca fuera de ahí, se desterritorializa, se desconecta del espacio físico o geográfico ordinario y de la temporalidad del reloj. Si bien, no son totalmente independientes del espacio-tiempo clásico de referencia para poder materializarse, sólo lo recortan tangencialmente escapando a sus atributos de ubicuidad, simultaneidad, distribución fragmentada o masivamente paralela.

Haciendo una retrospectiva histórica, podemos reconocer que la distinción del adentro y del afuera, el aquí y el allá, eran derivados artificiales de los límites de la velocidad, de las restricciones de tiempo impuestas a la libertad de movimientos. La distancia, lejos de ser objetiva,

impersonal, establecida, es un producto social cuya magnitud varía en función de la velocidad empleada en superarla. Con la implosión del tiempo de las comunicaciones, la reducción del instante a valor cero, el desplazamiento de la información independiente de sus transportadores físicos, los indicadores de espacio y tiempo pierden importancia y consecuentemente se relativizan.

2.2.2 Fundamento epistemológico.

La epistemología se asocia con el conocimiento. Comprende una disciplina con características abstractas, debido al énfasis en el reconocimiento o reflexión del conocer sobre el sujeto y el objeto, la realidad y el pensamiento, que permiten ver una realidad desde un punto de vista propio. La epistemología analiza los criterios por los cuales se justifica el conocimiento además de considerar las circunstancias históricas psicológicas y sociológicas que llevan a su obtención. En este contexto:

- El proyecto asocia el conocimiento con la investigación en escenarios reales, utilizando como método el diseño, desarrollo y puesta en marcha de topologías virtualizadas de redes de computadoras.
- Aplicar los procesos de diseño de las topologías para realizar la interconexión eficiente y de calidad.

La Virtualización en la educación.-

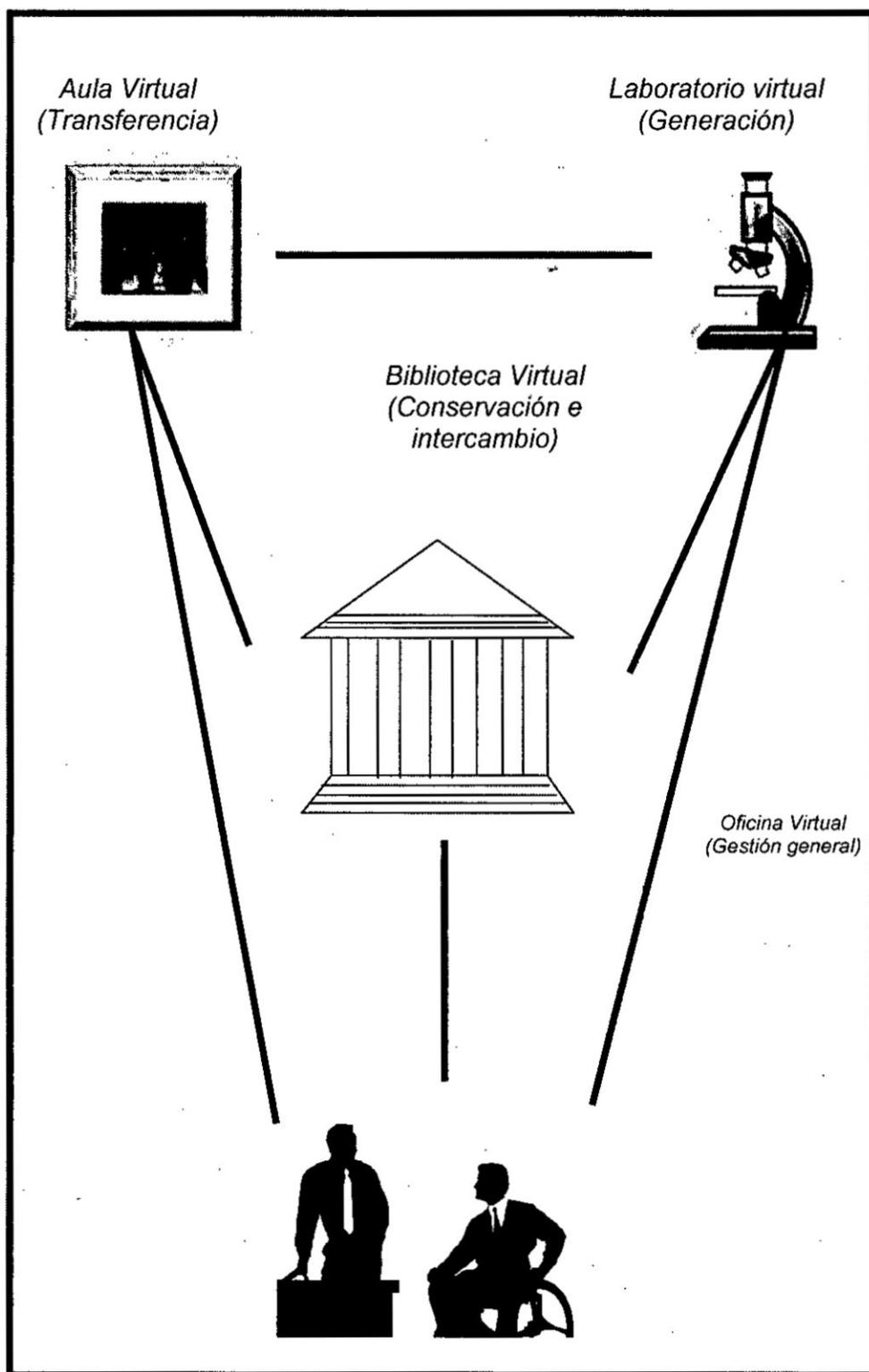
En términos generales, la Virtualización es un proceso y resultado al mismo tiempo del tratamiento y de la comunicación mediante computadora de datos, informaciones y conocimientos.

Sobre la base de estos sencillos principios tecnológicos se pueden representar espacios reales por espacios virtuales, que funcionan en un ambiente electrónico reticulado, donde ocurren procesos diversos y en los cuales participan actores que se valen de objetos y contenidos de información y conocimiento para realizar sus actividades. Es posible entonces construir y operar aulas virtuales (como espacios de enseñanza y aprendizaje), laboratorios virtuales (como espacios de investigación) y bibliotecas virtuales como espacios para la conservación y el intercambio de informaciones y conocimientos que sirven de soporte a la enseñanza, el aprendizaje y la investigación.

En la Tabla 2.2 hemos identificado los principales espacios virtualizables de una organización de educación superior, junto con las funciones del conocimiento a las cuales corresponden, los procesos típicos de la educación superior que ocurren en ellos, los actores involucrados, los objetos utilizados y las estructuras organizativas donde están insertados.

El resultado de este proceso de Virtualización debe traducirse en un campus virtual, con un conjunto de espacios virtuales cuyas funciones deben estar interrelacionadas, de la misma forma que lo están las funciones de la gestión del conocimiento. En un aula virtual se pueden generar conocimientos y un laboratorio virtual puede convertirse en un instrumento para transferir conocimientos. Asimismo, la biblioteca virtual no es sólo un reservorio de información sino un ambiente activo donde los usuarios generan y transfieren conocimiento.

Fig. 2.10 El Campus virtual y sus espacios virtuales
(Fuente propia)



Universidades y otras instituciones de educación como los Institutos Tecnológicos, especialmente las de países en vías de desarrollo como el nuestro, confrontan el problema de servir a una población cada vez mayor de estudiantes sin contar con la infraestructura requerida para tal fin, brindando un servicio educativo con muy poca calidad. Otra problemática existente es la de brindar a la población trabajadora una educación permanente, como respuesta a los requerimientos dinámicos de una sociedad del conocimiento en proceso de gestación, en la cual predomina un alto índice de innovación (Toffler, 1970, 1980 Y 1990). La adaptación a este tipo de sociedad y, más aún, participar en ella de manera proactiva, requiere de una alta tasa de renovación permanente de conocimientos. La Virtualización de estas organizaciones puede ser un factor transformador de sus estructuras y funciones, un instrumento para mejorar su cobertura, calidad, pertinencia y equidad de acceso y una manera de construir una nueva identidad y ocupar un lugar proactivo en esa nueva sociedad del conocimiento. La viabilidad y factibilidad de convertir a la virtualización en un factor de calidad académica dependerá del enfoque utilizado para implantarla y desarrollarla, y sobre todo, del papel que jueguen los usuarios.

La educación superior virtual en el mundo

Así como se han identificado grados y tipos de interactividad en las instituciones educativas superiores, se han podido distinguir grados y

distancia es aún incipiente si se considera que estas universidades representan sólo 1,3% del total de universidades en el mundo, los estudiantes a distancia 5,3% de la población estudiantil total y los profesores 1,9%. Su distribución es muy desigual y en ella se advierte el enorme esfuerzo realizado por los países asiáticos para atender su enorme demanda estudiantil a nivel superior. En Asia se concentra el 81,8% de la población estudiantil a distancia y 11% en Europa. Luego siguen América Latina y el Caribe con 3,3%, Oceanía 3,2 % y África 0,8%. Sin embargo, un estudio reciente sobre América Latina ha permitido identificar con mayor precisión un número mayor de programas de educación a distancia, con lo cual la importancia relativa de la región podría ser mayor que la indicada (Chacón y González, 2009). Por otra parte, estas cifras pueden modificarse sensiblemente si se incluyeran los datos de Estados Unidos y Canadá, aunque la importancia de Asia se mantendría por el esfuerzo notable que han hecho estos países en materia de educación a distancia. Las universidades a distancia constituyen un potencial importante de Virtualización del aprendizaje, por su vocación natural, pero son herederas de una tradición muy fuerte de uso de medios tradicionales de comunicación, que implica una gran inversión.

De acuerdo a la información de la UNESCO, en once países, 2 o más millones de personas cursan estudios superiores. Entre ellos figuran

desarrollo. Estas tres funciones se han identificado con tres procesos: enseñanza-aprendizaje, investigación y extensión. Para todas estas funciones, habría que crear ambientes virtuales estructurados de gestión de información y de comunicación entre las universidades y sus usuarios respectivos. ¿Hasta dónde debe avanzar la Virtualización, en función de su necesidad, deseabilidad, oportunidad, conveniencia y factibilidad?

Habría que preguntarse igualmente si, verdaderamente, dadas las condiciones precarias de funcionamiento de las universidades en los países en vías de desarrollo, es realista exigir esta integración multifuncional, cuando ellas aún no han logrado resolver sus problemas en su función de enseñanza y aprendizaje. La función de enseñanza es, sin duda, la que tiene más peso en el conjunto de funciones. Las organizaciones de educación superior y tecnológica, siguen estando sometidas a una fuerte presión social por el crecimiento de una población cada vez más numerosa deseosa de aprender. Se debe tener presente que el ritmo de crecimiento de esta población en los países en vías de desarrollo duplica el de los países desarrollados. A esta población se agrega la de profesionales y técnicos incorporados al mercado de trabajo que desean perfeccionar sus conocimientos, para mantenerse al día con las exigencias en materia de nuevos conocimientos, y la de personas incorporadas al mercado de trabajo que no pudieron acceder a la educación superior en su oportunidad y buscan una segunda oportunidad para superarse profesionalmente, con miras a convertirse en actores

eficaces en la nueva sociedad del conocimiento en proceso de gestación, donde la mayor parte de los trabajadores serán los llamados trabajadores del conocimiento o trabajadores simbólicos (Reich, 1992). En este contexto las universidades tendrán una demanda cada vez mayor de prestación de servicios. Los países en vías de desarrollo no escaparán a la transición hacia la sociedad del conocimiento. El desarrollo no es lineal y estos países no deberán necesariamente transitar la misma senda que los desarrollados antes de llegar a la sociedad del conocimiento. En virtud de la fuerte tendencia hacia la globalización de todas las actividades de la sociedad mundial, los países en vías de desarrollo como el nuestro, también tendrán que incorporarse a esta tendencia.

Existe un factor muy importante que influirá decisivamente en la evolución futura de la educación en sus distintos niveles y que no ha sido tomado con frecuencia en cuenta por muchos especialistas. Se trata del surgimiento de una nueva generación de jóvenes que están creciendo en un mundo impregnado de tecnología electrónica y medios electrónicos, totalmente opuesta a la filosofía de transmisión lineal de información sin interacción, que es el modelo de la televisión y otros medios de comunicación de masas. Estos jóvenes muestran una gran facilidad y versatilidad para el aprendizaje de esa tecnología, pues ella es esencialmente interactiva, muy adaptada a las características psicológicas, necesidades y aspiraciones de esos jóvenes. Por primera vez, una generación más joven domina una tecnología mejor y más rápido

que la generación adulta, lo cual no se había producido en toda la historia de la humanidad. Michel Cartier ha vislumbrado claramente este fenómeno y ha puesto de relieve el papel que podrían jugar las diferentes generaciones de usuarios en la futura sociedad del conocimiento (Cartier, 1997).

2.2.3 Fundamento metodológico.

La metodología básica consistirá en comparar la calidad de servicio con los métodos alternativos, es decir los métodos tradicionales de realizar la capacitación sobre redes de computadoras. Se proponen algunas maneras de determinar si vale la pena la utilización de la Virtualización en la capacitación en redes. Estos métodos se explican a continuación.

Método de Minimización de Costos.

Cuando los resultados de los métodos empleados son equivalentes, se escoge el menos costoso, y se determina el sistema menos costoso para alcanzar ciertos objetivos. Si los objetivos no se pueden cuantificar o comparar el método falla. Se debe basar en comparar los costos específicos, la utilidad y la efectividad para los mismos objetivos entre una capacitación tradicional y el empleo de la Virtualización. Prevalece la que puede demostrar que brinda atención a un mayor número de personas, con mejor calidad, en el menor tiempo y menor costo. La decisión final luego de compararlos se mide desde el balance netamente económico, dado el alto costo que significa la implementación completa de

laboratorios físicos. No se dispone de parámetros previos o comparativos con otros métodos utilizados en el pasado.

Análisis de Efectividad. -

Las consecuencias de técnicas utilizadas son medidas por medio de indicadores naturales expresados en las unidades físicas más apropiadas y se selecciona la más alta, por ejemplo, determinar el número de experiencias realizadas, número de participantes capacitados, porcentaje de aprendizaje, etc. Los niveles de exactitud establecidos deberán ser fijados con respecto a los niveles normalmente obtenidos mediante una capacitación tradicional. Los resultados se obtienen al comparar estos valores con los obtenidos con el uso de la Virtualización.

Análisis Costo-Beneficio

Se evalúan las consecuencias de los métodos utilizados en términos monetarios y el beneficio práctico que de ellos se obtiene, lo que permite confrontar los costos. Sin embargo, es difícil asignar este valor monetario. Este método es el más genérico y amplio de evaluación económica. Permite comparar directamente los costos y las ventajas de ambas alternativas.

Más que evaluar la inversión en tecnología y el costo de operación, se debe evaluar el costo implícito y la calidad del servicio, para lograr así los objetivos deseados, maximizando los beneficios de un presupuesto dado.

Un buen ejemplo de este tipo de análisis es el establecimiento de un servicio de educación a distancia, en donde se busca asegurar que exista un reporte oficial de capacitación de los participantes versus la disminución de los costos de funcionamiento. Ello se obtiene mejorando la calidad del servicio y reduciendo los costos de funcionamiento de manera global.

Por otro lado, para evaluar el uso de la Virtualización que pueda suministrar el soporte para el diseño de un método de capacitación en redes, se analizaran los siguientes puntos:

1. **Funcionalidad:** Debe permitir que los usuarios (participantes), cumplan con los laboratorios propuestos, proveyendo conectividad entre ellos y calidad de servicio.
2. **Escalabilidad:** Debe ser capaz de crecer, es decir, debe soportar el incremento en usuarios, servicios y aplicaciones sin mayores cambios estructurales, manteniendo la calidad de servicio.
3. **Adaptabilidad:** Debe ser diseñada para que pueda adaptarse a tecnologías futuras, además que no debe incluir elementos que limiten la implantación de nuevas tecnologías.
4. **Administrabilidad:** El diseño debe permitir el monitoreo y administración para asegurar la estabilidad del sistema.

2.3 Definiciones de términos básicos.

Emulador.- En informática, un emulador es un software que permite ejecutar programas de computadora o videojuegos en una plataforma (arquitectura hardware o sistema operativo) diferente de aquella para la cual fueron escritos originalmente.

Simulador.- El simulador sólo trata de reproducir el comportamiento del programa.

Virtualización.- Virtualización es la técnica empleada sobre las características físicas de algunos recursos computacionales, para ocultarlas de otros sistemas, aplicaciones o usuarios que interactúen con ellos. Esto implica hacer que un recurso físico, como un servidor, un sistema operativo o un dispositivo de almacenamiento, aparezca como si fueran varios recursos lógicos a la vez, o que varios recursos físicos, como servidores o dispositivos de almacenamiento, aparezcan como un único recurso lógico.

Hypervisor (Host).- Es la plataforma que nos permite aplicar diversas técnicas de control de Virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos en una misma computadora.

Máquina virtual (Guest).- Software que simula a una computadora y puede ejecutar programas como si fuese una computadora real.

Clúster.- Se aplica a los conjuntos o conglomerados de computadoras

construidos mediante la utilización de hardwares comunes y que se comportan como si fuesen una única computadora.

Almacenamiento compartido.- No es más que la integración de dispositivos de almacenamiento diferentes en un dispositivo de almacenamiento virtual.

Plantilla.- Es una máquina virtual pre instalada y sellada, que se utilizará para generar diferentes máquinas virtuales.

Nube.- Se refiere a todos los programas que se tiene acceso en red sin necesidad de instalación, y desde allí se puede generar contenidos, administrarlos, compartirlos, descargarlos y enviarlos, tal como se hace siempre, sólo que sin tener los programas en el computador.

VCenter (Virtual Center).- Es la forma más simple y eficaz de gestionar VMware vSphere, con independencia de si tiene decenas o miles de máquinas virtuales.

DRS: VMware Distributed Resource Scheduler (DRS).- Balancea dinámicamente las máquinas virtuales de un servidor VMware ESX/ESXi a otro servidor o servidores VMware ESX/ESXi para mejorar el tiempo de respuesta de las aplicaciones que las máquinas virtuales contienen.

Firmware.- Bloque de instrucciones de máquina para propósitos específicos, grabado en un chip, normalmente de lectura/escritura (ROM, EEPROM, flash, etc.),

Diferencia entre emulador y simulador

Un simulador sólo trata de reproducir el comportamiento del programa, un emulador trata de modelar de forma precisa el dispositivo, de manera que este funcione como si estuviese siendo usado en el equipo original.

CAPITULO III

VARIABLES E HIPOTESIS

3.1 Definición de las variables

Una variable es una cualidad susceptible de sufrir cambios. Aunque la virtualización es bastante conocida y está en franco desarrollo en los países desarrollados, en los nuestros, en proceso de desarrollo, sirve para cambiar la forma de la enseñanza de los conceptos de redes proporcionando una mejor calidad de la enseñanza y por tanto del país, aplicada en conjunto con otras medidas complementarias.

A= Calidad de educación tradicional.

B= Calidad de educación utilizando Virtualización.

3.2 Operacionalización de las variables.

Los resultados obtenidos podrán ser verificados por la evolución positiva que tengan las entidades académicas donde sean aplicados estas modificaciones o métodos de enseñanza utilizando Virtualización, o lo mínimo, por pruebas específicas de evaluación a los alumnos participantes de estos planes piloto.

$A = f(Y)$ Donde Y = Desarrollo tradicional de los laboratorios

$B = f(Z)$ Donde Z = Desarrollo de los laboratorios usando
Virtualización.

Si:

A > B Nuestra hipótesis es falsa.

B > A Nuestra hipótesis es verdadera.

3.3 Hipótesis general e hipótesis específicas

Una hipótesis de investigación representa un elemento fundamental en el proceso de Investigación. Después de formular un problema, el investigador enuncia la hipótesis, que orientará el proceso y permitirá llegar a conclusiones concretas del proyecto.

Hipótesis general: Es la que permite responder de forma amplia, a las dudas que el investigador tiene acerca de la relación que existe entre las variables. En este caso:

La Virtualización como herramienta para la enseñanza de redes de computadoras en la formación de los estudiantes de Ingeniería, influye significativamente en la calidad de servicio que se brinda en los laboratorios a un menor costo.

Hipótesis específicas: Es específica aquella hipótesis que se deriva de la general, y tratan de concretizar a la hipótesis general y hace explícitas las orientaciones concebidas para resolver la investigación. En este caso,

- a) Se pueden reducir las limitaciones físicas (cantidad de alumnos capacitados) utilizando Virtualización, mejorando de esta forma la calidad de servicio en los laboratorios de redes de computadoras.

- b) El costo que representa la implementación de laboratorios con redes físicas puede ser minimizado con la implementación de redes virtuales como herramienta en Ingeniería Eléctrica.
- c) Es mucho más flexible la implementación de topologías en redes virtuales que en redes físicas, reduciendo de esta forma los tiempos requeridos para la capacitación.

CAPITULO IV

METODOLOGIA

4.1 Tipo de Investigación.

El tipo de investigación Básica, denominada también pura o fundamental, busca el progreso científico, acrecentar los conocimientos teóricos, sin interesarse directamente en sus posibles aplicaciones o consecuencias prácticas; es más formal y persigue las generalizaciones con vistas al desarrollo de una teoría basada en principios y leyes.

La investigación Aplicada, guarda íntima relación con la básica, pues depende de los descubrimientos y avances de la investigación Básica y se enriquece con ellos, pero se caracteriza por su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos. La investigación Aplicada busca el conocer para hacer, para actuar, para construir, para modificar.

El tipo de investigación de esta tesis es del tipo Aplicada.

4.2 Diseño de la Investigación.

Virtualización se refiere a un concepto en el cual el acceso a una pieza de hardware, tipo un servidor, es coordinada de tal forma que múltiples sistemas operativos INVITADOS, pueden compartir esa única pieza de hardware, sin ningún los otros tengan conocimiento de su existencia. El sistema operativo invitado (OS guest) es un OS que es hospedado por el

sistema operativo de Virtualización de capa subyacente, el cual es a menudo llamado sistema "hospedero". Cada sistema operativo invitado, se muestra para la aplicación, como un sistema ejecutándose como un sistema operativo completo, que el mismo desconoce que está corriendo en la parte más alta de la capa del software de Virtualización, en lugar de hacerlo directamente en el hardware físico.

4.2.1 Conceptos básicos de sistemas de Virtualización

La importancia de la enseñanza de redes de computadoras está siendo reconocida. Por ejemplo, los grupos de trabajo que desarrollan los planes de estudio de redes en los últimos años, afirma que "la creación de redes es la base en gran parte de nuestra economía".

El dominio de la computación centrada en red implica tanto teoría y práctica. Se recomienda realizar experiencias de aprendizaje que impliquen la realización de experiencias y el análisis práctico, ya que refuerzan comprensión de los conceptos y su aplicación en problemas del mundo real. Los experimentos de laboratorio deben involucrar la recopilación y síntesis de datos, modelado empírico, análisis de protocolos a nivel de código fuente, monitoreo de paquetes de red, construcción de software, y evaluación de modelos de diseño alternativos. Todos estos son conceptos importantes que pueden entenderse mejor por experimentación en el laboratorio.

Este documento, también enumera los resultados del aprendizaje de

como instalar una "red simple con dos clientes y un único servidor estándar utilizando las herramientas de software de configuración de host DHCP", e "implementar un firewall de red".

También se reconoce en todo lugar, que el aprendizaje acerca de las redes requiere de experiencias prácticas (Agilent Technologies, 2001, Asia Computer Weekly, 1999, Costa, 2000, Kasim 2002, Lógica UK Ltd, 2002, Mateyaschuk, 1999, Montgomery, 2002, NORTEL REDES, 2002).

Sin embargo, el realizar el aprendizaje práctico de las experiencias puede ser problemático por:

- 1) Falta de fondos para establecer y mantener hardware de redes, y software en cantidad suficiente para que cada estudiante pueda tener acceso igual al ambiente de aprendizaje dentro y fuera de las clases programadas.
- 2) Falta de control espacio físico, ambos con aire acondicionado para los servidores, y hardware utilizado directamente por los estudiantes.
- 3) Falta de seguridad en el entorno de red que pueda proteger de manera fiable servicios prestados en las mismas máquinas o redes.
- 4) Los laboratorios son a menudo necesarios para múltiples temas con diversos software y hardware.

Afortunadamente, la tecnología de redes se ha convertido en una herramienta pedagógica esencial y es importante desarrollar un accesible

entorno virtual de aprendizaje para solucionar estos problemas.

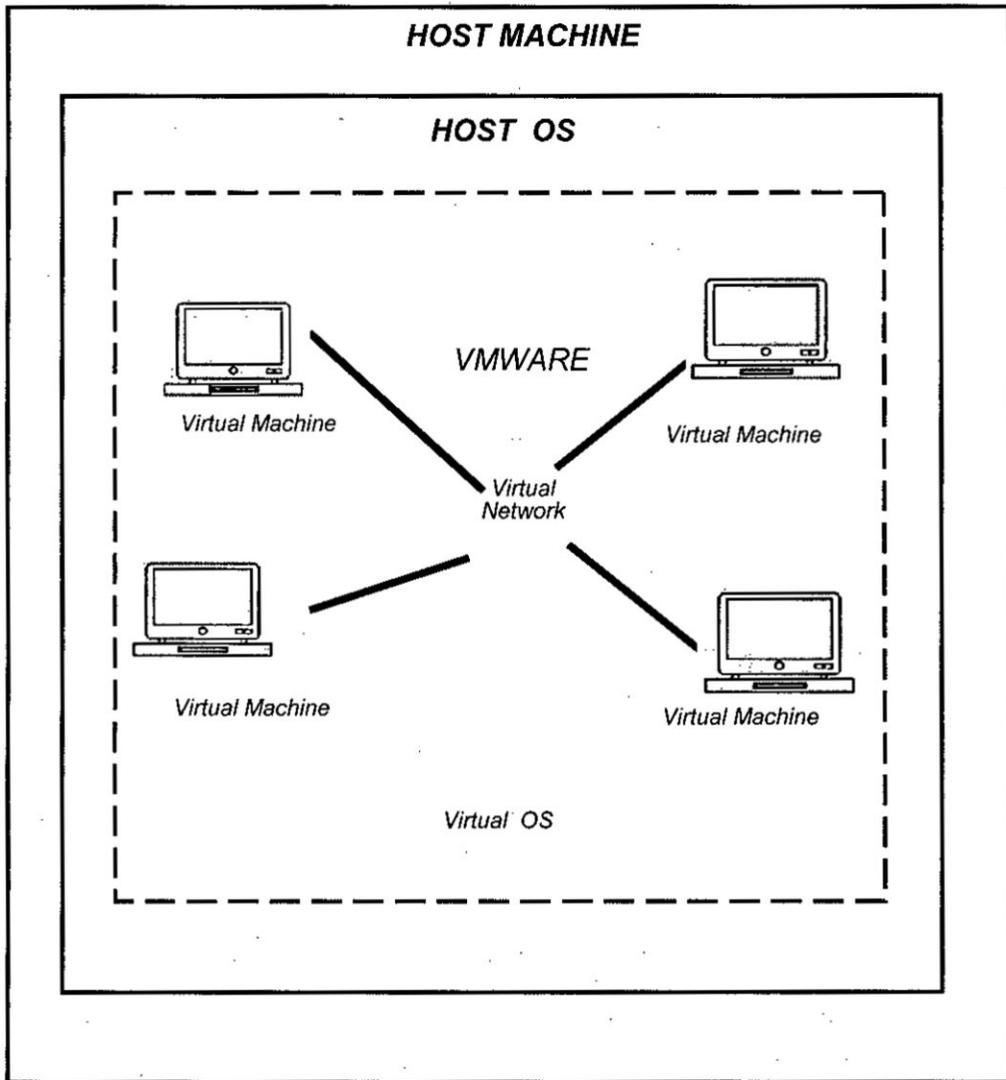
En este trabajo describimos nuestro método seguro y rentable enfocado a la creación de redes utilizando un sistema de aprendizaje virtual llamado Velnet (Entorno virtual para el aprendizaje de redes) (Kneale y Box, 2003). Hemos mejorado Velnet con una capa de realidad virtual. Velnet fue desarrollado y experimentado con éxito en el 2003 y han superado algunos de los problemas con la provisión de un auténtico ambiente de aprendizaje. Velnet nos brinda conceptos actuales de redes de computadoras sobre la configuración de dispositivos. El desarrollo de una capa de realidad virtual para Velnet permite presentar conceptos de redes informáticas sobre una topología física y lógica, así como la configuración de dispositivos.

4.2.2 Velnet (Entorno virtual para el aprendizaje de redes)

Velnet utiliza hardware y software existentes para presentar un ambiente de red virtual en la que los estudiantes, de forma segura pueden aprender y experimentar con Tecnologías de redes.

Los componentes de Velnet y sus relaciones, que se muestran en la Fig. 4.1, son: la máquina anfitriona, el sistema operativo de la máquina anfitriona (VMWare™), máquinas virtuales y sus sistemas operativos, una red virtual que conecta las máquinas virtuales y, software de pantalla remota. En la Fig. 4.2 se muestra Velnet sin la superposición, aparece como varias ventanas en el escritorio de la máquina anfitriona.

Fig. 4.1 Los componentes de Velnet
(Fuente *Virtualization for Dummies*)



A Máquina anfitriona (Host)

Velnet está diseñado para funcionar en un único host de escritorio. El computador anfitrión emulará varias máquinas virtuales. El número de máquinas virtuales que pueden existir simultáneamente en el ordenador host depende de la cantidad de memoria y velocidad de la CPU.

La cantidad de memoria (RAM) requerida en el host se calcula en función de los requisitos de memoria del sistema operativo del host, más la memoria requerida por los sistemas operativos virtuales que están corriendo simultáneamente en el host 3 GB de espacio en disco, requeriría un mínimo de capacidad total de disco del anfitrión de 18GB.

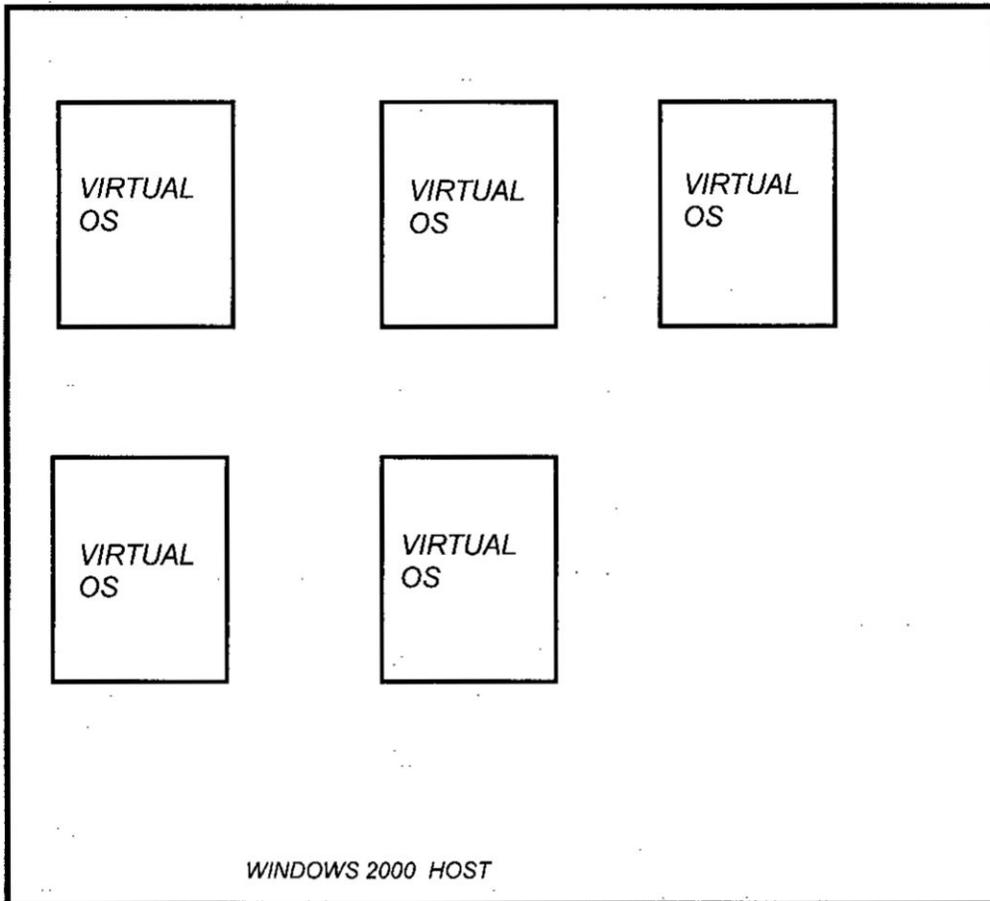
Nuestro primer experimento con Velnet tenía un ordenador principal corriendo con Windows® 2000 con cinco máquinas virtuales. Cuatro de las máquinas virtuales ejecutaron Windows® NT 4 Workstation y la quinta máquina virtual ejecuto Windows NT® 4 Server que actuaba como un dispositivo de enrutamiento.

El piloto de Velnet utilizó seis máquinas anfitrionas con Windows® XP, cada uno con tres máquinas virtuales. Uno Máquina virtual corrió con OpenBSD mientras que las otras dos máquinas virtuales corrían con Windows® NT Workstation. Herramientas de Windows® XP de escritorio remoto se utilizaron para proporcionar a los estudiantes conectividad remota.

B Sistema operativo del host (Sistema operativo anfitrión)

Windows® 2000 fue elegido inicialmente como el sistema para el host por su facilidad de configuración y la familiaridad del estudiante con el sistema. Se encontraron dificultades menores con este sistema operativo cuando VMWare y VNC estaban conectadas.

Fig. 4.2. Windows 2000 con 5 VM
(Fuente propia)



C VMWare™

Velnet requiere software que proporciona hardware múltiple en el equipo host. Las aplicaciones Open-source que proporcionan hardware de PC virtual no están disponibles generalmente. Dos productos comerciales fueron revisados para aplicar en este proyecto: VMWare™ (VMWare™ Workstation, 2002) y Virtual PC™ (Virtual PC™, 2002).

Ambas aplicaciones ofrecen hardware virtual Intel® x86, entornos

compatibles con varios sistemas operativos del host. Aunque ambas aplicaciones proporcionan entorno de hardware virtual, la configuración de la red deseada para fines pedagógicos requiere conexión de dos máquinas virtuales a través de una línea virtual serial. En el Tiempo de escritura, VMWare™ fue el único producto que provee la capacidad de conectar dos máquinas virtuales a través de una línea serial virtual (VMWare™, 2002). La configuración no necesita líneas serial aceptable para su uso con Virtual PC™ (Connectix, 2002).

D Máquina Virtual

La máquina virtual emula un hardware Intel® x86. Desde el momento de "encender" la máquina parece como si fuera una computadora real físicamente dicha, sólo que lo que inicialmente aparecería en un monitor si la máquina fuera real, ahora se limita a una ventana en el escritorio.

E Sistema operativo virtual (SO virtual)

La elección del sistema operativo depende de los resultados deseados de aprendizaje, el costo y la memoria disponible en el host.

Para el control del puntero, como las dos máquinas virtuales estaban ejecutando sistemas operativos basados en GUI, quitar VNC y el uso del acceso a escritorio remoto del Windows XP, resolvió este problema. El problema no era evidente para las máquinas virtuales que ejecutan sistemas operativos basados en texto como OpenBSD.

Aunque hay una máquina host, cada máquina virtual tiene una identidad

separada, y como tal, se debe obtener la licencia para cualquier sistema operativo, u otro software utilizado.

La elección del sistema operativo para las máquinas virtuales solo en el experimento inicial fue Windows® NT Workstation y Windows® NT Server. La elección del sistema operativo para las máquinas virtuales, para el piloto, fue OpenBSD y Windows® NT Workstation.

El uso cuidadoso de sistemas operativos de código abierto como Linux® y OpenBSD, ofrecen alternativas menos costosas que los productos patentados.

F Red Virtual

La red virtual se ejecuta en VMWare, como una función de esta aplicación. Algunos de los componentes de una red física tales como, switch y adaptadores de red se emulan en la red virtual. El enrutamiento es apoyado por los sistemas operativos que tienen esta función y están instalados en las máquinas virtuales

G Pantalla de escritorio remoto (RDD)

El software del escritorio remoto permite a los estudiantes controlar, de forma remota, el escritorio de la máquina residente del Velnet desde cualquier lugar de Internet. La mayoría de software RDD es de tipo cliente / servidor. La parte del servidor se ejecuta en la máquina anfitriona. La parte cliente del sistema corre en cualquier máquina a partir de la cual el estudiante desea controlar remotamente el escritorio de la máquina

software de configuración del host DHCP", e "implementar un firewall de red".

La cantidad de memoria (RAM) requerida en el host se calcula en función de los requisitos de memoria del sistema operativo del host, más la memoria requerida por los sistemas operativos virtuales que están corriendo simultáneamente.

La capacidad de disco necesaria en la maquina host es calculada sobre la base de los requisitos de almacenamiento de cada sistema operativo, independientemente de las maquinas que estén corriendo. Por ejemplo, una configuración de cinco máquinas virtuales, cada una de las cuales requiere 3 GB de espacio en disco, requiere un mínimo de capacidad total de disco del anfitrión de 18 GB.

El uso de RDD limita el número de usuarios de Velnet a uno por vez en cada máquina host. Con múltiples máquinas host esto no es un problema, por ejemplo, en el piloto con seis estudiantes, se utilizó seis máquinas anfitrionas.

H software

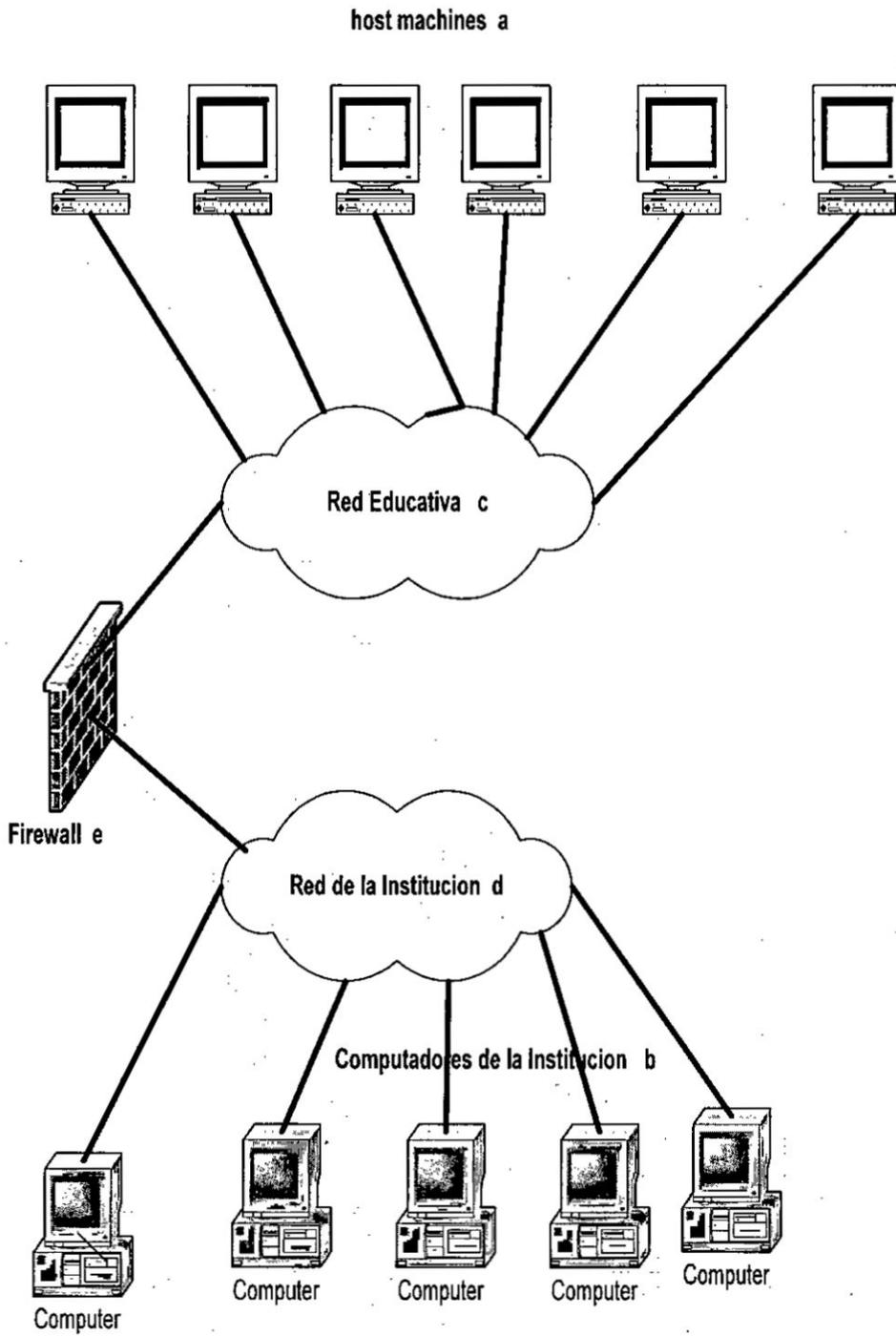
El software de escritorio remoto permite a los estudiantes interactuar con la red virtual desde cualquier lugar de la Internet. Para los propósitos de nuestro piloto, el acceso fue restringido a las computadoras cliente dentro de la red. Velnet se está ejecutando (seis veces) en seis máquinas host diferentes. Cada sesión de Velnet tiene una red virtual individual (Fig. 4.3a). Los estudiantes obtienen acceso remoto a través de un computador

(Fig. 4.3b) conectado a la red de la institución (Fig. 4.3d). Un firewall de red (Fig. 4.3e) se utiliza tanto para proteger la red comunitaria de acciones accidentales o maliciosas dentro de la red virtual, y restringir el acceso a la red virtual solo a aquellos estudiantes matriculados en la asignatura. El firewall está configurado para permitir sólo sesiones de RDD. Cualquier problema de configuración con las redes o los computadores anfitriones se limitarán a la red de enseñanza (Fig. 4.3c)

El primer piloto de Velnet restringió el acceso a las computadoras cliente dentro de la institución como se indicó anteriormente. Sin embargo, una vez que los problemas de seguridad para un acceso más amplio a Internet se resuelvan, sería posible que los estudiantes puedan conectarse desde cualquier lugar.

Como se mencionó el uso del acceso RDD a Velnet restringe el uso a una máquina anfitriona por estudiante a la vez. Hay beneficios al usar Velnet con RDD. Por ejemplo, el resultado para enseñar a "Instalar una simple red con dos clientes y un único servidor utilizando herramientas de software de configuración estándar para el host como DHCP", se necesita una computadora más software por estudiante, y no múltiples máquinas más software. Sin embargo, todavía la inversión es significativa. Sería una mejora usar Velnet, si pudieran acceder a un solo host muchos usuarios. Las mejoras a Velnet de correr en un solo host accedido por muchos usuarios nos llevan a considerar cómo las simulaciones y la realidad virtual pueden contribuir al aprendizaje en ambientes virtuales.

Fig. 4.3 Topología de laboratorios de redes
(Fuente propia)



Entornos virtuales de aprendizaje y realidad virtual

Winn y Jackson [10] presentaron 14 proposiciones sobre el uso de la realidad virtual en entornos de aprendizaje. Las aplicaciones para mejorar Velnet incluyen:

- a) Los entornos virtuales (VEs) son más baratos que los entornos físicos. Encontramos que Velnet accedido vía RDD ahorra costos, incluso con la RAM adicional, la CPU y el espacio en disco requerido. Si pudiéramos tener un host Velnet accedido a través de realidad virtual por muchos usuarios, esperamos que siga siendo más barato.

Winn y Jackson van más allá proponiendo que aunque un ambiente virtual puede ser menos real, como nuestra suposición de realidad virtual, el costo no hace que el resultado sea menor. Puede ser que las habilidades sean más fácilmente transferidas porque el entorno virtual es de menor probidad. Un estudiante que aprende en un VE de alta calidad puede esperar que el mundo real sea el mismo y por lo tanto confundirse con pequeños cambios. Los VE de menor fidelidad hacen que el estudiante generalice lo que ha aprendido en el real mundo.

- b) Los entornos virtuales son más seguros.

El VE proporciona un lugar seguro para practicar tareas arriesgadas. En nuestra situación la seguridad de la red es una preocupación. Otra es que los estudiantes se sientan seguros para experimentar sin causar daños de los que puedan sentirse

reprendidos. Esto también fue discutido por Forbus et Alabama. [12])

Velnet en un host con múltiples clientes de realidad virtual que podrían ser implementadas de forma similar a lo mostrado en la Figura 4.3. La diferencia es que no se requerirían seis hosts (Figura 4.3a), y los clientes (Figura 4.3b) tendrían cada uno un cliente de realidad virtual corriendo en lugar de RDD.

c) La interacción natural con el VE permite a los estudiantes experimentar conceptos metafóricos y fenómenos indetectables. En un ambiente real, los estudiantes pueden aplicar habilidades y conocimientos mediante el uso de un teclado, un ratón y un monitor para trabajar en un dispositivo o acceder a un dispositivo desde otro. Velnet emula esta interacción natural. Sin embargo, si queremos que los estudiantes vean, digamos un paquete en una red, no podemos hacer esto de un ambiente real. Podemos hacer esto en una simulación.

d) Cada vez hay más pruebas de que los estudiantes, particularmente aquellos que no están inclinados o comprometidos académicamente como la mayoría de los estudiantes que cursan estudios superiores (Biggs,[09]), tienen más probabilidades de hacerlo bien y desarrollan familiaridad con el material de un VE.

Esta proposición podría ser apoyada o refutada reflexionando sobre las experiencias de los maestros en el uso de Velnet, y la

superposición de la realidad virtual. Por ahora, estamos alentados por la creciente evidencia de que Velnet y sus nuevas versiones, mejoraran las experiencias de aprendizaje de nuestros estudiantes.

- e) Conceptos constructivistas de aprendizaje y experiencias actuales (Clancey, [21]) permite a los estudiantes familiarizarse con ellos y captar este nuevo conocimiento.

En este caso los estudiantes usarán una GUI, que es algo familiar, y sumaran conocimientos sobre la creación de redes que pueden ganar experimentando el VE.

El VE puede entonces ser usado para evaluar al estudiante en una actividad, donde él demuestre sus conocimientos usando problemas a resolver. Esta auténtica evaluación se realizará en base a la holística del rendimiento de las tareas (Montgomery [30]).

- f) La VE sitúa el aprendizaje en un contexto real.

La apariencia de cada máquina virtual en Velnet aparecería como si fuera una máquina física separada. Velnet tiene presencia; los estudiantes pueden estar convencidos de que están trabajando con una red real. Ellos directamente realizan sus experiencias con Velnet en una forma real. Velnet es "lo suficientemente real" para las herramientas comunes de Redes tales como analizadores de protocolos y software de gestión de redes para ser empleado para resolver problemas reales. Los estudiantes encontrarán los mismos desafíos con Velnet que en el mundo real: sistemas operativos

idiosincrásicos, implementaciones de software de red, y difícil de entender la documentación del usuario. De las 14 proposiciones presentadas por Winn y Jackson [38] encontramos que las seis discutidas anteriormente mejoran Velnet con una superposición de realidad virtual.

4.2.3 Software de Virtualización.

Respecto a la Virtualización de computadoras, existe una amplia oferta de software. VirtualBox es la herramienta que mejor se adapta a los requerimientos planteados. Cabe destacar que VirtualBox puede ser instalado en un servidor dedicado, tiene la capacidad de clonar VMs, está integrado a GNS3 y mediante phpVirtualBox se puede acceder a las distintas VMs a través de un navegador web. Se elige la herramienta VirtualBox, aun cuando no se trata de un software de distribución libre y phpVirtualBox no maneja el concepto de propiedad de una VM. VMware Server fue en algún momento el gran candidato, pero como el proyecto se ha discontinuado se le descartó.

Tabla 4.1 Algunas herramientas para Virtualización
(Fuente Virtualization for Dummies)

Herramienta	Packet Tracert	Boson NetSim	VNX	GNS3	Netkit	Marionet	CORE
Licencia	Privativo	Privativo	GPL	GPLv2	GPL	GPLv2	BSD
Ultima versión	5.3.3 feb. 2012	8.0 Nov. 2011	2.0 Mar. 2012	0.8.2 Mar. 2012	2.8 May. 2011	0.6 Feb. 2011	4.3 Mar. 2012
Sistemas operativos soportados	Windows Linux	Windows	Linux	Windows Linux Mac OS X	Linux	Linux	Linux FreeBS D
Soporta los TP	SI	SI	NO	SI	SI	SI	SI
Fácil de utilizar	SI	SI	NO	SI	NO	NO	NO
IOS Cisco	NO	NO	NO	SI	NO	NO	NO
GUI	SI	SI	SI	SI	NO	SI	SI
Conexión con equipos reales	NO	NO	SI	SI	SI	SI	SI

4.2.4 Laboratorios de Redes Virtuales. (Algunos laboratorios existentes).

Desde hace unos años se han presentado varios proyectos básicamente con el mismo objetivo. La idea es utilizar Virtualización como herramienta básica para su uso en laboratorios de redes virtuales. Los laboratorios creados de esta manera tienen varios propósitos, tales como, realizar experiencias de redes con protocolo IPv6, actividades educativas experimentales en general e investigación.

Se mencionan a continuación algunas de ellos.

Tabla 4.2 Características de software para Virtualización
(Fuente *Virtualization for Dummies*)

Herramienta	VirtualBox	Vmware Server	ESXi	XenServer	QEMU
Hypervisor	Tipo 2	Tipo 2	Tipo 1	Tipo 1	Tipo 2
Entorno subyacente en el servidor	Windows Linux	Windows Linux	Hardware	Hardware	Windows Linux Mac
Licencia	virtualBox PUEL	Gratuita	Gratuita	Gratuita	GNU GPL
Estado del proyecto	Activo	Discont.	Activo	Activo	Activo
Soporte de Software	SI	NO	SI	SI	SI
Admin. remota	CLI	WUI	GUI	CLI	CLI
	WUI			GUI	WUI
Entorno subyacente en el cliente	Windows Linux	Browser	Windows	Windows Linux	Windows Linux
	Browser				Browser
Integración con GNS3	SI	NO	SI	SI	SI
Interfaz de red virtual accesible	SI	SI	NO	NO	SI
Permisos y propiedad de la VMs	NO	NO	SI	SI	NO
Comp. Con hardware	Alta	Alta	Baja	Baja	Alta
Asistente para clonación	SI	NO	NO	NO	NO
Snapshots	SI	SI	SI	SI	SI

- **VNUML** (Virtual Network User Mode Linux). Es una herramienta open-source para Virtualización, diseñado para simular redes con computadores. Se basa en la UserModeLinux (UML) el cual fue desarrollado en el 2004 en Telematics Engineering Department (DET) de la Universidad Politécnica de Madrid.
- **UPM** Software diseñado como parte del proyecto de investigación Euro 6IX para la simulación de redes IPv6 con el software de enrutamiento open-source con zebra/quagga.
- **NETKIT** Es un software basado en el open-source y en la UserModeLinux. Su objetivo inicial era para uso experimental en el área de redes de computadores.
- **NETML** Está basado en lenguaje XML, fue diseñada para la descripción de la topología de red. El proyecto comenzó en 2005 en el Computer Networks Research Group (Universidad de Roma) como parte de LinuxUserGroup, LUGRoma 3, con el objetivo de crear entornos de educación a bajo costo.
- **IMUNES** Es una herramienta diseñada para la investigación en el área de sistemas distribuidos y redes informáticas. Este emulador de red se basa en el kernel del FreeBSD modificado. El proyecto se inició en el 2003 en la Electrotechnical Faculty (FER) de la Universidad de Zagreb (Croacia). Fue parte del desarrollo del proyecto Ethernet, enrutamiento y red de simulación con IPv4 e IPv6.

- **EINAR** Es un simulador de router, disponible como CDlive. Ha sido desarrollado para fines educativos y para la enseñanza de conceptos de enrutamiento. El proyecto fue desarrollado en el Royal Institute Technology (Suecia), basado en la plataforma Knoppix com, software de Virtualización Xen y software de enrutamiento Quagga.
- **VELNET** (Virtual Environment for Learning Networking) Es un laboratorio virtual para clases de redes de computadores basado en el software VMWare Workstation y varios sistemas operativos invitados (Windows XP, NT Workstation, Open BSD). Fue desarrollado en el año 2003 en la Facultad de Tecnología Informática y de Información en la Universidad de Western, Sydney, Australia.

Fig. 4.4 Arquitectura general de Virtualización sobre un servidor con cuatro máquinas virtuales.

(Fuente propia)

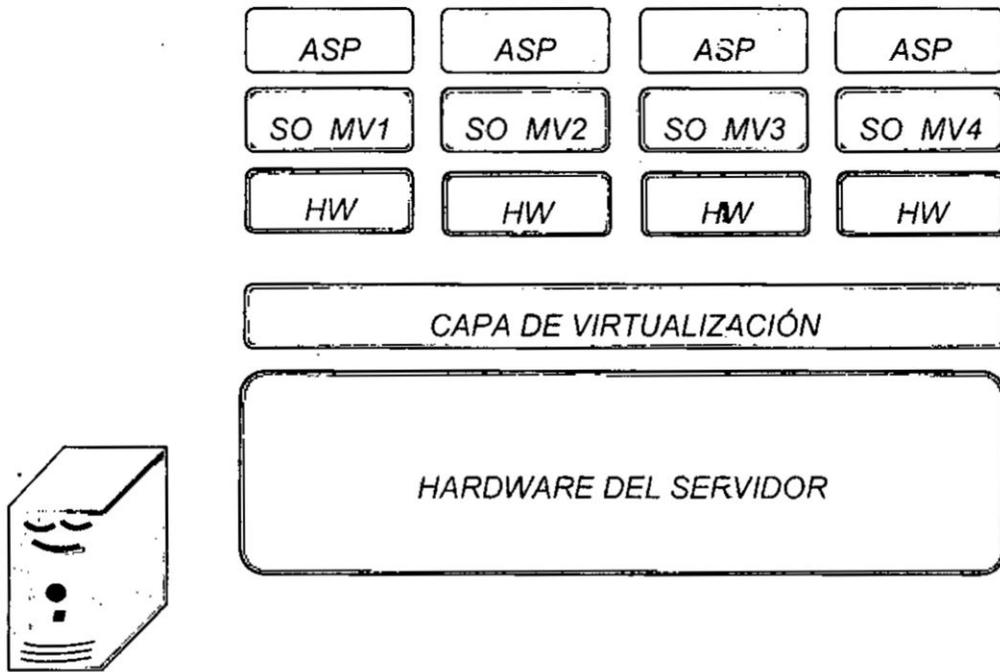


Fig. 4.5 Arquitectura general de un servidor sin Virtualización

(Fuente propia)

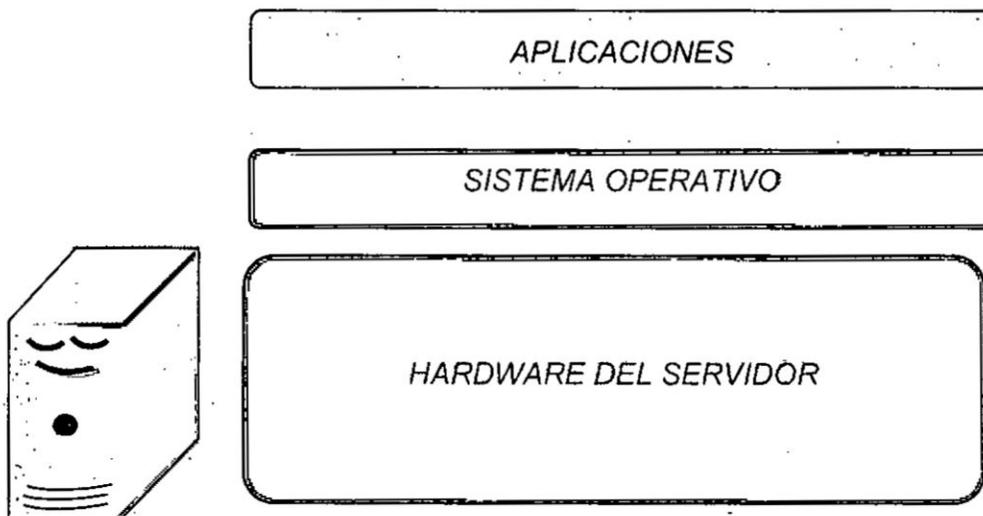
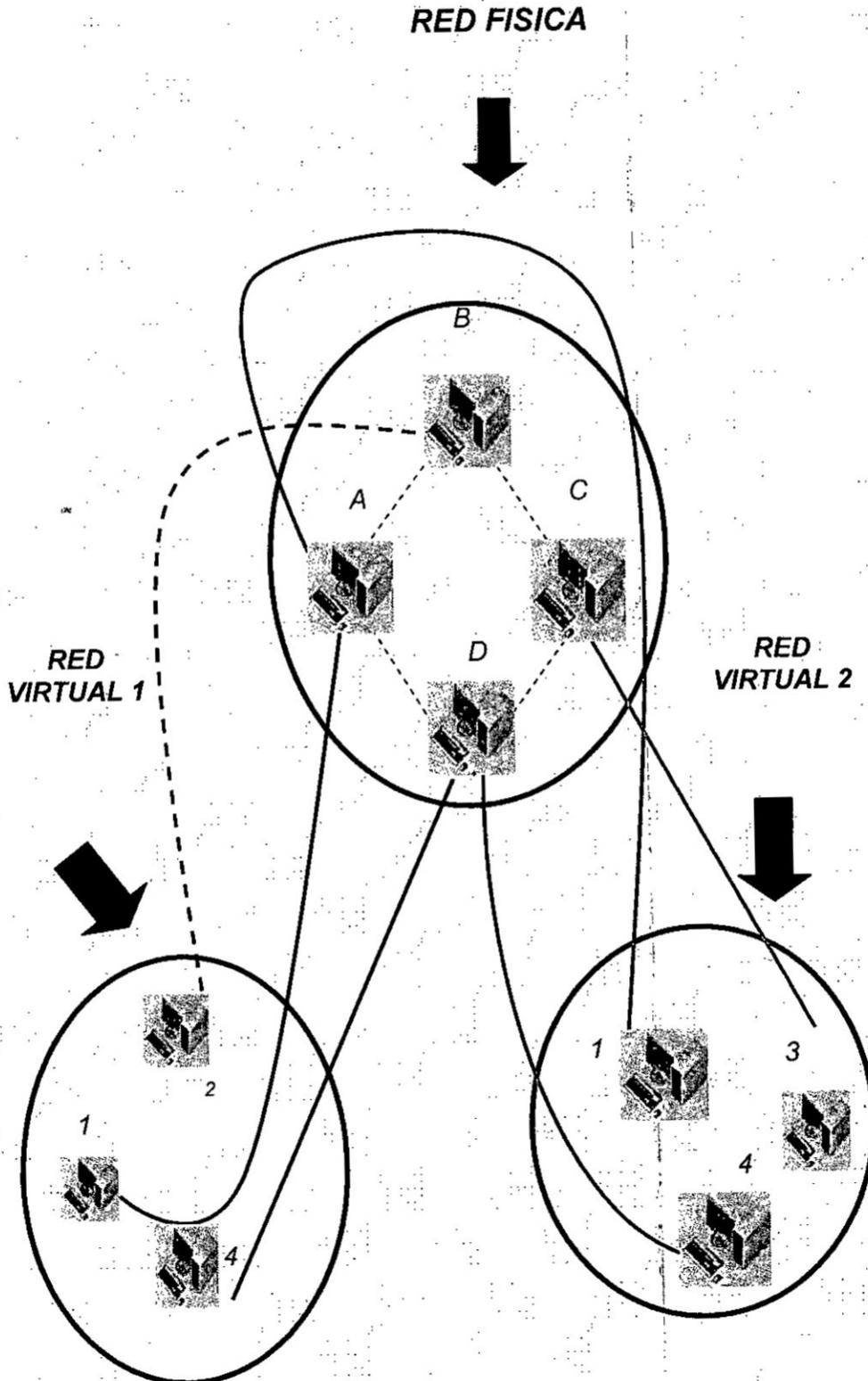


Fig. 4.6 Red física
(Fuente propia)



4.2.5 Implementación de laboratorios Virtuales.

Se describe a continuación un método para la implementación de laboratorios virtuales en la Technical faculty "Mihajlo Pupin" de Zrenjanini (Universidad de Novi Sad, Serbia & Montenegro). El laboratorio está planeado para ser usado en un curso de redes de computadores para enseñar entre otros, los siguientes tópicos: direccionamiento IP, ruteamiento estático y dinámico (RIP y OSPF), conceptos de firewall y servicios de red (Web y FTP). Para conseguir un costo accesible, la solución ha sido usar la plataforma Windows XP, debido a que el mismo laboratorio sería usado por otros cursos basados en la plataforma Windows. Las herramientas de software para la realización de los proyectos se limitan a VMWARE y PC Virtual, este último escogido por ser una versión licenciada.

La siguiente pregunta puede ser válida: ¿Cual puede ser lo más apropiado para usar con sistemas operacionales convidados que tienen que ser instalados en cada máquina virtual separadamente, y puede diferir del sistema operacional básico (Windows XP)? Considerando que el plan básico es desarrollar un ambiente de bajo costo, la elección lógica es usar Linux u otro sistema operativo open-source. Existen varias versiones Linux adecuados para su uso, entre ellos el Trustix Linux Server, compacto con instalación pequeña y bajos requisitos de hardware especialmente de memoria.

4.2.6 Ejemplos de los ejercicios en los laboratorios de redes virtuales

Una de las más importantes preguntas es, ¿Cómo organizar ejercicios de ruteamiento dinámico? Esto puede ser hecho usando varias versiones de software libre. Hay muchas versiones disponibles y estables de open-source en el mercado como Zebra, Quagga y XORP, software usado en los ejercicios descritos es GNU Zebra free routing software, con soporte para RIP, OSPF y BGP4 dynamic routing protocols.

Para implementar el web service fue usado un Server APACHE y para FTP, Proftpd.

Después de completada la instalación, máquinas virtuales con OS Linux y todo el software requerido fueron probadas durante el inicio y durante los ejercicios de laboratorio. Ellos fueron muy útiles y cumplieron adecuadamente la combinación de software para los ejercicios descritos.

Los resultados son mostrados en el capítulo siguiente. Para los ejercicios de laboratorio fue obligatorio instalar e iniciar todas las máquinas virtuales, en cada PC separadamente en el laboratorio real de computación donde los ejercicios estaban siendo efectuados. Todas las máquinas virtuales usadas pueden ser formateadas en un único PC usado para la preparación del ambiente. Después de eso todas las máquinas virtuales formateadas pueden ser copiadas a todos los otros computadores en el salón de clases.

Tabla 4.3 Laboratorios básicos de redes
(Fuente propia)

Laboratorio	Asunto	Máquina Virtual	Software
1	Direccionamiento IP	Rt1	Ifconfig. Netconfig.
2	Ruteamiento Estático	Ws1,Ws2,RT1,RT2 SRV1	Command Route
3	Protocolo RIP	Ws1,RT1,RT2,RT3 Rt4,SRV1	Zebra
4	Protocolo OSPF Un área	WS1,RT1,RT2,RT3 RT4,RT5,SRV1	Zebra
5	Protocolo OSPF Varias áreas	WS1,RT1,RT2,RT3 RT4,RT5,SRV1	Zebra
6	Web Service FTP Service	WS1,RT1,RT2 SRV1	Apache Web ServerProftpd
7	Firewall Conceptos	WS1,WS2,RT1,RT2 SRV1	Ip tables

Otra de las preguntas a ser hechas puede ser: ¿cómo serán organizados los ejercicios de ruteamiento dinámico? Una respuesta puede ser, usando varios sitios de software de enrutamiento. Existen muchas soluciones disponibles y estables de open-source como se explicó anteriormente.

4.2.7 Experiencias en laboratorio virtuales

El próximo paso fue la creación de los ejercicios de laboratorio para el proyecto de laboratorio virtual incluyendo el planteamiento y proyecto de la topología de red para todos los ejercicios considerando las necesidades del curso y la estructura de los ejercicios de los laboratorios. Una topología virtual de red que atiende estos requerimientos es presentada en la Fig. 4.7 La red necesaria para los ejercicios tiene 5 routers (RT1, RT2, RT3, RT4 y RT5), 2 workstations (WS1, WS2) y un servidor (SRV1), un total de 8 máquinas virtuales.

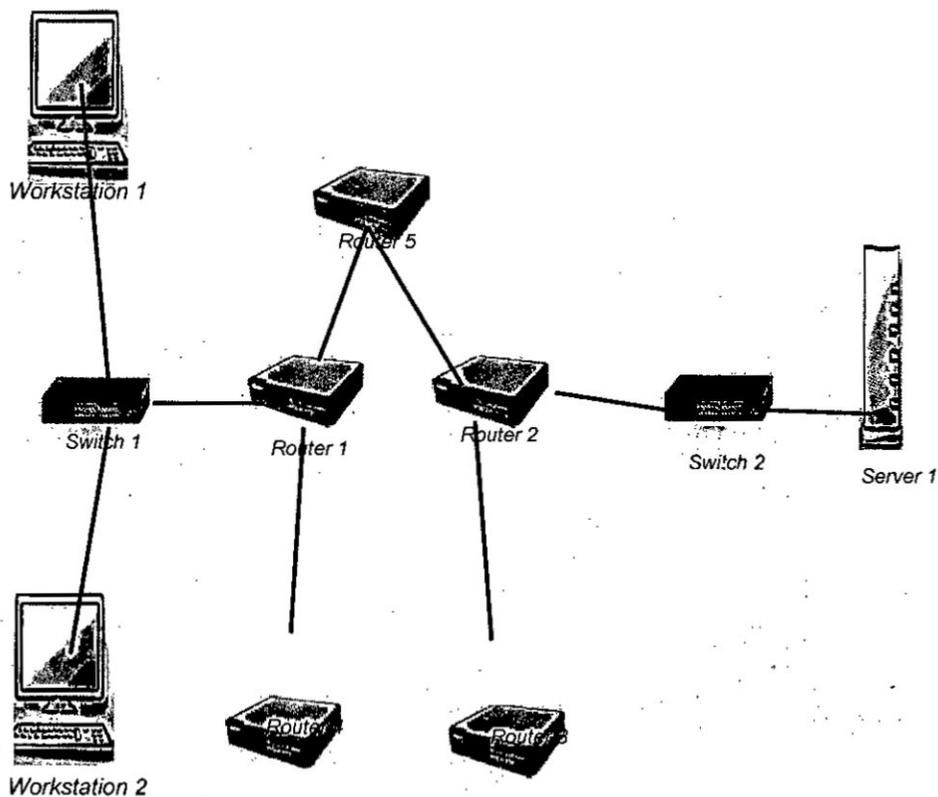
Sin duda que, en nuestro medio, la urgencia de estos mecanismos no es tan evidente si consideramos la condición de alta tecnología en que se sitúan, y en nuestro país todavía no es una necesidad básica tan prioritaria, pero para tener una idea más clara de la aceptación y lo que piensan los potenciales usuarios de esta tecnología, los alumnos, los hemos sometido a un cuestionario para evaluación, que mostró los resultados más adelante indicados.

- Siete ejercicios de laboratorio fueron probados durante el curso de

computadores. Un breve resumen de cada ejercicio incluyendo los tópicos considerados, como los componentes de software requeridos que están incluidos en la tabla 4.3. Puede observarse en esta tabla que el software de enrutamiento Zebra usado en los ejercicios de los protocolos de ruteamiento dinámico RIP Y OSPF tienen similar CLI (Command Line Interface) que los comandos de los routers Cisco.

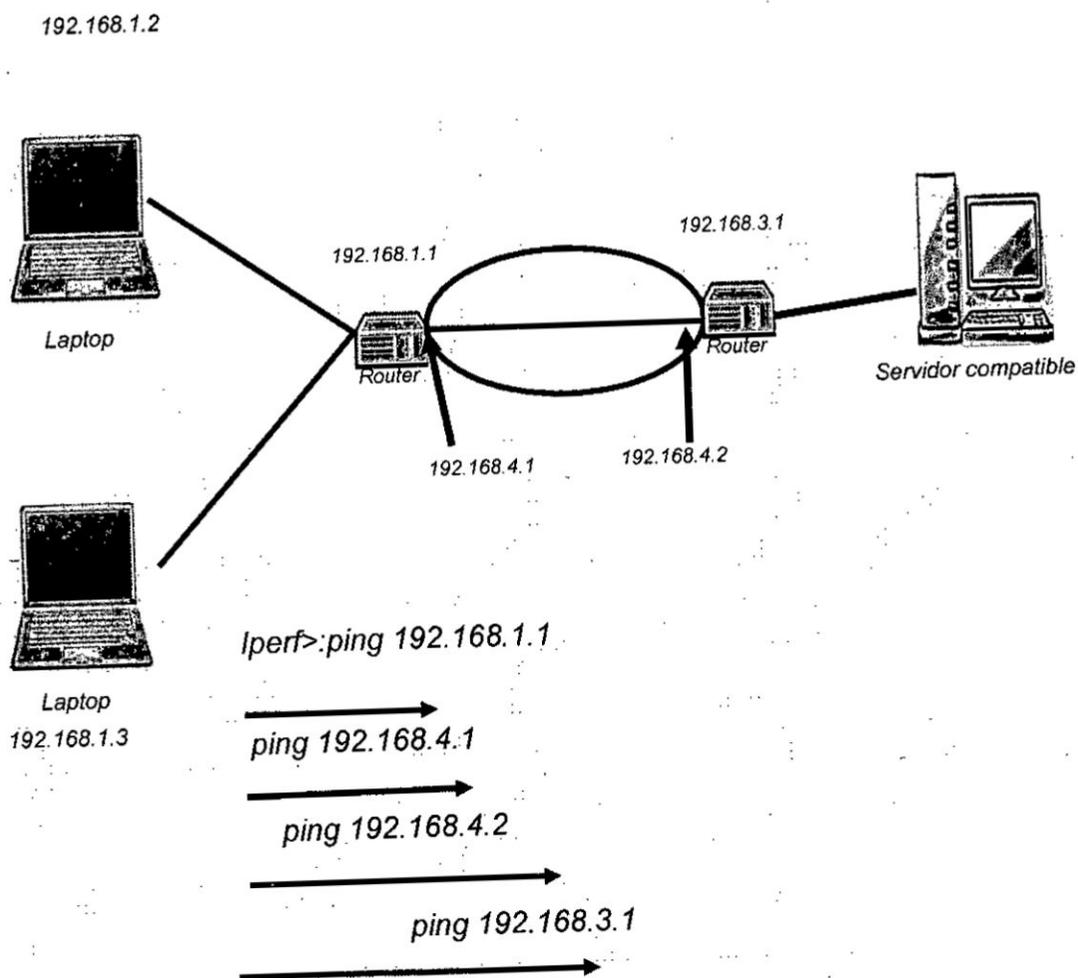
EJERCICIO DE "DIRECCIONAMIENTO IP"

Fig. 4.7 Topología física de partida (inicio)
(Fuente propia)



- 1- Topología física para todos los ejercicios: tabla 3
 - 2- Máquina virtual: Router 1/Router 2/Server
 - 3- Software: Ifconfig/Netconfig
 - 4- Prueba de este ejercicio: IPERF/Traceroute
- IPERF:>Ping (dirección origen) (dirección de destino) (ENTER)
- 5- Topología para este ejercicio:

Fig. 4.8 Topología básica para el ejercicio 1
(Fuente propia)



Ejemplo de configuración de router con software de ruteamiento Zebra (para la topología de Fig. 4.8).

```
Ospfd>enable
Ospfd# configure terminal
Ospfd(config)#router ospf
Ospfd(config-router)#passive-interface eth3
Ospfd(config-router)#net 192.168.11.0/24 area 1
Ospfd(config-router)#net 192.16.14.0/30 area 1
Ospfd(config-router)#net 192.16.15.0/30 area 1
Ospfd(config-router)#net 172.16.16.0/30 area 0
Ospfd(config-router)# area 1 stub no summary
Ospfd(config-router)#exit
Ospfd(config)#interface eth1
Ospfd(config-if)#ip ospf cost 20
Ospfd(config-if)#exit
Ospfd(config)#write
Configuration saved to /usr/local/etc/ospfd.conf
Ospfd(config)#exit
Ospfd#exit
Connection closed by foreign host
```

Conceptos de redes para laboratorios

1.- Direccionamiento IPv4

Uno de los principales parámetros que es necesario configurar en cualquier dispositivo conectado a una red es su dirección IP. La dirección IP es el identificador del dispositivo dentro de una red y debe ser único dentro de los límites de dicha red. El uso, formato, tipos y demás

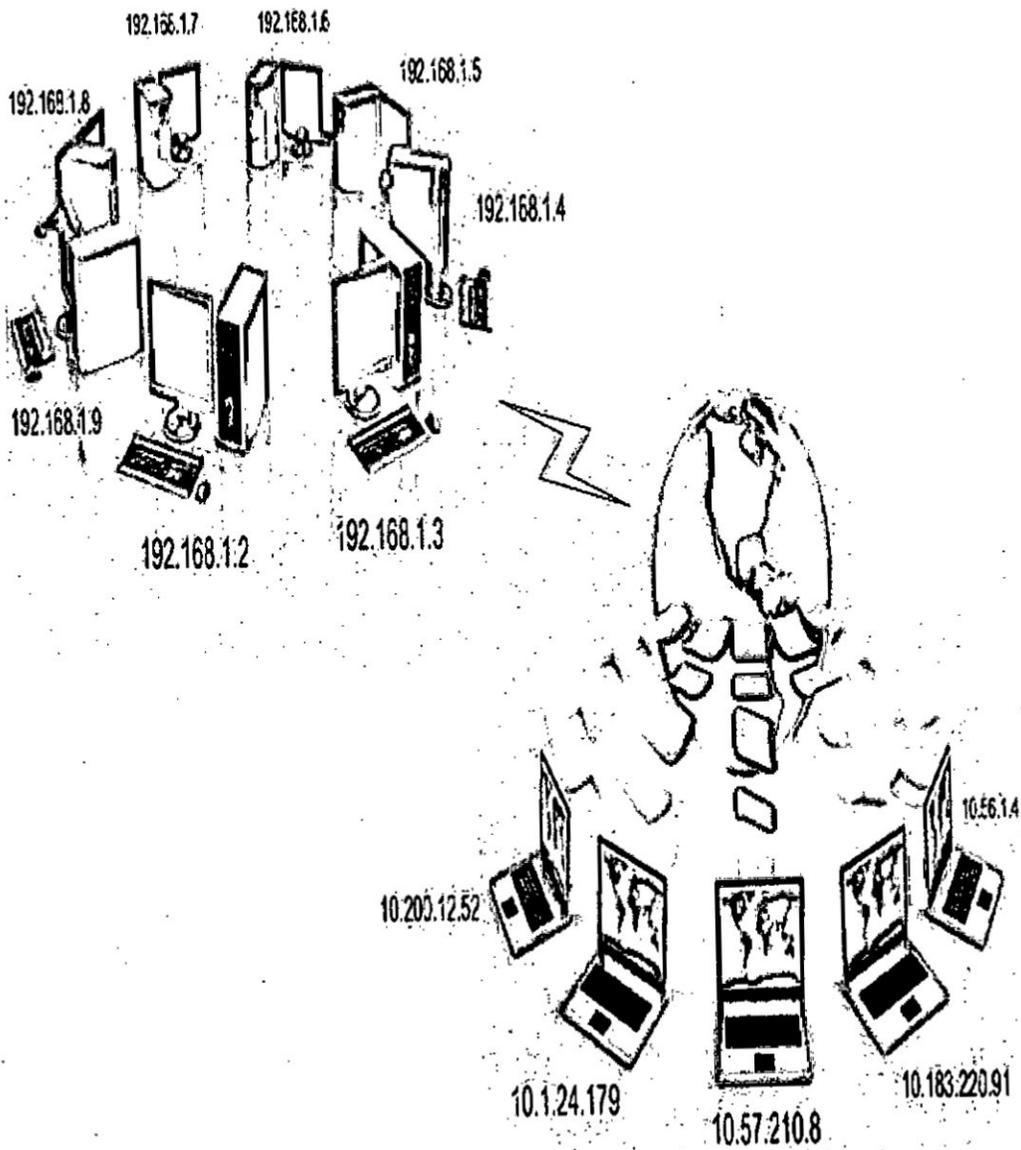
características del direccionamiento IP están incluidos en lo que se conoce como protocolo IP (Internet Protocol).

En la actualidad, cada vez es mayor el número y tipos diferentes de dispositivos que se conectan a redes de datos. Desde ordenadores de sobremesa o portátiles, videoconsolas, tablets, teléfonos (smartphones), televisores, todos ellos necesitan su propia dirección IP.

El agotamiento de las direcciones públicas utilizadas en la versión actual, versión 4 del protocolo IP, ha ocasionado el desarrollo de una nueva versión del protocolo llamada IPv6. Este nuevo protocolo lleva bastantes años desarrollado y ya ha comenzado el periodo de transición al mismo. Sin embargo, dicha transición está siendo muy lenta por lo que se espera que IPv4 se siga utilizando durante un tiempo más.

En este documento vamos a repasar y aclarar algunos conceptos sobre el direccionamiento IPv4 como parte de los ejemplos de aplicación de los laboratorios de Virtualización.

Fig. 4.9 Topología inicial para el ejercicio 2
(Fuente propia)



El direccionamiento IP proporciona un mecanismo para la asignación de identificadores a cada dispositivo conectado a una red. Antes de dar información más técnica, exponemos los principales conceptos:

- ✓ Todos los dispositivos conectados a una red que utilicen los protocolos TCP/IP (en la práctica todas las redes lo hacen) **deben tener una dirección IP** asignada.
- ✓ Una dirección IP es un **número**, que sirve para identificar de forma única a un dispositivo dentro de la red.
- ✓ La asignación de la dirección IP a un dispositivo se puede hacer de dos formas:
 - **Estática.** En este caso, alguien (yo, el administrador de la red, etc.) debe configurar manualmente todos los parámetros de red, incluyendo la dirección IP.
 - **Dinámica.** En este caso, en la red donde se conecta el dispositivo debe haber un equipo que se encargue de asignar de forma automática (sin nuestra intervención) una dirección IP válida.
- ✓ En cuanto a su alcance podemos distinguir dos tipos de direcciones:
 - **Direcciones públicas.** Son las direcciones asignadas a dispositivos conectados a Internet y cuya dirección IP debe ser única para toda la Red. Hay organismos que se encargan de gestionar dichas asignaciones.
 - **Direcciones privadas.** Son direcciones asignadas a dispositivos dentro de una red que no tiene "visibilidad" con Internet. Los dispositivos que tienen asignada una dirección

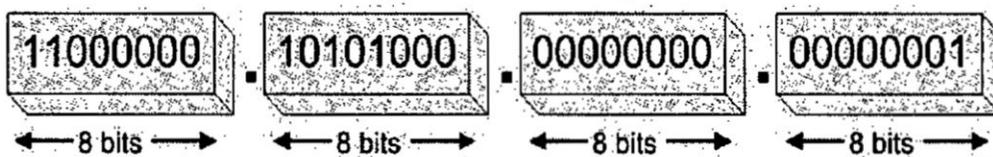
privada no pueden acceder a Internet con su dirección y necesitan un dispositivo que les "preste" una dirección pública. Una vez expuestas las ideas básicas pasemos a desarrollarlas un poco más.

Formato de una dirección IPv4

Como hemos señalado, la dirección IP es un número. En el caso de la versión 4 de IP, es un número formado por 32 dígitos binarios, es decir, 32 "unos" y "ceros":

11000000101010000000000000000000

Todos los sistemas informáticos manejan sus datos en formato binario, por lo que es lógico que la dirección IP sea un número binario. Sin embargo, la representación de un número binario puede no ser muy intuitiva para los que no somos "sistemas informáticos", por tanto, se decidió utilizar un formato un poco más amigable para representar una dirección IP (aunque internamente sigue siendo un número binario). Este sistema de representación de una dirección IPv4 se podría denominar **punto-decimal**. Consiste en dividir el número de 32 bits en cuatro grupos de 8 bits, llamados **octetos**, separando cada grupo por un punto:



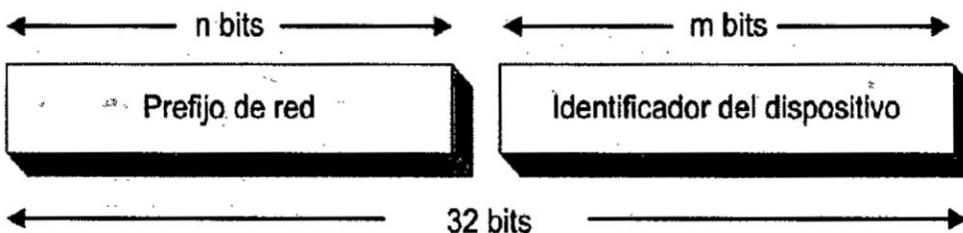
Para luego pasar cada octeto al sistema de numeración decimal, con lo que, para el ejemplo anterior quedaría:



Este formato es bastante más fácil de manejar. En definitiva, para nosotros, **una dirección IPv4 será un identificador numérico** que representamos con cuatro grupos de números entre 0 (00000000) y 255 (11111111) separados con un punto.

Jerarquía

El segundo aspecto importante de las direcciones IP es que tienen un componente jerárquico. Una parte de la dirección IP identifica la red (prefijo de red) y otra parte identifica al dispositivo (host) dentro de esa red.



Como se ve en la figura anterior, de los 32 bits que forman la dirección IP, algunos de ellos forman el prefijo de red y el resto identificarán el dispositivo, de forma que **todos los dispositivos conectados a la**

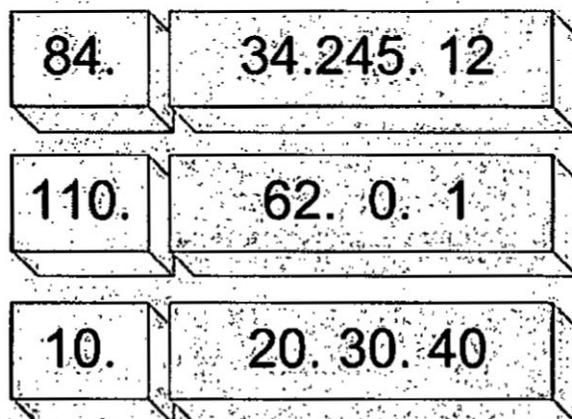
misma red tendrán su n primeros bits (prefijo de red) iguales. El número de bits que forman el prefijo de red y el número de bits que identifican los dispositivos lo establece el administrador de la red para el caso de redes privadas, o el organismo de gestión de direcciones públicas para el caso de direcciones públicas.

Hay valores de n y m que facilitan muchas las cosas. Por ejemplo:

- $n=8$ y $m=24$. A las redes que utilizan los 8 primeros bits para identificarse se denominan redes de **clase A**. Una red de clase A tiene $2^{24} = 16.777.216$ direcciones IP.

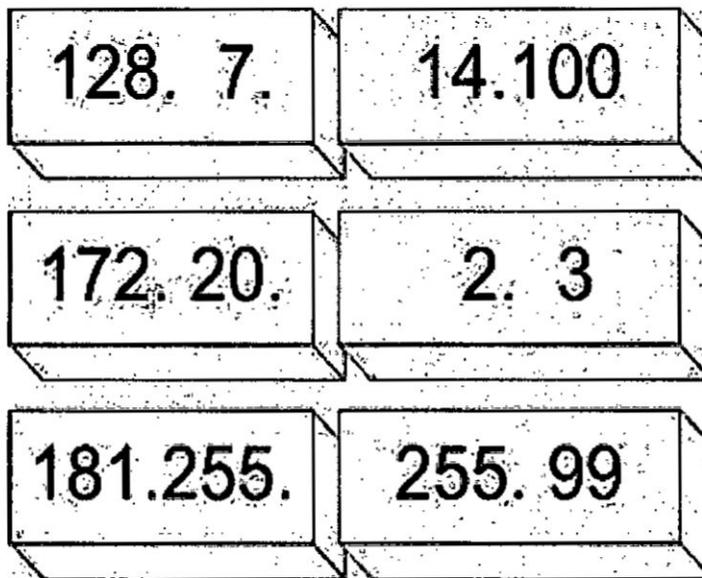
Todas las direcciones IP cuyo primer octeto sea un número entre 1 y 127 son direcciones que pertenecen a una red de clase A. Es decir, puede haber 128 redes de clase A.

Por ejemplo:



- **n=16 y m=16.** A las redes que utilizan los 16 primeros bits para identificarse se denominan redes de **clase B**. Una red de clase B tiene $2^{16} = 65.536$ direcciones IP.

Todas las direcciones IP cuyo primer octeto sea un número entre 128 y 191 son direcciones que pertenecen a una red de clase B. Por ejemplo:



n=24 y m=8. A las redes que utilizan los 24 primeros bits para identificarse se denominan redes de **clase C**. Una red de clase tiene $2^8 = 256$ direcciones IP.

Todas las direcciones IP cuyo primer octeto sea un número entre 192 y 223 son direcciones que pertenecen a una red de clase C.

Por ejemplo:

192.168. 0.	10
200.100. 50.	25
209. 0. 0.	73

Las clases fueron la primera forma de organización de las direcciones IP públicas, aunque, debido al gran crecimiento que experimentó Internet esta organización de las direcciones IP se volvió bastante ineficaz, y en la actualidad sólo se sigue empleando para redes con direccionamiento privado. Para el direccionamiento público el uso de clases se sustituyó por otro mecanismo conocido como CIDR.

Máscara de subred

Debido a que la dirección IP está realmente formada por dos partes y que, además, estas dos partes tienen una longitud variable y complementaria, es necesario utilizar algún método que permita delimitar cada una de dichas partes. Este método se basa en la utilización de un parámetro de red conocido como máscara de subred.

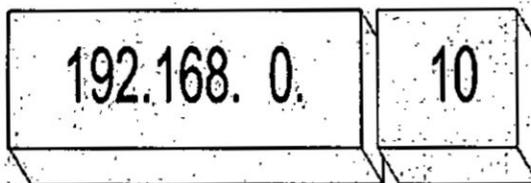
La máscara de subred, es un número binario de 32 bits que se representa en formato decimal. Por tanto, su "aparición" es similar a una dirección IP, sin embargo, **NO ES UNA DIRECCIÓN IP**. La máscara de subred es un número binario que está siempre asociado con una dirección IP y que

nos indica qué parte de esa dirección IP es el prefijo de red, y qué parte de esa dirección IP es el identificador de dispositivo.

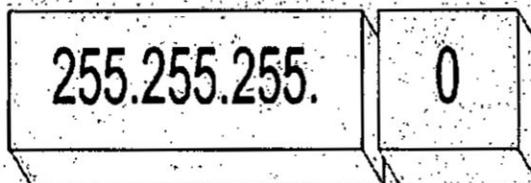
Para ello, todos los bits que se utilicen para definir el prefijo de red se ponen a valor 1 en la máscara, y todos los bits que se utilicen para definir los dispositivos dentro de la red se ponen a valor 0.

La máscara de subred se utiliza especialmente para configurar subredes en redes privadas y para trabajar con rangos CIDR en redes públicas. Su uso en redes privadas sin subredes es bastante simple. Se verá con unos ejemplos.

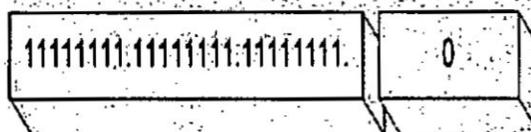
En redes privadas de clase C se utilizan los 24 primeros bits para definir el prefijo de red y los 8 últimos para definir los dispositivos dentro de la red. Por tanto, la máscara de subred para este tipo de redes privadas sin subredes tendrá siempre los primeros 24 bits a "uno".



Dirección IP de clase C

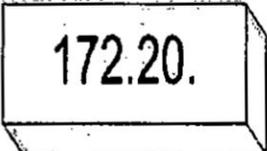
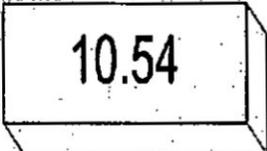


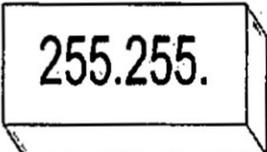
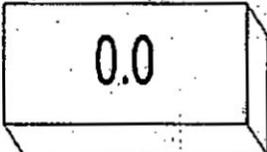
Máscara de subred asociada a una IP de clase C

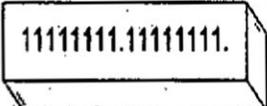
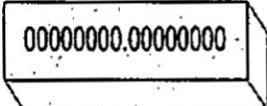


Máscara en binario

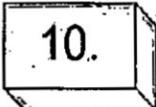
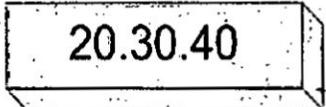
En redes privadas de clase B se utilizan los 16 primeros bits para definir el prefijo de red y los 16 últimos bits para definir los dispositivos dentro de la red. Por tanto, la máscara de subred para este tipo de redes privadas sin subredes tendrá siempre los primeros 16 bits a "uno".

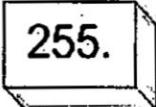
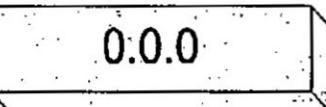
		Dirección IP de clase B
---	---	-------------------------

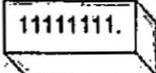
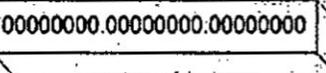
		Máscara de subred asociada a una IP de clase B
--	--	--

		Máscara en binario
---	---	--------------------

En redes privadas de clase A se utilizan los 8 primeros bits para definir el prefijo de red y los 24 últimos bits para definir los dispositivos dentro de la red. Por tanto, la máscara de subred para este tipo de redes privadas sin subredes tendrá siempre los primeros 8 bits a "uno".

		Dirección IP de clase A
---	---	-------------------------

		Máscara de subred asociada a una IP de clase A
---	---	--

		Máscara en binario
---	---	--------------------

Otra forma de expresar la máscara de subred es utilizando la notación CIDR, en la cual se escribe junto a la dirección IP una barra (/) y a continuación el número de bits del prefijo de red. Ejemplos:

192.168.0.10 / 24

172.20.10.54 / 16

10.20.30.40 / 8

Direcciones públicas y privadas

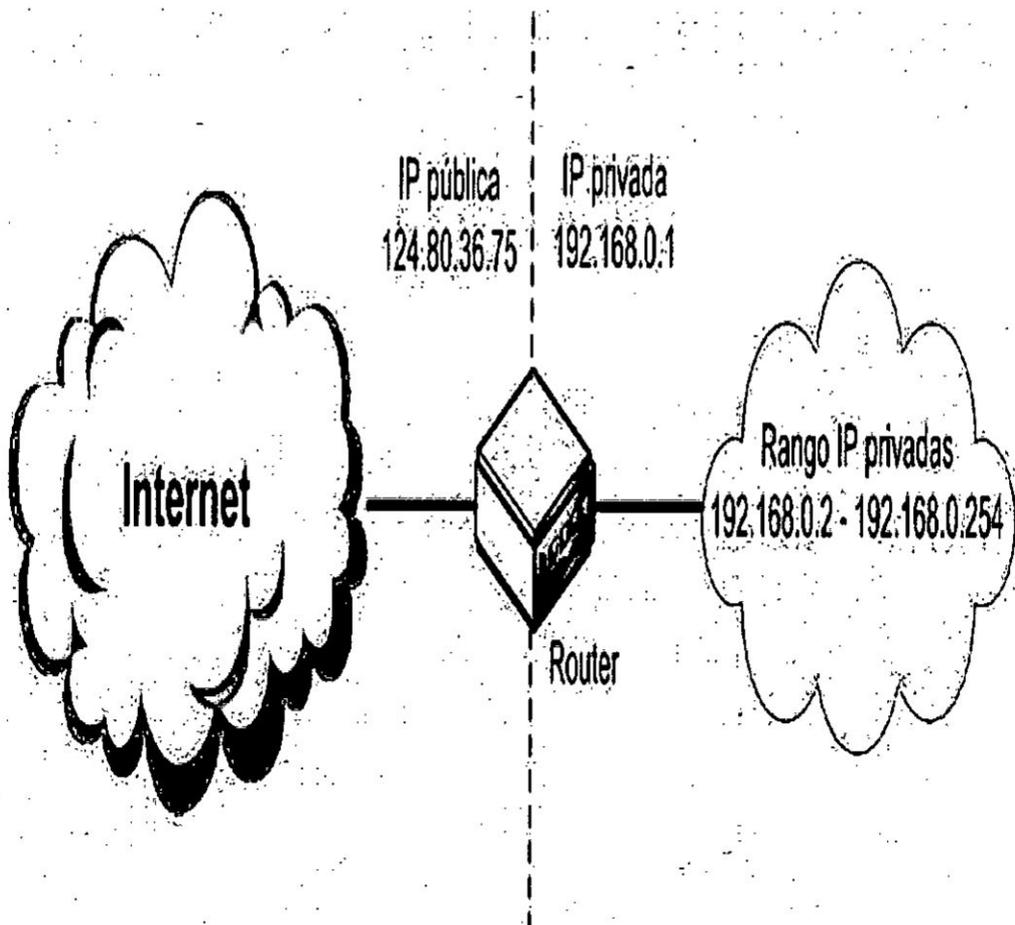
Han cambiado mucho las cosas desde el comienzo de Internet hasta la actualidad. En un primer momento, la idea es que todos los dispositivos conectados a Internet tuvieran su dirección IP pública, aunque se dejaron unos pocos rangos de direcciones reservados para redes privadas que utilizaran los protocolos TCP/IP pero que no estuvieran conectados a Internet.

Pero el gran crecimiento de Internet provocó un cambio en este modelo de direccionamiento de forma que las direcciones IP públicas se reservaron fundamentalmente para routers, servidores y en general, dispositivos que necesitaran "visibilidad directa" en Internet. Mientras que la mayor parte de las redes comenzaron a utilizar direccionamiento privado.

Para que el uso de direccionamiento privado fuera posible en equipos que necesitaban conexión con Internet se desarrolló una técnica llamada

NAPT (Network Address and Port Translation) que normalmente se implementa en el router que conecta la red con Internet. Gracias a esta técnica, todos los dispositivos de una red pueden acceder a Internet utilizando la dirección pública del router. Se podría decir, que la dirección IP pública del router se comparte por todos los dispositivos de la red privada.

Fig. 4.10 Direccionamiento público y privado
(Fuente propia)



El ahorro de direcciones IP públicas que supuso el uso de NAT ha servido para que IPv4 se haya podido utilizar hasta la actualidad.

El criterio de asignación de direcciones IP privadas es libre, es decir, se puede utilizar cualquiera de los rangos de direcciones IP privadas reservadas. Habitualmente, los operadores que proporcionan acceso residencial a Internet utilizan routers configurados con direcciones privadas de clase C, por ejemplo 192.168.0.1, 192.168.1.1... pero se podría utilizar cualquier otro rango de direcciones privadas.

El direccionamiento público está regulado por un organismo internacional llamado **IANA**. Dicho organismo se encarga de asignar los rangos de direcciones IP públicas a los llamados registradores regionales, que a su vez se encargan de la asignación de direcciones IP públicas a los ISP y estos a los clientes finales.

Asignación dinámica de direcciones IP (DHCP)

Como se ha mencionado anteriormente, la asignación de una dirección IP a un dispositivo que está conectado a una red se puede hacer de dos formas: estática o dinámica.

Asignación estática consiste en asignar a un dispositivo una dirección IP manualmente mediante alguna utilidad del sistema operativo. Para llevar a cabo esta asignación es necesario tener información sobre la red en la

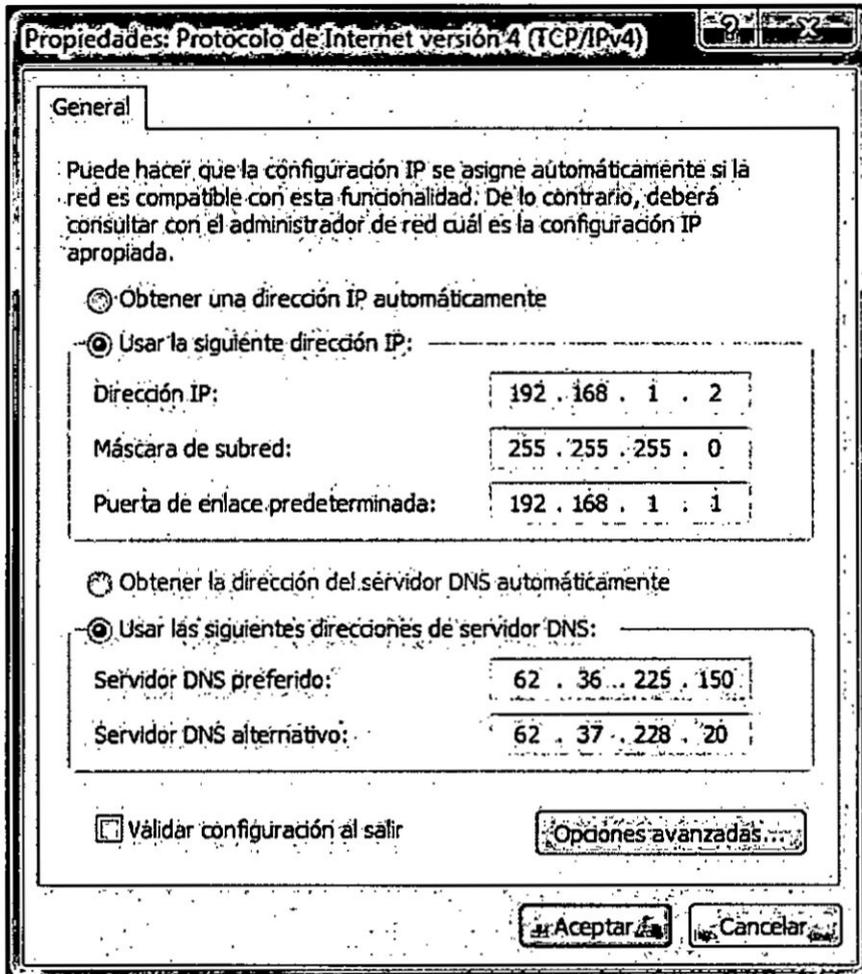
que nos encontramos y tener claro qué dirección IP podemos usar para dicha asignación.

Se muestra en la figura 4.11 la configuración de los parámetros de red en Windows 7.

Para facilitar la tarea de configurar los parámetros de red, existe la opción de utilizar la **asignación dinámica** de dichos parámetros mediante un protocolo conocido como DHCP (Dynamic Host Configuration Protocol).

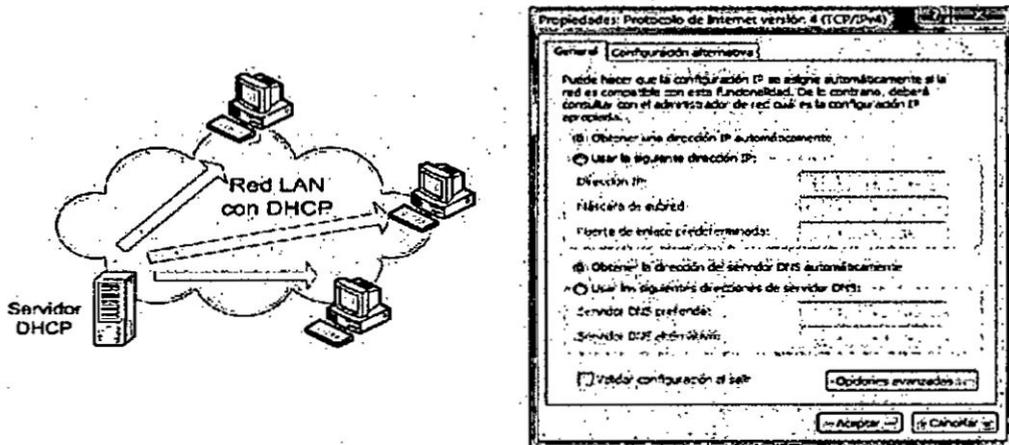
Para utilizar esta opción es necesario que en la red exista un **servidor DHCP**, es decir, un equipo que proporcione una configuración de red válida a cualquier equipo que la solicite.

Fig. 4.11 Ventana de configuración de parámetros en Windows
(Fuente propia)



En redes pequeñas, como por ejemplo en redes residenciales, el propio router de acceso a Internet proporciona la función de servidor DHCP. En este caso, basta con indicar al sistema operativo que los parámetros de red se obtendrán de forma automática.

Fig. 4.12 Configuración de DHCP
(Fuente propia)



Muchos de los dispositivos más utilizados en las redes actualmente, como los teléfonos inteligentes, tablets, consolas, etc, utilizan la opción de asignación automática de los parámetros de red, por ello, normalmente no es necesario hacer ninguna configuración manual de dichos parámetros.

Análisis del rango global de direcciones IPv4

Para finalizar lo relativo a IPv4 se incluye una tabla que representa el rango global de direcciones IPv4, que iría desde la primera dirección 0.0.0.0 a la última 255.255.255.255. En este rango hay $2^{32} = 4.294.967.296$ direcciones IP. En la tabla se indica el uso que tienen los diferentes bloques de direcciones.

Tabla 4.4 Clases de direcciones IP
(Fuente Virtualization for Dummies)

Clases	Primera dirección	Última dirección	Uso	Número de direcciones
A	0.0.0.0	0.255.255.255	Reservado	16.777.216
	1.0.0.0	9.255.255.255	Direcciones públicas	150.994.944
	10.0.0.0	10.255.255.255	Direcciones privadas	16.777.216
	11.0.0.0	126.255.255.255	Direcciones públicas	1.946.157.056
	127.0.0.0	127.255.255.255	Reservada	16.777.216
B	128.0.0.0	169.253.255.255	Direcciones públicas	721.289.216
	169.254.0.0	169.254.255.255	Reservado	65.536
	169.255.0.0	171.15.255.255	Direcciones públicas	17.891.328
	172.16.0.0	172.31.255.255	Direcciones privadas	1.048.576
	172.32.0.0	191.255.255.255	Direcciones públicas	333.447.168
C	192.0.0.0	192.167.255.255	Direcciones públicas	11.010.048
	192.168.0.0	192.168.255.255	Direcciones privadas	65.536
	192.169.0.0	223.255.255.255	Direcciones públicas	525.795.328
D	224.0.0.0	239.255.255.255	Direcciones de multimedios	268.435.456
E	240.0.0.0	255.255.255.255	Direcciones reservadas	268.435.256
			Total públicas	3.706.585.088
			Total privadas	17.891.328
			Total reservadas	570.490.880
			TOTAL	4.294.967.296

2.- Enrutamiento Estático

El enrutamiento es fundamental para cualquier red de datos, ya que transfiere información a través de una internetwork de **origen a destino**.

Los routers son dispositivos que se encargan de transferir paquetes de una red a la siguiente.

Las rutas estáticas son definidas manualmente por el administrador para que el router aprenda sobre una red remota. Las rutas estáticas necesitan pocos recursos del sistema, es recomendable utilizarlas cuando nuestra red esté compuesta por unos cuantos routers o que la red se conecte a internet solamente a través de un único ISP.

Las rutas estáticas son muy comunes y no requieren la misma cantidad de procesamiento y sobrecarga que, como veremos, requieren los protocolos de enrutamiento dinámico.

El comando para configurar una ruta estática es "ip route" y su sintaxis más simple es la siguiente:

```
router(config)#iproute dirección-red mascara-subred {direccion-ip| interfaz-salida}
```

Dónde:

dirección-red: Es la dirección de la red remota que deseamos alcanzar.

máscara-subred: máscara de subred de la red remota.

Dirección-ip: Dirección ip de la interfaz del router vecino (ip del siguiente salto).

Interfaz-salida: Interfaz que utilizará el router para enviar paquetes a la red remota de destino.

Por lo tanto, una ruta estática puede configurarse de 2 maneras:

```
router(config)#iproute direccion-red mascara-subred direccion-ip
```

```
router(config)#iproute direccion-red mascara-subred interfaz-salida.
```

Función del router

El router es una computadora diseñada para fines especiales que desempeña un rol clave en el funcionamiento de cualquier red de datos.

Los routers son responsables principalmente de la interconexión de redes por medio de:

- La determinación del mejor camino para enviar paquetes
- El reenvío de los paquetes a su destino

Los routers reenvían paquetes mediante la detección de redes remotas y el mantenimiento de la información de enrutamiento. El router es la unión o intersección que conecta múltiples redes IP. La principal decisión de envío de los routers se basa en la información de Capa 3, la dirección IP de destino.

La tabla de enrutamiento del router se utiliza para encontrar la mejor coincidencia entre la dirección IP de destino de un paquete y una dirección de red en la tabla de enrutamiento. La tabla de enrutamiento determinará finalmente la interfaz de salida para reenviar el paquete y el

router lo encapsulará en la trama de enlace de datos apropiada para dicha interfaz de salida.

Conexiones del Router

Para las conexiones WAN, los routers Cisco admiten los estándares EIA/TIA-232, EIA/TIA-449, V.35, X.21 y EIA/TIA-530 para conectores seriales, como se muestra. No es importante memorizar estos tipos de conexiones. Sólo debe saber que un router tiene un puerto DB-60 que puede admitir cinco estándares de cableado diferentes. Debido a que admite cinco tipos de cableado diferentes, este puerto a veces se denomina puerto serial cinco en uno. El otro extremo del cable serial cuenta con un conector adecuado para uno de los cinco estándares posibles.

Conexiones al Router

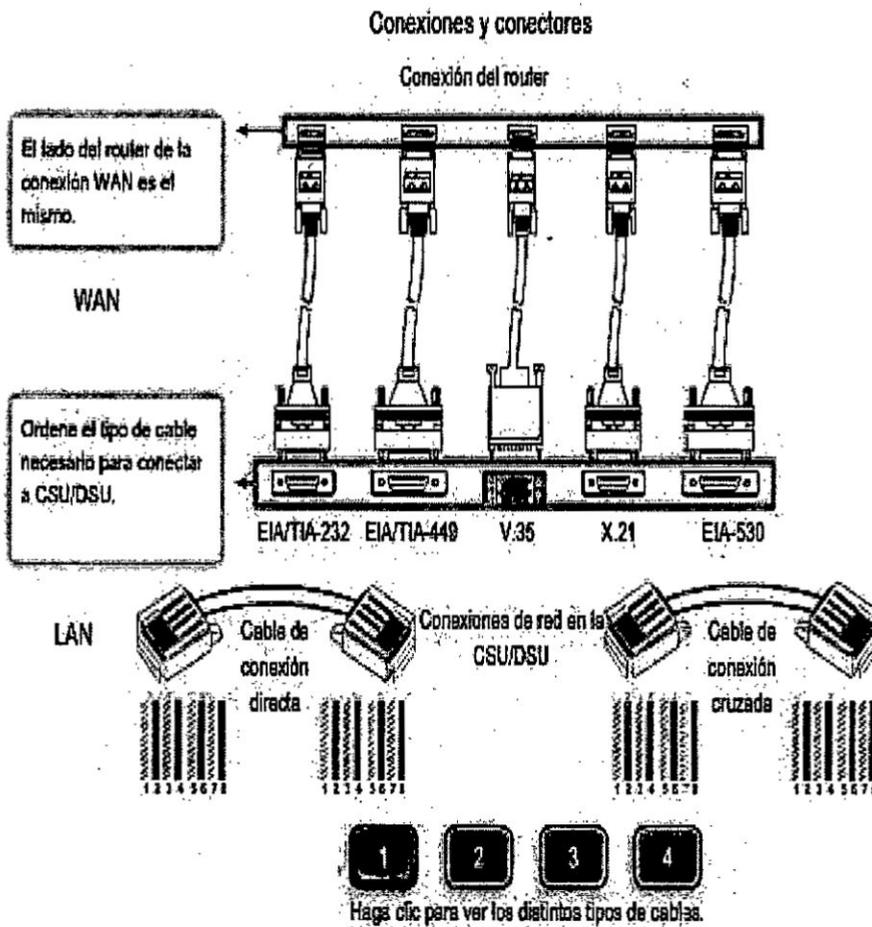
Existen 2 tipos de cables UTP

- 1) Conexión directa (straight)
- 2) Conexión cruzada (crossover) tiene conectado el cable 1 a 3 y 2 a 6.

STREIGHT	
Conectar	Switch con PC
	Router con Switch
	Hub con PC
	Router (consola o coaxial) con PC (Com1)

STREIGHT	
Conectar	Hub con Hub
	Switch con Hub
	PC con PC
	Router con PC o Servidor
	Router con Router

Fig. 4.13 Conexiones Switch – Router – Pc (CISCO)



Lectura de la tabla de enrutamiento

Vea la tabla 4.4 de enrutamiento. Observe que R1 ahora tiene una interfaz FastEthernet 0/0 "conectada directamente" como una red nueva. La interfaz se configuró con la dirección IP 172.16.3.1/24, lo que hace que sea miembro de la red 172.16.3.0/24.

Analice la siguiente línea de resultados de la tabla:

```
C 172.16.3.0 is directly connected, FastEthernet0/0
```

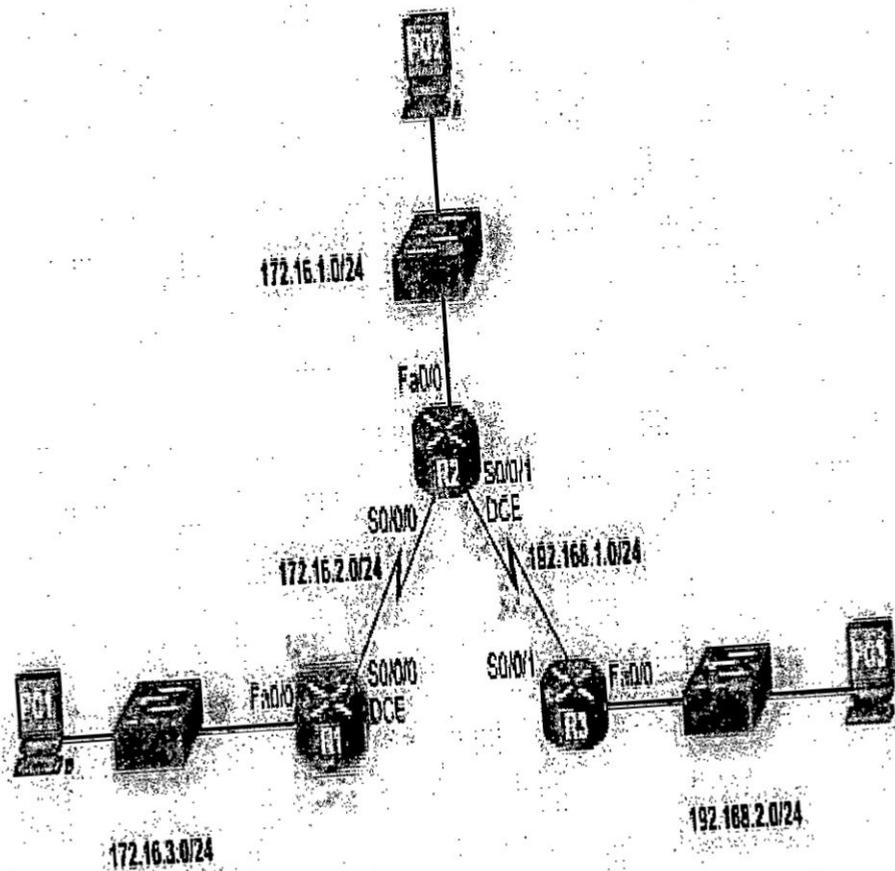
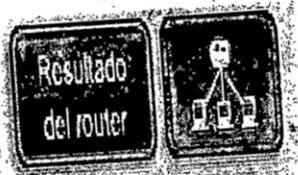
La letra C al comienzo de la ruta indica que es una red conectada directamente. En otras palabras, R1 tiene una interfaz que pertenece a esta red. El significado de C se define en la lista de códigos, en la parte superior de la tabla de enrutamiento.

La máscara de subred /24 para esta ruta se muestra en la línea que se encuentra encima de la ruta real.

```
172.16.0.0/24 es una subred
```

```
C 172.16.3.0 está directamente conectada, FastEthernet0/0
```

Fig. 4.14 Ejercicio de configuración de Router
(Fuente propia)



A continuación, configuraremos la interfaz serial 0/0/0 en el router R1. Esta interfaz se encuentra en la red 172.16.2.0/24 y se le asigna la dirección IP y la máscara de subred de 172.16.2.1/24. El proceso que

utilizamos para la configuración de la interfaz serial 0/0/0 es similar al proceso que utilizamos para configurar la interfaz FastEthernet 0/0.

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 172.16.2.1 255.255.255.0
R1(config-if)#no shutdown
```

Después de haber ingresado estos comandos, el estado de la interfaz serial puede variar según el tipo de conexión WAN. Utilizaremos conexiones punto a punto seriales y dedicadas entre dos routers. La interfaz serial se encontrará en estado up sólo después de que el otro extremo del enlace serial también haya sido configurado correctamente. Podemos mostrar el estado actual de la interfaz serial 0/0/0 utilizando el comando `show interfaces serial 0/0/0`, como se muestra en la Fig. 4.15.

Como puede verse, el enlace todavía está desactivado. El enlace está desactivado porque todavía no hemos configurado ni habilitado el otro extremo del enlace serial.

```
R1#show interfaces serial 0/0/0
Serial0/0/0 is administratively down, line protocol is down.
```

Configuraremos ahora el otro extremo de este enlace: enlace serial 0/0/0 para el router R2.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 172.16.2.2 255.255.255.0
R2(config-if)#no shutdown
```

Si ahora se ejecuta el comando show interfaces serial 0/0/0 en cualquiera de los routers, se comprobará que el enlace aún está up/down.

```
R2#show interfaces serial 0/0/0  
Serial0/0/0 is up, line protocol is down.
```

3.- PROTOCOLO RIP (ENRUTAMIENTO IP)

El protocolo RIP (Protocolo de información de encaminamiento) es un protocolo de puerta de enlace interna o IGP (Internal Gateway Protocol) utilizado por los routers, derivado del protocolo GWINFO de XEROX y que se ha convertido en el protocolo de mayor compatibilidad para las redes Internet, fundamentalmente por su capacidad para inter operar con cualquier equipo de encaminamiento, aun cuando no es considerado el más eficiente.

Existen tres versiones de RIP:

1- RIP v1: No soporta subredes ni CIDR (Encaminamiento Inter-Dominios sin Clases, estándar para la interpretación de direcciones IP). Tampoco incluye ningún mecanismo de autenticación de los mensajes. Actualmente en desuso. Se rige por la RFC 1058.

2.-RIP v2: Soporta subredes, CIDR y VLSM. Soporta autenticación utilizando uno de los siguientes mecanismos: no autenticación, autenticación mediante contraseña, autenticación mediante contraseña codificada mediante MD5 (desarrollado por Ronald Rivest). Se rige por la RFC 1723-2453.

3.- RIPng: RIP para IPv6. Se rige por la RFC 2080. El protocolo RIP, es una implementación directa del encaminamiento vector-distancia. Utiliza UDP para enviar sus mensajes a través del puerto 520. Calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias.

Esta distancia o métrica, la determina usando el número de saltos de router en router hasta alcanzar la red de destino. Para ello usa la métrica informada por su vecino más próximo más uno. La distancia administrativa (grado de conocimiento y confiabilidad) máxima es de 120 (RIP2)

Grupo de Routers A, B, C, D usando la estrategia de vector de distancia basada en métrica de saltos, como base del protocolo de encaminamiento dinámico

RIP 1 no es capaz de detectar rutas circulares, por lo que necesita limitar el tamaño de la red a 15 saltos. Al alcanzar el valor de 16, se considera como infinito y el destino es eliminado de la tabla (destino inalcanzable).

Las métricas solo se actualizan cuando se informan rutas más cortas o bien cuando los destinos indican nuevas rutas. Las rutas tienen un tiempo de vida de 180 segundos. Pasado este tiempo, si no se han recibido mensajes que confirmen que esa ruta está activa, se borra. Estos 180 segundos, corresponden a 6 intercambios de información.

RIP privilegia la ruta más corta independiente de cualquier otra consideración, sin embargo, puede resultar que un camino más largo sea

más conveniente.

RIP Modo de Operación

Cuando RIP se inicia, envía un mensaje a cada uno de sus vecinos (en el puerto bien conocido 520) pidiendo una copia de la tabla de encaminamiento del vecino. Este mensaje es una solicitud (el campo "command" se pone a 1) con "address family" a 0 y "metric" a 16. Los "routers" vecinos devuelven una copia de sus tablas de encaminamiento.

Cuando RIP está en modo activo envía toda o parte de su tabla de encaminamiento a todos los vecinos (por broadcast y/o con enlaces punto a punto). Esto se hace cada 30 segundos. La tabla de encaminamiento se envía como respuesta ("command" vale 2, aunque no haya habido petición).

Cuando RIP descubre que un valor ha cambiado, la difunde por broadcast a los demás "routers".

Cuando RIP recibe una respuesta, el mensaje se valida y la tabla local se actualiza si es necesario. Para mejorar el rendimiento y la fiabilidad, RIP especifica que una vez que un "router" (o host) ha aprendido una ruta de otro, debe guardarla hasta que conozca una mejor (de costo estrictamente menor). Esto evita que los "routers" oscilen entre dos o más rutas de igual costo.

Cuando RIP recibe una petición, distinta de la solicitud de su tabla, se devuelve como respuesta la medida para cada entrada de dicha petición fijada al valor de la tabla local de encaminamiento. Si no existe ruta en la

tabla local, se pone en 16.

Las rutas que RIP aprende de otros "routers" expiran a menos que se vuelvan a difundir en 180 segundos (6 ciclos de broadcast). Cuando una ruta expira, su medida cambia a infinito, la invalidación de la ruta se difunde a los vecinos, y 60 segundos más tarde, se borra de la tabla.

Ventajas de RIP

RIP es más fácil de configurar (comparativamente a otros protocolos). Es un protocolo abierto (admite versiones derivadas aunque no necesariamente compatibles).

Es soportado por la mayoría de los fabricantes.

Desventajas de RIP

Su principal desventaja, consiste en que, para determinar la mejor métrica, únicamente toma en cuenta el número de saltos, descartando otros criterios (AB, congestión, etc.).

RIP tampoco está diseñado para resolver cualquier posible problema de encaminamiento. El RFC 1720 (STD 1) describe estas limitaciones técnicas de RIP como graves y el IETF está evaluando candidatos para reemplazarlo aunque OSPF es el favorito. Este cambio, está dificultado por la amplia expansión de RIP y necesidad de acuerdos adecuados

4.- OSP (OPEN SHORTEST PATH)

OPEN SHORTEST PATH FIRST (OSPF)

El OSPF (Camino más corto abierto) es un protocolo de encaminamiento

jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible. Usa "cost" como su medida de métrica. Además, construye una base de datos enlace-estado idéntica en todos los encaminadores de la zona.

OSPF es probablemente el tipo de protocolo IGP más utilizado en redes grandes. Puede operar con seguridad usando MD5 (Message-Digest Algorithm 5, es un algoritmo de reducción criptográfico de 128 bits) para autenticar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado.

En general se ha planteado y se le supone sucesor natural a RIP. La última versión, la versión tres, es la más reciente. Esta soporta IPv6, así como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado utilizadas.

Algunas de las principales recomendaciones que rigen a este protocolo:

- 1.- RFC - 1583 OSPF v.2.
- 2.- RFC - 1793 Extensiones de OSPF que soportan demandas de circuitos.
- 3.- RFC - 1586 Guía de estudio para usar OSPF sobre Redes Frame Relay.

4.- RFC - 1584 Extensiones de Multienvío o Multidifusión para OSPF.

5.- RFC - 1403 Interacción entre OSPF y BGP

Características generales de OSPF

1.- Es uno de los más importantes IGP (Interior Gateway Protocol).

2.- Recomendado por IETF (Internet Engineering Task Force) para redes IP.

3.- Basado en algoritmo de Estado de Enlaces SPF (Shortest Path First).

4.- Soporta prefijos de longitud variable (VLSM, Variable Length Subnet Mask); prefijos + máscaras.

5.- Encaminamiento jerárquico (AS divididos en áreas, AS = Autonomous System (Sistema Autónomo)).

6.- Encaminamiento multimétrico.

7.- Control sobre la inyección de rutas externas.

8.- Descubrimiento dinámico de routers vecinos.

9.- Adaptación a redes locales.

10.- Soporte para autenticación de mensajes

OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.

Además una red OSPF se puede descomponer en redes más pequeñas.

Posee un área especial llamada área backbone que forma la parte central de la red y donde hay otras áreas conectadas a ella. Las rutas entre diferentes áreas circulan siempre por el backbone, por lo tanto, todas las

áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.

Los encaminadores en el mismo dominio de multidifusión, o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros.

Los encaminadores eligen a un encaminador designado (DR, Designed Router) y un encaminador designado secundario (BDR, Backup DR) que actúan como hubs para reducir el tráfico entre los diferentes encaminadores.

OSPF puede usar tanto multidifusiones como unidifusiones, para enviar paquetes de bienvenida y actualizaciones de enlace-estado. Las direcciones de multidifusiones usadas son 224.0.0.5 y 224.0.0.6. Al contrario que RIP o BGP, OSPF no usa ni TCP ni UDP, sino que usa IP directamente, mediante el IP protocolo 89*.

Protocolo 89: En el campo de datos del protocolo IP bajo la designación protocolo, el número 89 equivale a OSPF.

Las interfaces OSPF pueden encontrarse en uno de siete estados. Los vecinos OSPF progresan a través de estos estados, uno a la vez en el siguiente orden:

Estado Desactivado (Down State): No hay intercambiado de información con ningún vecino.

Estado de Inicialización (Init State): Los encaminadores OSPF envían

paquetes tipo 1, o paquetes Hello, a intervalos regulares con el fin de establecer una relación con los encaminadores vecinos, al recibir el paquete entra a estado de inicialización.

Estado de Dos-Vías (Two-Way): Empleando paquetes Hello, cada enrutador OSPF intenta establecer el estado de dos-vías, o comunicación bidireccional, con cada enrutador vecino en la misma red IP. Entre otros casos, el paquete Hello incluye una lista de los vecinos OSPF conocidos por el origen.

El estado de Dos-Vías es la relación más básica que vecinos OSPF pueden tener, pero la información de encaminamiento no es compartida entre estos.

Paquete OSPF

Este consiste en nueve campos.

- 1.- Versión Number: Identifica la Versión de OSPF.
- 2.- Type: Identifica el tipo de paquete OSPF (Hello, estado de la base de datos, estado y requerimientos del enlace).
- 3.- Packet Length: Especifica el tamaño del paquete incluida la cabecera.
- 4.- Router ID: Identifica el origen de los paquetes.
- 5.- Área ID: Identifica el área de la cual los paquetes pertenecen, todos los paquetes OSPF están ligados a un área.
- 6.- Cheksum: Permite el chequeo de la integridad del paquete.
- 7.- Authentication Type: Contiene el tipo de autenticación de OSPF

(seguridad).

8.-Authentication: Contiene la información de autenticación.

9.-Data: Contiene encapsulada la información de capas superiores.

DESCRIPCIÓN DE LAS OPERACIONES EN OSPF

La secuencia básica de operaciones realizadas por los "routers" OSPF routers es:

- a.- Descubrir vecinos OSPF.
- b.- Elegir el DR (designed router).
- c.- Formar adyacencias (elementos cercanos).
- d.- Sincronizar bases de datos.
- e.- Calcular la tabla de encaminamiento.
- f.- Anunciar los estados del enlace.

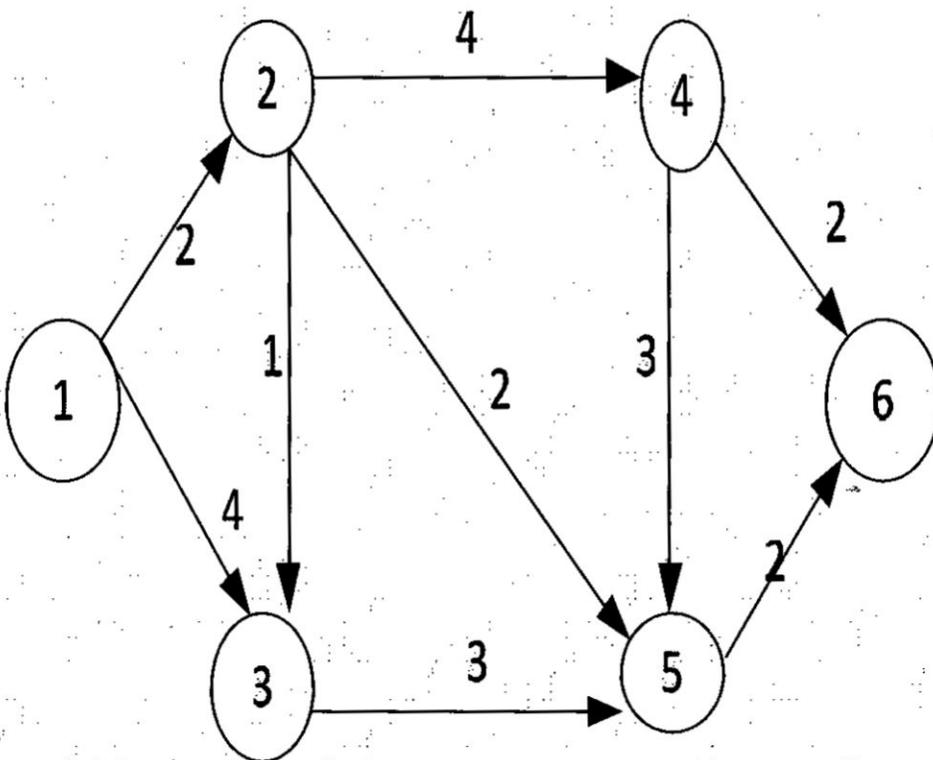
Los "routers" efectuarán todos estos pasos durante su activación, y los repetirán en respuesta a eventos de red. Cada "router" debe ejecutar estos pasos para cada red a la que está conectado, excepto para calcular la tabla de encaminamiento. Cada "router" genera y mantiene una sola tabla de encaminamiento para todas las redes.

SALIDA DEL ALGORITMO DE DIJKSTRA:

- El valor del resultado del algoritmo de DIJKSTRA (la salida).

- Corresponde al valor de la suma de los enlaces más cortos (camino más corto) entre los puntos de interés y no al camino mismo.
- Con una pequeña modificación, podemos obtener la secuencia de los enlaces.
- Valor: $D(1,6)=6$
- Enlaces= $\{1,2,5,6\}$

Fig. 4.15 Algoritmo de DIJKSTRA (Fuente Dummies)

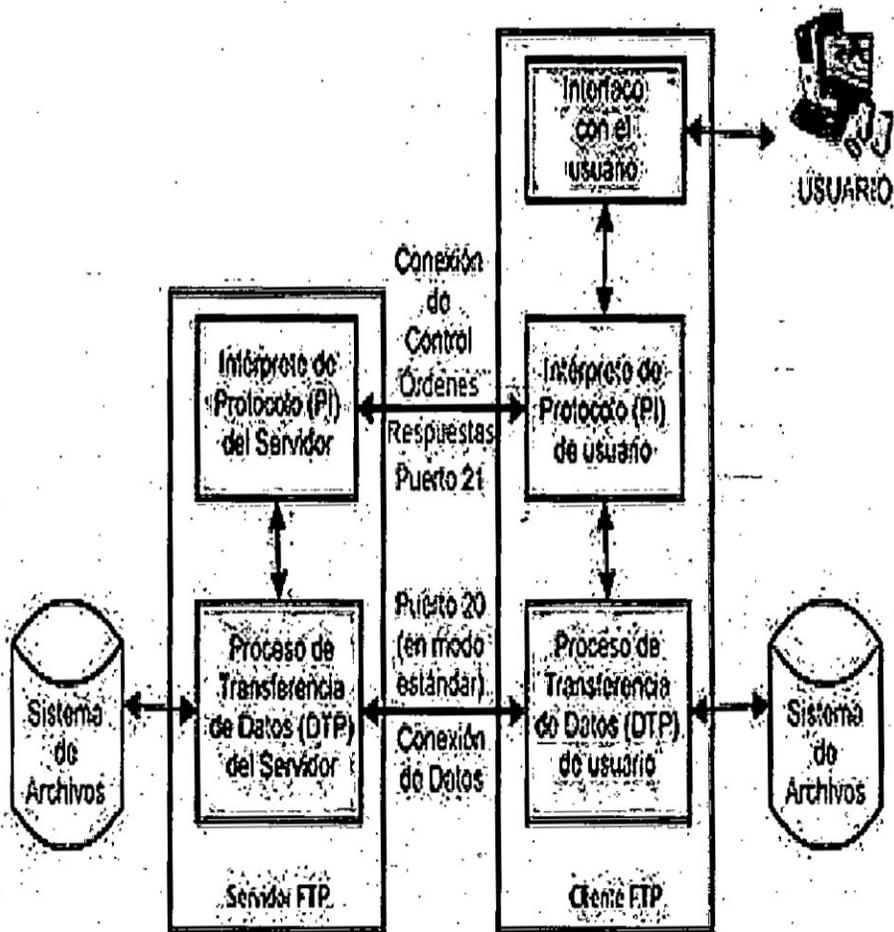


5.- FTP

El protocolo FTP se empezó a utilizar en abril de 1971, publicado como

el RFC 114, antes de que existiera la pila TCP/IP. La estructura general fue establecida en 1973. Fue modificado varias veces, añadiendo nuevos comandos y funcionalidades. Al final se publicó el RFC 959 en octubre de 1985, que es la que se utiliza actualmente.

Fig. 4.16 Modelo FTP
(Fuente *Virtualization for Dummies*)



En el modelo, el intérprete de protocolo (PI) de usuario inicia la conexión de control en el puerto 21. Las órdenes FTP estándar las genera el PI de

usuario y se transmiten al proceso servidor a través de la conexión de control. Las respuestas estándar se envían desde la PI del servidor hasta la PI de usuario por la conexión de control como respuesta a las órdenes.

Estas órdenes FTP especifican parámetros para la conexión de datos (puerto de datos, modo de transferencia, tipo de representación y estructura) y la naturaleza de la operación sobre el sistema de archivos (almacenar, recuperar, añadir, borrar, etc.). El proceso de transferencia de datos (DTP) de usuario u otro proceso en su lugar, debe esperar a que el servidor inicie la conexión al puerto de datos especificado (puerto 20 en modo activo o estándar) y transferir los datos en función de los parámetros que se hayan especificado.

Vemos también en el diagrama que la comunicación entre cliente y servidor es independiente del sistema de archivos utilizado en cada computadora, de manera que no importa que sus sistemas operativos sean distintos, porque las entidades que se comunican entre sí son los PI y los DTP, que usan el mismo protocolo estandarizado: el FTP.

También hay que destacar que la conexión de datos es bidireccional, es decir, se puede usar simultáneamente para enviar y para recibir, y no tiene por qué existir todo el tiempo que dura la conexión FTP. Pero tenía en sus comienzos un problema, y era la localización de los servidores en la red. Es decir, el usuario que quería descargar algún archivo mediante trump debía conocer en qué máquina estaba ubicado. La única

herramienta de búsqueda de información que existía era Gopher, con todas sus limitaciones.

Primer buscador de información

Gopher significa 'lanzarse sobre' la información. Es un servicio cuyo objetivo es la localización de archivos a partir de su título. Consiste en un conjunto de menús de recursos ubicados en diferentes máquinas que están intercomunicadas. Cada máquina sirve un área de información, pero su organización interna permite que todas ellas funcionen como si se tratase de una sola máquina. El usuario navega a través de estos menús hasta localizar la información buscada, y desconoce exactamente de qué máquina está descargando dicha información. Con la llegada de Internet, los potentes motores de búsqueda dejaron el servicio Gopher, y la localización de los servidores FTP dejó de ser un problema. En la actualidad, cuando el usuario se descarga un archivo a partir de un enlace de una página web no llega ni a saber que lo está haciendo desde un servidor FTP. El servicio FTP ha evolucionado a lo largo del tiempo y hoy día es muy utilizado en Internet, en redes corporativas, Intranets, etc. Soportado por cualquier sistema operativo, existe gran cantidad de software basado en el protocolo FTP.

Servidor FTP

Un servidor FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet (aunque puede estar

conectado a otros tipos de redes, LAN, MAN, etc.). Su función es permitir el intercambio de datos entre diferentes servidores/ordenadores.

Por lo general, los programas servidores FTP no suelen encontrarse en los ordenadores personales, por lo que un usuario normalmente utilizará el FTP para conectarse remotamente a uno y así intercambiar información con él.

Las aplicaciones más comunes de los servidores FTP suelen ser el alojamiento web, en el que sus clientes utilizan el servicio para subir sus páginas web y sus archivos correspondientes; o como servidor de backup (copia de seguridad) de los archivos importantes que pueda tener una empresa. Para ello, existen protocolos de comunicación FTP para que los datos se transmitan cifrados, como el SFTP (Secure File Transfer Protocol).

Ciente FTP

Cuando un navegador no está equipado con la función FTP, o si se quiere cargar archivos en un ordenador remoto, se necesitará utilizar un programa cliente FTP. Un cliente FTP es un programa que se instala en el ordenador del usuario, y que emplea el protocolo FTP para conectarse a un servidor FTP y transferir archivos, ya sea para descargarlos o para subirlos.

Para utilizar un cliente FTP, se necesita conocer el nombre del archivo, el

ordenador en que reside (servidor, en el caso de descarga de archivos), el ordenador al que se quiere transferir el archivo (en caso de querer subirlo nosotros al servidor), y la carpeta en la que se encuentra.

Algunos clientes de FTP básicos en modo consola vienen integrados en los clientes operativos incluidos el Windows, DOS, GNU/Linux y Unix. Sin embargo, hay disponibles clientes con opciones añadidas e interfaz gráfica. Aunque muchos navegadores tienen ya integrado FTP, es más confiable a la hora de conectarse con servidores FTP no anónimos utilizar un programa cliente.

Acceso anónimo

Los servidores FTP anónimos ofrecen sus servicios libremente a todos los usuarios, permiten acceder a sus archivos sin necesidad de tener un 'USER ID' o una cuenta de usuario. Es la manera más cómoda fuera del servicio web de permitir que todo el mundo tenga acceso a cierta información sin que para ello el administrador de un sistema tenga que crear una cuenta para cada usuario.

Si un servidor posee servicio 'FTP anonymous' solamente con teclear la palabra «anonymous», cuando pregunte por tu usuario tendrás acceso a ese sistema. No se necesita ninguna contraseña preestablecida, aunque tendrás que introducir una sólo para ese momento, normalmente se suele utilizar la dirección de correo electrónico propia.

Solamente con eso se consigue acceso a los archivos del FTP, aunque con menos privilegios que un usuario normal. Normalmente solo podrás leer y copiar los archivos que sean públicos, así indicados por el administrador del servidor al que nos queramos conectar.

Normalmente, se utiliza un servidor FTP anónimo para depositar grandes archivos que no tienen utilidad si no son transferidos a la máquina del usuario, como por ejemplo programas, y se reservan los servidores de páginas web (HTTP) para almacenar información textual destinada a la lectura en línea.

Acceso de usuario

Si se desea tener privilegios de acceso a cualquier parte del sistema de archivos del servidor FTP, de modificación de archivos existentes, y de posibilidad de subir nuestros propios archivos, generalmente se suele realizar mediante una cuenta de usuario. En el servidor se guarda la información de las distintas cuentas de usuario que pueden acceder a él, de manera que para iniciar una sesión FTP debemos introducir una autenticación (login) y una contraseña (password) que nos identifica unívocamente

Cliente FTP basado en Web

Un «cliente FTP basado en Web» no es más que un cliente FTP al cual podemos acceder a través de nuestro navegador web sin necesidad de tener otra aplicación para ello. El usuario se conecta mediante HTTP a un

servidor web, y el servidor web se conecta mediante FTP al servidor de archivos. El servidor web actúa de intermediario haciendo pasar la información desde el servidor FTP en los puertos 20 y 21 hacia el puerto 80 HTTP que ve el usuario.

Siempre hay momentos en que nos encontramos fuera de casa, no llevamos el ordenador portátil encima y necesitamos realizar alguna tarea urgente desde un ordenador de acceso público, de un amigo, del trabajo, la universidad, etc. Lo más común es que no estén instaladas las aplicaciones que necesitamos y en muchos casos hasta carecemos de los permisos necesarios para realizar su instalación. Otras veces estamos detrás de un proxy o cortafuegos que no nos permite acceder a servidores FTP externos.

Al disponer de un cliente FTP basado en Web podemos acceder al servidor FTP remoto como si estuviéramos realizando cualquier otro tipo de navegación web. A través de un cliente FTP basado en Web podrás, crear, copiar, renombrar y eliminar archivos y directorios. Cambiar permisos, editar, ver, subir y descargar archivos, así como cualquier otra función del protocolo FTP que el servidor FTP remoto permita.

Acceso de invitado

El acceso sin restricciones al servidor que proporcionan las cuentas de usuario implica problemas de seguridad, lo que ha dado lugar a un tercer tipo de acceso FTP denominado invitado (guest), que se puede

contemplar como una mezcla de los dos anteriores.

La idea de este mecanismo es la siguiente: se trata de permitir que cada usuario conecte a la máquina mediante su login y su password, pero evitando que tenga acceso a partes del sistema de archivos que no necesita para realizar su trabajo, de esta forma accederá a un entorno restringido, algo muy similar a lo que sucede en los accesos anónimos, pero con más privilegios.

Ejemplos de Clientes FTPs

Entre los varios clientes FTP que existen, se pueden mencionar los siguientes:

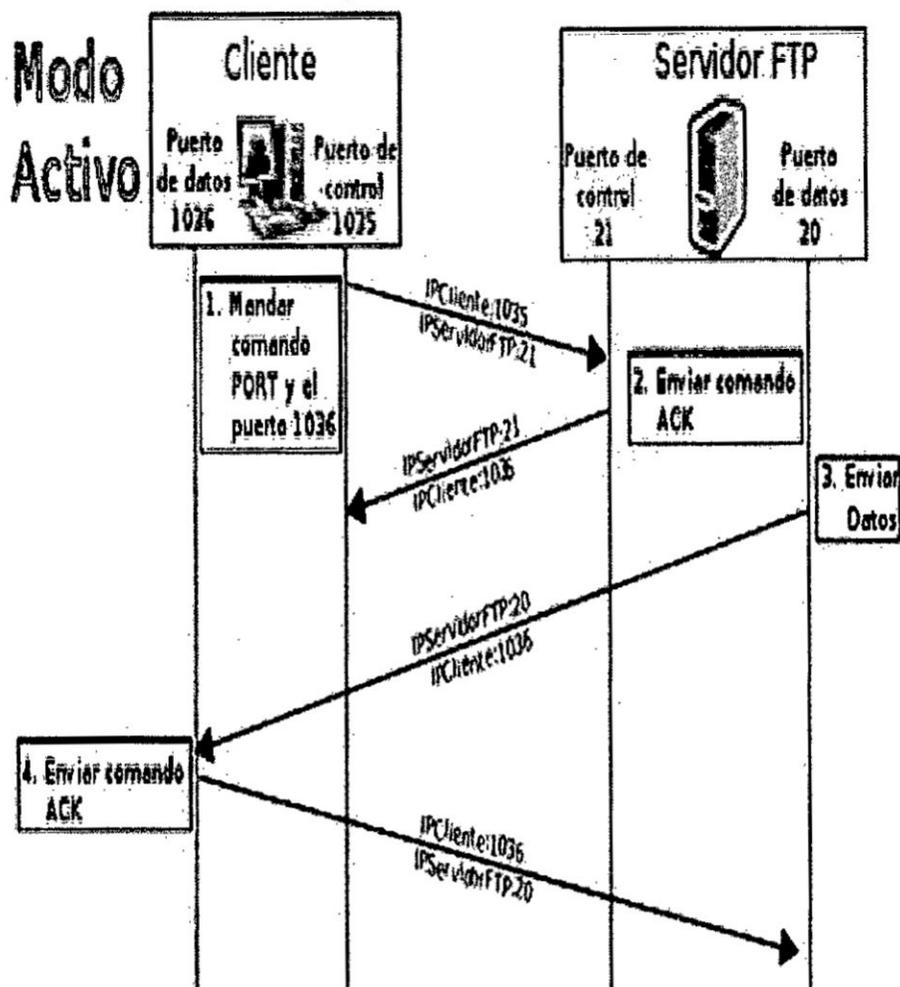
- Free FTP Upload Manager
- F->IT
- net2ftp
- Web FTP.co.uk
- Web-Ftp
- Jambai FTP
- ftp4net
- PHP FTP Client
- Asuk PHP FTP
- Weeble File Manager
- FileZilla

Modo de conexión del cliente FTP

FTP admite dos modos de conexión del cliente. Estos modos se denominan activo (o Estándar, o PORT, debido a que el cliente envía comandos tipo PORT al servidor por el canal de control al establecer la conexión) y pasivo (o PASV, porque en este caso envía comandos tipo PASV). Tanto en el modo Activo como en el modo Pasivo, el cliente establece una conexión con el servidor mediante el puerto 21, que establece el canal de control.

Fig. 4.17 Modo activo de conexión

(Fuente Virtualization for Dummies)



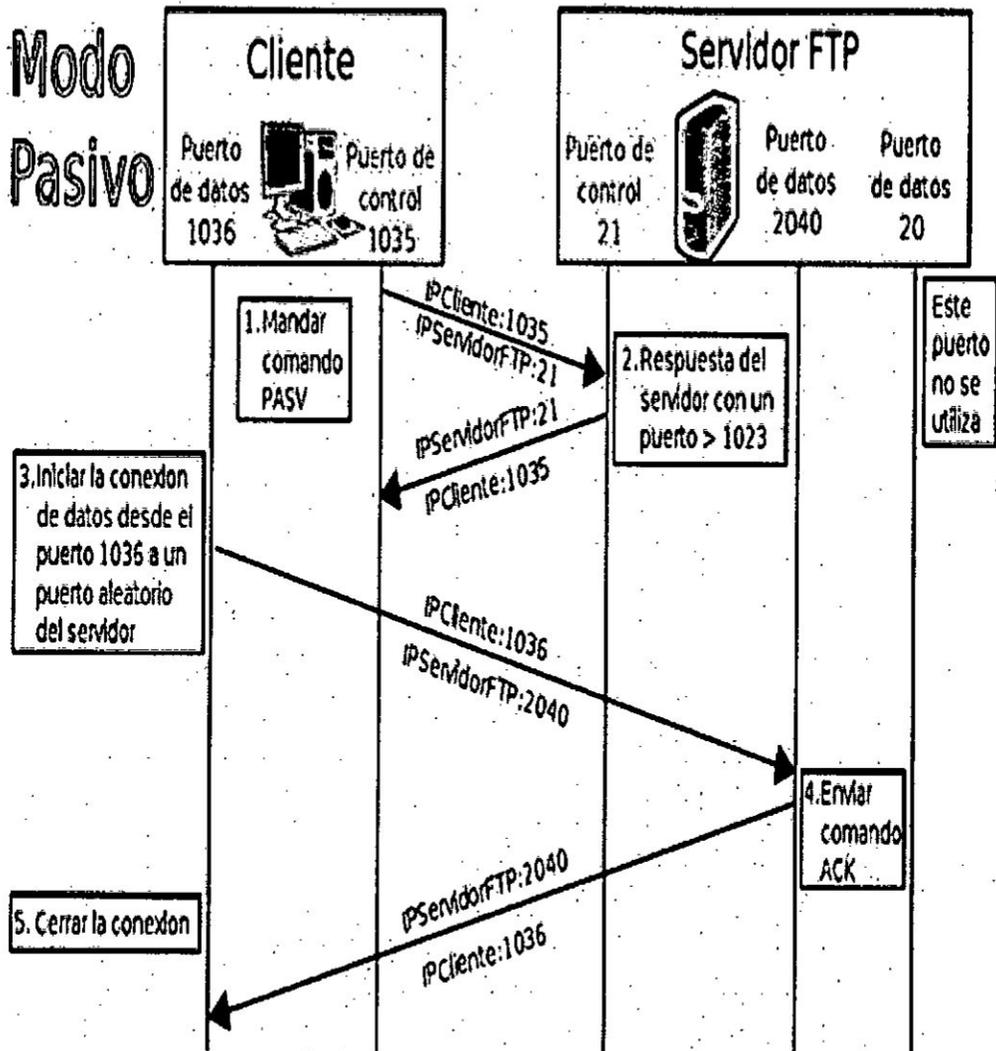
Modo activo.

En modo Activo, el servidor siempre crea el canal de datos en su puerto 20, mientras que en el lado del cliente el canal de datos se asocia a un puerto aleatorio mayor que el 1024. Para ello, el cliente manda un comando PORT al servidor por el canal de control indicándole ese número de puerto, de manera que el servidor pueda abrirle una conexión de datos

por donde se transferirán los archivos y los listados, en el puerto especificado.

Lo anterior tiene un grave problema de seguridad, y es que la máquina cliente debe estar dispuesta a aceptar cualquier conexión de entrada en un puerto superior al 1024, con los problemas que ello implica si tenemos el equipo conectado a una red insegura como Internet. De hecho, los cortafuegos que se instalen en el equipo para evitar ataques seguramente rechazarán esas conexiones aleatorias. Para solucionar esto se desarrolló el modo pasivo.

Fig. 4.18 Modo pasivo de conexión
(Fuente Virtualization for Dummies)



Modo pasivo.

Cuando el cliente envía un comando PASV sobre el canal de control, el servidor FTP le indica por el canal de control, el puerto (mayor a 1024 del servidor). Al que debe conectarse el cliente. El cliente inicia una conexión

desde el puerto siguiente al puerto de control hacia el puerto del servidor especificado anteriormente.

Antes de cada nueva transferencia tanto en el modo Activo como en el Pasivo, el cliente debe enviar otra vez un comando de control (PORT o PASV, según el modo en el que haya conectado), y el servidor recibirá esa conexión de datos en un nuevo puerto (aleatorio si es en modo pasivo o por el puerto 20 si es en modo activo).

Tipos de transferencia de archivos en FTP

En el protocolo FTP existen 2 tipos de transferencia en ASCII y en binarios. Es importante conocer cómo debemos transportar un archivo a lo largo de la red, si no utilizamos las opciones adecuadas podemos destruir la información del archivo. Por eso, al ejecutar la aplicación FTP, debemos acordarnos de utilizar uno de estos comandos (o poner la correspondiente opción en un programa con interfaz gráfica):

- **Tipo ASCII**

Adecuado para transferir archivos que solo contengan caracteres imprimibles (archivos ASCII, no archivos resultantes de un procesador de texto), por ejemplo, páginas HTML, pero no las imágenes que puedan contener. Se transforman algunos símbolos de control para mantenerlos compatibles entre diferentes sistemas, por ejemplo, si el archivo está alojado sobre un servidor `inux`, el salto de línea para los archivos de texto es `"\n"` (byte 10 en decimal). Si el cliente es un sistema Mac, el salto

de línea es “\r” (byte 13 en decimal), este modo cambia estos símbolos de control para que el archivo sea legible en ambos lados, al igual que si se envía a un sistema Windows, el salto de línea es “\r\n” (dos bytes, 13 y 10). Si se usa este modo en archivos que no son de texto plano, en el caso de intercambiarse entre diferentes sistemas, ese archivo quedará corrupto.

- **Tipo Binario**

Este tipo es usado cuando se trata de archivos comprimidos, ejecutables para PC, imágenes, archivos de audio, entre otros.

Ejemplos de cómo transferir algunos tipos de archivo dependiendo de su extensión:

6.- Cortafuegos

Es un medio de protección que se utilizan en sistemas computarizados con la finalidad de evitar el acceso a las mismas de usuarios no autorizados. En la figura siguiente se muestra el diseño de un cortafuego entre dos redes, una de área local y otra de área extendida. Con este tipo de diseño, se evita que la transferencia de datos entre los usuarios de ambas redes pueda realizarse con la seguridad que no son portadoras de virus.

Un cortafuego (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar los cortafuegos a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuego correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Historia del cortafuego

El término firewall/fireblock significaba originalmente una pared para

confinar un incendio o riesgo potencial de incendio en un edificio. Más adelante se usa para referirse a las estructuras similares, como la hoja de metal que separa el compartimiento del motor de un vehículo o una aeronave de la cabina. La tecnología de los cortafuegos surgió a finales de 1980, cuando Internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad. Los predecesores de los cortafuegos para la seguridad de la red fueron los routers utilizados a finales de 1980, que mantenían a las redes separadas unas de otras. La visión de Internet como una comunidad relativamente pequeña de usuarios con máquinas compatibles, que valoraba la predisposición para el intercambio y la colaboración, terminó con una serie de importantes violaciones de seguridad de Internet que se produjo a finales de los 80.

- Clifford Stoll, que descubrió la forma de manipular el sistema de espionaje alemán.
- Bill Cheswick, cuando en 1992 instaló una cárcel simple electrónica para observar a un atacante.
- En 1988, un empleado del Centro de Investigación Ames de la NASA, en California, envió una nota por correo electrónico a sus colegas que decía:

"Estamos bajo el ataque de un virus de Internet! Ha llegado a Berkeley, UC San Diego, Lawrence Livermore, Stanford y la NASA Ames".

- El Gusano Morris, que se extendió a través de múltiples vulnerabilidades en las máquinas de la época. Aunque no era malicioso, el gusano Morris fue el primer ataque a gran escala sobre la seguridad en Internet; la red no esperaba ni estaba preparada para hacer frente a su ataque.

Primera generación – cortafuegos de red: filtrado de paquetes El primer documento publicado para la tecnología firewall data de 1988, cuando el equipo de ingenieros Digital Equipment Corporation (DEC) desarrolló los sistemas de filtro conocidos como cortafuegos de filtrado de paquetes. Este sistema, bastante básico, fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad de Internet. En AT&T Bell, Bill Cheswick y Steve Bellovin continuaban sus investigaciones en el filtrado de paquetes y desarrollaron un modelo de trabajo para su propia empresa, con base en su arquitectura original de la primera generación.

El filtrado de paquetes actúa mediante la inspección de los paquetes (que representan la unidad básica de transferencia de datos entre ordenadores en Internet). Si un paquete coincide con el conjunto de reglas del filtro, el paquete se reducirá (descarte silencioso) o será rechazado (desprendiéndose de él y enviando una respuesta de error al emisor). Este tipo de filtrado de paquetes no presta atención a si el paquete es parte de una secuencia existente de tráfico. En su lugar, se filtra cada

paquete basándose únicamente en la información contenida en el paquete en sí (por lo general utiliza una combinación del emisor del paquete y la dirección de destino, su protocolo, y, en el tráfico TCP y UDP, el número de puerto).⁵ Los protocolos TCP y UDP comprenden la mayor parte de comunicación a través de Internet, utilizando por convención puertos bien conocidos para determinados tipos de tráfico, por lo que un filtro de paquetes puede distinguir entre ambos tipos de tráfico (ya sean navegación web, impresión remota, envío y recepción de correo electrónico transferencia de archivos...); a menos que las máquinas a cada lado del filtro de paquetes estén a la vez utilizando los mismos puertos no estándar.

El filtrado de paquetes llevado a cabo por un cortafuego actúa en las tres primeras capas del modelo de referencia OSI, lo que significa que todo el trabajo lo realiza entre la red y las capas físicas. Cuando el emisor origina un paquete y es filtrado por el cortafuego, esta última comprueba las reglas de filtrado de paquetes que lleva configuradas, aceptando o rechazando el paquete en consecuencia. Cuando el paquete pasa a través de cortafuegos, éste filtra el paquete mediante un protocolo y un número de puerto base (GSS). Por ejemplo, si existe una norma en el cortafuego para bloquear el acceso telnet, bloqueará el protocolo TCP para el número de puerto 23.

Segunda generación – Cortafuego de estado

Durante 1989 y 1990, tres investigadores de los laboratorios AT&T Bell,

Dave Presetto, Janardan Sharma, y Nigam Kshitij, desarrollaron la segunda generación de servidores de seguridad. Esta segunda generación de cortafuegos tiene en cuenta, además, la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el cortafuego, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

Tercera generación — Cortafuego de aplicación

Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un cortafuego de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

Un cortafuego de aplicación es mucho más seguro y fiable cuando se compara con un cortafuego de filtrado de paquetes, ya que repercute en las siete capas del modelo de referencia OSI. En esencia es similar a un cortafuego de filtrado de paquetes, con la diferencia de que también podemos filtrar el contenido del paquete. El mejor ejemplo de cortafuegos

de aplicación es ISA (Internet Security and Acceleration).

Un cortafuego de aplicación puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP y TFTP (GSS). Por ejemplo, si una organización quiere bloquear toda la información relacionada con una palabra en concreto, puede habilitarse el filtrado de contenido para bloquear esa palabra en particular. No obstante, los cortafuegos de aplicación resultan más lentos que los de estado.

Acontecimientos posteriores

En 1992, Bob Braden y DeSchon Annette, de la Universidad del Sur de California (USC), dan forma al concepto de cortafuegos. Su producto, conocido como "Visas", fue el primer sistema con una interfaz gráfica con colores e iconos, fácilmente implementable y compatible con sistemas operativos como Windows de Microsoft o MacOS de Apple. En 1994, una compañía israelí llamada Check Point Software Technologies lo patentó como software denominándolo FireWall.

La funcionalidad existente de inspección profunda de paquetes en los actuales cortafuegos puede ser compartida por los sistemas de prevención de intrusiones (IPS).

Actualmente, el Grupo de Trabajo de comunicación Middlebox de la Internet Engineering Task Force (IETF) está trabajando en la estandarización de protocolos para la gestión de cortafuego.

Otro de los ejes de desarrollo consiste en integrar la identidad de los usuarios dentro del conjunto de reglas del cortafuego. Algunos cortafuegos proporcionan características tales como unir a las identidades de usuario con las direcciones IP o MAC. Otros, como el cortafuego NuFW, proporcionan características de identificación real solicitando la firma del usuario para cada conexión.

Limitaciones de un Cortafuego

Las limitaciones se desprenden de la misma definición del cortafuego: filtro de tráfico. Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuego (por usar puertos TCP abiertos expresamente, por ejemplo) o que sencillamente no use la red, seguirá constituyendo una amenaza. La siguiente lista muestra algunos de estos riesgos:

- Un cortafuego no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.
- El cortafuego no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El cortafuego no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias, etc.) y sustraerlas del edificio.
- El cortafuego no puede proteger contra los ataques de ingeniería social.

- El cortafuego no puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.
- El cortafuego no protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen en Internet.

Políticas del Cortafuego

Hay dos políticas básicas en la configuración de un cortafuego que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva:** Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuego obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar las empresas y organismos gubernamentales.
- **Política permisiva:** Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el

resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a Internet.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido

4.3 Población y muestra

No se aplica para el presente trabajo de investigación.

4.4 Técnicas e instrumentos de recolección de datos.

El método deductivo es aquel que, partiendo de unas premisas teóricas dadas, llega a unas conclusiones determinadas a través de un procedimiento de inferencia o cálculo formal. El paso de las premisas a la conclusión o conclusiones se realiza a través de ciertas reglas lógicas específicas (por ejemplo, la regla del modus ponens o procedimientos silogísticos derivados de ella), o de ciertos procedimientos matemáticos.

Pondremos algún ejemplo: Todos los cisnes son blancos. Kuki es un cisne. La conclusión es que Kuki es blanco. Como se ve en el ejemplo, la verdad de la conclusión se encuentra dentro de las dos premisas iniciales.

El término "observación" lo utilizaremos en la forma más amplia que el de solo ver, por ello incluye un rango de monitoreo de condiciones y actividades que van desde las no conductivas hasta las conductivas.

En este punto trabajaremos con las formas denominadas "Observación Conductiva" y "Observación no Conductiva", debido a que conduciremos los hechos que se observan usando método Conductivo y también el no Conductivo porque estará centrada en la revisión de libros, revistas, etc.

De acuerdo con otra clasificación de observaciones podemos considerar los siguientes métodos: Observación Estructurada, la cual se caracteriza por determinar con anterioridad lo que se va a observar y la Experimental, cuyo propósito es fundamental en descubrir relaciones o resultados específicos.

4.5 Procedimiento de recolección de datos.

Para el análisis estadístico hemos usado el método de "Estadística Descriptiva" para cada variable, medidas de tendencia estándar o "medidas de variabilidad", como también son conocidas, incluyendo el rango de la desviación y la varianza.

Quienes estamos interesados en los datos, deseamos con frecuencia tener también una medida de la forma en que los valores individuales se desvían del promedio.

CAPITULO V

RESULTADOS

Este trabajo basa su aprobación en los resultados en 2 grandes áreas:

- El análisis de las características y comportamiento técnico de sus componentes, y
- Una investigación de opinión cuanto a su aceptación y adaptación por sus principales clientes: los alumnos.

5.1 Análisis de las características técnicas

EL laboratorio virtual fue probado en dos configuraciones diferentes de los computadores C1 y C2. (escenario 1 y escenario 2) Las medidas fueron efectuadas con el software **Microsoft Management Console**. La principal medida fue la del performance del procesador al inicio y durante el ejercicio. También fueron medidos la memoria y el uso del disco duro.

En la tabla 5.1 están resumidos los principales resultados obtenidos. La columna NVM muestra el número de máquinas virtuales utilizadas en los escenarios del laboratorio. 7XP es un escenario con una máquina virtual corriendo Redhat 9.0 con X-Windows en lugar de la instalación minimizada de Trustix Linux instalado en las otras máquinas.

La Workstation con RedHat requiere un considerable tamaño de 2.58 Gb

cuando comparada con los 400 MB del Trustix Linux. También la memoria del RedHat es de 128MB cuando comparada con los 16 MB del trustix. También trabajar con X- Windows es posible pero es mucho más lento.

Tabla 5.1 Resultados técnicos de los componentes
(Fuente propia)

C	NVM	ST	PU	PMU	HDU
C1	1	~ 1	7 - 38	329	0.39
C1	5	~ 2	15 - 73	199	1.92
C1	6	~ 4	16 - 76	168	2.31
C1	7	~ 5	31 - 88	137	2.7
C1	7XP	~ 6	47 - 100	91	5.33
C2	1	~ 1	7 - 48	331	0.39
C2	5	~ 3	56 - 95	225	1.92
C2	6	~ 5	58 - 97	194	2.31
C2	7	~ 6	72 - 100	169	2.7
C2	7XP	~ 7	79 - 100	68	5.33

5.2 Investigación de la opinión de los alumnos

A los alumnos que participaron en las clases de redes utilizando el laboratorio virtual, se les presentó un cuestionario con 3 preguntas después que concluyeron los ejercicios, las cuales respondieron dando valores de 1 a 5 a cada uno de los ítems considerados, siendo 5 la nota más alta.

- a.- Se les pidió que realicen una evaluación del Software Virtual PC 2004 utilizado en el desarrollo de los laboratorios programados de Redes Informáticas.
- b.- También debieron responder: ¿En qué grado consideran que el empleo del enfoque de Virtualización es útil en la enseñanza de los conceptos de redes?
- c.- Finalmente calificaron, en qué grado la utilización del enfoque de Virtualización les proporciona facilidades en su preparación profesional para el desarrollo en su trabajo con sistemas reales.

RESULTADOS DE LA ENCUESTA

Los 79 estudiantes que participaron en los laboratorios y que previamente habían realizado las pruebas en forma tradicional, quedaron muy satisfechos con el uso del software Virtual PC 2004. La media de las calificaciones fue 4.19, donde casi el 40% de los participantes optaron por la opción más alta (5), y aproximadamente 43% escogieron la opción

4 habiendo realizando una evaluación más exigente.

Con respecto a la segunda pregunta inicialmente los alumnos estaban menos convencidos de que el empleo de la Virtualización pudiese ayudarles en la captación de los conceptos de redes con mayor calidad. Aunque la media fue alta (3.95), se debe notar que el número de alumnos que asignaron como respuesta la opción 4 es prácticamente el mismo que en la pregunta anterior, aunque tuvo un decrecimiento en el número de alumnos deseando que optaron por la opción 5, aproximadamente 27% que son 22 alumnos.

Finalmente, de acuerdo con la media de las opciones asignadas a la tercera pregunta (3.84), el mayor porcentaje de los alumnos optaron por estar parcial o totalmente de acuerdo que este enfoque podría prepararlos para trabajar con sistemas de redes reales.

Esta pregunta obtuvo una aceptación total de 23 una parcial de 34 alumnos que representa un porcentaje muy aceptable

Tabla 5.2 Resultado da encuesta a los alumnos
(Fuente propia)

Pregunta	Promedio	Opción 5	Opción 4	Opción 3	Opción 2	Opción 1
1	4.19	31	34	12	2	0
2	3.95	22	35	18	4	0
3	3.84	23	34	12	6	4

CAPITULO VI

DISCUSIÓN DE RESULTADOS

6.1 Contrastación de la hipótesis con los resultados

Si: $A > B$, HIPOTESIS FALSA:

Si: $B > A$, HIPOTESIS VERDADEIRA

Nuestra hipótesis propone a la Virtualización como una herramienta para la adquisición de conocimientos en redes de computadoras de los estudiantes de ingeniería y de los participantes de Institutos Superiores Tecnológicos, de tal forma que influya significativamente en la calidad de servicio que se brinda en los laboratorios y a un menor costo.

En este caso podemos considerar básicamente, que la "participación directa" de una mayor cantidad de alumnos en el desarrollo de cada ejercicio de laboratorio planteado en el aula que, en las clases desarrolladas en forma tradicional en una menor cantidad de tiempo y una mejor calidad de servicio demostrarían que la utilización de la Virtualización es una buena opción. Es importante señalar que en este caso "participación directa" tiene un significado que cada participante en el laboratorio cuente con los elementos requeridos para realizar la practica propuesta como si estuviera solo, utilizando todo el equipamiento requerido para tal fin, y no como se realiza en forma tradicional en que solo un alumno, de un grupo de 7 a 10, realiza la experiencia realmente

mientras que los demás se limitan solo a mirar el desarrollo de la misma.

Para el presente trabajo de tesis hemos realizado un paralelo en el desarrollo de cada experiencia, una vez en la forma tradicional y la otra utilizando Virtualización. Llegamos a estimar que entre 25 y 30 alumnos es una cantidad ideal para el desarrollo de laboratorios utilizando Virtualización y menores de 20 para los laboratorios tradicionales.

Además de las facilidades y ventajas indicadas en este trabajo relacionadas con la enseñanza, debemos considerar que la INTERNET se ha tornado en una infraestructura de vital importancia para dar soporte. Sin embargo, enfrenta actualmente muchos desafíos especialmente para liberar nuevos servicios y soportar un más ancho espectro de aplicaciones de networking.

El mayor impedimento para soportar nuevos servicios recae en la inhabilidad de la actual arquitectura de la Internet de soportar la coordinación Interdominio de los nuevos servicios, porque los actuales Service Providers (Proveedores de Servicios-ISPs) raramente tienen responsabilidad sobre un enlace punto a punto de la entrega del servicio, y solamente nuevos servicios han sido implementados en pequeñas "islas" o situaciones muy particulares. Por consiguiente, cambios fundamentales en la arquitectura de redes son requeridos en la Internet de la próxima generación.

La Virtualización de red ha sido propuesta como un atributo clave en la

diversificación del futuro paradigma inter-redes y se espera que juegue un rol crucial en la Internet de la próxima generación.

6.2 Contrastación de resultados con otros estudios similares

Para este punto se usó la herramienta Virtual Network User-Mode-linux (VNUML) de libre distribución debido a que está específicamente destinado a la Virtualización de topologías de redes completas, lo que reduce los recursos necesarios para virtualizar diferentes dispositivos de red y facilita el despliegue de las infraestructuras de red necesarias para una asignatura como redes de computadores.

En este sentido las configuraciones sobre los dispositivos virtualizados en VNUML son directamente aplicables en dispositivos reales. Además, esta herramienta al estar basada en código abierto, permite ser instalada libremente en los laboratorios de práctica sin costo alguno, y en el caso de ser requerido, realizar los cambios o adecuaciones necesarias para solucionar cualquier problema que pueda aparecer, o incluso llevar a cabo aquellas mejoras que consideremos oportunas.

En el Paper "Experiencia con la herramienta de Virtualización VNUML para la enseñanza de computadoras" de los Drs. Antonio Ruiz Martínez, Rafael Martín López y otros del Departamento de Ingeniería Informática y Comunicaciones de la Facultad de Informática de la Universidad de Murcia. España 30100 Campus de Espinardo - Murcia se muestra la experiencia en la aplicación de dicha herramienta.

En los últimos años la Virtualización está experimentando un auge importante motivado por las importantes ventajas que ofrece su uso. En general podemos destacar las siguientes:

- Ahorro de costos de la Infraestructura.
- Mayor aprovechamiento de los recursos.
- Simplificación de la gestión.
- Reducción de los procesos de copias de seguridad.

En Murcia, los resultados muestran que la tasa de aprobados de las prácticas está alrededor del 100% ya que los alumnos, gracias a que pueden comprobar el funcionamiento de las soluciones planteadas, solo las presentan cuando están seguros de que gran parte de los requisitos que se les pide funcionar en su solución. Además, una vez entregada la práctica se lleva a cabo una entrevista donde los alumnos demuestran su funcionamiento y donde se realizan una serie de pruebas y preguntas acerca de la solución desarrollada con el fin de valorar el grado de funcionamiento de ésta, así como las cualidades de las soluciones adoptadas

Desde el punto de vista de la evaluación, el uso de la herramienta VNUML, permitió a los profesores probar ciertos casos de uso de forma rápida y sencilla, los cuales deberían estar desarrollados en la solución

planteada por el alumno. Además, permitió al profesor plantear, de la misma forma, casos inesperados a los que el alumno debió ser capaz de enfrentarse teniendo en cuenta lo aprendido durante la realización de la práctica.

De la aplicación de la metodología los profesores de la Universidad de Murcia recibieron muchos comentarios positivos a lo largo de estos años. Mediante una encuesta anónima que fue realizada a un grupo de 30 alumnos realizada en un curso, se les preguntó si las prácticas les habían ayudado a comprender mejor los distintos conceptos teóricos explicados a lo largo de la teoría, el 100% respondió que sí en una escala entre 7 y 10 sobre 10.

El único aspecto negativo que mencionaron fue la falta de ejemplos existentes para Quagga, ya que si bien es cierto esta herramienta presenta un alto grado de compatibilidad con los comandos de los routers Cisco, también es cierto que en algunos de ellos es diferente.

IX. REFERENCIAS BIBLIOGRAFICAS

[1] Asia Computer Weekly (2010): Network+interop99(n+i99) preview: Sign up for the atm classroom at fore university. Asia Computer Weekly:1.

[2] A. Keromytis, V. Misra, and D. Rubenstein. SoS, Secure Overlay Services. In Proceedings of ACM SIGCOMM 2002, Aug 2012.

[3] B. Krishnamurthy, C. Wills, and Y. Zhang. The use and performance of content distribution networks, 2011.

[4] Braathen, S. and Robles, M. (2008): The importance of assessment in business education. National Business Education Yearbook, 2008:11-24

[5] Cranitch G., Rees M., (2009) Virtualization: A case study in database administration laboratory work, In Same places, different spaces.

[6] Diskeeper Corporation, (2011) Virtualization and Disk Performance, http://files.diskeeper.com/pdf/-Virtualization_Performance.pdf [05.07.2011

[7] IBM Global Education White Paper, (2011) Virtualization in Education, <http://www07.ibm.com/solutions-/in/education/download/Virtualization>.

[8] J. Kannan, A. Kubota, K. Lakshminarayanan, I. Stoica, and K. Wehrle. Supporting Legacy Applications over Routing Overlays. Technical report,

UCB, 2008.

[9] J. D. Touch, Y.-S. Wang, L. Eggert, and G. G. Finn. A virtual internet architecture. ISI Technical Report ISI-TR-2003-570, Mar 2013.

[10] Janche Sang, Hands-on laboratory experiments with SOHO networking [technologies, Computer Applications in Engineering Education, **21**, 4, (586-595), (2010).

[11] M. Walfish, J. Stribling, M. Krohn, H. Balakrishnan, R. Morris, and S. Shenker. Middleboxes no longer considered harmful. To appear in OSDI, Dec 2011.

[12] Murcia F. Jorge, Redes del saber, Cooperativa Editorial Magisterio, Bogotá Colombia, 2014.

[13] S. Savage, et. al. Detour: a case for informed internet routing and transport. Technical Report TR-98-10-05, UW, 2007.

[14] Scheffy C., (2012) Virtualization For Dummies; AMD Special Edition, Wiley Publishing, Inc., New York.

[15] Stackpole B., Koppe J., Haskell T., Guay L., Pan Y., (2008)

Decentralized virtualization in systems administration education, Proceedings of the 9th ACM SIGITE conference on Information technology education, SIGITE '08, Cincinnati, OH, USA.

[16] Tucson Computer Society, (2011) a comparison between "vmware player, "oracle vm virtualbox", and "windows virtual pc" from a "windows" perspective.

[17] Tulloch M., (2010) Understanding Microsoft Virtualization Solutions from the Desktop to the Datacentre, Microsoft Press, Redmond, Washington.

[18] VMware WhitePaper, (2011) Virtualization Overview, .pdf, [05.07.2011].

[19] Zeljko Stojanov, Dalibor Dobrilovic and Tamara Zorić, Exploring students' experiences in using a physical laboratory for computer networks and data security, Computer Applications in Engineering Education, **25**, 2, (290-303), (2017).

ANEXOS

✓ Matriz de consistencia

VIRTUALIZACION COMO HERRAMIENTA DE LA ENSEÑANZA DE REDES DE COMPUTADORES				
PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	MÉTODOS
<p>General</p> <p>¿Cómo se puede utilizar la virtualización como herramienta para la enseñanza de redes de computadoras que mejoren la capacitación en las áreas de ingeniería?</p>	<p>General</p> <p>Haciendo uso de lo que nos ofrece la tecnología en el campo de la electrónica y las telecomunicaciones, utilizar la virtualización como herramienta económica y practica, que permita la enseñanza de redes de computadoras como herramienta de ingeniería y en especial de la eléctrica.</p>	<p>General</p> <p>La utilización de la virtualización como herramienta en la enseñanza de redes de computadoras para los estudiantes de ingeniería, influye significativamente en la calidad de servicio que se brinda en los laboratorios a un menor costo.</p>	<p>A = variable dependiente.</p> <p>Calidad de educación tradicional.</p> <p>$A=f(Y)$</p> <p>B = variable dependiente</p> <p>Calidad de educación con Virtualización.</p> <p>$B=f(Z)$</p>	<p>General</p> <p>Implementación de un modulo a ser probado con recursos de Virtualización por un determinado plazo, al final del cual será efectuada una evaluación frente a un modulo capacitado de forma tradicional.</p>
<p>Específicos</p> <p>- ¿Se pueden crear de laboratorios virtuales que permita mejorar la calidad de servicio en la obtención de conocimientos sobre el manejo y configuración de redes de computadoras como herramienta de ingeniería eléctrica?</p> <p>-¿Es posible disminuir los gastos relacionados con la implementación de laboratorios</p>	<p>Específicos</p> <p>-Mejorar la calidad de servicio que se brinda a los estudiantes de ingeniería eléctrica en su preparación sobre diseño, configuración y manejo de redes.</p> <p>-Utilizar la virtualización como herramienta que permita la reducción de costos en la implementación de laboratorios para la enseñanza de redes en ingeniería eléctrica.</p>	<p>Específicos</p> <p>-Se puede mejorar las limitaciones físicas (cantidad de alumnos capacitados) utilizando virtualización, mejorando de esta forma la calidad de servicio en los laboratorios de redes de computadoras.</p> <p>-El costo que representa la implementación de laboratorios</p>	<p>Si $A>B$=falso</p> <p>Si $B>A$=verdad</p>	

<p>especializados que permitan la enseñanza práctica de redes de computadoras como herramienta de ingeniería eléctrica?</p> <p>-¿Qué ventajas se obtendrían con la implementación de laboratorios utilizando virtualización?</p>	<p>-Utilizar la virtualización como herramienta que permitan la reducción de los tiempos necesarios para la capacitación del diseño de topologías de redes de computadoras en ingeniería eléctrica.</p>	<p>con redes físicas puede ser minimizado con la implementación de redes virtuales como herramienta en ingeniería eléctrica.</p> <p>-Es mucho más flexible la implementación de topologías en redes virtuales que en redes físicas, reduciendo de esta forma los tiempos requeridos para la capacitación.</p>		
--	---	---	--	--

Instrucciones para el llenado de la encuesta

La presente encuesta tiene por finalidad el evaluar la utilización del concepto de **virtualización** en la capacitación de redes.

La encuesta es personal y anónima. Se realizara luego de terminada cada una de las experiencias, debiendo ser lo más transparente y veraz posible, lo cual permitirá tener un acercamiento científico a la realidad concreta.

Para la calificación de cada interrogante de la encuesta, el alumno deberá marcar con una X el valor que asignará, debiendo tener en cuenta el significado de cada valor, los cuales se detallan a continuación:

- 1 Totalmente en desacuerdo en su uso.
- 2 En desacuerdo parcial en su uso.
- 3 No se obtiene ningún beneficio con su uso.
- 4 De acuerdo parcialmente en su uso.
- 5 Totalmente de acuerdo en los beneficios de su uso.

ENCUESTA TECNICA

Número de la experiencia:

Nombre

de

la

experiencia:

.....

.....

N°	PREGUNTA	1	2	3	4	5
1	Realice una evaluación del Software Virtual PC 2004 utilizado en el desarrollo del laboratorio programado de Redes Informáticas y asigne una calificación.					
2	¿En qué grado consideran que el empleo del enfoque de virtualización es útil en la enseñanza de los conceptos de la experiencia realizada?					
3	¿En qué grado la utilización del enfoque de virtualización les proporciona facilidades en su preparación profesional para el desarrollo en su trabajo con sistemas reales?					

DATOS AGRUPADOS DE LA ENCUESTA

Pregunta 1

Opción de respuest $a(X_i)$	Cantidad de alumnos (n_i)	$X_i \cdot n_i$
1	0	0
2	2	4
3	12	36
4	34	136
5	31	155
Total Alumnos	79	$331/79=4.189$

Media: 4.19

Pregunta 2

Opción de respuest $a(X_i)$	Cantidad de alumnos (n_i)	$X_i \cdot n_i$
1	0	0
2	4	8
3	18	54
4	35	140
5	22	110
Total Alumnos	79	$312/79=3.949$

Media: 3.95

Pregunta 3

Opción de respuesta $a(X_i)$	Cantidad de alumnos (n_i)	$X_i \cdot n_i$
1	4	4
2	6	12
3	12	36
4	34	136
5	23	115
Total Alumnos	79	$303/79=3.835$

Media: 3.84

REPRESENTACIÓN GRAFICA DE RESULTADOS DE LA ENCUESTA (%)

	Opc 1	Opc 2	Opc 3	Opc 4	Opc 5
Pregunta 1	0%	2.53%	15.19%	43.04%	39.24%
Pregunta 2	0%	5.06%	22.79%	44.30%	27.85%
Pregunta 3	5.06%	7.59%	15.19%	43.04%	29.11%

