UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

DISEÑO, IMPLEMENTACION Y PUESTA EN MARCHA DEL LABORATORIO DE REDES DEL POSGRADO EN CIENCIA E INGENIERÍA DE LA COMPUTACION

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A:

ANGEL HERNÁNDEZ SEGURA

ASESOR DE TESIS: DR. JAVIER GOMEZ CASTELLANOS

MÉXICO, D. F. 2008

Agradecimientos.

A mis Padres, por su constante apoyo, por su impulso y por ser nuestros guías.

A mis hermanos, por crecer y aprender juntos, sé que siempre podré contar con su apoyo y ustedes con el mío.

A toda mi familia, porque donde estamos ahora es el resultado del trabajo de muchas personas que estuvieron antes que nosotros, gracias por ayudar a construir el camino de esta familia, nosotros trataremos de hacerlo con el mismo entusiasmo.

Índice

Diseño, implementación y puesta en marcha del laboratorio de redes del Posgrado en Ciencia e Ingeniería de la Computación.

Introducción

El Posgrado en Ciencia e Ingeniería de la Computación.

"A pesar de que la computación surgió como una disciplina asociada fuertemente a las aplicaciones y la ingeniería, la potencialidad y el desarrollo acelerado del cómputo, propiciaron el planteamiento de problemas formales cuya solución requería un conocimiento teórico abstracto; esto dio origen a la ciencia de la computación.

Así, en el sentido más amplio, la computación se considera como la disciplina que estudia aspectos tanto teóricos como de realización del manejo y procesamiento de la información en todas sus formas. A partir de este enfoque, un programa de ingeniería resulta insuficiente para abarcar todo el espectro de la computación. Por otro lado, un programa orientado únicamente a la teoría de la disciplina omitiría la parte tecnológica indispensable, sobre todo debido a la rápida obsolescencia de algunos aspectos prácticos del área.

Para solucionar esta problemática la Universidad Nacional Autónoma de México, UNAM generó el Programa de Posgrado en Ciencia e Ingeniería de la Computación en donde se incluyen todas las vertientes de la materia que se cultivan en la universidad. Dicho programa ofrece además la ventaja de crear sinergias, fomentar la interdisciplinariedad y propiciar la conformación de grupos con espectros amplios de conocimientos horizontales en el área.

Así la misión del programa de Posgrado en Ciencia e Ingeniería de la Computación, de la UNAM, es formar expertos capaces de aplicar las tecnologías de manejo de la información en áreas estratégicas, tanto en aspectos prácticos como de investigación. Para ello, se estudian las herramientas teóricas que formalizan el procesamiento de datos en sistemas dinámicos y complejos. En particular se tienen dos niveles de conocimiento y profundidad, maestría y doctorado.

Los campos de conocimiento que se cultivan en el programa están asociados a los intereses de los profesores y tutores del programa y son:

· Ingeniería de Software y Base de Datos
· Inteligencia Artificial, Redes Neuronales y Sistemas Adaptables
· Ingeniería de Sistemas y Redes Computacionales
· Computación Científica
· Imágenes, Ambientes Virtuales y Procesamiento Digital de Señales"

Las principales característica del programa son:

· El reconocimiento a su calidad por parte de sus pares y avalado por el CONACYT proposición 2002 dentro de los posgrado nacionales de alto nivel para la maestría y en fomento para el nivel de doctorado.

· La constitución de un Comité Académico con diez y seis miembros como responsable de la conducción y planeación del programa. Este comité esta formado por los siete directores de las entidades académicas participantes e invitadas responsables del programa, los seis representantes de los tutores de todo el programa y dos alumnos del programa elegidos por los académicos y alumnos respectivamente.

· La integración de un sistema de tutores como elemento fundamental de supervisión y asesoría para los estudiantes y la creación de normas operativas claras que garantizan una funcionalidad del programa.

· La creación de grupos colegiados académicos encargados de la conducción del programa, lo cual responsabiliza a todos los actores del éxito del programa.

· La flexibilidad de los planes de estudios para que el tutor en conjunto con el estudiante construya las actividades académicas pertinentes para lograr una formación plena. Esto induce la interacción entre alumnos de diferentes áreas y permite definir perfiles específicos en función de los intereses y necesidades de los alumnos.

· La infraestructura disponible de la UNAM en todos sus aspectos. En particular el programa cuenta con aproximadamente cincuenta académicos de tiempo completo de la UNAM de los cuales el ochenta y seis por ciento tienen un doctorado y más del sesenta y dos por ciento son miembros del Sistema Nacional de Investigadores, SNI.

· Experiencia adquirida al ser uno de los primeros posgrados en ciencia de la computación del país.

· Acceso directo a las seis bibliotecas de las entidades responsables. En ellas se reciben más de cien revistas especializadas de las diversas áreas que se cultivan en el programa y se tienen más de quince mil libros relacionados con cómputo sin contar los ejemplares duplicados.

· Ocho laboratorios con equipos modernos que cubren los diversos campos del conocimiento del programa.

· Más del cincuenta por ciento de los proyectos de investigación reciben financiamiento externo a la UNAM. El resto de los apoyos proviene de fondo de la Dirección General de Apoyo al Personal Académico y la Dirección General de Estudios de Posgrado.

· Infraestructura asociada a los servicios de vigilancia, servicios médicos, servicios de fotocopias y dibujo, etc.

· Carácter Nacional con pluralidad disciplinaria. En particular se tiene la posibilidad de interactuar con académicos de otras disciplinas para inducir sinergias, asistir a eventos culturas, tener acceso al Centro de Idiomas y en general a la cultura, usar las redes de información vía la red UNAM y participar en reuniones académicas, tele-conferencias talleres de manera gratuita.

· Apoyo de la Dirección de Intercambio Académico para la firma de convenios y colaboraciones con otras instituciones de educación superior, tanto nacional como internacional.

· Apoyo de la Dirección General de Evaluación Educación para evaluar de manera continua los tutores y alumnos y darle seguimiento a la relación tutor alumno.

· Liderazgo académico en el ámbito nacional y latinoamericano."[1]

Área de Redes dentro del Posgrado.

Algunas de las materias que se imparten en el Área de Ingeniería de Sistemas y Redes de Computadoras son:

- Programación Concurrente
- Sistemas Distribuidos y Verificación
- Procesamiento Paralelo
- Teoría de la Información
- Redes de Computadoras
- Sistemas Operativos
- Sistemas en Tiempo Real
- Criptografía
- Redes Inalámbricas
- Computo de Alto Desempeño
- Sistemas Cooperativos
- Administración de Redes

Algunos de los académicos que imparten clase en esta área son:

- Dr. Héctor Benítez Pérez
- Dr. Enrique Daltabuit Godas
- Dr. Fabián García Nocetti
- Dr. Javier Gómez Castellanos
- Dr. Sergio Rajsbaum Gorodesky
- Dr. Víctor Rangel Licea
- Ing. Mario Rodríguez Manzanera
- Dr. Manuel Romero Salcedo
- Dr. Julio Solano González
- Dr. Gerardo Vega Hernández

[1] UNAM. Posgrado, Ciencia e Ingeniería de la Computación. Generalidades. Introducción. Véase el sitio Web: www.mcc.unam.mx

Por medio de esta tesis se propone aprovechar el equipo de computo y de redes con el que actualmente cuenta el laboratorio del Posgrado en Ciencia e Ingeniería de la Computación, se plantearán prácticas para que los alumnos puedan hacer uso de dichos equipos y se propondrán temas para que un futuro el laboratorio aumente su equipo y se planteen nuevos temas y alternativas de estudio.

Capitulo I
El laboratorio de redes del Posgrado en Ciencia e Ingeniería de la Computación.

“Objetivo.

Cubrir desde el punto de vista técnico y académico la necesidad de comprobar físicamente bajo una situación real, funcional y operativa los problemas derivados de la conectividad de dispositivos dedicados a dar servicio de conexión entre sistemas de cómputo, Host, PCs, Macs, etc., pudiendo establecer los sistemas necesarios para analizar virus, troyanos, gusanos y embates que pueden afectar el funcionamiento, la integridad y la seguridad de la red.

Justificación.

El mercado externo y la industria están requiriendo de personal que conozca las tecnologías de interconexión, hardware y software dedicado. Teniendo como única opción el dirigirse directamente a los fabricantes de equipos los que además de cobrar cantidades exorbitantes por certificaciones que caducan en el corto plazo se limitan al conocimiento de una sola marca.

El posgrado en ciencia e ingeniería de la computación requiere incluir dentro de su programa educativo un área dedicada a la seguridad de las comunicaciones, siendo indispensable que el alumno obtenga la experiencia de trabajar con dispositivos reales, mismos que encontrará en el mercado de trabajo al cual esta dirigida esta especialidad.

Desde el punto de vista académico-investigación el posgrado requiere contar con los elementos necesarios para poder manejar, crear, probar, desarrollar protocolos y programas de aplicación, inclusive el probar rutinas criptográficas, codificación y decodificación de llaves, simulación de fallas, conteo de paquetes, creación de algoritmos de enrutamiento, creación y prueba de política de campo no militarizado, etc.

La calificación de la materia de laboratorio será un factor primordial para la culminación en la preparación de alumnos interesados en comunicación de datos, redes de computadoras y seguridad.

Materia y temario.

Algunas de las actividades que se desarrollarán en el laboratorio son:

- Creación de un esquema de comunicación en base al modelo OSI.
- Prueba de interconexión de dispositivos.
- Creación de topologías de comunicación,
- Programación de parámetros y creación de políticas.
- Tablas de ruteo.

- Mediciones de tráfico.
- Mediciones eléctricas.
- Producción y detección de fallas.
- Redes mixtas alámbricas e inalámbricas.
- Prueba de protocolos.
- Descripción general del direccionamiento IP
- Emular una red mínima con una topología en delta lo cual permite emular trafico, fallas, redireccionamientos, disponibilidad de enlaces, redundancias, probar tablas de ruteo, direccionamiento estático y dinámico, etc."[2]

Requerimientos de Servicios y Aplicaciones.

Debido a la variedad de temas que se pretenden estudiar en este laboratorio se necesita una amplia gama de servicios, por ejemplo, para montar un servidor Web podemos utilizar Apache, para un servidor de Correo Sendmail o Postfix, para un servidor de Bases de Datos podemos utilizar MySQL o PostgreSQL, para un servidor de impresión CUPS, para un servidor de archivos NIS o SAMBA, todos los servicios anteriores se caracterizan por contar con una licencia GNU por lo que se pueden obtener de forma gratuita, se pueden redistribuir, incluyen el código fuente y en caso de ser necesario se pueden modificar dependiendo de lo que se necesite, lo que implica muchas ventajas.

Todos los servicios anteriores y algunos más se encuentran en el sistema operativo Linux, que cuenta con la licencia GNU, además cuenta con una implementación de muchos protocolos y estándares de red y seguridad que en la mayoría de los casos solo necesitan ser configurados para tenerlos funcionando.

A continuación se muestra una tabla que contiene los servicios y aplicaciones que se necesitarán y la función que proveen:

Servicio	**Descripción**
Apache HTTPD[3]	• Es un servidor WEB poderoso y flexible. • Implementa los últimos protocolos incluyendo HTTP/1.1 •Es altamente configurable y se le pueden agregar módulos para aumentar sus funciones. • Se puede personalizar, se pueden programar módulos utilizando el API de Apache. • Provee el código fuente completo.

[2] Documento de apoyo del Posgrado en Ciencia e Ingeniería de la Computación, elaborado por Juan Sánchez Herrera.
[3] The Apache Software Foundation. Véase: www.apache.org/

	• Corre sobre Windows 2003/XP/2000/NT/9x, Netware 5.x y superior, OS/2 y la mayoría de las versiones de UNIX así como en otros sistemas operativos. • Por default escucha en el puerto 80
VSFTD[4]	• Servidor FTP para sistemas Unix, incluyendo Linux. • Es seguro, extremadamente rápido y estable. • Soporta: Operación Stand-alone o por medio de inetd, configuración personalizada para cada usuario, configuración personalizada por IP, límites por IP, IPv6, encriptación a través de SSL, etc. • Por defalut escucha en el puerto 21
OpenSSH[5]	• Es una implementación gratuita de las herramientas de conexión de SSH. • Sustituye de forma segura a telnet o rlogin. • Open SSH encripta de forma segura todo el tráfico, incluyendo las contraseñas. • Adicionalmente provee capacidad de crear túneles seguros, distintos métodos de autenticación y soporta todas las versiones de SSH • Por default escucha en el puerto 22
qmail[6]	• Es un agente de transferencia de correo seguro, confiable y eficiente. • Esta diseñado para servidores UNIX • Garantiza que un mensaje una vez aceptado por el sistema no se perderá. • En un sistema Pentium qmail puede fácilmente enviar 200,000 mensajes locales al día. Las entregas remotas se ven limitadas por la lentitud del DNS y de SMTP. • qmail es mucho mas pequeño y ligero que cualquier SMTA. • Por default escucha en el puerto 25.

[4] vsftpd - Secure, fast FTP server for UNIX-like systems. Véase: http://vsftpd.beasts.org/
[5] OpenSSH. Véase: http://www.openssh.com/
[6] qmail:the Internet´s MTA of choice. Véase: http://cr.yp.to/qmail.html

Horde IMP[7]	• Provee acceso vía WEB a cuentas IMAP y POP3 • Soporta archivos adjuntos que cumplan con los protocolos MIME. • Se pueden definir preferencias y filtros para cada usuario • Los usuarios pueden leer, enviar y organizar correos, manejar y compartir calendarios, contactos, tareas y notas. • Trabaja sobre un servidor WEB, por lo que se accede por medio del puerto 80.
DHCPD[8]	• Un servidor DHCPD permite especificar los parámetros de configuración de red como, dirección IP, DNS, Gateway y máscara de red, en un servidor y lograr que las máquinas cliente se configuren a partir de este. • Evita estar configurando estáticamente las direcciones IP, ni siquiera es necesario configurar la dirección del servidor DHCP, este se reconoce a partir del envío de paquetes Broadcast. • Por default escucha en el puerto 67.
DNS[8]	• Servicio encargado de "traducir" un nombre de dominio en una dirección IP e inversamente. • Permite al usuario que desea abrir una página escribir solo en nombre de dominio y no tener que memorizar la dirección IP asociada, por ejemplo: para abrir la página de la UNAM escribimos en la barra de dirección de nuestro explorador www.unam.mx, pero también podríamos escribir 132.248.10.7 • Por default escucha en el puerto 53
CUPS[9]	• Provee una capa portable para impresión en los sistemas UNIX. • Utiliza el IPP, Internet Printing Protocol por sus siglas en inglés. • Tiene funcionalidad de impresión en red • Actualmente existen miles de controladores para distintas impresoras, lo que agrega compatibilidad con una gran cantidad de impresoras.

[7] The Horde Project. Véase: http://www.horde.org/
[8] Linux Home Networking and Linux Forums Help. Véase: http://www.linuxhomenetworking.com/
[9] Common UNIX Printing System. Véase: http://www.cups.org/

	• Por default escucha en el puerto 631
MySQL[10]	• Proporciona un servidor de base de datos SQL (Structured Query Languaje) muy rápido, multi-threaded, multi usuario y robusto. • Escrito en C y C++ • Funciona en diferentes plataformas • APIs disponibles para C, C++, Eiffel, Java, Perl, PHP, Python, Ruby, y Tcl. • Un sistema de privilegios y contraseñas que es muy flexible y seguro, y que permite verficación basada en el host. Las contraseñas son seguras porque todo el tráfico de contraseñas está encriptado cuando se conecta con un servidor. • Por default escucha en el puerto 3306
NIS[8]	• Network Information Service, su propósito es proveer información que debe ser conocida a través de la red hacia todas las máquinas, por ejemplo: logins, passwords, y directorios home, información de grupos, nombres de hosts e IPs, de esta forma, si su contraseña se encuentra en el servicio NIS, usted podrá acceder a cualquier máquina de la red, utilizando esta contraseña, de la misma forma accederá a sus archivos y configuraciones, con ayuda de servicios como SAMBA y NFS • Utiliza puertos variables, por medio del servicio portmap
NFS[11]	• Network File System, se desarrolló para permitir que distintas computadoras puedan montar particiones como si fueran discos locales. • Permite que los archivos se compartan de forma rápida y fácil • Distintos métodos de autenticación, con lo que se asegura que solo ciertas personas puedan ver cierta información. • Diseñado para ambientes de red con máquinas Linux. • Por default escucha en el puerto 2049
SAMBA[8]	• SAMBA es un software que permite compartir archivos e impresoras en un ambiente de máquinas Linux y Windows. • Incluye servicios de autenticación y autorización • Resolución de nombres.

[8] Linux Home Networking and Linux Forums Help. Véase: http://www.linuxhomenetworking.com/
[10] MySQL AB :: The world´s most popular open source database. Véase: http://www.mysql.com/
[11] Linux NFS faq. Véase: http://nfs.sourceforge.net/

	• Por default escucha en el puerto 139
Kerberos	• Protocolo de autenticación de red. • Diseñado para proveer seguridad en aplicaciones cliente/servidor • El protocolo utiliza una fuerte encriptación de forma que un cliente pueda probar su identidad a un servidor y viceversa. • También encripta todas las comunicaciones entre el cliente y el servidor, de forma que se asegura la integridad y privacidad de los datos. • Por defalult escucha en el puerto 750 y algunas versiones en el 88
Iptables[12]	• Software de filtrado de paquetes • Permite construir un firewall a partir de simples reglas de filtrado de paquetes • Permite usar NAT y enmascaramiento para compartir el acceso a Internet, en una red • Permite usar NAT para implementar PROXYs transparentes • Permite construir políticas de calidad de servicio • Permite manipular los paquetes, cambiando los valores de las cabeceras.
OpenVPN[13]	• Software que permite configurar una Red Privada Virtual • Permite utilizar los algoritmos de encriptación, autenticación y certificación de las librerías OpenSSL, para proteger el tráfico en la red. • Implementa las capas 2 y 3 del modelo OSI utilizando los estándares SSL/TLS
JAVA[14]	• Es un lenguaje de programación de alto nivel, robusto y versátil. • Permite a los programadores: programar en una plataforma y correr su programa en otra • Escribir programas para ser ejecutados dentro de un explorador WEB • Desarrollar programas para teléfonos celulares, PDAs y otros

[12] netfilter/iptables project homepage - The netfilter.org project. Véase: http://www.netfilter.org/
[13] OpenVPN - An Open Source SSL VPN Solution by James Yonan. Véase: http://openvpn.net/
[14] Java Technology. Véase: http://www.java.sun.com/

	dispositivos
Ethereal[15]	• Software analizador de protocolos, es usado alrededor del mundo para solucionar problemas de red, desarrollo de protocolos, análisis de paquetes y educación. • Corre sobre Unix, Linux y Windows • Los paquetes pueden ser capturados en tiempo real o incluso se pueden analizar archivos guardados previamente • Incluye 759 protocolos para análisis de tráfico.

Requerimientos de Hardware.

Tomando en cuenta los requerimientos de software y servicios, se elaboró la siguiente lista de requerimientos de Hardware:

Equipo de Redes con Cableado	
3 routers Cisco 2611XM y 3 switchs Cisco 2950	El propósito de tener tres routers es el de contar con una red mínima con una topología en delta lo cual permite emular trafico, fallas, redireccionamientos, disponibilidad de enlaces, redundancias, probar tablas de ruteo, direccionamiento estático y dinámico, etc. Estos equipos pueden utilizarse para administración y seguridad en redes.
Equipo de Redes Inalámbricas	
2 Access Points IEEE 802.11g D-LINK (DW-3200 AP)	Estos dispositivos serán conectados a diferentes segmentos de la red en el laboratorio para llevar a cabo handovers entre ellos, probar el protocolo de enrutamiento Mobile IP, llevar a cabo pruebas del comportamiento dinámico del IEEE 802.11 y muchas pruebas más. Se escogió este modelo de AP pues tiene un servidor RADIUS integrado, control de acceso por dirección MAC y administrable por SNMP, lo cual permite que también sea usado en las prácticas de seguridad en redes.
1 Access Point Bluetooth D-LINK DBT-900 AP	Access point de tecnología Bluetooth para permitir la conexión de Laptops y PDAs a la red con cables.
2 Laptops DELL 600m Intel Centrino	Los estudiantes usaran estas computadoras portátiles para llevar a cabo las diferentes prácticas de laboratorio con

[15] Ethereal A Network Protocol Analyzer. Véase: http://www.ethereal.com/

	tecnologías inalámbricas del tipo IEEE 802.11b/g y bluetooth. Se escogieron estas Laptops con un procesador centrino pues es el más apropiado para computadoras portátiles por su alto ahorro de energía.
2 PDAs HP IPAQ RX3715	Los estudiantes usaran estas dos PDAs para llevar a cabo las diferentes prácticas de laboratorio con tecnologías inalámbricas del tipo IEEE 802.11b/g y Bluetooth .Se escogen estas PDAs del modelo IPAQ pues incluyen interfaces IEEE 802.11 y Bluetooth, además de que cuentan con soporte en Linux.
2 tarjetas IEEE 802.11g PCMCIA LinkSys WPC54G	Estas dos tarjetas serán conectadas a las 2 laptops para conectarse a los puntos de acceso IEEE 802.11g. Se escogió el formato PCMCIA para estas tarjetas pues tienen mejor soporte en Linux (comparada con tarjetas IEEE 802.11 del tipo USB).
2 tarjetas Bluetooth, PCMCIA SOCKET CF Bluetooth	Estas tarjetas serán insertadas en las dos Laptops para uso con Access points de tecnología Bluetooth. Se escogió el formato PCMCIA para estas tarjetas pues tienen mejor soporte en Linux (comparada con tarjetas Bluetooth del tipo USB).
4 GPS Bluetooth i.Trek Bluetooth GPS Receiver	Las tecnologías inalámbricas actuales, junto con los dispositivos móviles están generando una tendencia hacia un cómputo ubicuo más flexible y poderoso. Una de las tecnologías inalámbricas de punta que se comienza a masificar es el uso de sistemas de posicionamiento global GPS. Ya existen dispositivos comerciales móviles muy económicos, lo que permite una adopción fácil para el desarrollo de proyectos novedosos y originales. El tipo de dispositivo que se propone cumple con estándares Bluetooth, lo que permitirá también realizar investigación aplicada sobre dicha tecnología, especialmente en combinación con dispositivos móviles (PocketPC's, Palms, Celulares y Laptops).
PCs para el laboratorio de computo	
10 PCs Dell Dimension 8400 con procesador de 3 Ghz, disco duro de 80 GB y memoria RAM de 1 GB.	Estos equipos remplazarán 10 PCs Pentium III de 500 Mhz y 256 MB de RAM que, de acuerdo a sus especificaciones, resulta ya imposible actualizar. Estos equipos nuevos se necesitan por su elevada capacidad de procesamiento, almacenamiento y memoria para dar el soporte necesario a aplicaciones de software que demandan grandes recurso de cómputo, tales como: Ambientes de Ingeniería de Software Asistida por Computadora (Borland Studio, Rational Rose, Select), Ambientes de desarrollo de software (Visual Studio .NET, Borland C++ 2005, JBuilder 2005), aplicaciones para procesamiento de imágenes, etc. Estos equipos apoyarán el

	proceso de desarrollo de tareas y trabajos de tesis de los alumnos, así como para impartir asignaturas de las diferentes áreas del conocimiento del Posgrado en Ciencia e Ingeniería de la Computación.

Capitulo II
Propuesta y justificación

Posibles topologías.

Dada la naturaleza del laboratorio lo ideal sería poder cambiar constantemente la topología de la red y de esa forma estudiar de una forma práctica las ventajas y desventajas de cada topología, sin embargo, no se pretende que todas las prácticas sean de topologías por lo que una topología deberá permanecer durante las prácticas en las que se experimente con otro temas, a continuación se presenta una breve descripción de las topologías que podrían estudiarse en el laboratorio, sus ventajas y desventajas y la topología que se presenta como propuesta para el resto de las prácticas:

Topología de Bus.

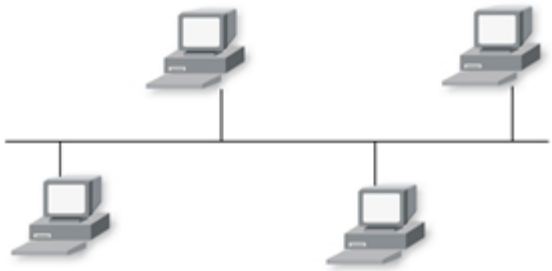


Imagen 1. Diagrama de Conexión de tipo Bus

Es la topología mas sencilla, todas las terminales están conectadas a un único canal de comunicaciones, no se cuenta con otro tipo de conexión entre ellas. Sus ventajas: Es simple, fácil de implementar, económica. Desventajas: Poco confiable, si un cable se rompe las terminales se quedan incomunicadas, no es eficiente, mientras mas terminales se estén comunicando existirán mas colisiones.

Topología de Estrella

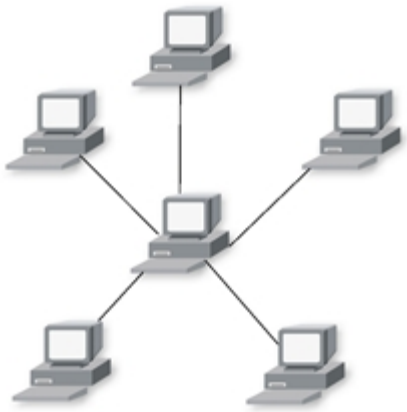


Imagen 2. Diagrama de Conexión tipo Estrella

Es una topología muy común en redes locales, todas las terminales están conectadas a un nodo central que retransmite los paquete que recibe, de esta forma, todos los nodos están comunicados, si algún nodo pierde su conexión, solo este se aísla, los demás siguen comunicados entre ellos, pero si el nodo central falla, todos los demás quedan incomunicados. Por lo general el nodo central es un Hub o un Switch. Sus ventajas: Fácil de implementar y de ampliar, es muy confiable, debido a que cada terminal tiene su propio canal de transmisión no existe tanto problema con las colisiones. Sus desventajas: El fallo del nodo central implica que toda la red falle, número de nodos limitados por el hardware del nodo central.

Topología de anillo.

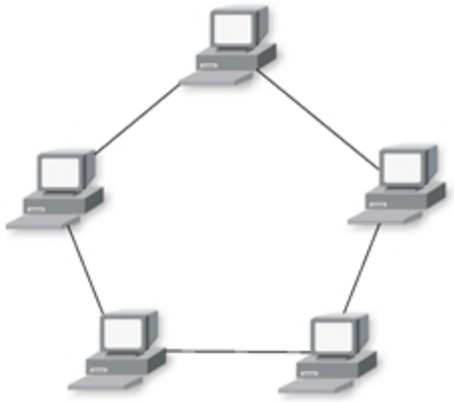


Imagen 3. Diagrama de Conexión tipo Anillo

En esta topología todas las terminales están conectadas a “sus vecinas”, cada una con la siguiente y la anterior, formando un “anillo”, en este tipo de topologías cada estación tiene un repetidor, que pasa la información a la siguiente estación, la comunicación se lleva a cabo mediante el paso de un token, lo que implica que solo una estación puede transmitir a la vez, de esta forma se minimizan las colisiones. También se pueden utilizar variaciones con dos “anillos”, de forma que se tiene comunicación full-duplex y se agrega redundancia, si un “anillo” falla el otro hará su función y la comunicación no se perderá. Sus ventajas: El token minimiza el número de colisiones, es económica y relativamente, su confiabilidad y su desempeño eran considerablemente mayores que los de las otras topologías. Sus desventajas: Si alguna terminal falla todas las terminales quedan incomunicadas, solo se tiene comunicación en una sola dirección, mas costosas que redes mas simples.

Topología de malla.

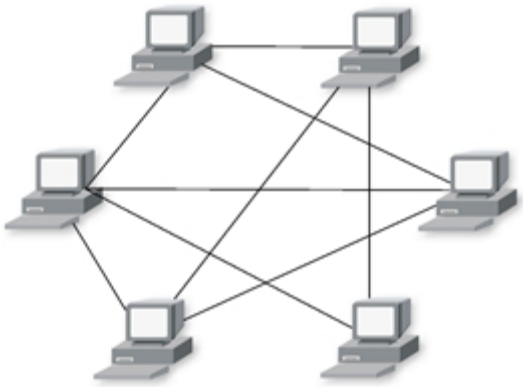


Imagen 4. Diagrama de Conexión tipo Malla

En este tipo de topología todos los nodos están conectados con uno o mas nodos de la red, de tal forma que para llegar a alguna terminal un nodo puede ocupar varios caminos, en el caso en que un nodo o un canal de comunicación falle, los nodos podrán seguir comunicándose mediante el uso de otras rutas. Sus ventajas: Confiable, la falla de un nodo no implica que los demás estén incomunicados, topología no centralizada, de esta forma todas las comunicaciones no dependen solo de una terminal. Sus desventajas: Es costosa, debido al excesivo uso de cables, cada terminal debe tener 2 o mas interfaces para conectarse, no es tan fácil de implementar, debido a que cada nodo debe mantener y actualizar tablas de ruteo para poder establecer las rutas que los paquetes que envía o reenvía deben tomar.

Topología propuesta.

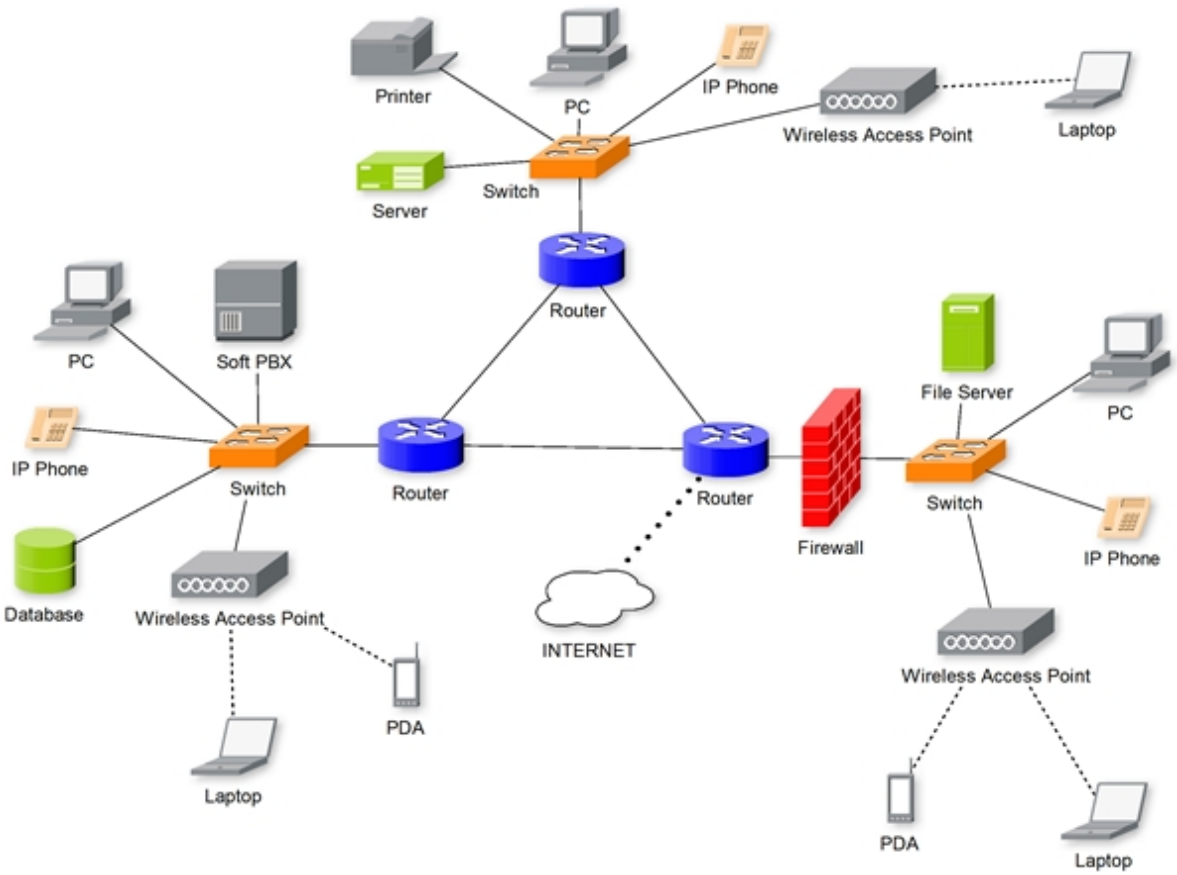


Imagen 5. Diagrama de Conexión propuesta

Se puede observar una topología de anillo en los 3 routers centrales o topología delta, esta con la finalidad de estudiar los algoritmos de ruteo como OSPF o RIP, se pretende desconectar alguno de los cables que comunican a los routers y observar que sucede con las tablas de ruteo de estos, así como con los paquetes. Después de cada router esta colocado un switch, por lo que la topología cambia a estrella, comunicando varios dispositivos como servidores de archivos, teléfonos IP, access points, entre otros de los que se hablará mas adelante.

Capa física.

Cables y medios de transmisión

Esta pensada como la primer parte del curso y se propone que se estudien los distintos tipos de cables y medios de transmisión, en algunos casos, como en el de las conexiones con cable coaxial, conseguir las tarjetas de red puede ser difícil debido a que ya casi no se usan, o en el caso de la fibra óptica, las tarjetas pueden ser costosas.

Tomando en cuenta la importancia que algunos estándares de Ethernet tuvieron en un momento dado, así como mejoras importantes estos son los cables que se propone se armen, conecten y prueben en el laboratorio:

Cable coaxial RG-58, estándar IEEE 802.3a, 10BASE2, introducido en 1985, las redes basadas en este estándar tienen un costo bajo debido a que no necesitan un nodo central, todas las terminales están conectadas al mismo medio de transmisión, pero actualmente las interfaces de red son difíciles de conseguir, se utilizan conectores tipo BNC al inicio y al final del cable y en las conexiones de cada terminal se utiliza un conector BNC tipo T. Solo una estación puede transmitir a la vez, de lo contrario se produce una colisión, su velocidad máxima de transmisión es de 10Mbps

Cable coaxial RG-8X, estándar IEEE 802.3, 10BASE5, introducido en 1980, fue el primer medio que se utilizó para ethernet, su principal beneficio es la longitud que puede alcanzar, de 500m, las tarjetas de red para este tipo de cable son difíciles de encontrar actualmente, transmite en half-duplex para disminuir las colisiones, tiene una velocidad de transmisión de 10Mbps.

Cable de cobre, "par trenzado", estándar IEEE 802.3 (23), 100BASE-T4, longitud máxima de 100m y velocidad de transmisión de 100Mbps, actualmente el más usado para redes locales cableadas, un cable consta de 8 hilos de cobre. Y existen dos estándares para acomodarlos en los conectores RJ-45:

T568A

Los alambres de cobre deben acomodarse de la siguiente forma en el conector RJ-45:

PIN 1	PIN 2	PIN 3	PIN 4	PIN 5	PIN 6	PIN 7	PIN 8
Blanco/Verde	Verde	Blanco/Naranja	Azul	Blanco/Azul	Naranja	Blanco/Café	Café

T568B

Los alambres de cobre deben acomodarse de la siguiente forma en el conector RJ-45:

PIN 1	PIN 2	PIN 3	PIN 4	PIN 5	PIN 6	PIN 7	PIN 8
Blanco/Naranja	Naranja	Blanco/Verde	Azul	Blanco/Azul	Verde	Blanco/Café	Café

En caso de que se quiera conectar un switch o un hub con una computadora, se debe utilizar cualquiera de los dos estándares para los dos extremos del cable (utilizando el mismo estándar para los dos extremos). Si se quiere conectar una computadora con otra computadora o un switch con un router, se debe utilizar un estándar distinto para cada extremo, este tipo de cable se conoce como cable cruzado.

Fibra óptica, IEEE 802.3, 100BASE-FX, dos líneas de fibra óptica multi-modo, logintud máxima de 400m para conexiones half-duplex o de 2 km para full-duplex, tiene una velocidad de 100Mbps

Fibra óptica, IEEE 802.3 TIA, 100BASE-SX, Velocidad de 100 Mbps, longitud máxima de 300 metros, a diferencia de 100BASE-FX no utiliza láseres como fuentes de luz, utiliza LEDs, lo que reduce los costos.

Estándares más actuales permiten alcanzar velocidades de hasta 10Gbps, pero se necesitarán cables e interfaces de red especiales, distintas a las que se tienen en el laboratorio actualmente.

Las prácticas referentes al cableado podrán consistir de tres partes fundamentales:

Reconocimiento del cable, las partes que lo conforman, las precauciones que se deben tener al manipularlo y el equipo necesario para hacerlo.
Armado del cable, estimar las longitudes correspondientes y compararlas con las máximas posibles para cada estándar, agregar los conectores correspondientes, conectar las tarjetas de red apropiadas en las computadoras e instalarlas y conectar los cables a las tarjetas ya instaladas.
Configuración y pruebas, configurar cada computadora con una dirección apropiada para lograr comunicación en la red, y llevar acabo pruebas de velocidad de transmisión máxima, número de colisiones detectadas en la red y longitud máxima de los cables.

Capa MAC

Wi-Fi

Wi-Fi es una marca registrada de la Wi-Fi Alliance y representa un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11 Ha sido desarrollado para proveer conexión a dispositivos móviles como PDAs, teléfonos móviles, laptops, etc. Aunque también puede utilizarse en otros dispositivos como PCs de escritorio o consolas de videojuegos.

Existen tres tipos de estándares aprobados de Wi-Fi, 802.11a, 802.11b y 802.11g, los dos últimos utilizan la banda de 2.4 GHz y tienen una velocidad de 11 y 54 Mbps respectivamente. El 802.11a, también conocido como WiFi 5, opera en la banda de 5 GHz.

Aunque son muchas las ventajas obvias de estos estándares: facilidad para implementar una red con o sin infraestructura, velocidad de transmisión aceptable, posibilidad de estar conectado en cualquier lugar sin la necesidad del cable de ethernet y movilidad. También cuenta con desventajas, algunas con las que se podría experimentar:

Captura de paquetes

El medio de transmisión de estos estándares es el espectro radioeléctrico y cuentan con un alcance de 30 metros, por lo que cualquier persona que se encuentre dentro del alcance de

transmisión y que cuente con una tarjeta y equipo de cómputo puede “ver” los paquetes que alguien este enviando o recibiendo por la red ya que los dos están compartiendo el medio. Esto se conoce como eavesdropping, y es un grave problema de seguridad en este tipo de redes debido al tipo de información que puede ser enviada, contraseñas, datos de cuentas, datos privados, etc. Sin embargo en algunos access points ya se encuentra implementada la opción de encriptar todo el tráfico, se propone hacer una práctica que consista en dos partes, la primera escuchar el tráfico no encriptado y reconocer datos e información importante. La segunda parte, consiste en encriptar el tráfico y capturarlo en otra computadora, de esta forma se verán las ventajas de encriptar el tráfico. Se requieren dos computadoras con tarjetas inalámbricas y un access point que nos permita acceder a internet.

Obtención de la semilla WEP.

Para evitar que alguien este “escuchando” la transmisión la encriptan de forma que aunque alguien la escuche no pueda descifrar los mensajes. Uno de las formas mas comunes en que se encriptan los datos es mediante el protocolo WEP, el cual se basa en el algoritmo de cifrado RC4 y el algoritmo de chequeo CRC. RC4 funciona mediante una semilla que genera una secuencia de números pseudo aleatorios de mayor tamaño a la que se le aplica la operación XOR junto con el mensaje para obtener el mensaje cifrado. El principal problema con este algoritmo es que al usar dos o más veces la misma semilla para cifrar los mensajes, la obtención de esta semilla se vuelve trivial, esto se trató de resolver mediante un vector de inicialización de 24 bits que es regularmente modificado y se concatena a la contraseña, esto genera el nuevo seed, pero a pesar de que se puedan crear muchos seeds a partir de esta concatenación, cuando la cantidad de paquetes que pasan por el access point aumenta, la posibilidad de que se encuentren dos o mas mensajes cifrados con la misma seed también aumenta.

Existen además, otro tipo de prácticas que se podrían llevar a cabo más relacionadas con el estudio de la tecnología:

Redes Ad-Hoc y con infraestructura

A partir de dos o mas dispositivos con tarjeta inalámbrica se puede crear una red Ad Hoc o red independiente, en este tipo de redes las terminales se comunican directamente entre sí y no requieren de un switch o un router inalámbrico para poder ser montadas.

Las redes con infraestructura si requieren un Access Point para poder existir, esté les permitirá además de comunicarse entre ellas poder comunicarse con una o varias redes externas como Internet.

Se propone una práctica en la que se monten los dos tipos de redes mencionadas antes.

Mobile IP

Mobile IP fue creado para soportar movilidad en los Hosts conectados a una red inalámbrica, estos pueden permanecer conectados a la red a pesar de su ubicación geográfica, incluso pueden mantener la misma dirección de capa 3 sin necesidad de permanecer en el mismo lugar de la red, esto les da verdadera movilidad, para realizar una práctica de este tipo será necesario contar con 2 Access Point, 2 computadoras con Linux instalado, 1 laptop con linux instalado y tarjetas inalámbricas.

Bluetooth.

Bluetooth es una tecnología de comunicaciones de corto alcance, permite liminar los cables entre algunos dispositivos y sus accesorios, por ejemplo, existen teclados, ratones y camaras web con bluettoth para comunicarse con una computadora, existen auriculares, manos libres e incluso relojes para comunicarse con un celular. Permite intercambiar archivos, tarjetas de negocio, sincronizar agendas, etc. Tiene un alcance de 10 a 100 metros dependiendo en el tipo de radio que se utilice, funciona en la frecuencia de los 2.4GHz, los radios utilizan saltos en frecuencia, comunicación full-duplex, la señal salta entre 79 frecuencias en intervalos de 1 MHz lo que provee inmunidad a la señal, la velocidad máxima es de 720 kb/s.

Los beneficios de las comunicaciones con bluetooth son muy conocidos entre dispositivos, sin embargo, no es muy común encontrar redes bluetooth que cuenten con un access point bluetooth, mencionado en el capitulo II, requerimientos de hardware, por medio de este, distintos dispositivos bluetooth se pueden comunicar con otras redes e incluso acceder a recursos compartidos, como archivos, impresoras, etc. Como práctica se puede establecer el access point bluetooth y configurarlo para permitir conexiones entrantes, analizar los paquetes enviados y recibidos, reconocer mensajes de establecimiento de red, etc. Lamentablemente el Posgrado en Ciencias e Ingeniería de la Computación no ha podido conseguir este dispositivo para el laboratorio de redes.

Capa de Red.

Esta capa es la tercer capa, según el modelo OSI, y proporciona conectividad entre dos o más terminales a pesar de que estén en distintos lugares geográficos, o en distintas redes, se encarga de encaminar los datos por medio de uno o de distintos canales, seleccionando alguno por medio de criterios, que pueden ser saturación del enlace, costo del enlace, número de saltos para llegar al destino.

RIP

Routing Information Protocol, es un protocolo que utiliza el número de saltos como métrica, implementa un algoritmo de vector de distancias. RIP es ampliamente usado para rutear paquetes y es un protocolo IGP (Interior Gateway Protocol), lo que significa que realiza el ruteo dentro de un sistema autónomo, AS por sus siglas en inglés. Un sistema

autónomo es un conjunto de redes dentro de la misma administración que comparten las mismas estrategias de ruteo. La última mejora de RIP es RIPv2, que permite que más información pueda ser incluida en los paquetes de RIP y mecanismos de autenticación.

Cisco ha implementado RIP en algunos de sus equipos, incluidos los que se mencionan en el capitulo II en la sección de requerimientos de hardware. Por lo que se propone que una práctica, que se presentará en el capitulo V, consista en la configuración de este protocolo, para tres distintas redes.

OSPF

Open Shortest Path First (OSPF), es un protocolo de ruteo de enlace-estado, que "pregunta" por el envio de LSAs (Link State Advertisements), Anuncios de Estado de Enlace, a los demás routers dentro de la misma área jerárquica. Estos anuncios incluyen información de las interfaces de cada router, la métrica utilizada y otras variables. Como los routers que utilizan OSPF acumulan información del estado del enlace, utilizan el algoritmo del camino más corto primero (SPF, Shortest Path First), para calcular el camino mas corto hacia cada nodo. Puede operar con seguridad con MD5 para autenticar a sus puntos, antes de enviar o recibir anuncios de estado de enlace.

De la misma manera que RIP, OSPF ha sido implementado por Cisco en una gran cantidad de routers, incluyendo los mencionados en el capitulo II en la sección de requerimientos de hardware. También se propone una práctica de configuración de OSPF en estos routers, además de observar que sucede con las tablas de ruteo cuando se modifica el estado de los enlaces.

NAT

NAT, Network Address Translation, permite que redes privadas IP que utilizan direcciones no registradas puedan acceder a otras redes como Internet. NAT opera en los routers, usualmente conectando dos redes, y traduce las direcciones privadas de la red interna en direcciones públicas antes de enviar paquetes a otra red. NAT puede ser configurado para anunciar solo una dirección de la red interna hacia el exterior, esto provee seguridad adicional al ocultar la red interna detrás de esta dirección.

Cisco ha implementado NAT en sus routers y existen diferentes formas de habilitarlo y configurarlo como IOS o por medio de la interfaz gráfica, de los dos métodos se hablará mas adellante.

VoIP.

VoIP, Voice over IP, define una forma de transportar llamadas de voz sobre una red IP incluyendo la digitalización y el empaquetado de las ráfagas de voz. La telefonía IP utiliza los estándares de VoIP para crear un sistema de telefonía donde se puedan utilizar

características avanzadas como direccionamiento de llamadas, correos de voz, centros de contactos, etc.

SIP (Session Initiation Protocol), es un protocolo de señalización punto a punto, desarrollado por la IETF. Utiliza protocolos IP existentes, como DNS, para establecer y terminar las llamadas. Desde su primer publicación en 1999, SIP ha generado un gran interés en la industria de VoIP.

A pesar de que no fueron pedidos teléfonos IP para el laboratorio de posgrado, en las últimas semanas del semestre 2007-1. se adquirieron 3 teléfonos IP con los que se pueden desarrollar prácticas, una propuesta es utilizar el software Asterisk, de código libre, con el fin de implementar un PBX basado en Software.

Wireless

Wireless es un término utilizado para describir un tipo de telecomunicaciones en las que las ondas electromagnéticas son el canal de comunicaciones en lugar de un cable, se encargan de llevar la señal hasta su destino. Algunos ejemplos de equipo inalámbrico utilizado hoy en día son: Teléfonos celulares, Sistemas de Posicionamiento Global (GPS, por sus siglas en inglés, Global Positioning System), Accesorios periféricos de las computadoras, televisión por satélite, redes inalámbricas de área local, etc.

GPS

GPS, Global Positioning System, es un sistema global de navegación por satélite que permite determinar en todo el mundo la posición de una persona, vehículo u objeto que cuente con un receptor, el cual calcula su posición al medir la distancia que existe entre sí mismo y tres satélites o más satélites GPS, midiendo el retraso de tiempo que existe entre la transmisión y la recepción de cada señal de radio GPS. Las señales además llevan información de la posición del satélite. Al determinar la posición de los satélites y la distancia hacia estos, el receptor puede calcular su posición por medio de triangulación.

Entre el equipo solicitado al Posgrado, se encuentran 4 receptores GPS que pueden transmitir información a aun computadora o a un dispositivo por medio de bluetooth, lo que los hace muy fácil de llevar a cualquier parte, se pueden utilizar lap-tops con Linux e instalar software como GPSDrive o GPS Bluetooth para recibir lecturas de la posición actual, este tipo de programas es de código abierto y para nuestro país no existen muchos mapas ni rutas, por lo que se pueden modificar estos programas para mostrar rutas dentro de Ciudad Universitaria o cualquier otro lugar del país o del mundo.

GPRS

GPRS, General Packet Radio Service, aumenta la capacidad de la velocidad de GPS y principalmente soporta transferencia de datos en forma intermitente o de ráfaga. Las velocidades ofrecidas al cliente son similares a las de ISDN (de 64 a 128 kbps).

Uno de los usos más comunes de GPRS es proveer acceso a Internet a cualquier dispositivo que pueda comunicarse con un teléfono celular, por ejemplo:

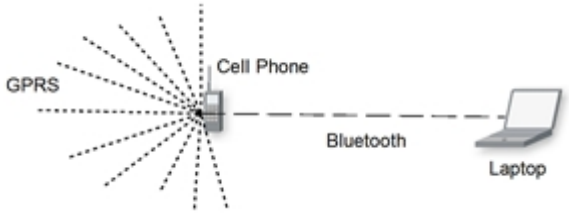


Imagen 6. Diagrama de conexión GPRS-Celular-Bluetooth-LapTop

Una Laptop se comunica por medio de bluetooth con un teléfono celular, la Laptop le solicita información de una página Web, el teléfono celular solicita y recibe esta información por medio de GPRS y se la envia a la Laptop por medio de Bluetooth, de esta forma se logra que la Laptop realmente este conectada a Internet en cualquier lugar, no importa que no haya un Access Point o que no se tenga acceso a uno, simplemente se necesita cobertura de un operador celular y que este provea el servicio GPRS. Este tipo de acceso se puede configurar a través de Windows o Linux, por lo que se propone una práctica en la que se configure GPRS en los dos sistemas y se documenten las diferencias en configuración y en desempeño.

Seguridad.

En los últimos años ha aumentado el número de profesionales en el área de seguridad en redes. Compañías, gobiernos y organizaciones buscan proteger su información de hackers, e intrusos que amenazan la integridad de sus datos y de sus operaciones.

La idea de enseñar fundamentos de seguridad en redes es educar a los alumnos en diseño e implementación de medidas que permitan disminuir el riesgo de perdida de información.

Sniffers.

Un sniffer es un programa que se utiliza para capturar las tramas de red que viajan en un medio de transmisión, este puede ser cable coaxial, UTP, espectro radioeléctrico, etc. Generalmente se utilizan para administrar la red, observar posibles errores de configuración, con finalidades docentes ya que se pueden observar las cabeceras y el contenido de los paquetes, pero también se usan con fines maliciosos ya que en el

contenido de los paquetes puede haber información importante como contraseñas o datos privados.

Los sniffers funcionan configurando la tarjeta de red en modo “promiscuo”, al hacer esto la tarjeta captura todos los paquetes que viajan en el medio en el que este conectada la tarjeta, no importa si están o no dirigidos a ella, los datos capturados son analizados por el sniffer que separa las cabeceras de los datos y los muestra en pantalla.

Es importante hacer notar que los sniffers funcionan solo en redes en las que el medio de transmisión es compartido por todas las terminales como en redes con cable coaxial o redes inalámbricas, en redes con UTP cuyo nodo central es un Hub, debido a que este repite la señal que recibe a todos los nodos, sin embargo, si el nodo central es un switch no existirá este problema porque el switch reenvía los datos solo al nodo destino.

Se propone una práctica en la que se implementen dos redes, una con un hub con nodo central y otra con un switch, en las dos existirá un nodo con un sniffer instalado y corriendo, los alumnos deberán capturar el tráfico y analizarlo, que tipo de protocolos pueden reconocer y los datos que observan. Como segunda parte en la red con un Hub como nodo central se deberá encriptar el tráfico y volver a observar con el sniffer, de esta forma a pesar de que se puedan recibir los paquetes en cualquier nodo, la información ya no será visible.

VPN

VPN, Virtual Private Network, una Red Privada Virtual utiliza Internet para conectar oficinas remotas, trabajadores, socios y compañeros a los recursos de una red privada. Es una manera confiable de mantener la privacidad de los datos y al mismo tiempo compartirlos con las personas adecuadas. Una VPN encripta el tráfico antes de enviarlo por la red pública y lo desencripta al recibirlo, la información encriptada viaja a través de un “tunel” seguro que se conecta con el gateway de la red que recibe los datos. El gateway identifica al usuario remoto y entonces lo deja acceder solo a la información a la que esta autorizado a recibir.

Una VPN se puede establecer desde los Routers Cisco e incluso desde una computadora con Linux, lo que reduce significativamente los costos de Hardware.

Para configurar una VPN por medio de los routers Cisco, se puede utilizar IOS, la interfáz gráfica e incluso SNMP, de los que se hablará mas adelante.

Para configurar una VPN por medio de una computadora con Linux se necesita del Software de acceso libre OpenVPN, instalar y configurar las interfaces de red que funcionarán como gateways.

De este tema se proponen dos prácticas de configuración de VPN, una utilizando los Routers Cisco y otra por medio de Linux.

RADIUS.

RADIUS, Remote Authentication Dial-In User Server, Es un protocolo de autenticación, autorización y manejo de cuentas. Es usado principalmente por ISPs, aunque también puede utilizarse por cualquier red que necesite autenticación manejo de cuentas centralizadas.

RADIUS utiliza UDP como protocolo de capa inferior. El puerto registrado para hacer esto es: 1812. En este caso se recomienda utilizar FreeRadius, un servidor de código libre de RADIUS, es rápido, flexible, configurable y soporta mas protocolos de autenticación que cualquier servidor comercial. Incluye soporte para SQL, LDAP, Radius Proxying, etc. Actualmente se encuentra en la versión 1.1.

Levantar y configurar servidores Radius es una tarea que ya se lleva a cabo en el Posgrado, ya que no requiere mas que una computadora que funcione como servidor y una computadora que funcione como cliente. Esta práctica también podría agregarse al laboratorio.

Capitulo III
Implementación.

A inicios del semestre 2006-1 el laboratorio de Posgrado ya contaba con parte del equipo solicitado para iniciar las prácticas y las configuraciones. Debido a la disponibilidad parte de ese equipo, específicamente los 3 Routers Cisco 2611 XM no fueron adquiridos, en su lugar se adquirieron 3 routers Cisco 2811.

Cabe mencionar que hasta ese momento yo no contaba con los conocimientos necesarios para configurar el equipo, así que los meses siguientes fueron de mucho estudio y experimentación. En este capitulo pretendo explicar, en base a lo que aprendí de esos meses, las principales características y las distintas formas de configurar los 3 switches Cisco Catalyst 2950 y los 3 routers Cisco 2811 que llegaron al Posgrado en Ciencias e Ingeniería de la Computación.

Cisco 2811 Integrated Service Router.

El Router Cisco 2811 de Servicios Integrados es parte de la serie 2800 de Routers de Servicios Integrados de Cisco.

Este Router provee:

- Desempeño de alta velocidad para servicios concurrentes como seguridad y voz
- Modularidad, lo que permite que se le puedan agregar nuevas funciones
- Cuatro ranuras para interfaces WAN de alta velocidad
- Una ranura para modulo de mejora de desempeño en red
- Soporte para mas de 90 módulos nuevos y existentes
- Dos puertos 10/100 Fast Ethernet integrados
- Soporte para PoE opcional
- Seguridad
    - Encriptación integrada
    - Soporte de hasta 1500 “túneles” VPN con el módulo AIM-EPII-PLUS
    - Defensa Antivirus a través del NAC, Network Admission Control
    - Prevención de intrusos así como un Firewall completamente operativo por medio de IOS

- Voz
    - Soporte para llamadas de voz análogas y digitales
    - Soporte opcional para correo de voz
    - Soporte Opcional para Cisco CallManager Express (Cisco CME) para procesamiento local de llamadas para un máximo de 36 teléfono IP

En la imagen 7, los 3 routers Cisco 2811 montados en su rack en el Posgrado en Ciencias e Ingeniería de la Computación.

Cisco 2950 Catalyst Switch

La serie de Switches Cisco Catalyst 2950 provee conectividad a velocidad de Fast Ethernet y Gigabit Ethernet. Este Switch ofrece dos distintos tipos de características de Software y una gran gama de configuraciones para permitir que redes pequeñas, medianas y grandes elijan la que mejor se ajuste a sus necesidades.

La imagen de software estándar es Cisco IOS, que provee funciones para datos básicos, voz y servicios de video. Para redes con requerimientos de seguridad adicional, calidad de servicio y una alta disponibilidad. Algunas características son: Capacidad de limitar la tasa de transmisión en una interfaz y filtrado de paquetes.

El Cisco Network Assistant (Asistente de Redes Cisco), es una aplicación gratuita para administración centralizada que simplifica la tarea de gestionar los router, switches y access points Cisco, ofrece una interfaz gráfica amigable para configurar, solucionar problemas y monitorear la red fácilmente.

En la imagen 8: dos de los tres Switches Cisco Catalyst 2950 con sus Paneles de Parcheo del Posgrado en Ciencia e Ingeniería de la Computación.

Cisco IOS Command Line Interface.

Entender y manejar Cisco IOS es esencial para el diseño, la implementación y administración de las redes con equipo Cisco.

Actualmente IOS opera en millones de sistemas activos, desde routers de pequeñas oficinas a sistemas complejos, es el Software de operación de redes mas distribuido en el mundo.

Optimizado para las redes actuales basadas en IP, extremadamente flexible, adaptable y escalable, Cisco IOS puede correr en Hardware avanzado y complejo o en sistemas simples con un solo procesador

Cisco IOS minimiza costos operacionales, maximiza el retorno de la inversión y mejora la productividad de los negocios.

- Minimiza la necesidad de nueva infraestructura. La expansión continua y la flexibilidad te permiten adaptarlo a nuevas necesidades

- Aumenta la productividad de una organización. Permite acceso a aplicaciones críticas de una manera confiable y sin importar la hora o el lugar.
- Protege la red de eventos maliciosos o de errores humanos. Minimiza los costos por soporte.

Cisco IOS sufre constantes mejoras con el tiempo para cumplir con las necesidades de cualquier red. IOS tiene una familia de distribuciones que junta cuenta con una gran diversidad de características y un gran número de dispositivos de hardware soportados.

La siguiente tabla muestra las distribuciones de IOS:

Tipo	Distribución	Descripción
IOS T	Maintenance Release 12.3 Maintenance Release 12.4	Las distribuciones de mantenimiento ayudan a solucionar algunos problemas de software. No se agrega soporte a Hardware en este tipo de distribuciones.
	Release 12.4 T	Provee soporte para Seguridad, Voz e inalámbricos para redes empresasariales, de acceso y comerciales.
IOS S	Release 12.2SB	Provee funcionalidad de software y hardware para aplicaciones de Banda ancha, MPLS. Diseñada para un rango de routers para redes de proveedores de servicio.
	Release 12.2SX	Proveen funcionalidad de software y hardware para redes Ethernet de área local, funcionalidad de Switch para redes centrales y de datos.
	Release 12.2SE Release 12.2SG	Proveen funcionalidad de hardware y de software para un rango de Switchs Ethernet LAN para redes distribuidas.
	Release 12.2SR	Provee funcionalidad de hardware y software para MPLS.
IOS XR	Release 3.2	Provee funcionalidad de hardware y software para el Cisco CRS-1 (Sístema de Ruteo de Portadoras) y la seri de Routers Cisco XR 1200. Diseñado para alcanzar velocidades de Terabit, cirtualización segura, alta disponibilidad y requerimientos de procesamiento distribuido de grandes redes de siguiente generación.

Cisco SDM Security Device Manager

Cisco SDM, es una herramienta WEB de administración diseñada para los routers Cisco capaz de aumentar la productividad de los administradores de red, simplificando las implementaciones y ayudando a resolver los problemas creados por redes complejas.

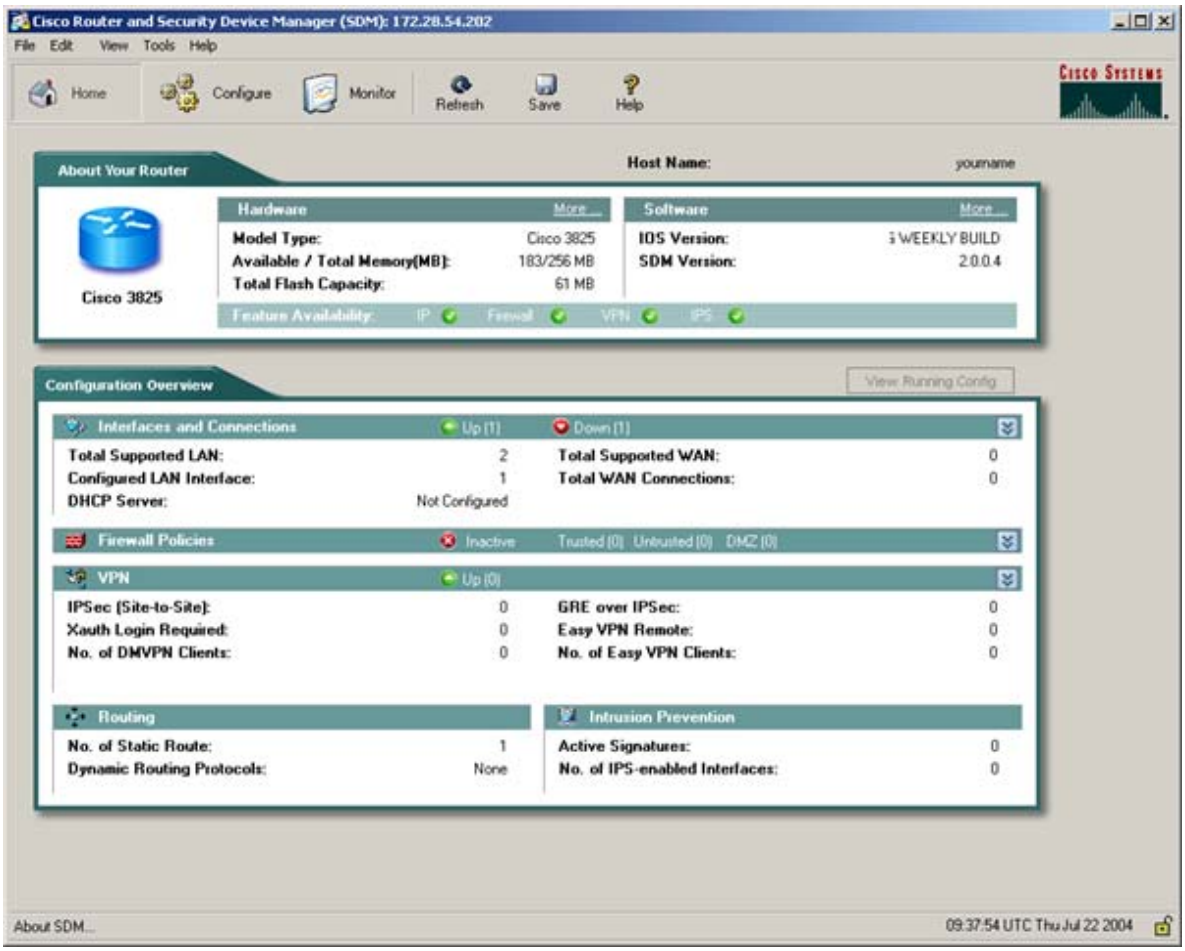
Soporta un gran rango de distribuciones IOS y esta disponible de forma gratuita en la serie de routers Cisco 830 a Cisco 7301. Se encuentra preinstalado en toda la serie de routers Cisco 850, Cisco 870, Cisco 1800, Cisco 2800 y Cisco 3800.

Cisco SDM se puede utilizar para implementar de una forma mas fácil y rápida servicios como ruteo dinámico, Acceso a redes WAN, WLAN, firewalls, VPNs, SSL, IPS y calidad de servicio.

Cuando se utiliza Cisco SDM para configurar un router la instrucción que se envía a este es una instrucción previamente revisada y aceptada por Cisco. SDM además muestra el monitoreo del router en estadísticas de desempeño, registros del sistema y registros del firewall en tiempo real

Cisco SDM ofrece asistentes para configuraciones de interfaces LAN y WAN, NAT, políticas de firewall, IPS, IPSec VPN y QoS. El asistente del firewall permite que por medio de un solo paso se puedan configurar políticas para seguridad alta media o baja.

Cisco SDM es una gran herramienta para hacer que la configuración y la implementación de red sea mucho más sencilla.



En la imagen 9: Una pantalla de Cisco SDM, mostrando, en la parte superior, estadísticas del estado de un router (modelo, memoria total y disponible, versión de IOS y de SDM), en la parte media e inferior la configuración (Interfaces conectadas y soportadas, políticas de firewall, configuración de VPN y configuración de ruteo).

Capitulo IV
Puesta en marcha.

En el semestre 2007-1 se empezaron a dar clases en el laboratorio de redes utilizando el equipo nuevo (routers, switches, PDAs, etc), con el Dr. Javier Gómez Castellanos como profesor, con su asesoría escribí las primeras prácticas:

Prácticas de laboratorio

Practica I

Configuración básica usando IOS

Introducción

Este documento describe cómo utilizar la interfaz de línea de comandos de Cisco IOS para realizar una configuración básica.

Plataformas soportadas

Cisco 1800 series routers
Cisco 2800 series routers
Cisco 3800 series routers

Prerrequisitos para la configuración básica usando la interfaz de línea de comandos cisco IOS

Es importante solamente tener conectados el cable de alimentación a la corriente y el cable RJ45 a DB9 del router a la computadora (Cable azul incluido con el equipo)

Configurando la terminal

El cable RJ45 a DB9 debe estar conectado al panel frontal del router, la interfaz marcada como terminal conectada al conector RJ45 y el conector DB9 a la computadora. En una computadora con Windows abrimos el programa Hyperterminal desde el menú de inicio, accesorios, comunicaciones.

Una vez iniciado el programa Hyperterminal, creamos una nueva conexión con cualquier nombre, es importante establecer que el puerto de comunicación será COMx, donde x es el numero de interfaz serial, generalmente 1 o 2, establecemos también, Bits por segundo en 9600, Bits de datos en 8, Paridad Ninguno, Bits de parada 1 y Control de Flujo Ninguno.

Hemos establecido una conexión permanente con nuestro router. Iniciaremos la configuración desde cero, por lo que se recomienda borrar cualquier configuración existente, lo hacemos con los comandos:

router> ***enable***
router# ***erase startup-config***
router# ***reload***

El router se reiniciara y nos preguntará si deseamos entrar al asistente de configuración, a lo que responderemos no.

Would you like to enter the inicial configuration dialog? [yes/no] : ***no***

Configurando el Hostname

El hostname se utiliza en el prompt de la interfaz de línea de comandos y en los nombres por default de los archivos de configuración. Sí no configuras un hostname, el router usa el hostname por default: "Router"

El hostname debe empezar con una letra, terminar con una letra o dígito y tener como caracteres interiores solo letras y guiones. Deben de ser de 63 caracteres o menos.

Los comandos son:

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#configure terminal	Entra al modo de configuración global
Paso 3	#hostname mirouter	Lista o modifica el hostname del equipo
Paso 4	Verificar el prompt con el nuevo hostname	
Paso 5	#end	(Opcional) Regresa el modo privileged EXEC

Configurando las contraseñas para enable y enable secret

Para proporcionar una capa adicional de seguridad, particularmente para contraseñas que viajan por la red o que son almacenadas en un servidor TFTP, se puede utilizar el comando *enable password* o el comando *enable secret*. Ambos comandos cumplen la misma función, permiten establecer una contraseña encriptada que los usuarios deben ingresar para cambiar al modo privileged EXEC.

Se recomienda utilizar el comando *enable secret* porque utiliza un algoritmo de encriptación mejorado. Utiliza el comando *enable password* solamente sí estas utilizando una imágen antigua del IOS que no reconozca el comando *enable secret.*

Sí configuras el comando *enable secret,* tiene preferencia sobre el comando *enable password* , los 2 comandos no pueden estar simultáneamente.

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#configure terminal	Entra al modo de configuración global
Paso 3	#enable password contraseña	(Opcional) Establece una contraseña para controlar el acceso a varios niveles privilegiados
Paso 4	#enable secret contraseña	Establece una contraseña para controlar el acceso a varios niveles privilegiados
Paso 5	#end	(Opcional) Regresa el modo privileged EXEC
Paso 6	#enable	Habilita el modo privileged EXEC, verifica que tu contraseña funcione.
Paso 7	#end	(Opcional) Regresa el modo privileged EXEC

Configurando las interfaces Fast Ethernet y Gigabit Ethernet.

Esta sección muestra como configurar una dirección IP y una descripción a alguna interfaz en el router.

Cada interfaz tiene asignado un nombre y un número para identificarlas, las interfaces incluidas en los routers 2811 son FastEthernet, al igual que las interfaces de las tarjetas agregadas. Las interfaces incluidas en el router son FastEthernet0/0 y FastEthernet0/1, dependiendo del puerto. Las interfaces de las tarjetas agregadas son FastEthernet0/0/0, FastEthernet0/0/1, FastEthernet0/0/2 y FastEthernet0/0/3.

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#show ip interface brief	Despliega una descripción, status y configuración
Paso 3	#configure terminal	Entra al modo de configuración global
Paso 4	#interface {fastethernet | gigabitethernet} 0/port	Especifica la interfaz Ethernet y entra al modo de configuración
Paso 5	#description texto	(Opcional) Agrega una descripcion a alguna interfaz
Paso 6	#ip address dir.ip mascara	Establece la dirección y máscara de una interfaz
Paso 7	#no shutdown	Habilita la interfaz
Paso 8	#end	(Opcional) Regresa el modo privileged EXEC
Paso 9	#show ip interface brief	Despliega una descripción, status y configuración

Ejemplo

```
!
interface FastEthernet0/0
 description primer interfaz del router
 ip address 192.168.26.2 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
```

Configurando VTL (Virtual Terminal Lines) para acceso remoto a la consola.

Las terminales virtuales se usan para permitir acceso remoto al router. Esta sección explica como configurar las terminales con una contraseña para que solo usuarios autorizados puedan acceder.

El router tiene 5 terminales por default, sin embargo, se pueden crear terminales adicionales.

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#configure terminal	Entra al modo de configuración global
Paso 3	#line vty numero-de-linea	Inicia el modo de configuración de alguna linea
Paso 4	#password contraseña	Establece la contraseña para una linea
Paso 5	#login	Habilita la autenticación para la linea
Paso 6	#end	Regresa el modo privileged EXEC
Paso 7	#show running-config	Despliega información de la configuración actual
Paso 8	Desde otro dispositivo de la red intenta abrir una conexión telnet hacia el router	Verificar remotamente que se puede acceder al router

Verificando conectividad de la red

Es necesario que el router tenga configurada por lo menos una interfaz y que está este conectada a un host.

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#ping [dir-ip | hostname]	Diagnostica conectividad basica de red
Paso 3	#telnet {dir-ip | hostname}	Intenta ingresar a algun host que soporte telnet

Ejemplo:

```
Router# ping

Protocol [ip]:
Target IP address: 192.168.7.27
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

Guardando tu configuración.

Esta sección describe como evitar perder tu configuración cuando se reinicie el sistema, almacenándola en el archivo de configuración inicial en la NVRAM

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#copy running-config startup-config	Almacena la configuración actual a la configuración de inicio

Guardando respaldos de tu configuración e imágenes del sistema.

Siempre es recomendable guardar respaldos del archivo de configuración e imágenes de IOS.

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#copy nvram: startup-config {ftp: | rcp: | tftp: }	Copia el archivo de configuración inicial hacia algun servidor
Paso 3	#show flash	Despliega el formato y contenido del archivo de memoria flash
Paso 4	#copy flash: {ftp: | rcp: | tftp: }	Copia un archivo desde memoria flash hacia el servidor

Ejemplo:

Copiando el archivo de la configuración de inicio hacia un servidor TFTP.

```
Router# copy nvram:startup-config tftp:

Remote host[]? 192.168.7.17

Name of configuration file to write [rtr2-confg]? <cr>
```

```
Write file rtr2-confg on host 172.16.101.101?[confirm] <cr>
![OK]
```

Anexo de práctica I

Procedimiento de recuperación de contraseñas.

Este documento describe el procedimiento para recuperar las contraseñas enable y enable secret. Estas contraseñas son utilizadas para acceder al modo privilegiado y configuraciones. La contraseña enable puede ser recuperada pero enable secret no debido a que esta encriptada, esta solo puede ser reemplazada por una nueva.

Por seguridad, para llevar a cabo este procedimiento es necesario tener acceso físico al equipo.

El siguiente procedimiento funciona para los equipos:

Cisco 806	Cisco 4700	Catalyst 2948G-L3
Cisco 827	Cisco AS5x00	Catalyst 4840G
Cisco uBR900	Cisco 6x00	Catalyst 4908G-L3
Cisco 1003	Cisco 7000 (RSP7000)	Catalyst 5500 (RSM)
Cisco 1004	Cisco 7100	Catalyst 8510-CSR
Cisco 1005	Cisco 7200	Catalyst 8510-MSR
Cisco 1400	Cisco 7500	Catalyst 8540-CSR
Cisco 1600	Cisco uBR7100	Catalyst 8540-MSR
Cisco 1700	Cisco uBR7200	Cisco MC3810
Cisco 2600	Cisco uBR10000	Cisco NI-2
Cisco 3600	Cisco 12000	Cisco VG200 Analog Gateway
Cisco 4500	Cisco LS1010	Route Processor Module
Cisco 1800	Cisco 2800	Cisco3800

Procedimiento.

1. Conecta el cable RJ45 a DB9 del puerto de consola del router hacia la PC. Utiliza la siguiente configuración:

   9600 baud rate

   No parity

   8 data bits

   1 stop bit

   No flow control

2. Si aún tienes acceso al router, escribe el comando **show version,** y escribe en una hoja el valor del registro de configuración, usualmente es 0x2102 ó 0x102

3. Si no cuentas con acceso al router (debido a que perdiste tu login), puedes considerar que el valor de registro es 0x2102

4. Utiliza el switch de energía para apagar y volver a encender el router.

5. Dependiendo del software que uses para la comunicación, la plataforma y el sistema operativo, presiona la tecla o la combinación correspondiente durante 60 segundos mientras el router lleva a cabo el proceso de encendido para ponerlo en modo ROMMON

Software	Platform	Operating System	Try This
Hyperterminal	IBM Compatible	Windows XP	Ctrl-Break ó Break
Hyperterminal	IBM Compatible	Windows 2000	Ctrl-Break
Hyperterminal	IBM Compatible	Windows 98	Ctrl-Break
Hyperterminal (version 595160)	IBM Compatible	Windows 95	Ctrl-F6-Break
Kermit	Sun Workstation	UNIX	Ctrl-\l Ctrl-\b
MicroPhone Pro	IBM Compatible	Windows	Ctrl-Break
Minicom	IBM Compatible	Linux	Ctrl-a f
ProComm Plus	IBM Compatible	DOS or Windows	Alt-b
SecureCRT	IBM Compatible	Windows	Ctrl-Break

Telix	IBM Compatible	DOS	Ctrl-End
Telnet	N/A	N/A	Ctrl-], then type **send brk**
Telnet to Cisco	IBM Compatible	N/A	Ctrl-]
Teraterm	IBM Compatible	Windows	Alt-b
Terminal	IBM Compatible	Windows	Break Ctrl-Break
Tip	Sun Workstation	UNIX	Ctrl-], then Break or Ctrl-c ~#
VT 100 Emulation	Data General	N/A	F16
Windows NT	IBM Compatible	Windows	Break-F5 Shift-F5 Shift-6 Shift-4 Shift-b (^$B)
Z-TERMINAL	Mac	Apple	Command-b
	Break-Out Box	N/A	Connect pin 2 (X-mit) to +V for half a second
	Cisco to aux port	N/A	Control-Shft-6, then b
N/A	IBM Compatible	N/A	Ctrl-Break

6. Escribe **confreg 0x2142** en el prompt *rommon 1>* para bootear desde la memoria Flash sin cargar la configuración.

7. Escribe **reset** en el prompt *rommon 2>* El router se reinicia pero ignora la configuración salvada.

8. Escribe **no** después de cada pregunta de la configuración inicial o **ctrl-c** para saltarse el procedimiento de configuración inicial.

9. Escribe **enable** en el prompt *Router>* Debe aparecer el prompt *Router#*

10. **Importante.** Escribe **configure memory** o **copy startup-config running-config** para copiar la NVRAM en la memoria. No ingreses **configure terminal**

11. Ingresa **write terminal** o **show running-config.** El commando show running-config y write terminal muestran la configuración del router. En esta configuración se pueden ver en las interfaces el comando shutdown, que significa que las interfaces están apagadas, además puedes ver las contraseñas (enable password, enable secret, vty, console passwords) encriptadas o no, según corresponda. Las contraseñas que no están encriptadas se pueden seguir utilizando, las encriptadas tendrán que ser reestablecidas.

12. Escribe **configure terminal** y haz la configuración. El prompt debe verse: **hostname(config)#**

13. Escribe **enable secret <password>** para cambiar la contraseña enable secret

14. Escribe **config-register 0x2102,** o el valor que guardaste en el paso 2.

15. Presiona **ctrl.+z** o escribe **end,** para salir del modo de configuración. El prompt debe verse: hostname#

16. Escribe **write memory** o **copy running-config startup-config,** para guarder los cambios

Practica II

Configuración de Router Information Protocol en Cisco IOS

Introducción

Este documento describe como configurar tres routers en una topología de red simple, a diferencia de los switches.

RIP es un protocolo distance-vector, que emplea el número de saltos como métrica de ruteo. El número máximo de saltos permitido por RIP es de 15, cada routeador RIP transmite, por default, actualizaciones de sus tablas cada 30 segundos, utiliza UDP por el puerto 520 para entregar los paquetes.

Comparado con otros protocolos de ruteo como EIGRP, OSPF o IS-IS, RIP tiene un tiempo de convergencia muy alto, por lo que se considera obsoleto en comparación con estos.

Prerrequisitos

Tener una terminal conectada y configurada por cada uno de los 3 routers.
No tener ninguna configuración en los equipos.

Antes de iniciar cualquier configuración es recomendable que establezcas tu consola en modo síncrono, lo que te servirá en el caso de que el router necesite mostrar información, esta no interrumpa el comando que tu estas ingresando.

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#configure terminal	Entra al modo de configuración global
Paso 3	#line console 0	Entra al modo de configuración de la consola
Paso 4	#logging synchronous	Establece el modo síncrono

Debemos configurar las interfaces como lo muestra la figura:

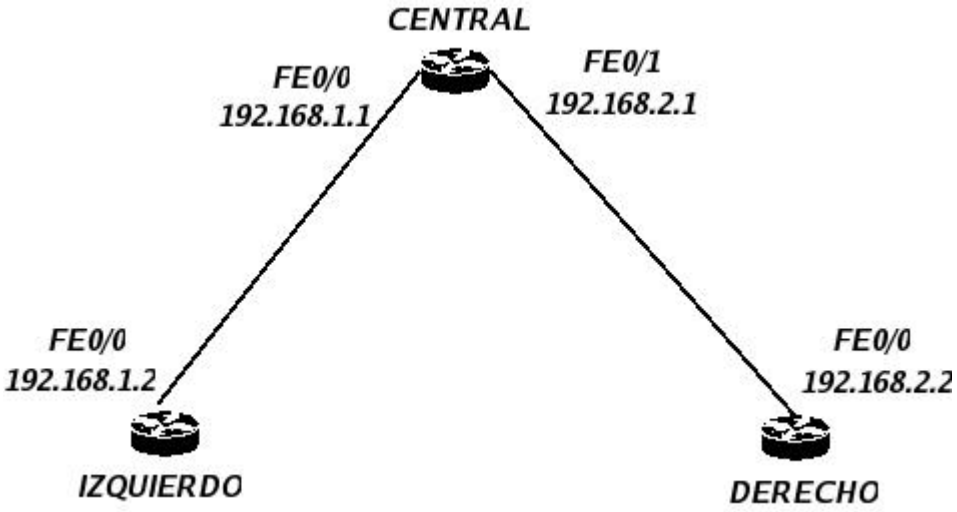


Imagen 10, Diagrama de conexión de los 3 routers Cisco.

De tal forma que tengamos:

Router Central:

```
hostname Central
interface FastEthernet0/0
    ip address 192.168.1.1 255.255.255.0
    no shutdown
interface FastEthernet0/1
    ip address 192.168.2.1 255.255.255.0
    no shutdown
```

Router Izquierdo:

```
hostname Izquierdo
interface FastEthernet0/0
    ip address 192.168.1.2 255.255.255.0
    no shutdown
```

Router Derecho:

```
hostname Derecho
interface FastEthernet0/0
    ip address 192.168.2.2 255.255.255.0
    no shutdown
```

También habilitaremos los mensajes del protocolo RIP, para poder ver la información de los paquetes de actualización enviados y recibidos por cada router, esto lo haremos en cada router:

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#debug ip rip	Habilita o deshabilita el debug de RIP

Iniciando RIP

Para el router central:

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#configure terminal	Entra al modo de configuración global
Paso 3	#router rip	Entra al modo de configuración del protocolo RIP
Paso 4	#network segmento-de-red en este caso: #network 192.168.1.0	Indica a RIP cual es el segmento de red conectado directamente al router
Paso 5	#network segmento-de-red en este caso: #network 192.168.2.0	Indica a RIP cual es el segmento de red conectado directamente al router
Paso 6	#end	(Opcional) Regresa el modo de configuración de terminal
Paso 7	#end	(Opcional) Regresa el modo privileged EXEC

Para el router izquierdo

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#configure terminal	Entra al modo de configuración global
Paso 3	#router rip	Entra al modo de configuración del protocolo RIP
Paso 4	#network segmento-de-red en este caso: #network 192.168.1.0	Indica a RIP cual es el segmento de red conectado directamente al router
Paso 5	#end	(Opcional) Regresa el modo de configuración de terminal
Paso 6	#end	(Opcional) Regresa el modo privileged EXEC

Para el router derecho

	Comando o acción	**Descripción**
Paso 1	#enable	Habilita el modo privileged EXEC
Paso 2	#configure terminal	Entra al modo de configuración global
Paso 3	#router rip	Entra al modo de configuración del protocolo RIP
Paso 4	#network segmento-de-red en este caso: #network 192.168.2.0	Indica a RIP cual es el segmento de red conectado directamente al router
Paso 5	#end	(Opcional) Regresa el modo de configuración de terminal
Paso 6	#end	(Opcional) Regresa el modo privileged EXEC

Una vez hecho esto comenzaras a ver los mensajes RIP viajando entre los routers, a medida que estos mensajes llegan a router, este los agrega a su tabla, siempre y cuando:

El mensaje RIP contiene una red que no este en la tabla actual
El mensaje RIP contiene una red con una mejor métrica (menos saltos) que alguna que ya tenga en su tabla.

Para ver las tablas de ruteo puedes usar el comando:

#show ip route

En caso de que quieras comprobar la conectividad entre las redes 192.168.1.0 y 192.168.2.0, puedes hacer un ping desde el router izquierdo hacia el derecho, para saber que RIP esta bien configurado debes obtener respuesta.

Practica III

VLANs

Configuración de HWICs

Las interfaces EthernetSwitch HWIC son capa 2 10/100 BaseT, con capacidad de ruteo de capa 3. El trafico entre VLAN's se rutea a través de la plataforma del router y no se lleva a cabo en la tarjeta. Un módulo adicional para proporcionar energía a través de la línea puede agregarse, esto para teléfonos IP.

Agregando VLAN's

Las interfaces EtherSwitch HWIC soportan hasta 15 VLAN's.
En modo privilegiado, sigue los siguientes pasos para configurar una interfaz FastEthernet como capa 2.

	Comando	**Explicación**
Paso 1	#vlan database	Ingresa al modo de configuración VLAN
Paso 2	#vlan *vlan_id* *ej. #vlan 2*	Agrega una VLAN Ethernet
Paso 3	#exit	Actualiza la base de datos VLAN, la porpaga a través del dominio y regresa al modo EXEC

Comprobando la configuración VLAN

Comando show
En el modo VLAN database ingresa el comando chow para verificar la configuración de la VLAN

```
Router(vlan)#show
  VLAN ISL Id: 1
  Name: default
  Media Type: Ethernet
  VLAN 802.10 Id: 100001
  State: Operational
  MTU: 1500
  Translational Bridged VLAN: 1002
  Translational Bridged VLAN: 1003
  …
Exiting....
router#
router#
```

Comando show vlan-switch

El comando show vlan-switch, en el modo EXEC para verificar la configuración de la VLAN

```
router#show vlan-switch
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
---------
1    default                          active    Fa0/1/1, Fa0/1/2,
Fa0/1/3, Fa0/1/4
                                               Fa0/1/5, Fa0/1/6,
Fa0/1/7, Fa0/1/8
                                               Fa0/3/0, Fa0/3/2,
Fa0/3/3, Fa0/3/4
                                               Fa0/3/5, Fa0/3/6,
Fa0/3/7, Fa0/3/8
2    VLAN0002                         active    Fa0/1/0
3    Red_VLAN                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ -
-----
1    enet  100001     1500  -      -      -        -    -        1002
1003
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1
1003
1003 tr    101003     1500  1005   0      -        -    srb      1
1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
router#
```

Eliminando una VLAN de la base de datos

No se puede eliminar las VLAN´s por default para los distintos medios: Para Ethernet VLAN 1, para FDDI o TokenRing VLAN's 1002 a 1005.
En modo privilegiado sigue los siguientes pasos:

	Comando	**Explicación**
Paso 1	#vlan database	Ingresa al modo de configuración VLAN
Paso 2	#no vlan *vlan_id* ej #no vlan 2	Elimina la VLAN
Paso 3	#exit	Actualiza la base de datos VLAN, la propaga a través del dominio y regresa al modo EXEC

Verificando la eliminación:

También se puede utilizar el comando **show** en el modo vlan database:

```
Router(vlan)#show
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003
  VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1003
<output truncated>
Router(vlan)#
```

También se puede utilizar el comando **show vlan-switch brief** en el modo priviliegiado:

```
Router#show vlan-switch brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
------
1    default                          active    Fa0/1/0, Fa0/1/1, Fa0/1/2
                                                Fa0/1/3, Fa0/1/4, Fa0/1/5
                                                Fa0/1/6, Fa0/1/7, Fa0/1/8
300  VLAN0300                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Router#
```

Configurando las características opcionales de las interfaces

Cuando configures la velocidad y modo de transmisión de una interface, ten en cuenta:

Si los dos extremos de la línea soportan auto negociación, Cisco recomienda mantener la configuración de auto negociación.
Si una interface soporta auto negociación y la otra no, configura el modo de transmisión y la velocidad en ambas interfaces, no utilices la configuración automática en la interfaz en que la soporta.

Si no soportan la configuración automática ninguna de las interfaces, configura ambas interfaces con la misma velocidad y modo de transmisión.

Modificar la velocidad de la interfaz y el modo de transmisión, produce que la interfaz se reinicie.

Configurando la velocidad

En modo de configuración global:

	Comando	**Explicación**
Paso 1	#interface fastethernet *id* ej. Interface fastethernet0/0/0	Selecciona la interfaz a configurar
Paso 2	#speed |10 |100 |auto	Selecciona la velocidad

En caso de que selecciones la velocidad auto en una interfaz Ethernet 10/100-Mbps, la velocidad y el modo de transmisión se negocian automáticamente.

Configurando el modo de transmisión

En modo de configuración global:

	Comando	**Explicación**
Paso 1	#interface fastethernet *id* ej. Interface fastethernet0/0/0	Selecciona la interfaz a configurar
Paso 2	#duplex [auto | full |half]	Selecciona el modo de transmisión

En caso de que selecciones el modo de transmisión auto en una interfaz Ethernet 10/100-Mbps, la velocidad y el modo de transmisión se negocian automáticamente.

Como vimos en la practica 1 también se puede configurar una descripción para la interfaz. Agregarlo a la práctica.

Configurando la interfaz como acceso de capa 2

Nos sirve para asignar alguna interfaz a una VLAN.
En modo de configuración global:

	Comando	**Explicación**
Paso 1	#interface fastethernet *id* ej. #interface fastethernet0/0/0	Selecciona la interfaz a configurar
Paso 2	#switchport mode access	Configura la interfaz como acceso de capa 2
Paso 3	#switch port access vlan *vlan_num* *ej #switchport access vlan 2*	Especifica la VLAN asociada
Paso 4	#no shutdown	Activa la interfaz
Paso 5	#end	Sale del modo de configuración

Verificando la configuración:

```
Router#show running-config interface fastethernet 0/1/2
Building configuration...
Current configuration: 76 bytes
!
interface FastEthernet0/1/2
  switchport access vlan 3
  no ip address
end
```

Ejemplo de configuración de una VLAN:

#**vlan database**
(vlan)#**vlan 1**
(vlan)#**vlan 2**
(vlan)#**exit**
#**configure terminal**
#**interface vlan 1**
#**ip address 192.168.27.155 255.255.255.0**
#**no shut**
#**interface vlan 2**
#**ip address 192.168.27.158 255.255.255.0**
#**no shut**
#**interface FastEthernet0/0/0**
#**switchport access vlan 1**
#**interface FastEthernet0/0/1**
#**switchport access vlan 2**
#**exit**

Inauguración del laboratorio.

El 23 de Junio del 2006 en el Posgrado de Ciencia e Ingeniería de la Computación se inauguró el laboratorio de Redes, asistieron, entre otras personas:

- Dr. Boris Escalante Ramírez, Coordinador del Posgrado en Ciencias e Ingeniería de la Computación
- Dr. Javier Gómez Castellanos, Docente del Posgrado en Ciencias e Ingeniería de la Computación, de la Facultad de Ingeniería e Investigador de tiempo completo.
- Dr. Víctor Rangel Licea, Docente del Posgrado en Ciencias e Ingeniería de la Computación, de la Facultad de Ingeniería e Investigador de tiempo completo.
- Muchos alumnos del Posgrado en Ciencias e Ingeniería de la Computación

Tuve la oportunidad de exponer frente a ellos mi experiencia en esos meses de trabajo, hablar sobre los routers y los switches, las cosas que se podían hacer con el equipo con el que se contaba e incluso proponer la compra de teléfonos IP con el fin de estudiar VoIP. Realice una demostración de ínter conectividad entre dos computadoras de distintos segmentos de la red utilizando aplicaciones de mensajería instantánea y video. Y finalmente se platicó de los planes del Posgrado para el laboratorio.

En la Imagen 11 se observan algunos Doctores del Posgrado durante la demostración.

En la Imagen 12, Algunos alumnos del Posgrado.

En la Imagen 13, Yo durante la explicación de los Routers

Capitulo V
Conclusiones.

Actualmente escuchamos de una gran gamma de aplicaciones y servicios que están surgiendo, voz sobre IP, video sobre IP, video bajo demanda, tele-conferencias en alta definición, etc. Esto se debe en gran medida a que los usuarios y las empresas se sienten cada vez más confiados en las telecomunicaciones y están dispuestos a poner su información en las redes, a realizar trámites, operaciones y transacciones por medio de estas. Es claro también, que las redes ofrecen muchos beneficios a los usuarios como ahorro de tiempo, seguridad, una rápida comunicación, etc., Sin embargo esto no se logra solo, no basta con invertir grandes sumas de dinero en equipos modernos y esperar que funcionen solos, debe ser parte integral de la educación de cualquier Ingeniero en Telecomunicaciones y mas aún de cualquier alumno de Posgrado relacionado con las Telecomunicaciones, conocer los estándares, los protocolos, los algoritmos, pero también la forma de configurar una red, como proteger la red de los intrusos, como limitar el ancho de banda para ciertos enlaces, como monitorear la red.

Creo que el equipo adquirido por el Posgrado es una excelente herramienta para sus alumnos, pueden experimentar con las practicas propuestas o pueden hacer muchas cosas mas, los asesores, el equipo y los temas están ahí, solo necesitan el interés y algunas horas después de clases.

Desde un punto de vista de Ingeniería, considero que el alcance de esta tesis fue cubierto con creces, he estudiado sobre los protocolos de red, sobre los equipos mencionados en la tesis y sus interfaces, y basado en esos conocimientos y los obtenidos durante la carrera desarrolle prácticas para que los alumnos de posgrado pudieran experimentar con estos equipos y además junto con el Dr. Javier Gómez Castellanos y el Dr. Víctor Rangel Licea, propuse temas para futuros estudios dentro del posgrado. Considero que el equipo de redes adquirido por el Posgrado será de mucha utilidad para que los alumnos puedan aprender trabajando directamente con los dispositivos, lo que sin duda, complementará lo visto en teoría. Algo que también me parece muy acertado, es la decisión de utilizar sistemas Unix para este laboratorio ya que permite “observar” y “estudiar” las aplicaciones y el tráfico de red desde cualquier perspectiva que se quiera hacer; podemos hacerlo a nivel físico, abriendo las computadoras, agregando y quitando hardware. Podemos hacerlo a nivel de enlace, aprovechando el código abierto de los controladores. A nivel de red, trabajando directamente con IP, incluso usando sniffers. Transporte, sesión, aplicación y presentación, tenemos todo para entrar a cualquiera de estos niveles a observar como se “transforman” los datos al agregar cabeceras, a donde viajan los paquetes cuando una ruta cambia e incluso el código de algún sniffer que estemos utilizando para “analizar” la red. Además, es importante mencionar que los sistemas UNIX son ampliamente utilizados en las empresas, no solo de telecomunicaciones, también están ganando terreno en las empresas medianas y grandes de casi cualquier giro.

Antes de que esta tesis fuera terminada, las prácticas propuestas en ella y otras mas ya están siendo estudiadas y puestas en marcha por los alumnos del posgrado, he tenido la oportunidad, gracias al Dr. Javier Gómez, de explicar en clases de laboratorio cuales son los objetivos de cada practica, cómo llevarlas a cabo y resolver dudas de estos alumnos, con

lo que he aprendido mucho respecto a estos equipos y también he ayudado a que mas alumnos aprendan. Cabe mencionar que los temas y las practicas expuestas en esta tesis no son los únicos que se están llevando a cabo en el laboratorio, ya que he visto como los alumnos implementan sistemas GPS utilizando programación en JAVA y sistemas UNIX, he escuchado de propuestas para incluir practicas de VoIP, incluso certificaciones de empresas reconocidas en el ramo como CISCO o Nortel, por lo que me da mucho gusto ver que las practicas quedaron al alcance de los alumnos y que la propuesta para el laboratorio esta actualmente en marcha.

Solo me queda agradecer a los Doctores Javier Gómez Castellanos y Víctor Rangel Licea, por la oportunidad de trabajar en el Posgrado de Ciencias e Ingeniería de la Computación, donde he aprendido las bases que me han ayudado a desarrollarme exitosamente en la industria.

Bibliografía

UNAM Posgrado, Ciencia e Ingeniería de la Computación: http://www.mcc.unam.mx

Cisco Catalyst Guide. Scalable, intelligent LAN switching for campus, branch, and data center networks of all sizes. Spring 2006 V.2. Cisco Systems.

Introducing Cisco's Integrated Services Routers. 2006 Cisco Systems, Inc.

Cisco Router and Security Device Manager Quick Start Guide. 2005 Cisco Systems, Inc.

Catalyst 2950 Switch Getting Started Guide. 2004. Cisco Systems, Inc.

Basic Software Configuration Using the Cisco IOS Command-Line Interface. 2004. Cisco Systems.

Understanding and Configuring Private VLANs. Software Configuration Guide – Release 12.2(11b)EW. 2005 Cisco Systems Inc.

Cisco IOS Network Address Translation. 2004. Cisco Systems.

Cisco 2800 Series Integrated Services Routers Quick Stara Guide. 2004. Cisco Systems.

Cisco Software Release Notes. 2003. Cisco Systems.

Configuration Example: Easy VPN. 2004. Cisco Systems.

CCNA Official Exam Certification Library. 2005. Cisco Press

Tanenbaum, Andrew S. Redes de computadoras. 2005. Pearson Educación.

Unix System Administration. 2004. Eleen Frisch. O'Reilly

The Apache Software FOundation. www.apache.org/

vsftpd - Secure, fast FTP server for UNIX-like systems. www.vsftpd.beasts.org/

OpenSSH. www.openssh.com/

qmail:the Internet´s MTA of choice www.cr.yp.to/qmail.html

The Horde Project. www.horde.org

Linux Home Networking and Linux Forums Help. www.linuxhomenetworking.com/

Common UNIX Printing System. www.cups.org/

MySQL AB :: The world´s most popular open source database. www.mysql.com/

Linux NFS faq. www.nfs.sourceforge.net/

netfilter/iptables project homepage - The netfilter.org Project. www.netfilter.org/

OpenVPN - An Open Source SSL VPN Solution by James Donan. www.openvpn.net/

Java Technology. www.java.sun.com/

Ethereal A Network Protocol Analyzer. www.ethereal.com/

Asterisk :: An Open Source PBX and telephony toolkit. www.asterisk.org/

FreeRADIUS: The world´s most popular RADIUS Server. www.freeradius.org/

Notas del curso de redes inalámbricas y móviles, Dr. Javier Gómez Castellanos

802.11 Wireless LAN Fundamentals. A Practical Guide to understanding, designing, and operating 802.11 WLANs, Pejman Roshan, Jonathan Leary, Cisco Press, 2004, Marzo 2005, Indianapolis, pags 281

Cisco Networking Academy Program, Academia de Networking de Cisco Systems, CCNA 1 y 2. Prácticas de Laboratorio, Vol. 1. Tercera Edición, Pearson Educación , S. A., Madrid, 2004, pags 572

CCDA Self-Study: Designing for Cisco Internetwork Solution (DESGN), Diane Teare, Cisco Press, Indianapolis, November 2004, pags 1022