UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

CUAUTITLÁN

IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED PARA LA TRANSMISIÓN DE DATOS DISEÑADA BAJO LA PLATAFORMA SOLARIS CON SISTEMA OPERATIVO LINUX, LA CUAL ESTA INTEGRADA POR DISPOSITIVOS DE INTERCONEXIÓN Y ESTACIONES DE TRABAJO

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECÁNICO ELECTRICISTA

PRESENTAN:

HECTOR JAIR HERRERA PEREA

HUGO LIRA HERNÁNDEZ

ASESOR: ING. JOSÉ LUIS RIVERA LÓPEZ

CUAUTITLÁN IZCALLI, EDO. DE MEX 2008

Agradecimientos

Esta tesis de licenciatura, si bien ha requerido un esfuerzo y mucha dedicación por parte de los autores y directores de tesis, no hubiese sido posible su finalización sin el apoyo desinteresado de todas y cada una de las personas que a continuación citaremos.

Héctor Jair Herrera Perea

A mis padres:

Por todas las comodidades, facilidades que me dieron durante tanto tiempo y preocuparse por darme las herramientas para salir adelante en este mundo. Además ustedes son una de las razones para seguir siendo mejor cada día.

A mi tío Marco Antonio (q.d.e.p.†):

En su memoria dedico este logro, en gran parte gracias a su apoyo incondicional. Uno de mis ejemplos a seguir y otra de mis razones para que cada día sea mejor en todo lo que hago.

A todos mis tíos:

Gracias familia, su apoyo es un estimulo y un aliciente en mi vida. Todas sus preocupaciones y consejos son un tesoro, el cual cuido y aprecio enormemente. En verdad no hay palabras para describir lo agradecido que me encuentro por ayudarme a ser una mejor persona.

Hugo Lira Hernández

A mis padres

Vuelvo a agradecerles infinitamente su paciencia, su esfuerzo y su cariño. Quiero recordarles que los quiero mucho y que gracias a ustedes siempre estuve motivado para poder alcanzar esta larga meta.

Sandy

Nena, tienes que saber que tu ánimo, tu cariño, tu ayuda y tu confianza han sido lo más importante para que pudiera terminar mi carrera. Tu apoyo y tu compañía, son lo que más he necesitado en cada momento para salir adelante. Lamento que el tiempo que le he dedicado a esto haya sido tiempo que no estuvimos juntos.

Te amo, pensar en ti me hace muy feliz y mucho más estar siempre contigo.

A mis Hermanos

Pensar en cada uno de ustedes es para mí algo muy especial: apoyo incondicional por siempre. También es tranquilidad, algo que me fortaleció bastante en todo momento. Gracias y recuerden que los adoro infinito.

A Diana, Javier y Arielita.

Nadie como mis sobrinos puede impulsarme más a ser mejor cada día, los quiero demasiado y me hace muy feliz estar con ustedes (aunque no sea muy seguido). Deseo que se sigan preparando para que en un futuro próximo me inviten a sus respectivas graduaciones, para lograr esto tienen que estudiar diario, disfrutarlo mucho y descubrir que les gustaría estudiar. Espero que por lo menos uno escoja ingeniería.

Un agradecimiento especial a nuestros asesores y directores de tesis José Luis Rivera López y Maricela Serrano Fragoso quienes nos ayudaron pacientemente en cada una de las difíciles etapas del presente trabajo. De igual forma un saludo al profesor Humberto: gracias profesor Debian, Adrian Santiago Adán, Roger Valdivieso, Román García, Juan Carlos Chávez y Francisco Alquicira.

INTRODUCCIÓN

En el presente trabajo se da a conocer el funcionamiento de una red y sus componentes, así como una serie de normativas que se deben de seguir para su instalación, o su implementación. A continuación se describe el contenido de cada uno de los temas brevemente.

Tema 1. Incluye un marco teórico e introductorio, en el cual se nombran las normativas a utilizar, además de algunas ejemplificaciones para mayor claridad y entendimiento de éstas. También se dan a conocer los distintos tipos de cableado que pueden ser utilizados en la construcción de una red.

Tema 2. Se define lo que es un dispositivo y sus características así como una breve explicación de los sistemas operativos que maneja cada uno de los dispositivos, este último contenido será retomado más a detalle en el siguiente tema.

Tema 3. Se abunda en las características de los sistemas operativos. Cabe mencionar que sólo se retoman los más relevantes, y se da un listado de los comandos más utilizados y recurridos.

Tema 4. Se describen las normativas mencionadas para la interconexión de cada uno de los dispositivos.

Tema 5. Se presentan las prácticas desarrolladas durante la implementación del laboratorio, con las cuales se coadyuva al uso del hardware y software utilizado.

Tema 6. Detalla la comprobación del buen funcionamiento de la red utilizando línea de comandos de GNU-Linux y Windows.

PRESENTACIÓN

"Los ingenieros no estudiamos una profesión para ejercerla toda la vida, debemos estudiar toda la vida para poder ejercer la profesión", Javier Jiménez Espriu.

La implementación de una red de computadoras tiene como principal objetivo enlazar la parte teórica y práctica aprendida en las materias de Transmisión de datos y Temas Selectos de Comunicaciones. Y aunque está dirigida principalmente a los alumnos de la carrera de Ingeniería Mecánica Eléctrica podría ser recurrida también por compañeros de otras carreras interesados en el tema. El objetivo principal es permitir a los alumnos desarrollar sus habilidades en la implementación de redes y su respectiva configuración en ambientes GNU-Linux/Solaris.

Por otro lado, la idea de trabajar con GNU-Linux/Solaris tiene una importante razón: un número considerable de pequeñas y medianas empresas (PYME), así como grandes organizaciones, están migrando sus servidores de datos, con sistemas operativos (SO) privativos, hacia software libre (SO). Es por esto que es sumamente importante desarrollar la habilidad durante la etapa escolarizada el trabajar con GNU-Linux. Hoy en día, en nuestra carrera no existe como tal un grupo de trabajo que abarque distribuciones como GNU-Linux o programar en lenguajes actuales como JAVA por ejemplo. Es decir, es un asunto de actualización.

Finalmente, las prácticas desarrolladas nos permitirán interconectar los diferentes dispositivos así como su respectiva configuración. Por último, se debe mencionar que la infraestructura del laboratorio nos permitirá la instalación y ejecución de las tecnologías en punta de software: Programación en Java y virtualización de sistemas operativos. Ésta última, muy recurrida en el ambiente empresarial.

ÍNDICE

TEMA 1

1. Fundamentos de redes.

En Informática y Telecomunicaciones, un protocolo es una convención, o estándar o acuerdo entre partes que regulan la conexión, la comunicación y la transferencia de datos entre dos sistemas. En su forma más simple, un protocolo se puede definir como las reglas que gobiernan la semántica (significado de lo que se comunica), la sintaxis (forma en que se expresa) y la sincronización (quién y cuándo transmite) de la comunicación.

Los protocolos pueden estar implementados bien en hardware (tarjetas de red), software (drivers), o una combinación de ambos.

La mayoría de los protocolos especifican una o más de las siguientes propiedades:

- Detección de la conexión física sobre la que se realiza la conexión (cableada o sin cables)
- Pasos necesarios para comenzar a comunicarse (Handshaking)
- Negociación de las características de la conexión.
- Cómo se inicia y cómo termina un mensaje.
- Formato de los mensajes.
- Qué hacer con los mensajes erróneos o corruptos (corrección de errores)
- Cómo detectar la pérdida inesperada de la conexión, y qué hacer en ese caso.
- Terminación de la sesión de conexión.
- Estrategias para asegurar la seguridad (autenticación, encriptación).

Estandarización

Los protocolos que son implementados en sistemas de comunicación que tienen un amplio impacto, suelen convertirse en estándares, debido a que la comunicación e intercambio de información (datos) es un factor fundamental en numerosos sistemas, y para asegurar tal comunicación se vuelve necesario copiar el diseño y funcionamiento a partir del ejemplo pre-existente. Esto ocurre tanto de manera informal como deliberada.

Existen consorcios empresariales, que tienen como propósito precisamente el de proponer recomendaciones de estándares que se deben respetar para asegurar la interoperabilidad de los productos.

Ejemplos de lo anterior son la IEEE que propone varios estándares para redes físicas, y la W3C (World Wide Web Consortium) que gestiona la definición aceptada sobre HTTP (1)

1.1. Niveles de abstracción

En el campo de las redes informáticas, los protocolos se pueden dividir en varias categorías, una de las clasificaciones más estudiadas es el modelo de referencia OSI. Éste modelo está dividido en 7 capas las cuales se muestran a continuación en l tabla 1.1.

Nivel	Nombre	Categoría
Capa 7	Nivel de aplicación	Aplicación
Capa 6	Nivel de presentación	
Capa 5	Nivel de sesión	
Capa 4	Nivel de transporte	
Capa 3	Nivel de red	Transporte de datos
Capa 2	Nivel de enlace de datos	
Capa 1	Nivel físico	

Tabla 1.1 Modelo de referencia OSI

A su vez, esos 7 niveles se pueden subdividir en dos categorías, las capas superiores y las capas inferiores. Las 4 capas superiores trabajan con problemas particulares a las aplicaciones, y las 3 capas inferiores se encargan de los problemas pertinentes al transporte de los datos.

Otra clasificación, más práctica y la más utilizada es el modelo de referencia TCP/IP, sus diversos niveles o capas se muestran en la Tabla 1.2.

Los protocolos de cada capa tienen una interfaz bien definida. Una capa generalmente se comunica con la capa inmediata inferior, la inmediata superior, y la capa del mismo nivel en otros computadores de la red. Esta división de los protocolos ofrece abstracción en la comunicación.

Una aplicación (capa nivel 7) por ejemplo, solo necesita conocer como comunicarse con la capa 6 que le sigue, y con otra aplicación en otro computador (capa 7). No necesita conocer nada entre las capas de la 1 y la 5. Así, un navegador web (HTTP, capa 7) puede utilizar una conexión Ethernet o PPP (capa 2) para acceder a la Internet, sin que sea necesario cualquier tratamiento para los protocolos de este nivel más bajo. De la misma forma, un router sólo necesita de las informaciones del nivel de red para enrutar paquetes, sin que importe si los datos en tránsito pertenecen a una imagen para un navegador web, un archivo transferido vía FTP o un mensaje de correo electrónico.

Nivel
Capa de Aplicación
Capa de Transporte
Capa de Red
Capa de Enlace de Datos
Capa Física

Tabla 1.2 Modelo de referencia TCP/IP

1.2. Modelo de referencia OSI

Siguiendo el esquema de este modelo se crearon numerosos protocolos, por ejemplo X.25, que durante muchos años ocuparon el centro de la escena de las comunicaciones informáticas. El advenimiento de protocolos más flexibles donde las capas no están tan demarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo sigue siendo muy usado en la enseñanza como una manera de mostrar cómo puede estructurarse una "pila" de protocolos de comunicaciones (sin importar su poca correspondencia con la realidad).

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, sino que suele hablarse de modelo de referencia. Este modelo está dividido en siete capas:

Capa Física (Capa 1)

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

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

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

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados, coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

Codificación de la señal

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

En el caso más sencillo el medio es directamente digital, como en el caso de las fibras ópticas, dado que por ellas se transmiten pulsos de luz. Cuando el medio no es digital hay que codificar la señal, en los casos más sencillos la codificación puede ser por pulsos de tensión (por ejemplo 5 V para los "unos" y 0 V para los "ceros"). Otros medios se codifican mediante presencia o ausencia de corriente. En general estas codificaciones son muy simples y no apuran bien la capacidad de medio. Cuando se quiere sacar más partido al medio se usan técnicas de modulación más complejas, y suelen ser muy dependientes de las características del medio concreto.

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

Topología y medios compartidos

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

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

Así por ejemplo la fibra óptica no permite fácilmente conexiones multipunto y por el contrario las conexiones inalámbricas son inherentemente multipunto. Hay topologías como el anillo, que permiten conectar muchas máquinas a partir de una serie de conexiones punto a punto.

Equipos adicionales

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

Capa de enlace de datos (Capa 2)

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

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

Ejemplos de Protocolos

- **Capa 2: Nivel de enlace de datos**
    - Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, HDLC.

Capa de red (Capa 3)

El cometido de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Es decir que se encarga de encontrar un camino manteniendo una tabla de enrutamiento y atravesando los equipos que sea necesario, para hacer llevar los datos al destino. Los equipos encargados de realizar este encaminamiento se denominan en castellano encaminadores, aunque es más frecuente encontrar el nombre inglés *routers* y, en ocasiones enrutadores.

Adicionalmente la capa de red debe gestionar la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red (similar a un atasco en un cruce importante en una ciudad grande). La PDU de la capa 3 es paquetes.

Ejemplos de Protocolos

- **Capa 3: Nivel de red**
    - ARP, RARP, IP (IPv4, IPv6), X.25, ICMP, IGMP, NetBEUI, IPX, Appletalk.

Capa de transporte (Capa 4)

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación. Otra característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación. En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes.

Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte. Por ejemplo, la comunicación puede ser manejada para que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío. Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión finalice. Todo el servicio que presta la capa está gestionado por las cabeceras que agrega al paquete a transmitir.

Para finalizar, podemos definir a la capa de transporte como:

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la destino, independizándolo del tipo de red física que se esté utilizando. La PDU de la capa 4 se llama Segmentos.

Ejemplos de Protocolos

- **Capa 4: Nivel de transporte**
    - TCP, UDP, SPX

Capa de sesión (Capa 5)

Esta capa ofrece varios servicios que son cruciales para la comunicación, como son: 1 Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta). 2 Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo). 3 Mantener puntos de verificación (checkpoints), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcialmente, o incluso, totalmente prescindibles.

En conclusión esta capa es la que se encarga de mantener el enlace entre los dos computadores que estén trasmitiendo archivos.

Ejemplos de Protocolos

- **Capa 5: Nivel de sesión**
    - NetBIOS, RPC, SSL.

Capa de presentación (Capa 6)

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

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

Por lo tanto, podemos resumir definiendo a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos. Esta capa también permite cifrar los datos y comprimirlos.

Ejemplos de Protocolos

- **Capa 6: Nivel de presentación**
    - ASN.1, MIME, SSL/TLS, XDR.

Capa de aplicación (Capa 7)

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

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

Ejemplos de Protocolos

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

- HTTP (HyperText Transfer Protocol) el protocolo bajo la www
- FTP (File Transfer Protocol) (FTAM, fuera de TCP/IP) transferencia de ficheros

- SMTP (Simple Mail Transfer Protocol) (X.400 fuera de tcp/ip) envío y distribución de correo electrónico
- POP (Post Office Protocol)/IMAP: reparto de correo al usuario final
- SSH (Secure Shell) principalmente terminal remoto, aunque en realidad cifra casi cualquier tipo de transmisión.
- Telnet otro terminal remoto, ha caído en desuso por su inseguridad intrínseca, ya que las claves viajan sin cifrar por la red.

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

- SNMP (Simple Network Management Protocol)
- DNS (Domain Name System)

1.2.1. Unidades de datos

El intercambio de información entre dos capas **OSI** consiste en que cada capa en el sistema fuente agrega información de control a los datos, y cada capa en el sistema de destino analiza y remueve la información de control de los datos como sigue:

Si un ordenador (host A) desea enviar datos a otro (host B), en primer término los datos deben empaquetarse a través de un proceso denominado encapsulamiento, es decir, a medida que los datos se desplazan a través de las capas del **modelo OSI**, reciben encabezados, información final y otros tipos de información, un ejemplo de esto se observa a continuación.

N-PDU (Unidad de datos de protocolo)

Es la información intercambiada entre entidades pares, es decir, dos entidades pertenecientes a la misma capa pero en dos sistemas diferentes, utilizando una conexión(N-1).

Está compuesta por:

N-SDU (Unidad de datos del servicio)

Son los datos que se necesitan las entidades (N) para realizar funciones del servicio pedido por la entidad (N+1).

N-PCI (Información de control del protocolo)

Información intercambiada entre entidades (N) utilizando una conexión (N-1) para coordinar su operación conjunta.

N-IDU (Unidad de datos del interface)

Es la información transferida entre dos niveles adyacentes, es decir, dos capas contiguas.

Está compuesta por:

N-ICI (Información de control del interface)

Información intercambiada entre una entidad (N+1) y una entidad (N) para coordinar su operación conjunta.

Datos de Interface-(N)

Información transferida entre una entidad-(N+1) y una entidad-(N) y que normalmente coincide con la (N+1)-PDU.

1.2.2. Transmisión de los datos

La capa de aplicación recibe el mensaje del usuario y le añade una cabecera constituyendo así la PDU de la capa de aplicación. La PDU se transfiere a la capa de aplicación del nodo destino, este elimina la cabecera y entrega el mensaje al usuario. Para ello ha sido necesario todo este proceso:

1-Ahora hay que entregar la PDU a la capa de presentación para ello hay que añadirla la correspondiente cabecera ICI y transformarla así en una IDU, la cual se transmite a dicha capa.

2-La capa de presentación recibe la IDU, le quita la cabecera y extrae la información, es decir, la SDU, a esta le añade su propia cabecera (PCI) constituyendo así la PDU de la capa de presentación.

3- Esta PDU es transferida a su vez a la capa de sesión mediante el mismo proceso, repitiéndose así para todas las capas.

4-Al llegar al nivel físico se envían los datos que son recibidos por la capa física del receptor.

5-Cada capa del receptor se ocupa de extraer la cabecera, que anteriormente había añadido su capa homóloga, interpretarla y entregar la PDU a la capa superior.

6-Finalmente llegará a la capa de aplicación la cual entregará el mensaje al usuario.

Toda esta información se ve ejemplificada en la figura 1.1, en la cual se puede observar como es empaquetada la información, mostrando paso a paso el proceso antes mencionado, con esto se pretende dar una idea más clara de este proceso.

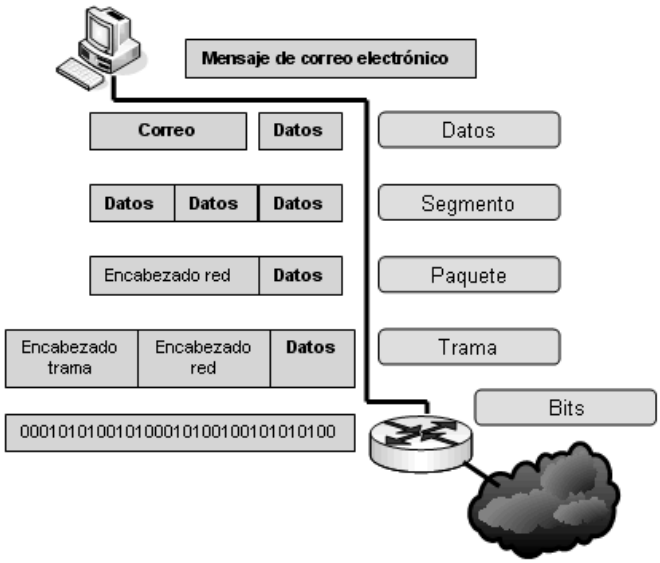


Figura 1. 1 Empaquetamiento de datos.

1.2.3. Formato de los datos

Estos datos reciben una serie de nombres y formatos específicos en función de la capa en la que se encuentren, debido a como se describió anteriormente la adhesión de una serie de encabezados e información final. Los formatos de información se pueden ver ejemplificado en la Figura 1.2 y son los siguientes:

APDU

Unidad de datos en la Capa de aplicación.

PPDU

Unidad de datos en la Capa de presentación.

SPDU

Unidad de datos en la capa de sesión.

TPDU

Unidad de datos en la capa de transporte.

Paquete

Unidad de datos en el Nivel de red.

Trama

Unidad de datos en la capa de enlace.

Bits

Unidad de datos en la capa física.

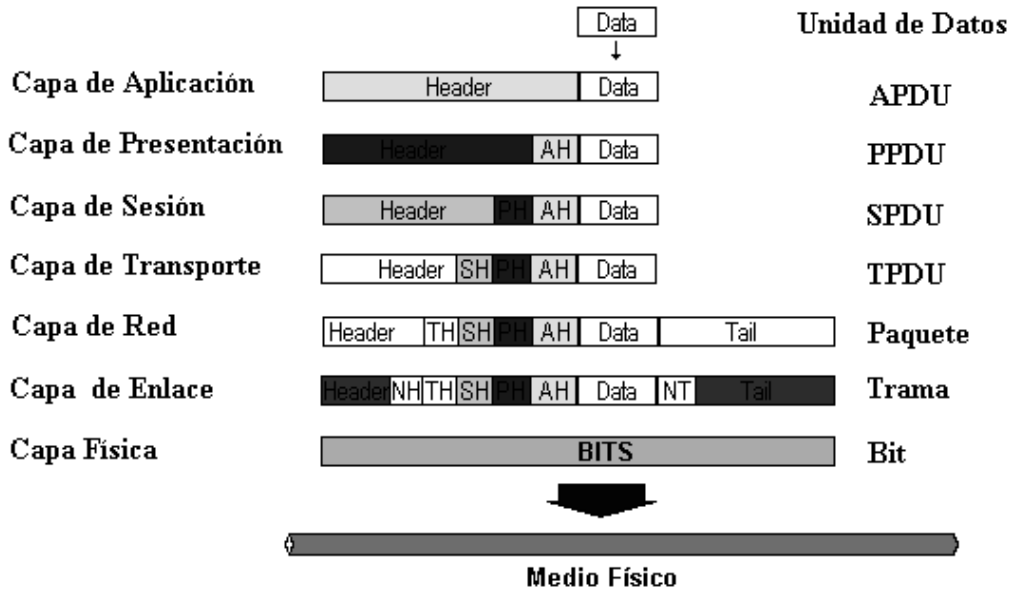


Figura 1.2 Formato de los datos

1.3. Medios y conexiones

En términos generales, una **interfaz** es el punto, el área, o la superficie a lo largo de la cual dos cosas de naturaleza distinta convergen. Por extensión, se denomina interfaz a cualquier medio que permita la interconexión de dos procesos diferenciados con un único propósito común.

En electrónica, telecomunicaciones y hardware, una interfaz (electrónica) es el *puerto* (circuito físico) a través del que se envían o reciben señales desde un sistema o subsistemas hacia otros. No existe un interfaz universal, sino que existen diferentes estándares (Interfaz USB, interfaz SCSI, etc.) que establecen especificaciones técnicas concretas (características comunes), con lo que la interconexión sólo es posible utilizando el mismo interfaz en origen y destino. En materia de hardware encontramos términos que se refieren a las interfaces: puerto, puerto de datos, bus, bus de datos, slot, slot de expansión. También, en materia de hardware, se considera interfaz al medio mediante el cual un disco duro se comunica con los demás componentes del ordenador; puede ser IDE, SCSI, USB o Firewire

1.3.1. Los tipos de cables

Actualmente, la gran mayoría de las redes están conectadas por algún tipo de cableado, que actúa como medio de transmisión por donde pasan las señales entre los equipos. Los cables se pueden agrupar en tres grupos principales:

1. Cable coaxial.
2. Cable de par trenzado (apantallado y no apantallado).
3. Cable de fibra óptica.

EL CABLE COAXIAL

Es un cable formado por un conductor central macizo o compuesto por múltiples fibras al que rodea un aislante dieléctrico (plástico) de mayor diámetro. Presenta propiedades mucho más favorables frente a interferencias y a la longitud de la línea de datos, de modo que el ancho de banda puede ser mayor. Esto permite una mayor concentración de las transmisiones analógicas o más capacidad de las transmisiones digitales. Su estructura se puede apreciar en la Figura 1.3.

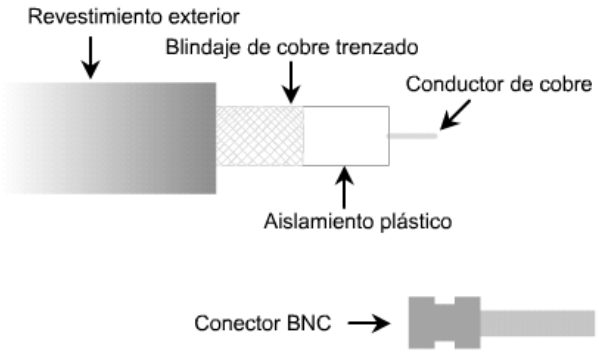


Figura 1.3 Estructura del cable coaxial

Una malla exterior aísla de interferencias al conductor central. Por último, utiliza un material aislante para recubrir y proteger todo el conjunto. Presenta condiciones eléctricas más favorables. En redes de área local se utilizan dos tipos de cable coaxial: fino y grueso.

Tiene una capacidad de llegar a anchos de banda comprendidos entre los 80 Mhz y los 400 Mhz (dependiendo de si es fino o grueso). Esto quiere decir que en transmisión de señal analógica se puede tener del orden de 10.000 circuitos de voz.

TIPOS DE CABLE COAXIAL

Hay dos tipos de cable coaxial:

1. Cable fino (Thinnet): es un cable coaxial flexible de unos 0,64 centímetros de grueso (0,25 pulgadas). Este tipo de cable se puede utilizar para la mayoría de los tipos de instalaciones de redes, ya que es un cable flexible y fácil de manejar.
2. Cable grueso (Thicknet): es un cable coaxial relativamente rígido de aproximadamente 1,27 centímetros de diámetro. Al cable Thicknet a veces se le denomina Ethernet estándar debido a que fue el primer tipo de cable utilizado con la conocida arquitectura de red Ethernet. El núcleo de cobre del cable Thicknet es más grueso que el del cable Thinnet. Cuanto mayor sea el grosor del núcleo de cobre, más lejos puede transportar las señales.

CABLE DE PAR TRENZADO

El cable par trenzado está compuesto de conductores de cobre aislados por papel o plástico y trenzados en pares. Esos pares son después trenzados en grupos llamados unidades, y estas unidades son a su vez trenzadas hasta tener el cable terminado que se cubre por lo general por plástico. El trenzado de los pares de cable y de las unidades disminuye el ruido de interferencia, mejor conocido como diafonía. Los cables de par trenzado tienen la ventaja de no ser caros, ser flexibles y fáciles de conectar, entre otras. Como medio de comunicación tiene la desventaja de tener que usarse a distancias limitadas ya que la señal se va atenuando y puede llegar a ser imperceptible; es por eso que a determinadas distancias se deben emplear repetidores que regeneren la señal.

Los cables de par trenzado se llaman así porque están trenzados en pares como se puede observar en las Figuras 1.4, 1.5 y 1.6. Este trenzado ayuda a disminuir la diafonía, el ruido y la interferencia. El trenzado es en promedio de tres trenzas por pulgada. Para mejores resultados, el trenzado debe ser variado entre los diferentes pares. Existen dos tipos de cable par trenzado:

1.- **UTP (Unshielded Twisted Pair Cabling)**, o cable de par trenzado sin blindaje.
2.- **STP (Shielded Twisted Pair Cabling)**, o cable de par trenzado blindado.
3.- **FTP (Foiled Twisted Pair)**, o cable de par trenzado con pantalla global.

El estándar EIA-568 en el adendum TSB-36 diferencia tres categorías distintas para este tipo de cables.

- Categoría 3: Admiten frecuencias de hasta 16 Mhz
- Categoría 4: Admiten frecuencias de hasta 20 Mhz
- Categoría 5: Admiten frecuencias de hasta 100 Mhz

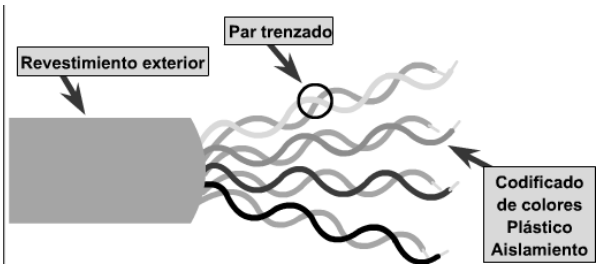


Figura 1.4 Cable UTP

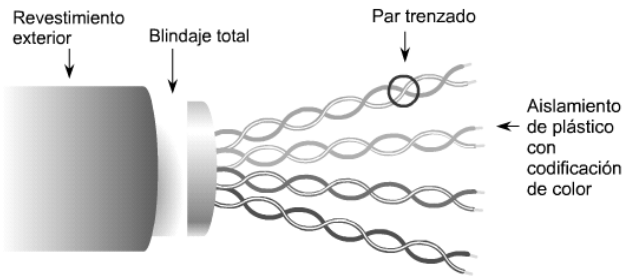


Figura 1.5 Cable STP

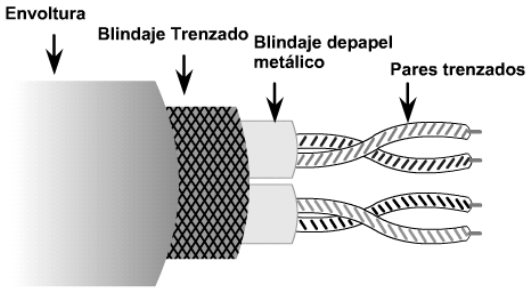


Figura 1.6 Cable FTP

EL CABLE DE FIBRA ÓPTICA

Es un filamento de vidrio sumamente delgado diseñado para la transmisión de la luz. Las fibras ópticas poseen enormes capacidades de transmisión, del orden de miles de millones de bits por segundo. Además de que los impulsos luminosos no son afectados por interferencias causadas por la radiación aleatoria del ambiente. Actualmente la fibra óptica está remplazando en grandes cantidades a los cables comunes de cobre.

TIPOS DE FIBRA ÓPTICA

Actualmente se utilizan tres tipos de fibras ópticas para la transmisión de datos:

Monomodo: Permite la transmisión de señales con ancho de banda hasta 2 GHz
Multimodo de índice gradual: Permite transmisiones hasta 500 MHz
Multimodo de índice escalonado: Permite transmisiones hasta 35 MHz

Se han llegado a efectuar transmisiones de decenas de miles de llamadas telefónicas a través de una sola fibra, debido a su gran ancho de banda. Otra ventaja es la gran fiabilidad, su tasa de error es mínima. Su peso y diámetro la hacen ideal frente a cables de pares o coaxiales. Normalmente se encuentra instalada en grupos, en forma de mangueras, con un núcleo metálico que les sirve de protección y soporte frente a las tensiones producidas. Su principal inconveniente es la dificultad de realizar una buena conexión de distintas fibras con el fin de evitar reflexiones de la señal, así como su fragilidad. Algunos de los cables se pueden apreciar en la figura 1.7. (3)

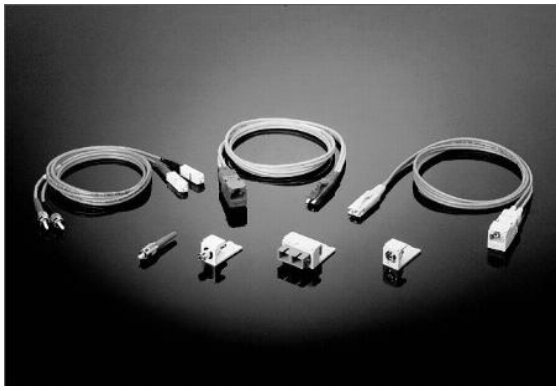


Figura 1.7 Cables de fibra óptica.

Conector RJ-45

El RJ45 es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e y 6). *RJ* es un acrónimo inglés de *Registered Jack* que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho 'pines' o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado.

Es utilizada comúnmente con estándares como EIA/TIA-568B, que define la disposición de los pines o wiring pinout.

Una aplicación común es su uso en cables de red Ethernet, donde suelen usarse 8 pines (4 pares). Otras aplicaciones incluyen terminaciones de teléfonos (4 pines o 2 pares), estos conectores se pueden observar en la figura 1.8.

Figura 1.8 Conectores RJ-45

Red por microondas

Es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. El protocolo más frecuente es el IEEE 802.11b y transmite a 2.4 GHz, alcanzando velocidades de 11 Mbps (Megabits por segundo). Otras redes utilizan el rango de 5,4 a 5,7 GHz para el protocolo IEEE 802.11ª.

Red por radio

Es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red. Hoy en día es muy utilizada en distintas empresas dedicadas al soporte de redes en situaciones difíciles para el establecimiento de cableado, como es el caso de edificios antiguos no pensados para la ubicación de los diversos equipos componentes de una Red de ordenadores.

Los dispositivos inalámbricos que permiten la constitución de estas redes utilizan diversos protocolos como el Wi-Fi: El estándar IEEE 802.11. El cual es para las redes inalámbricas, lo que Ethernet para las redes de área local (LAN) cableadas. Además del protocolo 802.11 del IEEE existen otros estándares como el HomeRF, Bluetooth y ZigBee.

1.3.2. Conexión

Para que todos los cables funcionen en cualquier red, se sigue un estándar a la hora de hacer las conexiones. Los dos extremos del cable llevan un conector RJ45 (Figura 1.9), con los colores en el orden indicado en la figura. El pin 1 corresponde al izquierdo cuando se mira la clavija de frente, con la pestaña de seguridad mirando hacia arriba.

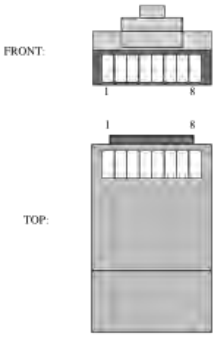


Figura 1.9 Conector RJ45 en switch Ethernet.

Cable recto de red

El esquema más utilizado en la práctica es el 568-B. Existe otra distribución distinta, que sería la 568-A. No existe diferencia alguna en la conectividad entre la distribución 568-B y la distribución 568-A. En la figura 1.3.2.2 se muestra el orden de conexión

Aunque se suelen unir todos los hilos, para las comunicaciones Ethernet solo hacen falta los pines '1 y 2' y '3 y 6', usándose los otros para telefonía (el conector RJ-11 encaja dentro del RJ-45, coincidiendo los pines 4 y 5 con los usados para la transmisión de voz en el RJ-11).

Cable recto (normal/paralelo) T568B

Pin Nº	Extremo 1	Extremo 2	Color	Función
1			Blanco - Naranja	Transceive data +
2			Naranja	Transceive data -
3			Blanco - Verde	Receive data +
4			Azul	Bi-directional Data +
5			Blanco - Azul	Bi-directional Data -
6			Verde	Receive data -
7			Blanco - Marrón	Bi-directional Data +
8			Marrón	Bi-directional Data -

Figura 1.10 Configuración de un cable recto.

Cable cruzado

Si solo se quieren conectar 2 computadoras, existe la posibilidad de colocar el orden de los colores de tal manera que no sea necesaria la presencia de un hub. Es lo que se conoce como un cable cruzado, su conexión se muestra en la Figura 1.11.

Actualmente la mayoría de hubs o switches soportan cables cruzados para conectar entre sí. A algunas tarjetas de red les es indiferente que se les conecte un cable cruzado o normal, ellas mismas se configuran para poder utilizarlo PC-PC o PC-Hub/switch. (4)

Cable cruzado (4 pares, tarjetas 10/100) T568B

Pin Nº	Extremo 1	Extremo 2	Función
1			Transceive data +
2			Transceive data -
3			Receive data +
4			Bi-directional Data +
5			Bi-directional Data -
6			Receive data -
7			Bi-directional Data +
8			Bi-directional Data -

Figura 1.11 Configuración de un cable cruzado.

2. Elementos que conforman la red.

2.1. Introducción

Un dispositivo es todo aquel equipo conectado directamente a un segmento de red. Los dispositivos se dividen en dos clasificaciones:

- **Dispositivos de usuario final**. Incluyen computadoras, impresoras, escáneres y otros dispositivos que proporcionan servicios directamente al usuario.
- **Dispositivos de red**. Abarcan todos los dispositivos que conectan los dispositivos de usuario final para permitir que se comuniquen.

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean.

Los dispositivos de usuario final que proporcionan al usuario una conexión a la red también se conocen como **hosts**. Estos dispositivos permiten al usuario compartir, crear y obtener información y se interconectan físicamente a los medios de red mediante una **NIC** (**Network Interface Card**, tarjeta de interfaz de red). A las NIC también se les conoce como adaptadores de red. Cada NIC tiene un código único llamado dirección MAC.

El objetivo de la Interconexión de Redes (internetworking) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios.

Los dispositivos de interconexión de red proporcionan el transporte de los datos que deben ser transferidos entre dispositivos de usuario final. Los dispositivos de red extienden las conexiones por cable,

concentran las conexiones, convierten los formatos de los datos y administran las transferencias de los datos. (2)

Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta.

En este capítulo se describen los elementos de interconexión utilizados para la implementación del laboratorio, así como una breve explicación de los sistemas operativos que contienen, los cuales serán explicados más a fondo en el siguiente capítulo.

2.2. Características de los elementos de interconexión

2.2.1. Linksys router BEFSR41

LAN/WAN WAN:	1 puerto RJ45 10Base-T para router Cable/ADSL
Velocidad :	10/100 Mbits
Standards:	PC Card 16-bit standard, IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX), IEEE 802.11b (Wireless)

Figura 2.1. Router Inalámbrico BEFSR41, Cisco.

2.2.2. Router Cisco Serie 2500

Requerimientos de energía		
Salida	40W	135 (Btu/hora)
Voltaje de entrada AC	100 a 220 VAC	
Frecuencia	50-60Hz	
Corriente de entrada AC	1.0 a 0.5A	
Voltaje de entrada DC	-48 VDC	

Router Cisco Modelo 2511 serie 2500	
Interfaces	1 puerto RJ-45 10Base-T
	8 puertos asíncronos de alta velocidad
	RJ-45 Auxuiliar y de Consola
	Interface auxiliar RJ-45
	2 Puertos seriales sincronos
Arquitectura de Memoria Flexible	Respaldo de imagen almacenada en M-Flash
	2 Modulos DRAM socket SIMM para buffer de paquetes y tablas de ruteo
Procesador	68030 a 20MHz
Memoria Flash	8 a 16 MB
Memoria de sistema de paquetes	4 a 16 MB

(14)

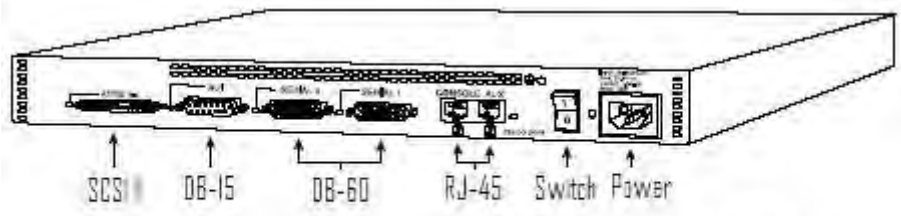


Figura 2.2. Parte trasera de router Cisco serie 2500 modelo CISCO 2509. (13)

2.2.3. Switch SMC-EZ1024DT

Cantidad de puertos	24 x Ethernet 10Base-T, Ethernet 100Base-TX
Velocidad de transferencia de datos	100 Mbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Tecnología de conectividad	Cableado
Modo comunicación	Semidúplex, dúplex pleno
Protocolo de conmutación	Ethernet
Tamaño de tabla de dirección MAC	8K de entradas
Indicadores de estado	Actividad de enlace, modo puerto dúplex, alimentación, dispositivo conectado a 100M
Características	Control de flujo, capacidad dúplex, enlace ascendente, conmutador MDI/MDI-X, negociación automática
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3x

Figura 2.3. Switch SMC-EZ1024DT (15)

2.2.4. Sun Fire X2100 Server

PROCESADOR	Un modelo de AMD Opteron procesador de 100 series, single-core (modelos 146.148, 154, 156) o dual-core (modelos 180, 185).
MEMORIA	Cuatro ranuras de DIMM, DDR1/400 ECC inseparado DIMMs (128-bit más data bus de ECC), 512 MB, un GB, dos GB DIMMs soportados, configuración del sistema a partir de 512 MB a ocho GB

DISCO INTERNO	Hasta dos accionamientos de disco hot-pluggable de 3.5 pulgadas SATA; INCURSIÓN 0, 1 onboard; Discos de 80 GB, de 250 GB y de 500 GB soportados.
INTERFACES ESTANDAR INTEGRADAS	SATA.- Cuatro canales de interface SATA, solo acceso interno. NETWORK.- Dos puertos Ethernet 10/100/1000 Base-T SERIAL.- Un puerto DB9 asíncrono USB.- Seis puertos USB 2.0 (dos frontales, cuatro posteriores)
SISTEMAS OPERATIVOS	• Solaris 10 OS (12/05) o posterior, 64-bit • Red Hat Enterprise Linux 3 U6 o posterior, 32-bit/64-bit • Red Hat Enterprise Linux 4 U2 o posterior, 32-bit/64-bit • SUSE LINUX Enterprise Server 9 SP2 o posterior, 64-bit • Windows Server 2003, Standard o Enterprise Edition SP1, 32-bit/64-bit

Figura 2. 4. Servidor Sunfire X2100, Sun Microsystems. (16)

2.2.5. Sun Ultra 10, Sun Microsystems

ARQUITECTURA	300, 333, 360, o 440-MHz UltraSPARC[tm]-IIi

MEMORIA	Cuatro ranuras DIMM. Instalar DIMMs en pares (16 MB, 32 MB, 64 MB, 128 MB, y 256 MB DIMMs); para un mayor rendimiento.1 GB máximo.
DISCOS	Hasta dos de 4.3 GB (4500 RPM) o 9.1/20.4 GB (7200 RPM), 3.5-in. IDE realzado HDD
CD-ROM:	CD-ROM 24X-, 32X, o 48X-speed
FLOPPY	Disco blando 1.44-MB

INTERFACES ESTANDAR

Audio	Cuatro puertos audio: auricular (hacia fuera), línea-entrada, línea-hacia fuera y micrófono (adentro) que usan estándar de EIA gatos de 0.125 pulgadas (3.5-milímetro)
Ethernet	Una Ethernet/conectador estándar de conductor doble retorcido rápido de Ethernet (10BASE-T/100BASE-T) (RJ-45)
Gráficos	Un puerto de gráficos(HD15), onboard 24 bit buffer
Teclado y ratón	Un puerto estándar del teclado/de ratón (mini DIN-8) Paralelo Un IEEE 1284 puertos paralelos (bidireccionales) (DB25)
PCI	Cuatro ranuras de 32 bits PCI full size, 33 megaciclos, 5 voltios
Serial	Un puerto serial síncrono/asincrónico (DB25); un puerto serial asincrónico (DB9)
Ranura de gráficos UPA	Una ranura de los gráficos de 100-MHz UPA; opciones de alto rendimiento de los gráficos, soporta Creator, Creator3D, y Elite3D (16)

Figura 2. 5. Equipo de trabajo Sun Ultra 10, Sun Microsystems.(17)

2.3. Interfaz respectiva de las estaciones de trabajo.

Aurora SPARC Linux (Utilizado en las estaciones SUN ULTRA 10); basado en Fedora, para las computadoras SPARC. Aurora fue creada originalmente después de que la ayuda de Red Hat cayera para la arquitectura de SPARC, después del sombrero rojo Linux 6.2.

El nombre deriva del codename interno del sol para el SPARCStation 5 chasis. Puesto que él Aurora se deriva de Fedora, y la mayor parte de sus reveladores están situados en los E.E.U.U., se mantienen solamente los paquetes legalmente distribuibles en los Estados Unidos.

Figura 2. 6. Logotipo del Sistema Operativo Aurora. (18)

Windows XP (utilizado en una PC) es una línea de sistemas operativos que fueron hechos públicos el 25 de octubre de 2001 por Microsoft. Se considera que están en el mercado 400 millones de copias funcionando. Las letras "**XP**" provienen de la palabra ***exp****erience*.

Windows XP es una línea de sistemas operativos desarrollada por Microsoft, orientada a cualquier entorno informático incluyendo computadoras domésticas o de negocios, computadoras portátiles, las llamadas "Tablet PC" y *media center*. Windows XP es el sucesor de Windows 2000 y Windows ME, y el primer sistema operativo de Microsoft orientado al consumidor que se construye con un núcleo y arquitectura de Windows NT y que se encuentra disponible en versiones para PC de 32 y 64 Bit.

Las ediciones de Windows XP más comunes son la edición HOME destinada al hogar y la PROFESSIONAL que tiene características adicionales tales como la posibilidad de unirse a un dominio, en vez de solo a grupos de trabajo, y soporte para procesadores duales. Dos versiones de 64 bits, fueron lanzadas, Windows XP edición 64 bits para los procesadores Itanium y otra diseñada para procesadores AMD64 y EM64T.

Windows XP a diferencia de sus versiones anteriores presenta mejoras en la estabilidad y eficacia de Windows. Presenta una Interfaz gráfica de usuario (GUI) perceptiblemente reajustada, un cambio de Microsoft promovido para un uso más fácil que en las versiones anteriores de Windows. Es también la primera versión de Windows que utiliza la activación del producto para reducir la piratería del software, una restricción que no sentó bien a algunos usuarios.

Figura 2. 7. Logotipo del Sistema Operativo Windows XP. (19)

Solaris (Utilizado en el Server Sun Fire X2100), es un sistema operativo desarrollado por Sun Microsystems. Es un sistema certificado como una versión de UNIX. Aunque Solaris en sí mismo aún es software propietario, la parte principal del sistema operativo se ha liberado como un proyecto de software libre

denominado *Opensolaris*. Solaris puede considerarse uno de los sistemas operativos más avanzados. Sun denomina así a su sistema operativo.

IOS son las siglas de (Internetwork Operating System, Sistema Operativo de Interconexión de Redes) creado por Cisco Systems para programar y mantener equipos de interconexión de redes informáticas como switches (conmutadores) y routers (enrutadores).

Al arrancar un dispositivo de Cisco este realiza un Bootstrap (comprobación de hardware).

Después intentará cargar una imagen IOS desde la memoria Flash o desde un servidor TFTP. En el caso de no hallarla ejecutará una versión reducida de la IOS ubicada en la ROM.

Tras el arranque del sistema localizará la configuración del mismo, generalmente en texto plano. Puede estar ubicada en la memoria NVRAM o en un servidor de TFTP. En el caso de no encontrarla iniciará un asistente de instalación (modo Setup).

3. SISTEMAS OPERATIVOS

3.1. Sistema operativo Solaris Sun Microsystems (Linux).

Solaris es un sistema operativo desarrollado por Sun Microsystems y certificado como una versión de UNIX. Aunque Solaris en sí mismo aún es software propietario, la parte principal del sistema operativo se ha liberado como un proyecto de software libre denominado Opensolaris.

Historia

En 1982, cuatro hombres fundaron SUN™ Microsystems, Inc (20). En el mismo año, SUN™ creó su propio sistema operativo, SunOS (21). Estaba basado en BSD, la versión libre de UNIX mantenida por la universidad de Berkeley. En 1991 (el mismo año en que un estudiante finlandés conseguía la especificación POSIX y empezaba a trabajar en un kernel para GNU) SUN™ se pasó a una nueva versión basada en System V, Solaris®.

Solaris® suele verse como el UNIX comercial más avanzado, resaltan sus avances en *hotplug* o "enchufe en caliente"; las últimas versiones permiten hacer trasplantes de cerebro en caliente, es decir cambiar procesadores defectuosos sin parar la máquina.

Desde sus primeros momentos Solaris® proporcionó un excelente soporte para aplicaciones de red en protocolos IP, y fue el primer entorno donde se desarrolló el sistema JAVA® y prácticamente todas las funcionalidades típicas de los sistemas UNIX en entorno servidor, como sockets, multitarea, Threads, entorno de ventanas basado en X-Window en el que se pueden usar diferentes escritorios como Open Look o GNOME.

Recientemente SUN™ Microsystems ha sacado a la luz la versión 10.0 de su sistema operativo Solaris® del que ha liberado su código fuente (23). Su producto se distribuye bajo la licencia CDDL (Common Development and Distribution License) (24), un nuevo tipo de licencia desarrollada por SUN™ y presentada el 14 de diciembre de 2004 al Open Source Initiative (OSI), y se aprobó el 14 de enero de 2005 como licencia Open Source valida.

La modalidad de licenciamiento CDDL está basada en la licencia MPL 1.1 (Mozilla Public License), con algunas condiciones no incluidas en la mayoría de las licencias open source. Por ejemplo, permite tener cualquier tipo de código dentro de la misma solución, sea cual sea la licencia del mismo (la licencia GPL está fuertemente limitada, y sólo permite la concatenación con el propio código GPL).

Con la apertura del código fuente, SUN™ Microsystems libera a la comunidad de código abierto más de 1600 innovaciones patentadas, y su objetivo de proporcionar acceso a estas patentes es promover la innovación y ayudar a desarrolladores y usuarios a lanzar al mercado nuevos productos y tecnologías de código abierto de forma más rápida y sin tener que obtener licencias de de patentes de SUN™.

SUN™ Solaris® funciona principalmente sobre la arquitectura SPARC en 32 y 64 bits (esta última conocida como UltraSparc) o sobre procesadores x86 con tecnología de 32 bits y 64 bits de las marcas Intel® o AMD® Opteron. Solaris tiene una reputación de ser muy adecuado para el multiprocesamiento simétrico (SMP), soportando un gran número de CPUs.

3.1.1. OpenSolaris

La base de OpenSolaris fue alimentada el 14 de junio de 2005 a partir de la entonces actual base de desarrollo de código de Solaris. Es posible descargar y licenciar versiones tanto binarias como en forma de código fuente sin coste alguno. Sun ha anunciado que las versiones futuras de Solaris se derivarán a partir de OpenSolaris.

Algunas características de Solaris:

- Sistema preventivo de auto reparación (27).

Solaris® 10.0 puede, automáticamente, diagnosticar, aislar y recuperar muchas fallas en lo recursos de hardware y aplicaciones reduciendo los tiempos de caída y no disponibilidad de los centros de datos.

- D trace (28) (Administrador de Aplicaciones)

Denominado también rastreo dinámico, que busca el fondo y llega a la raíz de los problemas de rendimiento en tiempo real. Dicha herramienta trabaja utilizando sondas inteligentes del sistema que pueden acceder a áreas de más lento rendimiento o con cuellos de botella, estas sondas están dispersados por todo el sistema, que ilumina cada rincón oscuro del sistema solaris. Con estas nuevas herramientas de diagnóstico, los desarrolladores pueden lograr mecanismos de detección de fallas y solución de problemas en milisegundos o minutos y no de horas o días como ocurría en el pasado.

- Solaris® Containers (29)

Solaris® 10.0 es el único sistema operativo que provee múltiples particiones de software con más de 8000 *containers*. Los recursos del sistema pueden ser reubicados consiguiendo un incremento del 80% en la capacidad de utilización del sistema.

- Zfs (30)

Es un nuevo sistema de archivos dinámico del sistema operativo solaris ofrece una administración sencilla que automatiza y consolida complicados conceptos de almacenamiento y por otro lado protege todo los datos con sumas de 64 bits que detectan y corrigen el daño de datos silenciosos. Es el primer sistema de archivos de 128 bits, ofrece una capacidad de 16.000 millones de veces superior a la de los sistemas de 32 o 64 bits, virtualmente es el único sistema de archivos con capacidad de almacenamiento prácticamente ilimitada.

- Process rigths management (31)

Solaris 10 ofrece una solución para el modelo de usuario "todo o nada" mediante la integración de mínimos privilegios de seguridad directamente dentro de la base del sistema operativo. Gracias a esta nueva función, Solaris se mantiene como el único sistema operativo UNIX que ofrece este modelo de seguridad completamente integrado dentro de sus componentes del núcleo del sistema operativo, cada aplicación solaris

tiene una lista cerrada de los privilegios específicos impuestos por el núcleo, en lugar de un solo privilegio de raíz todopoderoso.

Adicionalmente cada servicio solaris ha sido convertido para que utilice sólo los privilegios mínimos necesarios, lo cual hace aún más difícil violar el sistema y utilizar los servicios. Los administradores pueden asignar grupos de privilegios por funciones para diferentes tipos de administradores y desarrolladores.

Libre de virus por más de 20 años, solaris incluye la tecnología del trusted solaris ampliamente utilizada por el gobierno de los Estados Unidos para garantizar la seguridad de sus sistemas.

- Sun update connection (32)

Utilizando solaris 10 los usuarios disponen de un servicio de actualizaciones que les permitirá estar al día con las innovaciones y el entorno del nuevo ambiente operativo.

- Compatibilidad garantizada (33)

SUN™ ofrece Solaris® Application Guarantee la cual asegura que las aplicaciones previas de Solaris® pueden correr en Solaris® 10.0, extendiendo la cobertura de compatibilidad hasta la versión Solaris® 2.6.

3.1.2. Networking

El crecimiento exponencial en la conectividad, servicios y aplicaciones de red se logra mejorando su rendimiento. El reto de Solaris es mejorar el rendimiento de red sin comprometer las aplicaciones existentes, en lugar de eso se busca incrementar el rendimiento vía el cache de la capa de red 7 e incrementando de TCP/IP y UDP/IP. Adicionalmente, Solaris 10 soporta las especificaciones de IPv6, alta disponibilidad, flujo, y voz sobre IP (VoIP) a partir de enrutamiento extendido.

3.1.2.0 Como configurar una interfaz en Solaris

Este procedimiento explica como determinar qué interfaces están disponibles en el sistema y su estado. Además, también muestra cuales de ellas están "habilitadas". Hay que señalar que para poder configurar las interfaces es necesario accesar al sistema como root o superusuario.

 # dladm show-link Determina tanto las interfaces están instaladas en sistema, así como los controladores que encuentra, sin considerar si están configuradas.

 # ifconfig -a Determina que interfaces están habilitadas en el sistema y muchas otras funciones.

El procedimiento para levantar la interfaz de red es el siguiente:

 # dladm show-link

 # ifconfig *interface* **plumb up**

En el caso del servidor sería:

 # ifconfig bge0 **plumb up** Habilita la tarjeta de red bge0.

 # ifconfig bge0 192.168.1.2 **netmask +** 255.255.255.0 Asigna una dirección IP y su máscara de red.

 # ifconfig -a Verifica que las interfaces están configuradas y habilitadas.

 # reboot -- -r Reinicia el sistema.

(Opcionalmente) Para hacer que la configuración de la interfaz persista en el reinicio, realiza los siguientes pasos:

a) Crear un archivo /etc/hostname.interface para cada una de las interfaces a configurar

b) Editar el archivo /etc/hostname.interface. Al menos debe de contener la dirección IPV4 de la interfaz, también se puede agregar la máscara de red e información adicional.

c) Agregar las entradas de las nuevas interfaces en el archivo /etc/inet/ipnodes, por ejemplo:

10.0.0.14 myhost
192.168.84.3 interface-2
192.168.84.72 interface-3

d) Agregar las entradas de las nuevas interfaces en el archivo /etc/inet/hosts, por ejemplo:

Internet host table
#
127.0.0.1 localhost
10.0.0.14 myhost
192.168.84.3 interface-2
192.168.84.72 interface

e) Inicio de reconfiguración personalizada

 # reboot -- -r

f) Verificar que la interfaz que se creó haya sido configurada

 # ifconfig -a

3.1.2.1 Solaris DHCP

DHCP es el acrónimo de Dynamic Host Configuration Protocol (que podría traducirse como "Protocolo Dinámico de Configuración de Puestos"). Diseñado por Microsoft, su principal tarea consiste en asignar de

manera automática las direcciones IP a los puestos de una red TCP/IP (65), Esta acción se denomina alquilar una dirección IP a un equipo cliente o facilitarle una concesión.

Esencialmente el funcionamiento de este protocolo consiste en que, cuando un cliente DHCP (uno de los ordenadores de nuestra red) se inicia, envía un mensaje de difusión de manera que el servidor DHCP pueda detectarlo. En este mensaje indica que se está iniciando y que necesita una nueva dirección IP.

El servidor DHCP que está a la escucha contesta a la petición de alquiler del cliente con otra difusión (el cliente aún no tiene asignada la IP, por lo que se debe hacer de este modo para que pueda recibir la información). Cuando recibe la primera de estas ofertas el cliente siempre la acepta., enviando en ese instante otro mensaje de difusión informando de la dirección IP que acaba de aceptar, de manera que todos los servidores a la escucha sepan que la petición ya ha sido atendida. Por fin, el servidor DHCP le alquila la dirección IP, le devuelve una especie de "acuse de recibo" al cliente, el cual puede empezar a usar esta nueva IP sin problemas.

Si no se indica lo contrario este "alquiler" de la dirección IP se mantiene durante la configuración establecida, al cabo de los cuales el cliente debe solicitar una renovación. Si el servidor DHCP que hizo la concesión todavía está en funcionamiento, y la dirección IP no ha sido requerida por nadie tras haber expirado, se renueva el alquiler de manera automática. Si la dirección no estuviese disponible (por ejemplo, porque el cliente estuvo apagado durante varios días y se le ha concedido su IP a otro cliente nuevo) se deberá iniciar de nuevo el proceso de difusión para solicitud de un nueva IP (66).

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- Asignación manual o estática: Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.

- Asignación automática: Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.

- Asignación dinámica: el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se

inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red (65).

3.2. Comandos UNIX

A continuación se enlistan los comandos más recurridos durante la instalación y configuración de Solaris 10 en el servidor Sun Microsystems x2100.

Sintaxis

Ingresar los comandos en el prompt, éstos serán ejecutados de izquierda a derecha. Hay que separar los comandos por uno o más espacios.

3.2.1. Comandos de ayuda

help		Lista las principales categorías de ayuda
help	categoría	Muestra ayuda para todos los comandos en la categoría. Utiliza solamente la primera palabra de la descripción de la categoría
help	comando	Muestra ayuda para un comando individual.

3.2.2. Comandos de teclado de emergencia

install – install files

/usr/ucb/install [-cs] [-g *group*] [-m *mode*] [-o *owner*] *filename1 filename2*
/usr/ucb/install [-cs] [-g *group*] [-m *mode*] [-o *owner*] *filename... directory*
/usr/ucb/install -d [-g *group*] [-m *mode*] [-o *owner*] *directory*

Install es utilizado dentro de los creadores de archivos para copiar nuevas versiones de archivos dentro de un directorio destino y que además crea el directorio destino.
Las primeras dos formas son similares al comando cp agregando además que en los archivos ejecutables pueden modificarse los permisos.
La tercer forma puede ser utilizada para crear un directorio destino y conservando los permisos propios y de grupo.
Nota: el comando install no utiliza privilegios especiales para copiar archivos de un lugar a otro. Esto implica que:

- Se deben tener los permisos para leer los archivos a ser instalados
- Se deben tener los permisos para copiar en el archivo o directorio destino
- Se deben tener los permisos para cambiar los modos sobre la copia final del archivo, puede utilizar la opción –m para cambiar los modos.
- Si se quiere especificar la propiedad del archivo a ser instalado debe ser Superusuario (Root) con –o. Si uno no es Root o si –o no hace efecto el archivo instalado será de su propiedad, ya sin importar de quien es el original.

-c Copia archivos. De hecho install siempre copia archivos, pero la opción –c se mantiene para compatibilidad con sistemas anteriores que por alguna razón se interrumpan.

-d Crea un directorio. Los directorios origen faltantes fueron creados en su momento por medir –p. Si el directorio aún existe, el propietario, grupo y modo deberá ser establecido de acuerdo a los valores dados sobre la línea de comandos.

-s Encuera (de permisos) los archivos ejecutables mientras son copiados

-g group Establece el propietario de grupo del archivo o directorio a ser instalado (establecido por defecto)

-m mode Establece el modo del archivo o directorio a ser instalado (0755 por defecto)

-o owner Si se corre como Root, se establece la propiedad del archivo al usuario –ID del propietario

Nombre	**chmod**	Cambia los permisos de un archivo
Resumen	**chmod (-fr)**	archivo en modo absoluto
Descripción		chmod cambia o asigna el modo de los archivos. También puede ser usado para modificar una Lista de Control de Acceso (ACLs) sobre archivos y directorios.

Modo absoluto: una especificación de modo absoluto posee el siguiente formato:

chmod (opciones) absolute-mode file... donde modo-absoluto es especificado utilizando números octales nnnn definidos a continuación:

n	un número del 0 al 7. Un modo absoluto a partir de OR de cualquiera de los siguientes modos:
400	Establece ID de usuario al ejecutarse
20 # 0	Establece ID de grupo al ejecutarse si el # es 7, 5, 3 o 1
0007	Permite leer, escribir y ejecutar (buscar) por otros

Para los directorios, el bit setgid no puede ser establecido (o borrado) en modo absoluto, este debe ser puesto (o borrado) en modo simbólico utilizando g+s (o g -s).

Modo simbólico

Una especificación de modo simbólico tiene el siguiente formato:

chmod (options) symbolic-mode-list file... donde la symbolic-mode-list es una lista separada por coma (sin espacios en blanco) de expresiones en modo simbólico de la forma:

(who) operator (permissions)

Las operaciones son ejecutadas en el orden dado. Las letras de los permisos van seguidas de un operador simple y llevan a cabo las operaciones correspondientes simultáneamente.

who cero o los caracteres u, g, o y a especifican que permisos serán cambiados o asignados:

u	permisos de usuario
g	permisos de grupo
o	otros permisos
a	todos los permisos (usuario, grupo y otros)

Si who es omitido, se establece **a** por defecto, pero el establecimiento de la máscara de creación en el modo de archivo es tomado en cuenta (ver umask in sh (I) para más información). Cuando **who** es omitida, chmod no reemplaza las restricciones de los bits de enmascaramiento usuario.

operador +, -, = indican que permisos serán cambiados

+	Añade permisos Si los permisos son omitidos, nada se añade Si **who** es omitido, se añaden bits de modo al archivo representado por los permisos.
-	Elimina permiso Si los permisos son omitidos, nada se hace Si **who** es omitido, se borran bits de modo al archivo representados por permisos, excepto cuando estos corresponden a bits de enmascaramiento.

Si who está presente, borra los bits de modo del archivo representados por permisos.

=	Asigna permisos absolutos Si **who** es omitido, borra todos los bits de modo del archivo; si **who** es presente, borra los bits de modo del archivo representados por **who**. Si los permisos son omitidos, no se hace nada Si **who** es omitido, añade bits de modo al archivo que representan permisos, excepto los bits de mascara. Si **who** está presente, añade bits de modo al archivo que representan permisos. A diferencia de otras operadores simbólicos, = tiene un efecto absoluto en que éste resetea todos los otros bits representados por **who**. Omitiendo los permisos es utilizado solamente con = para eliminar todos los permisos.
Permisos	cualquier combinación compatible de las siguientes letras:
l	bloqueado
r	permiso de lectura
s	establecer ID de usuario o grupo
t	bit sticky
w	permiso de escritura
x	permiso para ejecutar
X	permiso de ejecución si el archivo es un directorio o si hay un permiso de ejecución para uno de los otros usuarios de clase.
u, g, o	indican que los permisos son tomados de los usuarios habituales, grupos u otros.

Los permisos para un archivo pueden variar dependiendo del número de identificación de usuario o del número de identificación del grupo (GID). Los permisos son descritos en tres secuencias cada una con tres caracteres:

Usuario	Grupo	Otros
rwx	rwx	rwx

Este ejemplo demuestra (usuario, grupo, y otros tienen todos los permisos para leer, escribir y ejecutar un archivo dado) demuestra dos categorías para conceder permisos: el tipo de acceso y los permisos mismos.

La letra **s** solo es significativa con u o **g**, y **t** solamente trabaja con **u**.

El bloqueo de un archivo con (**l**) para lectura o escritura se establece mientras un programa accede al archivo.

En un directorio con bit ID de grupo establecido (con ----s----- o ----l----- en el desplegado del comando -ls o -ld), heredaran la ID de grupo del archivo de origen, no los del proceso en curso.

No se permite la ejecución de grupo ni bloquear un archivo en ejecución a la vez. Además, no es posible establecer el bit ID de grupo ni bloquear archivos en ejecución a la vez. Los siguientes ejemplos, por lo tanto, son inválidos y despliegan mensajes de error:

chmod g+x, +l file
chmod g+x, +l file

Solamente el propietario de un archivo o directorio (o el root) pueden cambiar el modo de archivo o directorio.

Nombre chown -cambiar de propietario a un archivo

Sinopsis **chown** [-fhR] propietario [: grupo] archivo...

chown -R [-f] [H| -L | -P] propietario [: grupo] archivo...

Descripción

chown asigna la ID de usuario del archivo al propietario especificado y, opcionalmente, establece la ID de grupo al grupo especificado.

Si chown es invocada por el usuario, la ID actual es eliminada.

Solamente el propietario de un archivo o el superusuario pueden cambiar la propiedad del archivo.

El sistema operativo posee una opción de configuración {_POSIX_CHOWN_RESTRICTED}, para restringir los cambios de propietario. Cuando se ejecuta esta acción el usuario es prevenido. Solamente el superusuario puede cambiar arbitrariamente las ID de propiedad. Para establecer esta opción de configuración, incluya la siguiente línea en /etc/system:

set rstchown = 1

Para deshabilitar la opción, incluya la siguiente línea en /etc/system:

set rstchown = 0

{_POSIX_CHOWN_RESTRICTED} es habilitado por defecto.

Opciones /usr/bin/chown and
/usr/xpg4/bin/chown

Las siguientes opciones están disponibles:

-f Forzar. No reporta errores

-h Si el archivo es un link simbólico, esta opción cambia su propietario. Sin esta opción, el propietario del archivo es cambiado.

-H Si el archivo especificado en línea de comandos es un link simbólico referente a un directorio, se cambia la propiedad del directorio y todo el árbol contenido. Si el link se encuentra dentro del árbol, la propiedad del archivo en cuestión es cambiada sin afectar los demás archivos.

-L Si el archivo es un link simbólico, la opción cambia la propiedad del archivo referenciado por el link simbólico. Si el archivo es especificado en línea de comandos, o dentro de un árbol de archivos, o es un link referente a un archivo dentro de un directorio, entonces esta opción cambia la propiedad, sin afectar al resto.

-P Si el archivo especificado sobre una línea de comandos es un link simbólico dentro de un árbol de archivos, la

opción cambia la propiedad del link sin afectar a ningún otro elemento del árbol de archivos.

/usr/bin/chown Son disponibles las siguientes opciones:

-R Recursiva. chown desciende a través de un directorio, y subdirectorios, aplicando las ID de propiedad especificadas. Cuando un link simbólico es encontrado, el propietario del archivo blanco es cambiado, excepto los archivos especificados con la opción -h o -P. Tampoco hay recursión si se especifican los archivos con las opciones -H o -L.

Name mkdir -crea directorios

Sinopsis **mkdir** [-m mode] [-p] dir...

Descripción El comando mkdir crea directorios en modo 777 (posiblemente alterados por la máscara del modo de archivo **umask** [1]).

Las entradas estándar son establecidas automáticamente. mkdir no puede crear estas entradas por nombre. La creación de un directorio requiere permisos de escritura en los directorios origen.

Las ID de propietario y grupo de los nuevos directorios son asignadas del usuario en curso.

setgid y mkdir

Para cambiar el bit setgid sobre un directorio recién creado, se debe utilizar chmod g+s después de ejecutar mkdir.

La configuración del bit setgid es heredada del directorio origen.

Nombre **chgrp**

Esta instrucción permite cambiar el grupo. Cada fichero Unix tiene un usuario y un grupo, que corresponden con el usuario y el grupo de quien lo creó. El usuario root puede cambiar a cualquier fichero el grupo. Los demás usuarios solo pueden hacerlo con los ficheros propios y grupos a los que pertenezca.

Sintaxis:

chgrp nuevo grupo archivo1 [archivo2 archivo3 ...]
Cambia el grupo de archivo1 archivo2, etc. que pasará a ser nuevo grupo.

chgrp -R nuevo grupo directorio cambia el grupo para que pase a ser nuevo grupo a *directorio*, todos los archivos y subdirectorios contenidos en él, cambiándolos también de forma recursiva en todos ficheros de los subdirectorios.

El sistema operativo tiene una opción de configuración _POSIX_CHOWN_RESTRICTED, para restringir los cambios de propiedad. Cuando esta opción tiene efecto, la propiedad del archivo cambia al grupo al cual pertenece el propietario. Solamente el superusuario

		puede cambiar las ID's de grupo arbitrariamente, sino es así la opción no tendrá efecto. Para establecer esta configuración, hay que incluir lo siguiente sobre la línea de comandos /etc/system: set rstchown = 1 Para deshabilitar esta opción, incluir lo siguiente sobre línea de comandos /etc/system: set rstchown = 0 _POSIX_CHOWN_RESTRICTED es habilitada por omisión.
more	/etc/netmasks	Indica cual es la máscara de subred en el sistema que se está ejecutando
uname		Indica el nombre del sistema que se esta ejecutando.
cat	/etc/nsswitch.conf	Indica el servicio de nombres que utiliza este sistema. Un servicio de nombre guarda la información en un lugar central, lo que permite a los usuarios, equipos y aplicaciones se comuniquen en la red. Algunos ejemplos de la información que se guarda son los nombres y direcciones de host y las contraseñas.
domainname		Proporciona el nombre del dominio en que reside el sistema.

getent ipnodes dns

Para ver la dirección ip del servidor. Deberá introducir un mínimo de una y un máximo de tres direcciones IP.

El sistema de nombres de dominio (DNS) es el servicio de nombres que Internet proporciona para redes TCP/IP. DNS proporciona los nombres host al servicio de direcciones IP. DNS simplifica la comunicación utilizando nombres de equipo en vez de direcciones IP numéricas. DNS también sirve como una base de datos para la administración de correo.

reboot

Comando que arranca de nuevo el sistema

Nombre pwd -nombre del directorio trabajando

Sinopsis /usr/bin/pwd

Descripción

El comando pwd muestra un registro de los directorios que se han ejecutado durante la sesión actual.

mount

Es un comando que se utiliza para agregar más dispositivos (montar dispositivos) en un sistema de archivos, ya que al cargar el sistema operativo, solo se cargan los archivos básicos.

Montar es hacer que el sistema operativo "reconozca un sistema de archivos" en un enlace lógico. Cuando se desocupa se rompe el enlace y se sigue trabajando con los mismos archivos básicos. Para realizar esto Linux dispone de comando *mount*. *mount* es un comando GNU/Linux que prepara una unidad de almacenamiento para su uso por el sistema operativo.

Sintaxis # mount -t tipo_dispositivo /dev/dispositivo_montar /destino

-t:	Este argumento significa "type" y nos permitirá indicar el dispositivo tipo_dispositivo: Indica qué es lo que queremos montar • iso9660 (Para el cdrom) • msdos (Disquetera) • NTFS (Si se trata de una partición de este tipo)
/dev/dispositivo_montar:	Es el nombre del dispositivo que se encarga de realizar la función de controlar la unidad, por ejemplo: /dev/cdrom se encarga del CD-ROM, mientras que /dev/fd0 se encarga de la disquetera.
/destino:	Es el directorio donde queremos visualizar el contenido del dispositivo, ya sea un cd, un disquete, o una partición. (20) Ejemplo de uso: Montando un cdrom `# mount -t iso9660 /dev/cdrom /mnt/cdrom`

Nota: /mnt/cdrom lo crean por defecto la mayoría de las distribuciones, también podemos crear un directorio y montarlo en él.

IMPORTANTE: Colocar un cd en el interior del cdrom.

umount	Este comando nos permitirá desmontar un dispositivo, cualquiera de los anteriores, por ejemplo para desmontar el cdrom, suponiendo que está en /cdrom, simplemente hay que teclear: #umount /cdrom

El **tipo** de sistema de archivos puede ser por ejemplo:

- auto (intenta descubrir automáticamente el sistema de archivos).
- iso9660 (sistema de archivos de los CDs y DVDs).
- ext2 (sistema de archivos muy extendido en maquinas Linux).
- ext3 (igual que ext2 pero además añade journaling).
- reiserfs (otro sistema muy utilizado en maquinas Linux).
- msdos (para dispositivos que usen FAT12 o FAT16).
- vfat (para dispositivos que usen FAT32).
- ntfs (sistema de archivos NTFS de Windows NT, XP, etc...).
- smbfs (sistema de archivos de Samba).
- nfs (sistema de archivos de red NFS).
- hfs y hfsplus (acceden a sistemas de archivos de Apple Macintosh).

Los **dispositivos** se encuentran dentro de /dev. Así es como se designan los más comunes:

- fd0 Primera unidad de disquetes (a: en sistemas MS-DOS y Windows).
- fd1 Segunda unidad de disquetes (b: en sistemas MS-DOS y Windows).
- hda Primer disco duro IDE (Primary Master).
- hda0 Primera partición del primer disco duro IDE (Primary Master).
- hda1 Segunda partición del primer disco duro IDE (Primary Slave).
- hdb0 Primera partición del segundo disco duro IDE (Secondary Master).
- hdb1 Segunda partición del segundo disco duro IDE (Secondary Slave).
- sda Primer disco duro SCSI.
- sda1 Primera partición del primer disco duro SCSI.
- sdb4 Cuarta partición del segundo disco duro SCSI.
- scd0 Primera unidad de CD-ROM SCSI.
- scd1 Segunda unidad de CD-ROM SCSI.
- sga Primer dispositivo genérico SCSI (scanner, etc.).
- sgb Primer dispositivo genérico SCSI.
- sg0 Primer dispositivo genérico SCSI en sistemas nuevos.
- sg1 Segundo dispositivo genérico SCSI en sistemas nuevos.

- Desde la aparición de las unidades de almacenamiento USB (pendrives) y los discos duros SATA (serial ATA), estos han empezado a usar también la denominación propia de los dispositivos SCSI (sda1, sdb3, etc...). Aun así, algunas veces se pueden encontrar unidades IDE con nombres del tipo sda, sdb, etc... ya que ciertas distribuciones utilizan la emulación IDE-SCSI. De esta forma se utiliza una capa de software común para el manejo de todos los discos duros, CD-ROM, etc...

- Algunos ejemplos de montaje de dispositivos son:

- # mount –t vfat /dev/fd0 /mnt/floppy
- # mount –t iso9660 /dev/hdb0 /mnt/cdrom

3.2.3. Opciones comunes para comandos de arranque en UltraSparc

boot [dispositivo especificado] [nombre del archivo] [opciones]

[dispositivo especificado] El nombre del dispositivo, ruta o alias. Ejemplo:

cdrom (CD-ROM) drive

disk (disco duro)

net (Ethernet)

tape (SCSI tape)

[nombre del archivo] Nombre del programa a ejecutar.

[opciones] **-a** Prompt interactivo para el dispositivo y nombre del archivo de arranque.

-h Detener después de cargar el programa

boot cdrom Permite arrancar desde el DVD o CD local e iniciar la GUI de instalación de Solaris.

Boot cdrom –text Permite arrancar desde el DVD o CD local e iniciar el instalador basado en texto en una sesión del escritorio.

	-text Indica que se debe ejecutar el instalador basado en texto en una sesión del escritorio. Utilice esta opción para ignorar el instalador gráfico predeterminado.
ok boot cdrom – nowin	Para arrancar desde el DVD o CD local e iniciar el instalador basado en texto en una sesión de la consola, escriba el siguiente comando.
	nowin Indica que se debe ejecutar el instalador basado en texto en una sesión de la consola. Utilice esta opción para ignorar el instalador gráfico predeterminado.

3.3. Software Cisco IOS

IOS son las siglas de (Internetwork Operating System), Sistema Operativo de Interconexión de Redes creado por Cisco Systems para programar y mantener equipos de interconexión de redes informáticas como switches y routers. A través del IOS se consigue configurar los equipos Cisco mediante la denominada "Command Line Interface" (Interfaz de Línea de Comandos) que sirve de intérprete entre el usuario y el equipo. (62)

3.3.1. Etapas de la secuencia de arranque de un router

Un router se inicializa cargando el **bootstrap**, el sistema operativo y un archivo de configuración. Lo más habitual es que el router busque los comandos boot system guardados en la NVRAM. Sin embargo, es importante mencionar que el router puede ser configurado para introducir orígenes fallback, para cargar el software. Una vez que se inicia, si es necesario el router utiliza estos comandos en secuencia.

Si el router no encuentra el boot system en la NVRAM, el sistema busca por defecto el software Cisco IOS almacenado en la memoria **Flash.** Y si la memoria flash está vacía, el router intenta a continuación utilizar el protocolo trivial de transferencia de archivos (**TFTP**) para cargar una imagen del software Cisco IOS de la red. El router utiliza el valor del registro de configuración para formar un nombre de archivo desde el que arrancar una imagen predeterminada del sistema almacenada en un servidor de la red. Si no está disponible un servidor TFTP, el router cargará la versión limitada de la imagen del software Cisco IOS almacenada en la ROM.

Tras el arranque del sistema localizará la configuración del mismo, generalmente en texto plano. Puede estar ubicada en la memoria NVRAM o en un servidor de TFTP. En el caso de no encontrarla iniciará un asistente de instalación (modo Setup). (62)

3.3.2. Comandos

Name	boot system	Comando que se utiliza para especificar la secuencia fallback de arranque del router.

Router #	**configure terminal**	*//Utilizar comandos en modo config*
Router (config) #	**boot system flash IOS_filename**	//Arrancar sistema desde NVRAM
Router (config) #	**boot system tftp IOS_filename tftp_address**	//Arrancar sistema desde la red
Router (config) #	**boot system rom**	//Arrancar sistema desde ROM
[Ctrl+Z]		
Router #	**copy running-config startup-config**	//Guarda los comandos en la NVRAM

Name	show startup-config	Indica que commandos boot system se han introducido.

Arranque desde la memoria flash

Este arranque implica cargar el sistema desde la memoria EEPROM, en el siguiente ejemplo se carga el archivo gsnew-image desde la memoria flash.

Router #	**configure terminal**
Router # (config)#	**boot system flash gsnew-image**
[Ctrl+Z]	
Router #	**copy running-config startup-config**

Arranque desde un servidor de la red

En caso de que la memoria flash esté dañada, una copia de seguridad puede proporcionar una imagen del sistema especificando que debe cargarse desde un servidor TFTP. El siguiente ejemplo # indica que el archivo de imagen test.ext se cargará desde el servidor TFTP en la dirección IP 192.168.2.70

```
Router #                    configure terminal
Router # (config) #         boot system tftp IOS_image 192.168.2.70
[Ctrl+Z]
Router #                    copy running-config startup-config
```

Arranque desde la rom

Si la memoria Flash está dañada y el servidor de red falla al cargar la imagen, arrancar desde la rom es la opción de arranque final del software, sin embargo es una imagen que carece de los protocolos, elementos y configuraciones del software Cisco IOS completo

```
Router #                    configure terminal
Router # (config) #         boot system rom
[Ctrl+Z]
Router #                    copy running-config startup-config
```

3.3.3. Valores del registro de configuración

El registro de configuración es un registro de 16 bits almacenado en la NVRAM. Los 4 bits más bajos del registro de configuración (bits 3, 2, 1, 0) forman el campo boot. En el registro de configuración podemos seleccionar la secuencia a partir de la cual el router cargará la imagen de IOS, dentro del campo boot. Éste campo puede reconfigurarse con el comando de configuración global config-register. Esto se realiza introduciendo un número hexadecimal como argumento para este comando, como se muestra en el siguiente ejemplo:

```
Router#  configure terminal
Router (config)# config-register 0x10F
[ Ctrl  -Z]
```

El registro de configuración está establecido de manera que el router examinará el archivo de inicio que hay en la NVRAM para buscar las opciones de arranque del sistema. Para cambiar el campo boot y dejar los demás bits configurados a sus valores originales, se siguen estas pautas:

- Configure el valor del registro de configuración a 0x100 si necesita entrar en el monitor ROM. Desde este monitor, se arranca el sistema operativo manualmente utilizando el comando b en la línea de comandos del monitor ROM. Este valor establece los bits del campo boot a 0-0-0-0.
- Se configura el registro de configuración a 0x101 para hacer que el sistema arranque automáticamente desde la imagen limitada del software Cisco IOS almacenada en la ROM. Este valor configura el campo boot a 0-0-0-1.
- Se programa el registro de configuración a cualquier valor entre 0x102 y 0x10F para hacer que el sistema utilice los comandos de arranque del sistema de la NVRAM. Ésta configuración es la predeterminada. Estos valores establecen los bits del campo boot entre 0-0-1-0 y 1-1-1-1.

Si no hay comandos boot system en la NVRAM, el sistema buscará normalmente en la memoria Flash la imagen del software Cisco IOS.

Para comprobar la configuración del campo de arranque y verificar el comando config-register, se utiliza el comando show version. (37)

Existen diversas formas de acceder a un router CISCO para su configuración:

1. Mediante un terminal asíncrono (por ejemplo, un PC con un software de emulación de terminales) conectado al puerto serie del router.
2. Mediante protocolos o aplicaciones TCP/IP desde otra máquina accesibles desde alguna de las redes a las que esté conectado el router. En particular, se puede configurar utilizando telnet, un navegador web o mediante el protocolo de gestión SNMP.

En este caso nos centraremos exclusivamente en la configuración mediante telnet.

Nota: se recomienda utilizar como cliente de telnet "**Putty**", instalado en todos los ordenadores del laboratorio.

1 - ACCESO MEDIANTE TELNET

Para acceder al router haga un telnet a la dirección IP del CISCO desde una máquina conectada a una de sus subredes. Por ejemplo:

> telnet 192.168.12.1
User Access Verification
Password:

A continuación teclee el password de acceso ("cisco") y obtendrá el "prompt" del modo no privilegiado de configuración:

Cisco2>

En este modo es posible consultar multitud de parámetros del router, pero no es posible cambiar la configuración del mismo. El interfaz de configuración de un CISCO mediante línea de comandos es similar a la interfaz que ofrece una "shell" de UNIX. Esto es, es posible recuperar los comandos introducidos previamente mediante el uso de las flechas arriba/abajo, y editarlos mediante las flechas derecha/izquierda. Además, no es necesario teclear el nombre completo de los 2 comandos; pueden dejarse incompletos, tecleando únicamente las primeras letras; o bien completarse automáticamente mediante la tecla "Tab". Por ejemplo, el comando "show version" puede abreviarse en "sh ver".

El router ofrece una ayuda muy completa, que permite consultar los parámetros de cada comando. Por ejemplo, si tecleamos "show ?", nos mostrará todas las opciones del comando "show". Si escogemos la opción "ip" de dicho comando, podremos consultar las distintas opciones sin más que teclear: "show ip ?". Para acceder al modo privilegiado de configuración, el cual permite modificar la configuración del router, es necesario teclear:

Cisco2> enable

Password:

Tras introducir el password ("cisco"), el "prompt" cambiará a:

Cisco2#

Para indicar que estamos en modo privilegiado. Si se teclea "help" en este modo, se apreciara que el número de comandos disponibles ha aumentado sensiblemente. Por ejemplo, se teclea "**show conf**" para ver la configuración completa del router.

2 - MODIFICACIÓN DE LA CONFIGURACIÓN

Para cambiar la configuración del router desde el modo privilegiado, es necesario utilizar el comando "**configure**":

Cisco2# configure
Configuring from terminal, memory or network [terminal]?

Se teclea "terminal" o directamente retorno de carro para configurar desde terminal:

Enter configuration commands, one per line. End with CNTL/Z
Cisco2(config)#

A partir de este momento es posible introducir nuevos comandos de configuración. Por ejemplo, si se quisiera añadir una ruta IP, se tecletaría:

Cisco2(config)# ip route 138.4.3.0 255.255.255.192 138.4.3.1
Cisco2(config)# ^Z
Cisco2#

El control-Z final permite salir del modo de configuración (nótese el cambio del "prompt"). También se puede salir de dicho modo tecleando "**end**". Para borrar un comando de configuración se utiliza el método

anterior, pero anteponiendo al comando la palabra "no". Por ejemplo, para borrar la ruta anterior tecletaría el siguiente comando:

Cisco2(config)# no ip route 138.4.3.0 255.255.255.192 138.4.3.1

Una vez fuera del modo de configuración, es necesario teclear el comando "**write**" para que la configuración se guarde en la memoria no-volátil:

Cisco2# write
Building configuration...
[OK]
Cisco2#

Si no se ejecuta el comando "**write**", los cambios se perderán cuando el router se apague o rearranque.

Los comandos de configuración de un router CISCO se clasifican en dos tipos:

- **Comandos generales**, que afectan al router en su conjunto. Por ejemplo, el comando "**ip route** ...", y
- **Comandos particulares de interfaz**, que afectan únicamente a un interfaz del router.

Por ejemplo, si se quisiera cambiar la MTU de uno de los interfaces ethernet, se debería teclear:

Cisco2# conf term
Enter configuration commands, one per line. End with CNTL/Z
Cisco2(config)# interface ether0
Cisco2(config)# ip mtu 1000
Cisco2(config)# ^Z

Es decir, es necesario introducir el nombre del interface (en este caso: **ethernet0** o, de forma abreviada, **ether0**) correspondiente antes de teclear el comando.

3 – GRABACIÓN Y RECUPERACION DE CONFIGURACIONES

Es posible salvar la configuración de un router a un fichero en el servidor de tftp. Esta opción es útil si se va a realizar la práctica en varias sesiones y se quiere conservar las configuraciones de una sesión para la siguiente.

Para salvar la configuración de un router a un fichero en el servidor de tftp utiliza el comando "**write net",** proporcionando la dirección del servidor de tftp y el nombre del fichero a utilizar (para evitar interferencias, se utilizan mnemónicos). Para recuperar la configuración, se siguen los pasos descritos en el apartado anterior.

4 - RECOMENDACIONES GENERALES

• NO MODIFICAR bajo ningún concepto las direcciones IP de los interfaces Ethernet.

Si se cambian podría dejar inaccesible el router, requiriendo la conexión de un cable a la consola del mismo para poder reconfigurarlo.

• Asegurarse de que nadie más está utilizando los routers que ha reservado. Para ello se puede utilizar el comando "show users", que muestra los usuarios actualmente conectados al router vía telnet.

5 - COMANDOS DE INTERÉS

Se enumeran a continuación algunos comandos de interés. (38)

show: muestra información del sistema. Por ejemplo:

show ip routes: muestra las tablas de encaminamiento del router.

show arp: muestra el contenido de la tabla caché de ARP.

show interfaces: muestra información sobre los interfaces de red del router.

show ip traffic: muestra estadísticas sobre el tráfico IP cursado por el router.

clear

clear arp: borra el contenido de la tabla caché de ARP.

clear ip redirect: borra el contenido de la tabla caché de redirecciones.

clear ip route *: borra las entradas en las tablas de encaminamiento aprendidas mediante RIP u otro protocolo de encaminamiento dinámico.

clear counters: borra los contadores de estadísticos de los interfaces.

debug: permite activar las trazas de depuración del router. MUY IMPORTANTE: para visualizar dichas trazas en pantalla cuando se está conectado mediante telnet, es necesario teclear previamente el comando "**terminal monitor**". Para desactivar las trazas utilice el comando "**undebug**". Si quiere desactivar todas las trazas de una vez, utilice "**undebug all**".

debug ip packets: muestra trazas sobre los paquetes IP que son encaminados por el router.

debug ip icmp: muestra trazas sobre los mensajes ICMP enviados o recibidos por el router.

debug isdn *: muestra trazas sobre la actividad del interfaz RDSI.

debug ip rip: muestra trazas sobre la actividad del protocolo de encaminamiento RIP.

configure: permite cambiar la configuración del router.

ip route "destination" "mask" "router": permite añadir una nueva entrada a las tablas de encaminamiento.

ip address "address" "mask" secondary: permite añadir una dirección IP secundaria a uno de los interfaces.

ping: permite realizar un ping desde el router.

traceroute: permite realizar un traceroute desde el router. (37)

4. INTEGRACIÓN DE LA RED

4.1. ESPECIFICACIÓN Y TERMINACIÓN DE CABLE

Los cables de comunicaciones tienen códigos de color para identificar los pares individuales. El código de color es el mismo para todos los cables de comunicaciones de Norteamérica. El uso del código de color asegura la uniformidad al identificar los pares de cables individuales. Cada cable coloreado está asociado con un número específico. (62)

Código de color de cuatro pares

En la mayoría del cableado de voz y datos se usa cable UTP. Estos cables tienen cuatro pares de hilos trenzados en cada cable. El código de color de los cuatro pares es el siguiente:

- Par 1. Blanco / azul
- Par 2. Blanco / naranja
- Par 3. Blanco / verde
- Par 4. Blanco / marrón

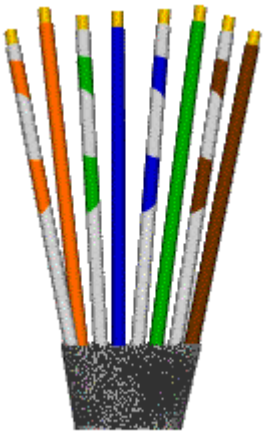


Figura 4.1. Cable UTP.

El par 1 siempre aparece en las posiciones, o pines, 4 y 5 en un jack o plug de 8 pines. El par 4 siempre aparece en posiciones, o pines, 7 y 8 en un jack o plug de 8 pines. Los otros pares tienen diferentes apariencias dependiendo de la norma (T568A o T568B) usada en el plan de cableado.

Figura 4.2. RJ-45

Siempre deben usarse T568A y T568B para este plan de cableado. Debe crearse un nuevo plan de cableado porque cada cable tiene un propósito específico. Si el cableado no es correcto, los dispositivos de cada extremo no serán capaces de comunicar, o experimentarán un rendimiento muy degradado.

Los jacks RJ-45 son jacks de ocho conductores diseñados para aceptar plugs RJ-45 o RJ-11. Los jacks deben cablearse según las normas T568A y T568B.

Figura 4.3. Jack RJ-45.

Los plugs RJ-45 tienen ocho pines que se ajustarán hasta cuatro pares de cables. Como con los plugs y jacks RJ-11, el par 1 siempre termina en los pines centrales; en este caso, los pines 4 y 5. El par 4 (blanco / marrón) siempre termina en los pines 7 y 8. Los pares 2 y 3 pueden diferir dependiendo del plan de cableado. Usando T568B, el par 2 (blanco naranja) termina en los pines 1 y 2. El par 3 (blanco / verde) termina en los pines 3 y 6. T568A invierte los pares 2 y 3 de modo que el par 2 termine en los pines 3 y 6, mientras que el par 3 termina en los pines 1 y 2.

Un jack RJ-45 termina un extremo del cable. El otro extremo de cable generalmente termina en un match panel con un conector estilo 110 o un bloque de conexión estilo 110.

Planificación de la estructura del cableado

El primer paso es reunir los datos necesarios para diseñar la red. Para que una red sea activa y sirva a las necesidades de sus usuarios, estos datos deben reunirse según una serie sistemática de pasos pre planeado. Estos pasos proporcionan una guía para descubrir completamente los datos necesarios para crear la red.

El primer paso del proceso es reunir información sobre la organización. Esta información debe incluir lo siguiente:

- Historia de la organización y estado actual.
- Crecimiento proyectado.
- Políticas operativas y procedimientos de administración.
- Diagramas de construcción (proyectos).
- Diagramas y documentación existentes. (62)

Obviamente, en nuestro caso se trata de un proyecto pequeño en el cual el primer punto comienza con la creación del laboratorio y no se prevé un crecimiento significativo. En cuanto a las políticas operativas y administración de la red, esto significa identificar los recursos y las restricciones del laboratorio. Los recursos del laboratorio que pueden afectar a la implementación de un nuevo sistema y en cuanto a la administración, por ejemplo, se asignaran los siguientes permisos:

Profesores.- Tendrán acceso como superusuarios (root), esto quiere decir que tendrán un control total del sistema.

Usuarios privilegiados.- El supersusuario creará estas cuentas para las personas interesadas en ejecutar programas especializados dentro del servidor, programas tales como Java, Perl, Webmin, etc.

Alumnos.- Se les asignarán privilegios de usuarios de escritorio, esto significa que podrán crear archivos (con acceso a lectura, escritura y ejecución y no podrán borrar archivos ni directorios de otros usuarios) solo en su carpeta de usuario. La carpeta de usuario solo puede ser creada por el superusuario.

Invitados.- Serán usuario con mínimos privilegios, solo podrán ejecutar archivos de solo lectura.

Otro punto importante que se incluye dentro de la administración sería por ejemplo cambiar el sistema operativo del sistema, modelo de los routers, etc. el cual tendría que documentarse.

Con respecto a los proyectos o diagramas de construcción, por ser un proyecto pequeño solo se diseño un pequeño arreglo (figura 4.4). Los diagramas y documentación existente, con respecto al proyecto, serán almacenados en una base de datos encriptada dentro del servidor, solo podrá accederse a ella cuando el superusuario así lo autorice.

Figura 4.4. Arreglo del laboratorio de Transmisión de datos y TSC.

4.3.

Instalación Estructurada del cableado.

Un sistema de cableado estructurado es la infraestructura de cable destinada a transportar, a lo largo y ancho de un edificio, las señales que emite un emisor de algún tipo de señal hasta el correspondiente receptor. Un sistema de cableado estructurado es físicamente una red de cable única y completa.

Los sistemas de cableado estructurado se refieren al cableado de telecomunicaciones integrado de una manera aprobada, normalizada, comenzando en el punto de demarcación, trabajando a través de los distintos recintos de equipo, y continuando por el área de trabajo.

Antes de continuar, es necesario mencionar que existen dos tipos de de redes: redes estructuradas y redes convencionales.

Redes convencionales: Como se puede observar en la figura en las redes interiores actuales, el diseño de la red se hace al construir el edificio y según hagan falta modificaciones se harán colocando cajas interiores, según lo crea oportuno el proyectista y sin ninguna estructura definida. Todo ello tiene el inconveniente de que no siempre tenemos una caja cerca y el cableado hasta la caja, cada instalador la hace por donde lo cree más conveniente, teniendo así el edificio infinidad de diferentes trazados para el cableado.

Además de todo ello, para cada traslado de un solo nodo tenemos que re cablear de nuevo y normalmente dejar el cable que se da de baja sin desmontar, siendo este inutilizable de nuevo muchas veces por no saber y otras por la incompatibilidad de distintos sistemas con un cable.

Pero el mayor problema lo encontramos cuando queremos integrar varios sistemas en el mismo edificio. En este caso tendremos además de la red telefónica la red informática así como la de seguridad o de control de servicios técnicos. Todo ello con el gran inconveniente de no poder usar el mismo cable para varios sistemas distintos bien por interferencias entre los mismos o bien por no saber utilizarlo los instaladores. Los cables están por lo general sin identificar y sin etiquetar.

Desventajas:

- Diferentes trazados de cableado.
- Reinstalación para cada traslado.

- Cable viejo acumulado y no reutilizable.
- Incompatibilidad de sistemas.
- Interferencias por los distintos tipos de cables.
- Mayor dificultad para localización de averías.

Redes estructuradas.- A diferencia de una red convencional, en el cableado estructurado, como su mismo nombre indica, la red se estructura (o divide en tramos), para estudiar cada tramo por separado y dar soluciones a cada tramo independientemente sin que se afecten entre sí.

En el tipo de cableado estructurado se solucionan muchos de los problemas de las redes convencionales, por ejemplo el poder reutilizar el cable para distintos sistemas así como poder compartirlo entre sí sin interferencias. También tenemos que al tratarse de un mismo tipo de cable se instala todo por el mismo trazado (dentro de lo posible) no hace falta una nueva instalación para efectuar un traslado de equipo, siempre que se haya sobredimensionado bien la red, lo cual trae como consecuencia que no existan cables viejos inutilizables. (62)

Ventajas:

- Trazados homogéneos.
- Fácil traslados de equipos.
- Convivencia de distintos sistemas sobre el mismo soporte físico.
- Transmisión a altas velocidades para redes.
- Mantenimiento mucho más rápido y sencillo.

4.3.1. Reglas del cableado estructurado para LANs

Las tres reglas siguientes ayudan a asegurar que los proyectos de diseño de cableado estructurado sean a la vez efectivos y eficaces:

- Buscar una solución de conectividad completa. Una solución óptima para la conectividad de la red incluye todos los sistemas diseñados para conectar, enrutar, administrar e identificar los sistemas de cableado estructurado. Una implementación basada en las normas ayudará a asegurar que pueden soportarse tecnologías actuales como las futuras. Seguir las normas asegura que el proyecto tenga rendimiento y fiabilidad a largo plazo.
- Plan para el crecimiento futuro. El número de circuitos instalados debería cumplir también los requisitos futuros. Deberían considerarse cuando sean posibles las categorías 5e y 6, así como las soluciones de fibra óptica, para asegurarse de que se cumplan las necesidades futuras. Debe ser posible planificar una instalación física que funcione diez años o más.
- Mantener la libertad de elección de los distribuidores. Aún cuando un sistema patentado y cerrado puede ser menos caro inicialmente, puede terminar mucho más costoso a largo plazo. Un sistema no estándar a partir de un solo distribuidor puede hacer más difícil efectuar movimientos, añadidos y cambios con posterioridad (62).

Diseñar una infraestructura de cableado estructurado que enrute, proteja, identifique y termine adecuadamente los medios de cobre o fibra es de importancia crítica para el rendimiento de la red y un buen futuro. Otros puntos importantes son listados a continuación:

Escalabilidad

Si una LAN puede ajustarse en tamaño al crecimiento futuro, se dice que es escalable Es importante planificar con anticipación al estimar el número de recorridos de cable y de derivaciones de cable en un área de trabajo. Siempre es más fácil ignorar los cables instalados que no tenerlos cuando se los necesita. (62)

Interconexión de dispositivos.

Una vez que se ha llevado la implementación del cableado, procede la interconexión de los diferentes dispositivos que conforman a la red. Según las especificaciones para Ethernet, en el cable UTP de categoría 5, sólo los hilos 1, 2, 3 y 6 se emplean para transmitir (TD) y recibir señales (RD). Los cuatro hilos restantes no se emplean.

Se puede emplear un cable recto para conectar dispositivos como PC o routers a otros dispositivos como switchs o hubs. Como se observa en la figura 4.5, se debe utilizar un cable recto sólo cuando un puerto este designado con la letra x.

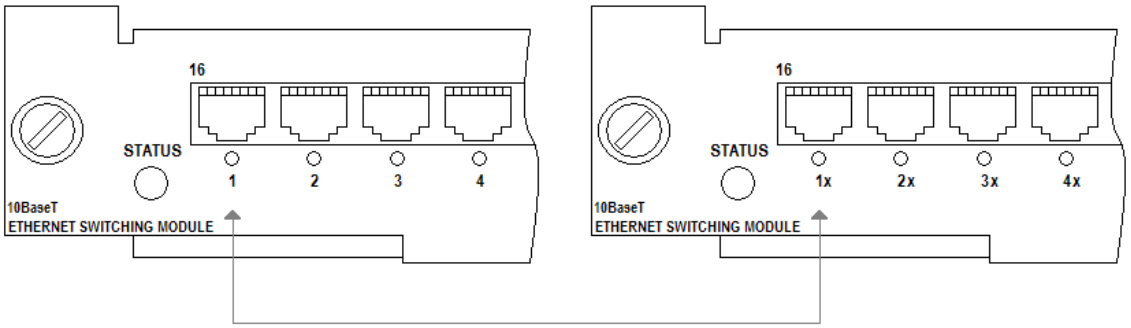


Figura 4.5. Dispositivos interconectados empleando un cable recto.

Con un cable cruzado, los conectores RJ-45 de ambos extremos muestran que alguno de los hilos de un extremo del cable está cruzado con un pin diferente del otro extremo del cable. Según las especificaciones de Ethernet, el pin 1 se une en el otro extremo, al pin 3 y el pin 2 al pin 6. Se utiliza un cable cruzado para conectar dispositivos similares por ejemplo switch con switch o switch con hub. La figura 4.6 muestra el empleo de un cable cruzado cuando los puertos están designados con una x o cuando ninguno de ellos lo está.

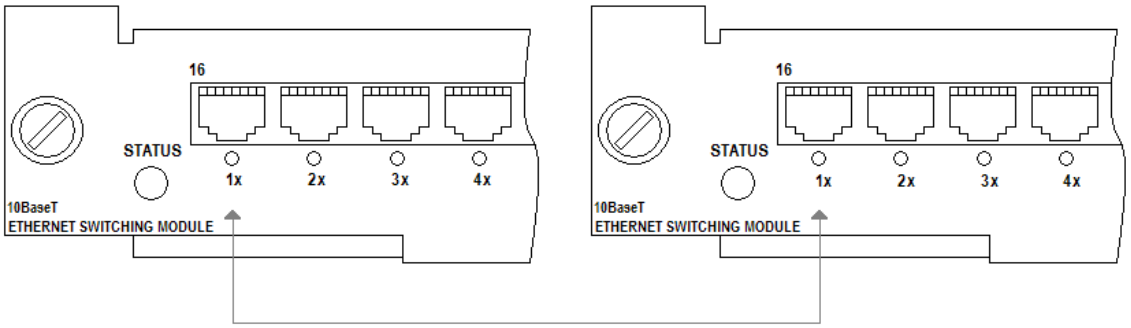


Figura 4.6. Implementación UTP: cable cruzado.

Estas son algunas directrices que se pueden seguir para comprobar el tipo de cable que debe utilizar cuando interconecte dispositivos de red.

Se utiliza un cable recto para el siguiente cableado:

- Switch a router
- Switch a PC o servidor
- Hub a PC o servidor

Se utiliza un cable cruzado para el siguiente cableado:

- Switch a Switch.
- Switch a hub.
- Hub a hub.
- Router a router
- PC a PC
- Router a PC. (62)

4.4. CONFIGURACIÓN DE PARÁMETROS GLOBALES DE LA RED

A continuación se presentará la configuración de archivo smb.conf, el cual pertenece al programa Samba, éste paquete es quien permite compartir archivos entre equipos Linux y Windows:

```
#====================== Global Settings =====================

[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
   workgroup = lab-electronica

# server string is the equivalent of the NT Description field
   server string = %h Solaris10

#### Networking ####

# The specific set of interfaces / networks to bind to
# This can be either the interface name or an IP address/netmask;
# interface names are normally preferred
;   interfaces = 127.0.0.0/8 qfe0

####### Authentication #######

# "security = user" is always a good idea. This will require a Unix account
# in this server for every user accessing the server. See
# /usr/share/doc/samba-doc/htmldocs/Samba3-HOWTO/ServerType.html
# in the samba-doc package for details.
;   security = user
```

```
# You may wish to use password encryption.  See the section on
# 'encrypt passwords' in the smb.conf(5) manpage before enabling.
   encrypt passwords = true

# If you are using encrypted passwords, Samba will need to know what
# password database type you are using.
   passdb backend = tdbsam

   obey pam restrictions = yes

;   guest account = nobody
   invalid users = root

# This boolean parameter controls whether Samba attempts to sync the Unix
# password with the SMB password when the encrypted SMB password in the
# passdb is changed.
;   unix password sync = no

############ Misc ############

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting
;   include = /home/samba/etc/smb.conf.%m


#======================= Share Definitions =======================

# Un-comment the following (and tweak the other settings below to suit)
# to enable the default home directory shares.  This will share each
# user's home directory as \\server\username
;[homes]
```

```
;   comment = Home Directories
;   browseable = no

# By default, \\server\username shares can be connected to by anyone
# with access to the samba server.  Un-comment the following parameter
# to make sure that only "username" can connect to \\server\username
;   valid users = %S

# By default, the home directories are exported read-only. Change next
# parameter to 'yes' if you want to be able to write to them.
;   writable = no

# File creation mask is set to 0600 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0664.
;   create mask = 0600

# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.
;   directory mask = 0700

# Un-comment the following and create the netlogon directory for Domain Logons
# (you need to configure Samba to act as a domain controller too.)
;[netlogon]
;   comment = Network Logon Service
;   path = /home/samba/netlogon
;   guest ok = yes
;   writable = no
;   share modes = no

# Un-comment the following and create the profiles directory to store
# users profiles (see the "logon path" option above)
# (you need to configure Samba to act as a domain controller too.)
# The path below should be writable by all users so that their
```

```
# profile directory may be created the first time they log on
;[profiles]
;   comment = Users profiles
;   path = /home/samba/profiles
;   guest ok = no
;   browseable = no
;   create mask = 0600
;   directory mask = 0700

# Uncomment to allow remote administration of Windows print drivers.
# Replace 'ntadmin' with the name of the group your admin users are
# members of.
;   write list = root, @ntadmin              (41)
```

TEMA 5

5.1. Portada del manual de prácticas

UNIVERSIDAD NACIONAL AUTONÓMA DE MÉXICO
FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
INGENIERÍA MECÁNICA Y ELÉCTRICA
SECCIÓN ELECTRÓNICA

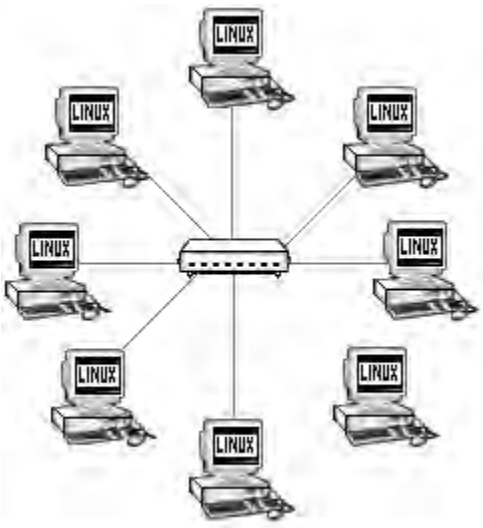
UNAM
CUAUTITLÁN

LABORATORIOS DE SISTEMAS DIGITALES

Y COMUNICACIONES

LABORATORIO

DE TRANSMISIÓN DE DATOS Y TEMAS SELECTOS DE COMUNICACIONES



5.2. Contraportada del manual de prácticas

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

INGENIERIA MECÁNICA Y ELÉCTRICA

SECCIÓN ELECTRÓNICA

LABORATORIO DE SISTEMAS DIGITALES Y COMUNICACIONES

LABORATORIO DE TRANSMISIÓN DE DATOS Y TEMAS SELECTOS DE COMUNICACIONES.

AUTORES: Hugo Lira Hernández

Héctor Jair Herrera Perea

ASESORES: Ing. José Luís Rivera López

Ing. Maricela Serrano Fragoso

5.3. ÍNDICE DE PRÁCTICAS

Practica # 1 Introducción al laboratorio de Transmisión de datos y Temas selectos de comunicaciones

OBJETIVOS

- Obtener los conocimientos básicos y generales de una red.
- Conocer y manejar las herramientas básicas utilizadas para la instalación de una red.
- Conocer e identificar las diferentes configuraciones de cable de acuerdo a la norma de cableado TIA/EIA-568-B.
- Elaboración de cables BNC y UTP.
- Identificar y conocer los distintos dispositivos de interconexión de una red.

INTRODUCCIÓN.

Una red de computadoras es una red de ordenadores y otros dispositivos que usan un protocolo común de red para compartir recursos entre sí a través de un medio de red. El término dispositivo se usa para representar cualquier entidad que está conectada a una red. Tales entidades pueden ser computadoras, impresoras, bridges switchs, routers y muchos otros dispositivos.

Los dispositivos pueden ser locales o remotos. El dispositivo que origina la comunicación a través de una red se llama dispositivo local o transmisor, y cualquier dispositivo dentro de la red al que se tiene acceso desde el dispositivo local se llama dispositivo remoto o receptor.

Para intercambiar información a través de una red, todos los miembros del grupo deben ser capaces de comunicarse entre sí. Esto implica dos términos específicos de red: conectividad y lenguaje. La conectividad se refiere a un enlace o conexión física entre miembros; el lenguaje se refiere a las reglas de comunicación que los miembros deben acatar.

El ambiente físico usado para conectar elementos de red se denomina medio. Los medios de red se clasifican en dos categorías: cables e inalámbricos. En el primer caso podemos mencionar el cable UTP, coaxial o la fibra óptica, y el segundo caso se refiere a ondas de radio (incluidas las microondas y la comunicación por satélite) y la radiación infrarroja.

El cable de par trenzado es probablemente el tipo de cable de mayor uso actualmente en las redes. Éste funciona con todos los tipos diferentes de redes y está constituido en por lo menos dos alambres de cobre aislados y torcidos entre sí. La transmisión de los datos requiere cuatro alambres (dos pares): una para transmitir los datos y otro para recibirlos.

La EIA/TIA (Electronic Industries Association y la Telecomunications Industry Association) proporciona los estándares para UTP. La EIA/TIA especifica el tipo de cable permitido para una velocidad dada, el tipo de conectores que pueden usarse para un cableado dado y la topología de red que es permitida en una instalación de cables. Dentro del estándar EIA/TIA-568 se tiene una versión A y una B que se usan para redes industriales y no industriales, respectivamente.

El cable coaxial es un cable formado por dos conductores concéntricos:

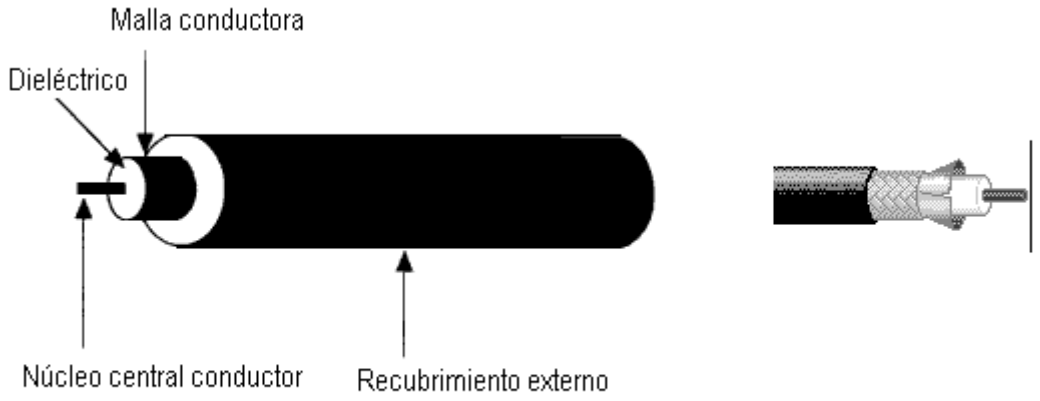


Figura i. Cable Coaxial

El conductor central está formado por un hilo sólido o trenzado de cobre (llamado vivo o positivo) el cual está rodeado por un aislante dieléctrico de mayor diámetro. Una malla exterior aísla de interferencias al conductor central. Por último, posee un material aislante para recubrir y proteger todo el conjunto. Existen múltiples tipos de cable coaxial, cada uno con un diámetro e impedancia diferentes. Se utiliza principalmente en redes de banda ancha y cables de banda base, pues es capaz de lograr altas velocidades de transmisión.

Los cables coaxiales más comunes son el RG-58 (impedancia de 50 Ohm, fino) y el RG-59 (impedancia de 75 Ohm, fino). El tipo de conector que utiliza es el conector BNC.

EQUIPO

- 1 Pinzas ponchadoras
- 1 Pinzas de corte
- 1 Pinzas de mecánico o de electricista
- 1 Probador de cable (Tester)
- 2 Equipos de trabajo Sun Microsystems Ultra 10
- 1 Hub
- 1 Switch
- 1 Router

MATERIAL

- 8m de cable UTP categoría 5
- 8 conectores RJ-45
- 2 conectores tipo BNC tipo macho
- 4m de cable coaxial
- Conectores para el cable coaxial

DESARROLLO

Construcción del cable UTP

I. Tome el cable UTP categoría 5 y corte 2m.
II. Colocar una de las puntas del cable UTP C-5 de 2m dentro de las pinzas ponchadoras, corte y retire el forro como se muestra en la figura 1

Figura 1. En esta imagen se muestra la eliminación del forro.

III. Una vez visibles los cuatro pares de cable, "péinelos" y ordénelos de acuerdo a la configuración que le indique su asesor de laboratorio, ya sea la norma TIA/EIA-568-A o TIA/EIA-568-B. Ver figura 2.

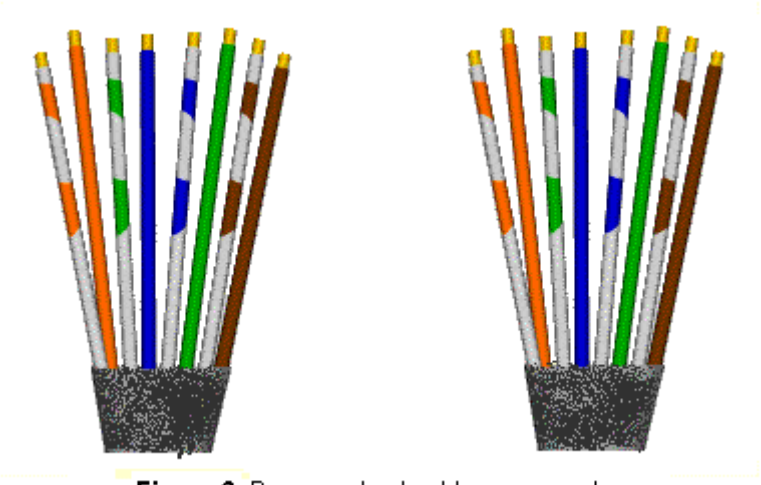


Figura 2. Preparando el cable para ponchar

IV. Coloque la punta del cable ya "peinada" y configurada dentro del conector RJ-45 como se indica en la figura 3.

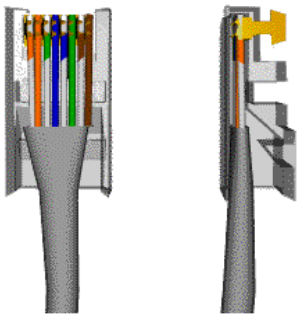


Figura 3. Colocando el cable dentro del conector RJ-45

5. "Ponche" el cable y su conector como se observa en la siguiente figura.

Figura 4. Ponchando el cable.

Las configuraciones a fabricar son las siguientes: cable recto, rollover y crossover, ver figura 5.

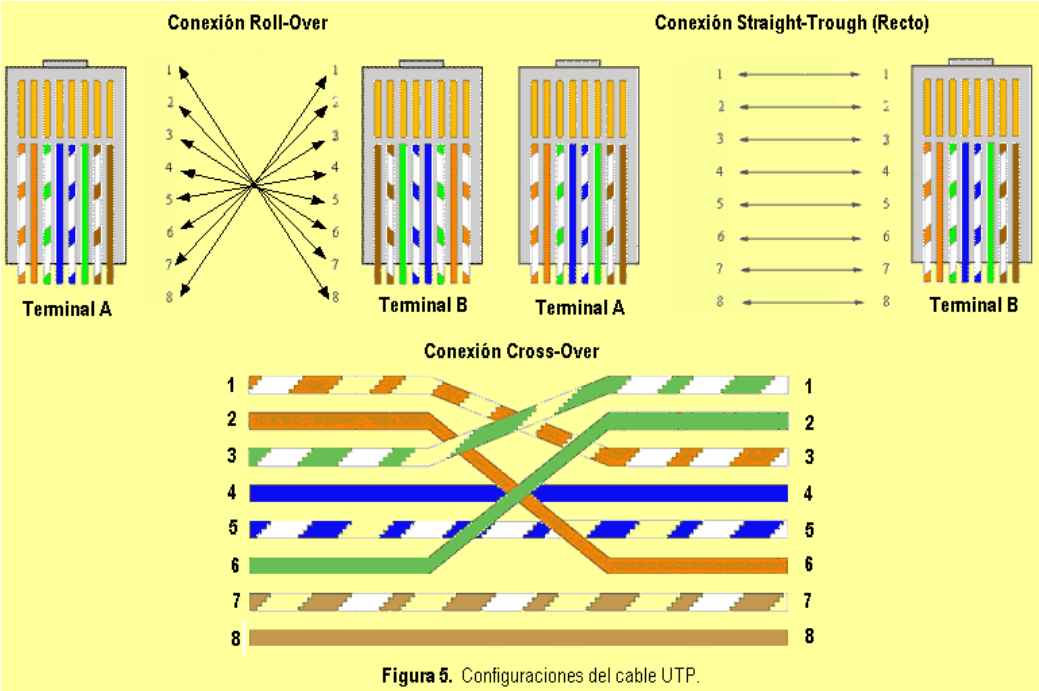


Figura 5. Configuraciones del cable UTP.

Finalmente, se comprueba la continuidad y configuración correcta mediante un probador de cables (Tester). El método varía según el equipo que se utilice, por lo que se debe consultar el instructivo del mismo. Generalmente se conectan los extremos del cable a dos ranuras presentes en los tester's. En la pantalla nos señalará si el cable está correctamente conectado o, en caso contrario, que pares de hilos no lo están. En la figura 6 se puede observar un probador; la prueba puede también realizarse con un Óhmetro.

Fig 6. Tester.

Construcción del cable Coaxial.

Se comienza desforrando aproximadamente 2cm de la punta del cable, posteriormente se retira también una porción de aislante blanco cuidando de no dañar el conductor central, observe la figura 7.

Figura 7. Preparación del cable coaxial.

Una vez listo el cable, se procede a colocar el conector BNC. Éste se colocará tomando en cuenta lo siguiente:

i. Se comienza colocando el aro metálico del conductor BNC en el cable,
ii. Colocar el conductor central dentro del orificio más pequeño del BNC,
iii. El segundo anillo del BNC se coloca entre la malla y el aislante blanco del cable coaxial,
iv. Se asegura con fuerza el aro metálico, de preferencia con pinzas que no sean de corte, en la figura 8 se muestra un cable coaxial terminado.

Nota: en ocasiones los conectores BNC no poseen el aro metálico, en su lugar poseen una prolongación metálica. Ésta, tendrá la misma función que el aro metálico y tendrá que prensarse de la misma manera.

Figura 8. Conector BNC

Dispositivos de Interconexión

Hasta este punto, solo se mostraran cuales son los dispositivos de interconexión, en prácticas posteriores se llevara a cabo su interconexión y ésta se verificará. Estas son algunas directrices que se pueden seguir para comprobar el tipo de cable que debe utilizar cuando interconecte dispositivos de red.

Se utiliza un cable recto para el siguiente cableado:

- Switch a router
- Switch a PC o servidor
- Hub a PC o servidor

Se utiliza un cable cruzado para el siguiente cableado:

- Switch a Switch.
- Switch a hub.
- Hub a hub.
- Router a router
- PC a PC
- Router a PC.
- En el caso de interconectar 3 o más computadoras es recomendable utilizar un concentrador hub, switch o router dependiendo la necesidad específica de cada red.

- Si la red es muy grande es recomendable utilizar una computadora de servidor dedicado del resto de la red, configurando en ella un Proxy, y los servicios que la red requiera.

Conclusiones

Cuestionario

1. ¿Qué es un servidor proxy? ¿Cuál es su uso más común? Mencione ventajas y desventajas
2. Realice un resumen de las siete capas del modelo de referencia OSI y mencione a que capa corresponde cada uno de los dispositivos de interconexión vistos en el laboratorio.
3. ¿Cuál es la función de cada uno de los dispositivos mencionados en la pregunta 2?
4. Defina el protocolo CSMA/CD (Carrier Sense Multiple Access / Collision Detect) y mencione su importancia.
5. ¿Qué es un protocolo? Mencione uno y explíquelo detalladamente.

REFERENCIAS

Practica # 2 Conectando interfaces LAN en Routers

OBJETIVOS

- Identifique interfaces Ethernet o interfaces de Ethernet Rápidos sobre el router.
- Localice los cables apropiados para conectar el router y el ordenador personal a un hub o un switch.
- Use los cables para conectar el router y el ordenador personal al hub o al switch.

INTRODUCCIÓN

Esta práctica se enfoca en la capacidad de conectar de forma física dispositivos LAN de Ethernet como hubs, switchs y el interfaz de Ethernet apropiado sobre un router.

LAN es la abreviatura de Local Área Network (Red de Área Local). Una red local es la interconexión de varios ordenadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de unos pocos kilómetros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc; para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información. Los elementos más comunes que constituyen una red LAN son los siguientes:

Servidor: El servidor es aquel o aquellos ordenadores que van a compartir sus recursos hardware y software con el resto de los equipos de la red.

Estación de trabajo: Se refiere a computadoras que aprovechan o tienen a su disposición los recursos que ofrece la red, así como los servicios que proporcionan los Servidores a los cuales pueden acceder.

Tarjeta de red: También se denominan NIC (Network Interface Card). Básicamente realiza la función de intermediario entre el ordenador y la red de comunicación. En ella se encuentran grabados los protocolos de comunicación de la red. La comunicación con el ordenador se realiza normalmente a través de las ranuras de expansión que éste dispone, ya sea ISA, PCI o PCMCIA. Aunque algunos equipos disponen de este adaptador integrado directamente en la placa base.

Medio: Constituido por el cableado y los conectores que enlazan los componentes de la red. Los medios físicos más utilizados son el cable de par trenzado, par de cable, cable coaxial y la fibra óptica (cada vez en más uso esta última).

Concentradores de cableado: Una LAN en bus usa solamente tarjetas de red en las estaciones y cableado coaxial para interconectarlas, además de los conectores, sin embargo este método complica el mantenimiento de la red ya que si falla alguna conexión toda la red deja de funcionar. Para impedir estos problemas las redes de área local usan concentradores de cableado para realizar las conexiones de las estaciones, en vez de distribuir las conexiones el concentrador las centraliza en un único dispositivo manteniendo indicadores luminosos de su estado e impidiendo que una de ellas pueda hacer fallar toda la red.

Nota: El ordenador (es) y el router deberían ser pre configurado con los ajustes de red de IP correctos. Comience este laboratorio con el ordenador (es), el router y el hub todo apagado y desconectado.

MATERIAL

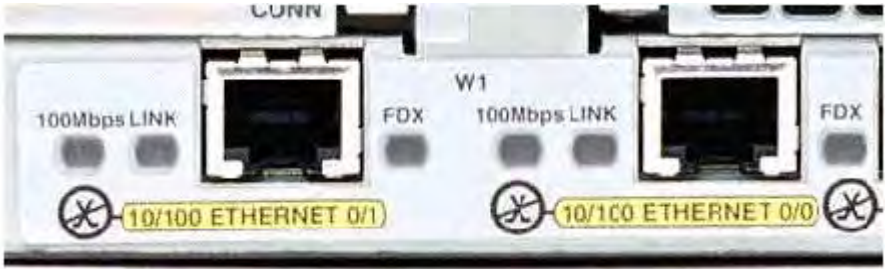
- ✓ Al menos una terminal de trabajo con Ethernet 10/100 NIC instalado
- ✓ Un switch de Ethernet o hub
- ✓ Un router con Ethernet RJ-45 o el interfaz de Ethernet Rápido, o una interfaz AUI
- ✓ 10BASE-t AUI, transreceptor DB-15 a RJ-45, para un router serie 2500 con una interfaz de Ethernet AUI
- ✓ Varios cables de Ethernet deben de ser escogidos entre directo - cruzado para conectar la terminal de trabajo y el router al hub o el switch.

PROCEDIMIENTO

A. Identifica interfaces Ethernet o FastEthernet sobre el router

1. Examine el router

2. ¿Cuál es el modelo del router?
3. Localice uno o varios conectores RJ-45 sobre el router con etiqueta Ethernet 10/100 en la serie 2500 o 10/100 Ethernet Rápida sobre la serie 2600. Este identificador puede variar dependiendo el tipo de router usado. Un router de serie 2500 tendrá un AUI DB-15 el puerto de Ethernet etiquetó AUI 0. Estos requerirán un transreceptor 10BaseT que una al cable de RJ-45.



4. Identifique los puertos de Ethernet mostrados que podría ser usado para conectar los router. Registre la información debajo. Registre los números de puerto de AUI si el router es un router Cisco de serie 2500.

Router	Puerto	Puerto

B. Identifica los cables apropiados y conecta el router

1. La conexión entre el router y el hub será lograda usando un cable directo Categoría 5. Localice un cable que sea bastante largo para conectar el router al hub. Esté seguro para examinar las terminales del cable con cuidado y seleccionar sólo cables directos.
2. Usar un cable para conectar la interfaz de Ethernet que usa la designación 0 sobre el router a un puerto sobre el hub o el switch. También, use el transreceptor 10BaseT AUI para la serie 2500.

C. Localiza el adaptador RJ-45 a DB-9

El ordenador (es) también se unirá al hub usando un cable directo. Extienda cables de Categoría 5 de cada ordenador personal a donde el switch o el hub estén localizados. Conecte un extremo de estos cables al conector RJ-45 sobre el ordenador NIC y conecte otro extremo a un puerto sobre el hub o el switch. Esté seguro para examinar las conexiones de cable con cuidado y seleccionar sólo cables directos.

D. Localiza o construye un cable de rollover

1. Conectar y prender routers, computadoras, y hub o switch.

2. Para verificar la conexión del router, asegúrese de que la luz de interconexión en la interfaz del router y la interfaz del switch/router estén encendidas
3. Para verificar las conexión de ordenador, asegure que la luz de conexión sobre el NIC y el interfaz del hub ambas estén encendidas.

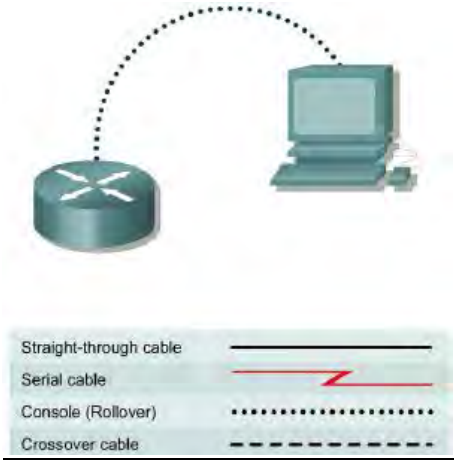
CONCLUSIONES

CUESTIONARIO

1. En tus propias palabras define una LAN
2. Desglose el significado de la nomenclatura 10BASE-T?
3. ¿Qué significado tienen las siglas UTP y STP y qué norma las rige?
4. Mencione y defina los distintos tipos de concentradores que existen.
5. ¿Qué otros dispositivos de interconexión pueden utilizarse en una red LAN?

REFERENCIAS

Practica # 3 Interconexión física entre host & router



OBJETIVO

- Conecte un ordenador personal a un router usando el cable rollover (o un cable de consola).

INTRODUCCION

Un router es un dispositivo de hardware para interconexión de redes de computadoras que opera en la capa tres. Comúnmente los routers se implementan también como puertas de acceso a Internet (por ejemplo un router ADSL), usándose normalmente en casas y oficinas pequeñas.

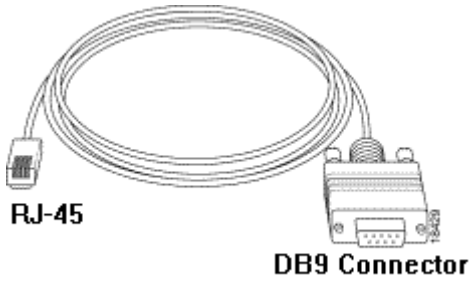
Un router debe tener dos o más interfaces físicas para la interconexión de LAN y/o los servicios de transmisión WAN. El router aprende sobre las direcciones de las computadoras o las redes que están de algún modo conectadas a través de cada una de sus interfaces. La lista de estas direcciones se guarda en tablas que correlacionan las direcciones de Capa 3 y los números de puerto con los que están directa o indirectamente conectadas.

Un router utiliza dos tipos de protocolos de networking, que operan ambos en la Capa 3. Son los protocolos enrutables y de enrutamiento. Los protocolos enrutables, también conocidos como protocolos enrutados, son aquellos que encapsulan la información del usuario y los datos en paquetes. Un ejemplo de protocolo enrutado es IP. IP es responsable de encapsular los datos de la aplicación a través de una red para

los destinos apropiados. Los protocolos de enrutamiento se utilizan entre los routers para determinar las rutas disponibles, comunicar lo que se sabe sobre las rutas disponibles, y remitir los paquetes del protocolo enrutado a lo largo de esas rutas. El propósito de un protocolo de enrutamiento es proporcionar al router toda la información que necesita sobre la red para enrutar los datagramas.

La tarea del router es sencilla: sólo tiene dos interfaces. Cualquier paquete recibido por una de sus interfaces se entrega
switch o cualquier otro dispositivo de Capa 2. El valor real del router reside en determinar las rutas a destinos que se encuentran en redes no adyacentes.

El *cable de consola o rollover* se trata de un cable transpuesto, es decir, el pin 1 de un extremo está conectado al pin 8 del otro; el pin 2 al pin 7; y así sucesivamente. En ocasiones, lo más común es que en terminal de cable para la conexión con el PC sea mediante el puerto serie utilizando un adaptador de RJ-45 a DB9.



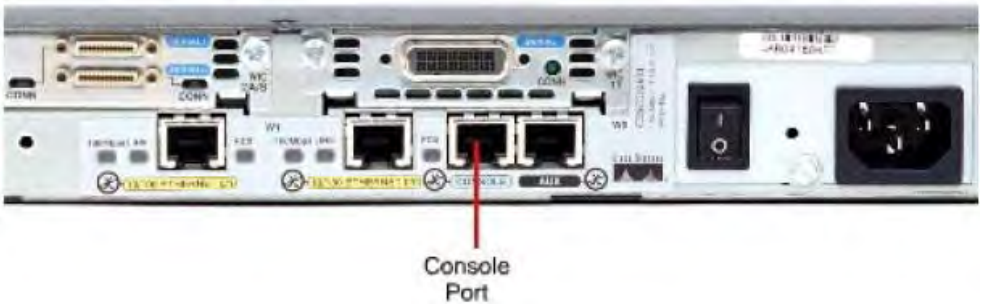
MATERIAL

- ✓ Un ordenador con una interfaz serial.
- ✓ Un Router Cisco.
- ✓ Un cable de Consola o rollover para conectar la terminal del ordenador al router.

PROCEDIMIENTO

1. Identificando conectores y componentes

Examine el router e identifique el conector RJ-45 con la etiqueta consola



2. Identificando la interfaz serial de la computadora (COM 1 o 2)

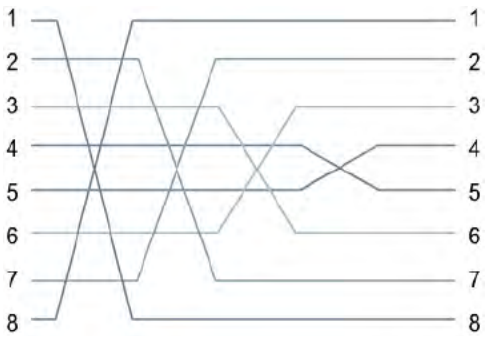
Examine la computadora y localice el conector macho con la etiqueta serial de 9-pines o 25-pines. Es posible que no esté identificado.

3. Localizando el adaptador para el cable de consola

Localice el adaptador de RJ-45 a DB-9 o RJ-45 a DB-25 dependiendo del puerto serial que se encuentre en la PC

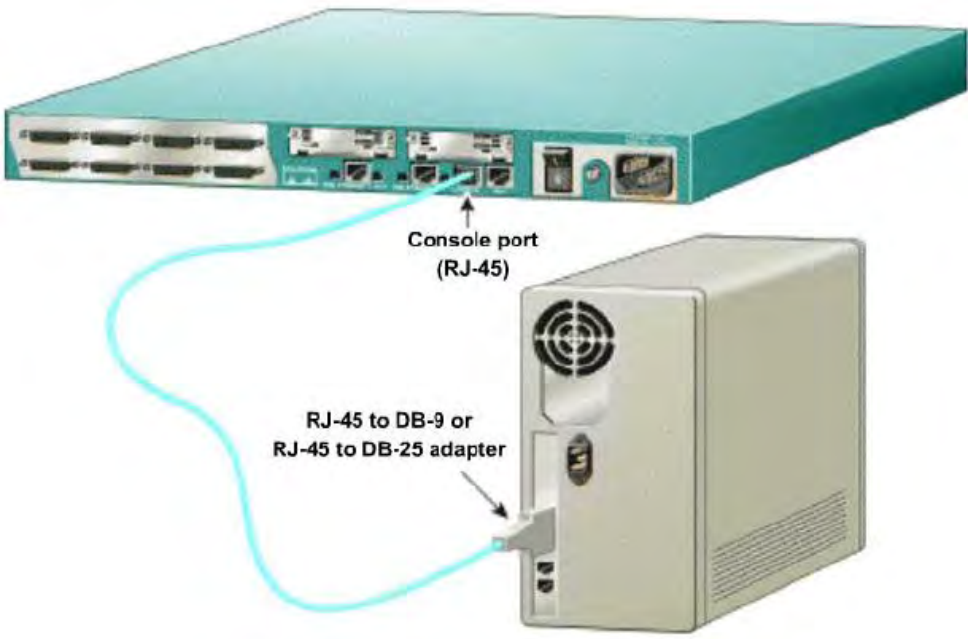
4. Construyendo un cable rollover

Use un cable de consola o rollover de longitud adecuada para conectar el router a uno de los terminales de trabajo. Haga un cable rollover si fuera necesario, como se realizó en la práctica uno.



5. Conectando componentes

Conecte el cable de consola o rollover al puerto de consola del router, un conector RJ-45. Después, conecte el otro extremo de la consola o el cable rollover al RJ-45 a DB-9 o RJ-45 al adaptador DB-25 dependiendo el puerto serie de ordenador personal disponible. Finalmente adjunte el adaptador a un puerto serie de ordenador personal, DB-9 o DB-25, dependiendo el ordenador.



CONCLUSIONES

CUESTIONARIO

1. ¿Qué es una lista de control de acceso (ACL) y cuál es su función?
2. ¿Qué estándar rige el cableado para una red? Y ¿Cuáles son sus variantes?
3. ¿Qué longitud máxima puede tener un cable UTP para su mayor eficiencia?
4. ¿En qué casos es necesario interconectar 2 routers y qué tipo de cable utilizaría?
5. Menciona una situación en la cual el router pueda ser sustituido por otro dispositivo de interconexión (por ejemplo un switch o hub).

REFERENCIAS

Practica #4 Establecimiento una Sesión de Consola con Hyperterminal

OBJETIVO

- Conectar el router y la PC usando un cable de consola
- Configurar Hyper Terminal para establecer una sesión de consola con el router.

INTRODUCCIÓN

Hyperterminal es una simple terminal basada en ventanas que emula un programa, el cual es usado para conectarse al puerto de consola en el router. Una PC con Hyperterminal nos provee de un teclado y un monitor para el router. Conectando al puerto de consola con el cable rollover y usando Hyperterminal es el camino más básico para acceder al router para checar o cambiar su configuración.

HyperTerminal es un programa que se puede utilizar para conectar con otros equipos, sitios Telnet, sistemas de boletines electrónicos (BBS), servicios en línea y equipos host, mediante un módem, cable de módem nulo o Ethernet. Aunque utilizar HyperTerminal con un servicio de boletín electrónico para tener acceso a información de equipos remotos es una práctica que está dejando de ser habitual gracias al World Wide Web, HyperTerminal sigue siendo un medio útil para configurar y probar el módem o examinar la conexión con otros sitios.

HyperTerminal graba los mensajes enviados o recibidos por servicios o equipos situados al otro extremo de la conexión. Por esta razón, puede actuar como una valiosa herramienta para solucionar problemas de configuración y uso del módem. Para confirmar que el módem está bien conectado o ver su configuración, puede enviar comandos a través de HyperTerminal y ver los resultados. HyperTerminal ofrece la funcionalidad de desplazamiento, que le permite revisar el texto recibido que sobrepase el espacio de la pantalla.

HyperTerminal sirve también para transferir archivos grandes de un equipo a un equipo portátil a través del puerto serie, en lugar de realizar la configuración del portátil en una red.

Puede utilizar HyperTerminal para ayudar a depurar el código fuente desde un terminal remoto. También puede utilizar HyperTerminal para comunicarse con los equipos antiguos basados en caracteres.

HyperTerminal está diseñado para ser una herramienta fácil de utilizar y no viene a sustituir a otras herramientas principales disponibles en el mercado. HyperTerminal puede utilizarse para realizar las tareas específicas descritas, pero no debe intentar utilizarlo para necesidades de comunicación más complejas.

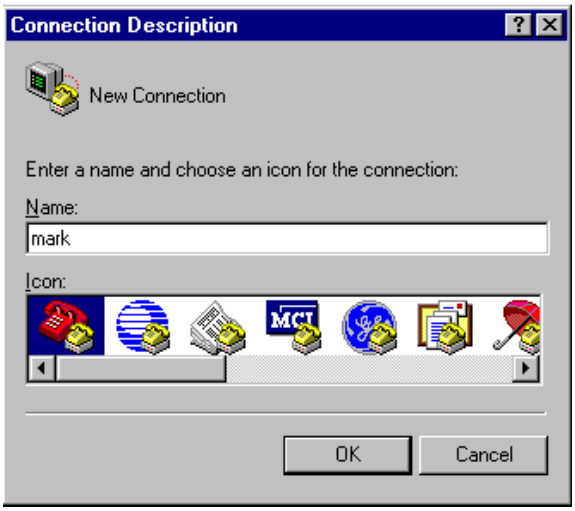
MATERIALES

- ✓ Una PC con una interfaz serial e Hyperterminal
- ✓ Un router Cisco
- ✓ Cable de consola (rollover) para conectar la PC con el router

PROCEDIMIENTO

1. Conectar el cable rollover al puerto de consola en el router y el otro extremo a la PC con el adaptador DB-9 o DB-25 al puerto COM1. Esto debe de realizarse antes de prender cualquier equipo.
2. Prenda la computadora y el router
3. En la barra de inicio localice el programa de Hyper Terminal

   Start > **Programs** > **Accessories** > **Communications** > **Hyper Terminal**



4. En el pop-up de "Descripción de la conexión", introduzca un nombre para la conexión y pulse OK.

5. En el pop-up "Conectar con", use las flechas para manipular el campo de "Conectar usando:", hasta que aparezca "COM1" y dar click en OK
6. En el pop-up de "Propiedades de COM!" modifica los campos para que aparezcan de la siguiente forma:

Bits per second: **9600**

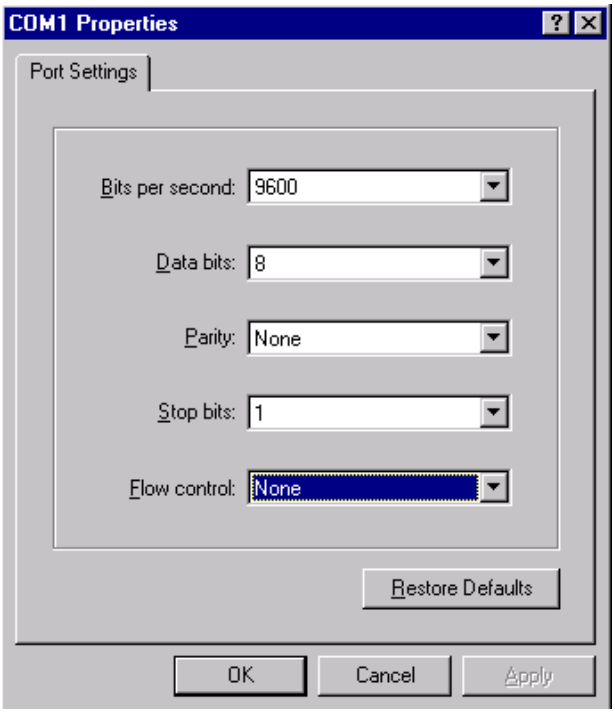
Data bits: **8**

Parity: **None**

Stop bits: **1**

Flow control: **None**

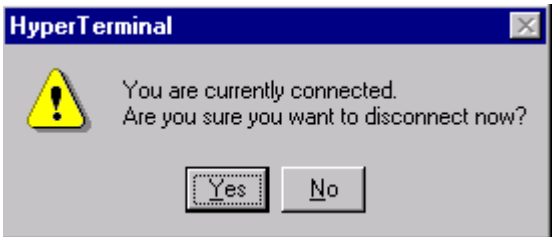
De click en OK



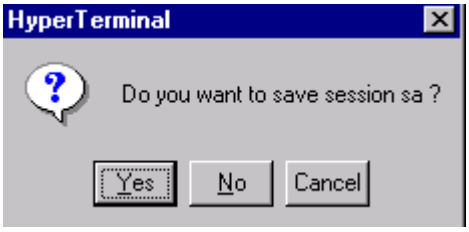
7. Cuando la ventana de sesión Hyperterminal aparezca, conecte el router. Si el router ya está conectado, presione la tecla Enter. Debería haber una respuesta del router. Si hay respuesta, entonces la conexión ha sido satisfactoriamente completada. Si no hay ninguna conexión, solucione como es necesario. Por ejemplo, verifique que el router esté conectado. Compruebe la conexión al puerto COM 1 sobre el ordenador personal y el puerto de consola sobre el router. Si no hay en ninguna parte ninguna conexión, pida al instructor la ayuda.
8. Para terminar la sesión de consola de una sesión Hyperterminal, seleccione:

   File > **Exit**

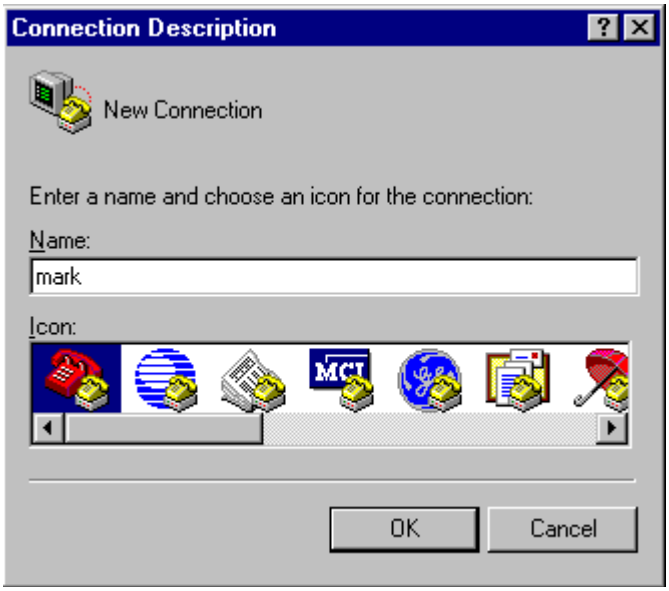
9. Cuando el Hyperterminal desconecta la advertencia pop-up aparece, seleccione YES



10. El ordenador entonces preguntará si la sesión debe ser salvada. Seleccione Yes.



11. En el pop-up de "Connection Description", seleccione cancelar.



12. Para abrir la sesión de consola salvada del Hyperterminal, seleccione:

    File > **Open**

    La sesión salvada ahora aparecerá y presionando dos veces el ratón sobre el nombre, la conexión abrirá sin configurarlo de nuevo cada vez.

13. Cierre Hyperterminal y apague el router

CONCLUSIONES

CUESTIONARIO

1. ¿Qué es el IOS?
2. ¿Para qué es usada hyperterminal?
3. Menciona brevemente ¿qué es Telnet?
4. Describe con tus propias palabras qué relación existe entre Telnet e Hyperterminal

5. ¿Qué es un cable de módem nulo?

REFERENCIAS

Practica #5 Fundamentos de Línea de comandos

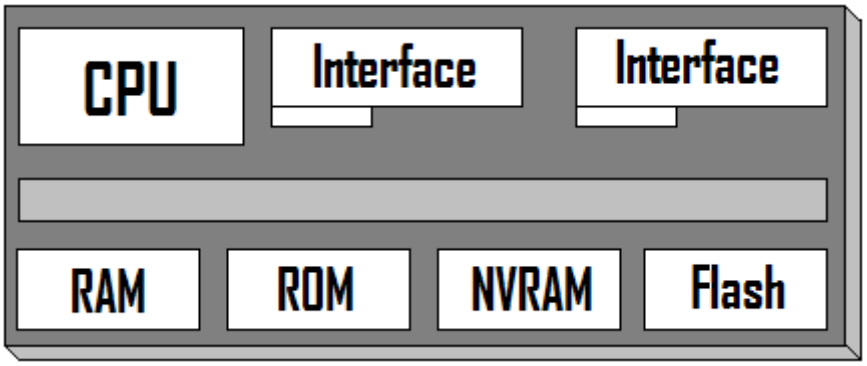
OBJETIVOS

- Entrar en el router e ir al modo privilegiado
- Utilizar algunos comandos básicos del router para determinar su configuración.
- Utilizar la ayuda del router
- Utilizar el historial de comandos y editar sus características
- Salir del modo privilegiado

INTRODUCCIÓN

Un *router* es una computadora especializada en conmutar datagramas IP. Dependiendo de las prestaciones que deba ofrecer, un *router* posee una estructura similar a la de un PC: CPU, memoria, buses e interfaces de red. Para el almacenamiento de datos es habitual utilizar memoria ROM, memoria FLASH, memoria RAM y memoria RAM no volátil (NVRAM).

- RAM: código, tablas de encaminamiento, buffers, cache ARP, etc.
- NVRAM (No volátil): fichero de configuración "startup-config"
- Flash (no volátil): imagen del IOS
- ROM (no volátil): parte de imagen IOS, código bootstrap.



Un *router* se inicializa cargando el ***bootstrap*** , el sistema operativo y un archivo de configuración. Si el *router* no puede encontrar un archivo de configuración, entonces entra en el modo de configuración (*setup*).

El *router* almacena una copia de seguridad de la nueva configuración del modo de configuración en la memoria de acceso aleatorio no volátil (**NVRAM**).

El objetivo de las rutinas de inicio para el software Cisco IOS es iniciar las operaciones del *router*: Para ello, las rutinas de inicio deben de hacer lo siguiente:

a. Asegurarse de que el *router* carga la ROM
b. Encontrar y cargar la imagen del software Cisco IOS que el *router* utiliza para su sistema operativo
c. Encontrar y aplicar les directivas de configuración, incluyendo las funciones de protocolo y las direcciones de interfaz.

Hyperterminal es un programa de emulación de terminal simple basado en ventanas que se puede utilizar para conectar con el puerto de la consola de los *router*s. Una PC con Hyperterminal proporciona un teclado y un monitor para trabajar sobre él. El conectar con el puerto de la consola con un cable del rollover y usar HyperTerminal es la manera más básica de tener acceso a un *router* para comprobar o cambiar su configuración.

Los router con IOS disponen de un conjunto de modos llamados de configuración que permiten la visualización y configuración del router. Los modos de configuración son los siguientes:

Modo BOOT o ROM monitor: se usa en casos de emergencias (prompt típicamente rmon) como puede ser la recuperación de un password, de un registro de configuración, etc.
Modo de SETUP: permite una configuración por menú sencilla y básica del router.
Modo USER EXEC: es el modo de visualización sin privilegios (prompt R>) o **Modo PRIVILEGED EXEC**: modo de visualización con privilegios (prompt R#)
Modo de Configuración Global o CONFIGURE: permite configurar aspectos sencillos del router como pueden ser la configuración del nombre del router, passwords, etc (prompt R (config)#)
Modo de configuración específicos: permiten configurar protocolos, interfaces o en general aspectos más complejos del router (prompt R(config-if)#, R(config-route)#, R(config-line)#, etc.)

Al arrancar el router podemos pasar al modo SETUP, que permite dar una primera configuración al router cuando éste carece de una configuración preestablecida, o bien pasar al modo USER EXEC, cuando el router sí dispone de una configuración preestablecida.

En modo USER EXEC podemos consultar aspectos básicos de la configuración del router. Para consultar aspectos más críticos de la configuración del router debemos pasar a modo PRIVILEGED EXEC. Para pasar de modo USER EXEC a modo PRIVILEGED EXEC es necesario usar un password (que se conoce como "*enable secret password*" que se puede establecer desde el modo CONFIGURE ejecutando enable secret <passwd>)

Desde los modos USER EXEC y PRIVILEGED EXEC no podemos modificar la configuración del router. Para hacerlo debemos pasar del modo PRIVILEGED EXEC al modo de configuración general (CONFIGURE). Desde allí podemos configurar aspectos generales del funcionamiento del router o pasar a modos de configuración específicos de cada interfaz, algoritmo de encaminamiento, etc.

Cuando estamos en modo USER EXEC el prompt que nos muestra el router es "**>**". Cuando estamos en PRIVILEGED EXEC el prompt es "**#**" y en el modo de configuración global el prompt es **(config)#**.

MATERIALES

- ✓ Una PC con una interfaz serial e Hyperterminal
- ✓ Un router Cisco
- ✓ Cable de consola (rollover) para conectar la PC con el router

PROCEDIMIENTO

1. Comience una sesión de HyperTerminal según lo realizado para establecer una sesión laboratorio en HyperTerminal.
2. Entre en el router. Si se le indica que puede entrar en el modo inicial de la configuración, conteste no. Si se menciona la introducción de una contraseña, teclee Cisco.
3. Si el prompt muestra "router" este es el predeterminado. Algunos pueden aparecer diferente si se ha nombrado al router.

4. Introduzca el comando de ayuda tecleando el símbolo ? en el prompt de ejecución del usuario en el router

Router>**?**

Catalogue ocho órdenes disponibles de la respuesta del router.

5. Escriba **enable** para usar el comando enable. Si preguntan una contraseña para entrar introduzca class en el prompt

6. Entre en el modo de ayuda escribiendo un signo de interrogación (?) en el prompt de ejecución privilegiada del router.

Router#**?**

7. Catalogue diez (10) órdenes disponibles de la respuesta del router.

8. Lista todos los comandos cuando introduces **show ?** en el prompt de ejecución privilegiada del router

Router#show ?

9. Desplegar la configuración del router introduciendo el comando **show running-config** en el prompt de ejecución privilegiada del router.

Router#**show running-config**

10. Catalogue seis pedazos claves de información mostrada con este comando:

11. Cuando la palabra "more" aparezca, presione la barra espaciadora. Presionando la barra espaciadora el router mostrara la siguiente página de información.
12. Use el historial de comandos para ver y reutilizar las órdenes antes entradas. Presione en la flecha (arriba) o Ctrl-p para ver el último comando entrado. Presiónelo otra vez para ir al comando anterior e este. Presione la flecha abajo o Ctrl-n para volver por la lista. Esta función deja ver el historial de comandos.
13. Cierre Hyperterminal y apague el router.

CONCLUSIONES

CUESTIONARIO

1. ¿Qué PROMPT exhibió el router?
2. ¿Qué significa el símbolo después del nombre del router?
3. ¿Es **enable** uno de los comandos disponibles mostrados en el paso 4?
4. ¿Qué cambió en el prompt que muestra el router en el paso 5 y qué significa esto?
5. ¿Es running-config uno de los comandos disponibles para el modo ejecución privilegiada del router?

REFERENCIAS

Practica #6 Modo de Comandos e Identificación del Router

OBJETIVOS

- Identifique los modos del router básicos de usuario EXEC y EXEC privilegiado.
- El empleo de comandos para entrar en modos específicos.
- Familiarizase con el prompt del router para cada modo.
- Asignar un nombre al router

INTRODUCCIÓN

Los sistemas operativos de los routers comerciales están especialmente diseñados para facilitar las tareas de conmutación de paquetes, la ejecución de algoritmos de encaminamiento, configuración de interfaces, etc. Un ejemplo de este tipo de sistemas operativos es el IOS. El IOS tiene una arquitectura simple y normalmente ocupa un espacio de memoria reducido. Cuando encendemos un router, se ejecuta un programa de bootstrap cargado en la ROM que testea el sistema y carga en la RAM una imagen del IOS, normalmente desde la memoria flash.

Configuraremos el router utilizando un interface de comandos en línea (CLI). Normalmente se hace a través de una conexión por la línea serie conectada al puerto CONSOLE del router, usando por ejemplo la aplicación HYPERTERMINAL. Los parámetros necesarios para conectarse son los siguientes: Baud Rate 9600 bps, 8 bits/carácter, 2 bits de Stop, No paridad y control de flujo Hardware.

Por su acrónimo en inglés CLI por Command line interface, es un programa informático que actúa como Interfaz de usuario para comunicar al usuario con el sistema operativo mediante una ventana que espera comandos textuales ingresados por el usuario en el teclado, los interpreta y los entrega al sistema operativo para su ejecución. La respuesta del sistema operativo es mostrada al usuario en la misma ventana. A continuación, la *shell* queda esperando más instrucciones. Se interactúa con la información de la manera más simple posible, sin gráficas, solo el texto crudo.

La configuración activa del router se encuentra en un fichero llamado running-config. Si apagamos el router, dicha configuración se perdería y no estaría presente al volver a activar el router. Podemos guardar dicha configuración en un archivo de configuración (startup-config) que normalmente se graba en una memoria NVRAM. Al arrancar el router, la configuración que se activa es la guardada en el archivo startup-config.

MATERIALES

- ✓ Una PC con una interfaz serial e Hyperterminal
- ✓ Un router Cisco
- ✓ Cable de consola (rollover) para conectar la PC con el router

PROCEDIMIENTO

1. Conectarse al router e ingresar.
2. Escribir **enable** en el prompt de modo de usuario y si pregunta por una contraseña introducir **class**

```
Router>enable
```

3. Escriba **configure terminal** en el prompt de modo privilegiado

```
Router#configure terminal
```

4. Introduzca **router rip** en el modo de configuración global

```
Router(config)#router rip
```

5. Introducir **exit** en el prompt para regresar al modo de configuración global

```
Router(config-router)#exit
```

6. Introduzca **interface serial 0** en el modo de configuración global

```
Router(config)#interface serial 0
```

7. Introducir **exit** en el prompt para regresar al modo de configuración glob

Router(config-if)#exit

8. Asigne un nombre al router, con el comando **hostname**, por ejemplo:

Router(config)#hostname GAD

9. Introducir **exit** en el prompt para salir del router. En el modo de EXEC (ejecución) privilegiado escriba **exit** para salir y apague el router.

GAD(config)#exit

BORRADO DE L ROUTER

1) Entrar al modo EXEC privilegiado escribiendo **enable.** Si el sistema pregunta por una clave introduzca **class** y si esta no funciona pregunte al profesor.

Router>**enable**

2) En el modo EXEC privilegiado introduzca el comando **erase startup-config.**

Router#**erase startup-config**

3) La línea de respuesta que aparecerá será aparecida a los siguiente:

Erasing the nvram filesystem will remove all files! Continue?
[confirm]

4) Presione **Enter** para confirmar. La respuesta deberá ser algo parecido a lo siguiente:

Erase of nvram: complete

5) Ahora en el modo EXEC privilegiado, introduzca el comando **reload.**

Router#**reload**

6) La línea de respuesta de este comando será similar a:

System configuration has been modified. Save? [yes/no]:

7) teclee que **n** y después presione **Enter.** La línea de respuesta será algo similar a:

Proceed with reload? [confirm]

8) Presione Enter para confirmar. La primera línea de respuesta será algo parecido a:

Reload requested by console.

9) Después de que el router se haya recargado, la línea de respuesta será algo similar a:

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

10) Escriba **n** y después presione Enter. La línea de respuesta será similar a:

Press RETURN to get started!

11) Presione entrar. El router está listo para ser configurado en un laboratorio.

CONCLUSIONES

CUESTIONARIO

1. ¿Qué prompt muestra el router en el paso 3? Y ¿Qué significado tiene?
2. ¿Qué prompt muestra el router en el paso 4? Y ¿Qué significado tiene?
3. ¿Qué prompt muestra el router en el paso 6? Y ¿Qué significado tiene?
4. Menciona todos los tipos de memoria que existen en el router y qué tipo de información se guardan cada una de ellas.
5. ¿Qué es el modo de monitor de ROM?

REFERENCIAS

Practica #7 Verificación De Conectividad Entre Computadoras En Red Tipo LAN

OBJETIVOS

Comprobar la conectividad entre dos computadoras utilizando el comando ping.

Traceroute

Netstat

INTRODUCCIÓN

En esta práctica se comprobará experimentalmente la comunicación entre dos computadoras pertenecientes a una misma red y dominio. Esto se llevará a cabo mediante los comandos ping, traceroute y netstat.

ICMP es el componente del conjunto de protocolos TCP/IP que se encarga del fallo de IP para asegurar la entrega de datos. ICMP envía mensajes de error al emisor de los datos indicando que se han producido problemas en la entrega de los datos. En la siguiente figura se muestra la ubicación de ICMP dentro del modelo TCP/IP.

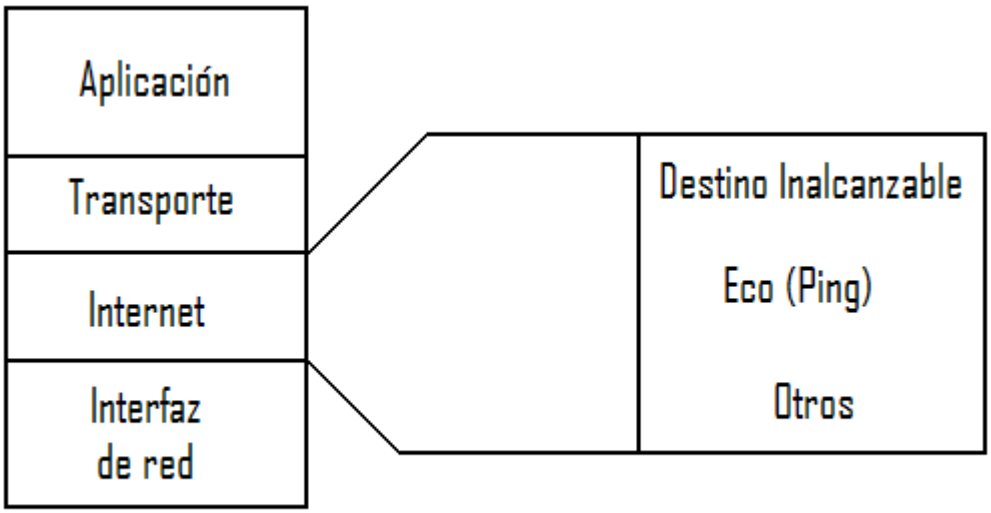


Figura 1. ICMP y el modelo TCP/IP

Los mensajes de ICMP se envían y entregan utilizando el protocolo IP. Tales mensajes son encapsulados en datagramas de la misma forma que otros datos se entregan mediante IP. En la tabla 1 se puede observar la encapsulación de un paquete ICMP dentro del área de datos del datagrama IP. La cabecera de la trama puede ser de un protocolo LAN o WAN.

Cabecera de la trama	Cabecera del datagrama	Cabecera ICMP	Datos ICMP
Cabecera de la trama	Cabecera del datagrama	Área de datos del datagrama IP	
Cabecera de la trama	Área de datos de la trama		

Tabla 1. Encapsulación ICMP

Los mensajes ICMP se transmiten en la misma forma que otros datos, por lo tanto son propensos a los mismos fallos de entrega y además son un buen indicador del estado de comunicación dentro de una red. Cuando se producen errores en la entrega de un datagrama, ICMP informa de esos errores al emisor de datagrama.

El protocolo ICMP se puede utilizar para probar la disponibilidad de un destino en particular. Esto se prueba mediante el comando ping: un mensaje de petición de eco al dispositivo remoto. Cuando este último recibe la petición de eco ICMP, formula un mensaje de respuesta de eco que se enviará al origen de la petición.

Si el emisor recibe la respuesta de eco, confirma que el dispositivo de destino puede alcanzarse utilizando el protocolo IP. Ping es la petición de eco (ECHO): retorno al que se refiere cuando un paquete que enviamos es devuelto.

En algunas referencias se menciona que PING es un acrónimo que significa el Packet Internet Groper (I), este no es el caso. Ping fue nombrado debido al sonido del sistema de barrido de un sonar. Inclusive existe una historia en la cual se dice que un administrador de sistemas escribió un script que repetidamente hacia un ping a una computadora en la red y obtenía una respuesta audible de un "ping" por cada éxito. El administrador de sistemas entonces era capaz de ir metódicamente alrededor de su red revisando conectores BNC hasta encontrar el conector fallido que había estado haciendo ping en su red — cuando el sonido se detenía, había encontrado su repuesta (2).

Ping es el comando por excelencia para comprobar que las funciones básicas de una red TCP/IP funcionan correctamente. La herramienta manda a otro ordenador un pequeño paquete de datos, ordenándole que una vez recibido lo devuelva de inmediato. Si esto funciona, ping se lo indicará con un mensaje, con lo que se asegura la capacidad de transmisión básica de la red.

Existen muchas otras opciones de PING, y se mostraran las más útiles en orden alfabético. Es importante mencionar que el PING de Windows tiene diferencias con el PING de Linux. La sintaxis correspondiente se presenta a continuación:

ping [opción(es)] nombre_computadora | dirección IP

Opciones:

-f Flor (desbordamiento): Envía tantos paquetes de datos como sea posible. Comando usado para probar al límite la capacidad de una red, pero que sin embargo sólo puede ser usado por root. Es decir, se puede aclarar cuantas veces por segundo se quiere pinguear.

-c número: Determina el número total de paquetes enviados, tras lo cual el programa se cierra. No hay limitaciones por defecto.

-i valor: Segundos transcurridos entre el envío de dos paquetes de datos; el valor predeterminado es un segundo.

PING en Linux

-a Ping audible

-b Permite pinguear direcciones de broadcast

-d Setea la opción DEBUG en el socket utilizado

-I Aclaro la IP de donde se ejecuta ping

-n Solo salida numérica

-p Se especifican 16 bytes que se quieren para el paquete

-q No muestra nada, salvo el sumario al comienzo y fin

-r Saltea la tabla de ruteo y envía directo el paquete a un host

-s Especifica los bytes a enviar (por default es 56+8 del ICMP header)

-v Muestra la salida "verboseada", o más aclarada que lo normal

-w Se especifica el tiempo que se quiere pinguear

El comando ping también puede utilizarse utilizando el nombre DNS del dispositivo destino (asumiendo que DNS está disponible)

Traceroute

Traceroute es un programa disponible en muchos sistemas, rastrea la ruta que toma un paquete hacia un destino. Es lo más utilizado para depurar los problemas de enrutamiento entre hosts pues muestra cualquier enrutamiento mal configurado o falla en el camino enrutado. Si un host en particular es ilocalizable, se puede utilizar traceroute para ver que ruta sigue el paquete hacia el host remoto y descubrir la falla posible. Traceroute se utiliza para descubrir las rutas que los paquetes toman hacia sus destinos. También puede utilizarse para comprobar la capa de red, sobre una base salto-a-salto y proporcionar puntos de referencia sobre el rendimiento.

La salida del comando traceroute genera una lista de los saltos alcanzados satisfactoriamente (round trip time). Esta información puede ser útil para visualizar tráfico lento entre dos host.

Netstat

El comando netstat nos genera el estado de la red y estadísticas de protocolo. Se puede desplegar el estado de TCP, SCTP y UDP en un formato de tabla. También se puede generar tablas de enrutamiento e información de interfaces.

El comando netstat despliega diferentes tipos de datos de red, dependiendo de la opción seleccionada. La información generada por este comando es más útil durante la administración del sistema. La sintaxis básica para el estado de red es la siguiente:

netstat [-m] [-n] [-s] [-i | -r] [-f *address-family*]

Opciones

[vacío]	Despliega el estado de los protocolos de transporte en un sistema
-s	Muestra estadísticas de protocolos para UDP, TCP, SCTP, ICMP e IP.
-p	Genera un protocolo de transporte en particular de un sistema
-a	Solicita el estado de sockets
-f	Muestra estadísticas relacionadas a la transmisión de paquetes IPv4 o IPv6 de una dirección en particular
-r	Presenta una tabla de ruteo de un host local. Dicha tabla muestra el estado de todas las rutas que un host conoce.

Desarrollo

Ping

Como determinarse un host remoto esta activo

Ejecute la Terminal.

Tecleé el siguiente comando en el sistema local:

sunserver@lab% ping *hostname*

ó

sunserver@lab% ping *dirección IP*

Si el host remoto acepta las transmisiones ICMP, el mensaje desplegará respectivamente:

sunserver@lab% *hostname* is alive

ó

Desplegará en pantalla el número de paquetes enviados, recibidos y perdidos, si es que fuese el caso.

Este mensaje indica que el *hostname* responde a la ICMP solicitada. Sin embargo, si el hostname estuviera apagado o no pudiera recibir los paquetes ICMP, se desplegaría el siguiente mensaje:

sunserver@lab% no answer from *hostname*

Como determinar si el host está perdiendo paquetes

Utilice la opción –s del comando ping para determinar si el host remoto esta activo y sin perder paquetes

sunserver@lab% ping -s

Las estadísticas de paquetes perdidos indican si el host ha perdido paquetes. Si el comando ping falla, cheque el estado de la red con el comando ifconfig o netstat.

Traceroute

Como encontrar la ruta a un host remoto

Ejecute la Terminal.

Tecleé el siguiente comando en el sistema local:

sunserver@lab% traceroute destino-hostname

Ejemplo:

sunserver@lab% traceroute farhost.faraway.com

Utilizando el comando traceroute para mostrar la ruta a un host remoto.

La siguiente salida mostrará los routers que los paquetes siguen desde el host local hasta el host remoto. La salida mostrará también el tiempo por paquete que atraviesa cada router. Si existe algún fallo, traceroute indicará el salto específico en donde se produjo. Si aparece un asterisco (*) el paquete falló.

Como trazar todas las rutas

Este procedimiento utilicé la opción –a del comando traceroute para trazar todas las rutas.

Teclear el siguiente comando en el sistema local:

sunserver@lab% traceroute –a hostname

Ejemplo:
sunserver@lab% traceroute –a v6host.remote.com

Monitorear la red con el comando netstat

Generando el estado de los protocolos de transporte TCP y SCTP

Teclear el siguiente comando en el sistema local:

sunserver@lab% netstat

Desplegando el estado de un protocolo de transporte en particular.

Teclear el siguiente comando en el sistema local

sunserver@lab% netstat –P tcp

Solicitando el estado de las interfaces de la red

3. Teclear el siguiente comando en el sistema local

sunserver@lab% netstat –i

Visualizar el estado de los sockets

4. Teclear el siguiente comando en el sistema local

sunserver@lab% netstat –a

Despliegue del estado de las transmisiones por paquete IPv4 o IPv6 de una dirección específica

5. Teclear el siguiente comando en el sistema local

sunserver@lab% netstat –f inet | inet6

Desplegando una tabla de ruteo IP

Teclear el siguiente comando en el sistema local

sunserver@lab% netstat –r

Conclusiones

Cuestionario

1. Al ejecutar ping –s ¿en cuántas secciones se divide la salida y que información proporciona cada una de ellas?
2. ¿Cuál de los tres comandos utilizaría para analizar el estado de una red y porque?
3. ¿Qué diferencia existe entre el comando ping y snoop?
4. Durante la utilización del comando netstat, ¿Cómo interpretaría que los paquetes de entrada (IpKts) son mayores que los paquetes de salida (Opkts)? Respuesta en página 188 del ipsol
5. Mencione por lo menos otros tres comandos de red que pudieran ser útiles y explíquelos.

Referencias

6. Puesta en marcha de la red

6.1. Verificación básica de la red.

La verificación básica de la red contiene varios pasos a seguir. Los comandos, entiéndase software, se trataran a lo largo de este capítulo, debido a que estos son un poco más complejos de lo que puede ser la verificación física. Éstos nos sirven para descartar un defecto físico, en caso de haber una falla en la red. A continuación se enlista el procedimiento más utilizado:

- Verificación de la alimentación de energía de todos los equipos y que estén encendidos.
- Chequeo del cableado de red:
    - Prueba del correcto funcionamiento del cable de red mediante un tester.
    - Comprobar el uso del cable correcto entre equipos.
    - Confirmar que todos los cables estén conectados.
- Inspección del(los) switch(es); (checar las luces indicadoras de actividad).

6.2. Prueba de la capa de aplicación utilizando el programa telnet

Telnet es el nombre de un protocolo (y del programa informático que implementa el cliente) que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

Sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero fue una herramienta muy útil para arreglar fallos a distancia sin necesidad de estar físicamente en el mismo sitio que la máquina que los

tenía. También se usaba para consultar datos a distancia, como datos personales en máquinas accesibles por red, información bibliográfica, etc.

Aparte de estos usos, en general telnet se ha utilizado (y aún hoy se puede utilizar en su variante SSH) para abrir una sesión con una máquina UNIX, de modo que múltiples usuarios con cuenta en la máquina, se conectan, abren sesión y pueden trabajar utilizando esa máquina. Es una forma muy usual de trabajar con sistemas UNIX.

Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como *texto plano* (cadenas de texto sin cifrar). Esto facilita que cualquiera que espíe el tráfico de la red pueda obtener los nombres de usuario y contraseñas, y así acceder él también a todas esas máquinas. Por esta razón dejó de usarse, casi totalmente, hace unos años, cuando apareció y se popularizó el SSH (Secure Shell), que puede describirse como una versión cifrada de telnet.

6.2.1. MANEJO DE TELNET

Para iniciar una sesión con un intérprete de comandos de otro computador, puede emplear el comando *telnet* seguido del nombre o la dirección IP de la máquina en la que desea trabajar, por ejemplo si desea conectarse a la máquina *purpura.micolegio.edu.com* deberá teclear telnet purpura.micolegio.edu.com, y para conectarse con la dirección IP 1.2.3.4 deberá utilizar telnet 1.2.3.4.

Una vez conectado, podrá ingresar el nombre de usuario y contraseña remota para iniciar una sesión en modo texto a modo de consola virtual (ver Lectura Sistema de usuarios y manejo de clave). La información que transmita (incluyendo su clave) no será protegida o cifrada y podría ser vista en otros computadores por los que se transite la información (la captura de estos datos se realiza con un packet sniffer.

Una alternativa más segura para telnet, pero que requiere más recursos del computador, es SSH. Este cifra la información antes de transmitirla, autentica la máquina a la cual se conecta y puede emplear mecanismos de autenticación de usuarios más seguros.

6.2.2. SEGURIDAD

Hay tres razones principales por las que el telnet no se recomienda para los sistemas modernos desde el punto de vista de la seguridad:

- Los demonios de uso general del telnet tienen varias vulnerabilidades descubiertas sobre los años, y varias más que podrían aún existir.

- Telnet, por defecto, no cifra ninguno de los datos enviados sobre la conexión (contraseñas inclusive), así que es fácil interferir y grabar las comunicaciones, y utilizar la contraseña más adelante para propósitos maliciosos.

- Telnet carece de un esquema de autentificación que permita asegurar que la comunicación esté siendo realizada entre los dos anfitriones deseados, y no interceptada entre ellos.

En ambientes donde es importante la seguridad, por ejemplo en el Internet público, telnet no debe ser utilizado. Las sesiones de telnet no son cifradas. Esto significa que cualquiera que tiene acceso a cualquier router, switch, o gateway localizado en la red entre los dos anfitriones donde se está utilizando telnet puede interceptar los paquetes de telnet que pasan cerca y obtener fácilmente la información de la conexión y de la contraseña (y cualquier otra cosa que se mecanografía) con cualesquiera de varias utilidades comunes como tcpdump y Wireshark.

Estos defectos han causado el abandono y depreciación del protocolo telnet rápidamente, a favor de un protocolo más seguro y más funcional llamado SSH, lanzado en 1995. SSH provee de toda la funcionalidad presente en telnet, la adición del cifrado fuerte para evitar que los datos sensibles tales como contraseñas sean interceptados, y de la autentificación mediante llave pública, para asegurarse de que el computador remoto es realmente quién dice ser.

Los expertos en seguridad computacional, tal como el instituto de SANS, y los miembros del newsgroup de comp.os.linux.security recomiendan que el uso del telnet para las conexiones remotas debiera ser descontinuado bajo cualquier circunstancia normal.

Cuando el telnet fue desarrollado inicialmente en 1969, la mayoría de los usuarios de computadoras en red estaban en los servicios informáticos de instituciones académicas, o en grandes instalaciones de investigación privadas y del gobierno. En este ambiente, la seguridad no era una preocupación y solo se

convirtió en una preocupación después de la explosión del ancho de banda de los años 90. Con la subida exponencial del número de gente con el acceso al Internet, y por la extensión, el número de gente que procura crackear los servidores de otra gente, telnet podría no ser recomendado para ser utilizado en redes con conectividad a Internet. (53)

6.3. Prueba de la capa de red utilizando el comando ping

Un **ping** se trata de una utilidad que comprueba el estado de la conexión con uno o varios equipos remotos por medio de los paquetes de solicitud de eco y de respuesta de eco (definidos en el protocolo de red ICMP) para determinar si un sistema IP específico es accesible en una red. Es útil para diagnosticar los errores en redes o enrutadores IP.

Muchas veces se utiliza para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos, y por ello, se utiliza entre los aficionados a los juegos en red el término **PING** para referirse al lag o latencia de su conexión.

Existe otro tipo, **Ping ATM**, que se utiliza en las redes ATM (como puede ser una simple ADSL instalada en casa) y, en este caso, las tramas se transmiten son ATM (nivel 2 del modelo OSI).

Este tipo de paquetes se envían para probar si los enlaces ATM están correctamente definidos.

6.3.1. COMANDO PING UTILIZANDO PARA LA VERIFICACION DE TRANSFERENCIA DE DATOS

El comando 'ping' es ampliamente utilizado para verificar el estado de las conexiones entre dos PC dentro de una red.

Se suele utilizar digitando en la línea de comandos: **ping** ***+ IP_del_otro_pc***

Por ejemplo:

En Windows:

C:\>ping 192.168.0.1

Haciendo ping a 192.168.0.1 con 32 bytes de datos:

Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

En Linux:

linux-pc@linux-user:/$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.219 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.187 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.178 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.167 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.168 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.186 ms

--- 192.168.1.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.167/0.184/0.219/0.019 ms
nachosama@nkun:/$

Lo que se verá en la pantalla es un informe mostrando el tamaño en bytes de los paquetes que se están enviando y el tiempo que demoran éstos en retornar.

Al final del test se muestra un resumen con las estadísticas de la prueba.

El procedimiento **ping** se invoca de la misma manera tanto en Windows como en Linux aunque difiere en la gramática de sus argumentos.

- *Para Windows existen los siguientes parámetros:*

Uso:

ping [-t] [-a] [-n cuenta] [-l tamaño] [-f] [-i TTL] [-v TOS] [-r cuenta] [-s cuenta] [[-j lista-host] | [-k lista-host]] [-w tiempo de espera] nombre-destino

Opciones:

-t	Ping el host especificado hasta que se pare. Para ver estadísticas y continuar - presionar Control-Inter; Parar - presionar Control-C.
-a	Resolver direcciones en nombres de host.
-n cuenta	Número de peticiones eco para enviar.
-l tamaño	Enviar tamaño del búfer.
-f	Establecer el indicador No fragmentar en los paquetes.
-i TTL	Tiempo de vida.
-v TOS	Tipo de servicio.
-r cuenta	Ruta del registro para la cuenta de saltos.
-s count	Sello de hora para la cuenta de saltos.
-j	lista-host Afloja la ruta de origen a lo largo de la lista- host.
-k	lista-host Restringir la ruta de origen a lo largo de la lista- host.
-w	tiempo de espera Tiempo de espera en milisegundos para esperar cada respuesta.

Parámetros en Linux:

ping [-LRUbdfnqrvVaA] [-c count] [-i interval] [-w deadline]

[-p pattern] [-s packetsize] [-t ttl] [-I interface or address]
[-M mtu discovery hint] [-S sndbuf]
[-T timestamp option] [-Q tos] [hop1 ...] destination

Opciones en Linux:

-c count Para después de enviar (y recibir) count paquetes ECHO_RESPONSE.

-d Establece la opción SO_DEBUG en el socket en uso.

-f Envío masivo de pings. Envía paquetes a la misma velocidad a la que regresan o cien veces por segundo, lo que sea mayor. Por cada ECHO_REQUEST enviado se escribe un ".", mientras que por cada ECHO_REPLY recibido se escribe un backspace. Esto proporciona una muestra rápida de cuántos paquetes se están perdiendo.
Sólo el súper-usuario puede utilizar esta opción. Esto puede resultar muy peligroso en una red y debe usarse con precaución.

-i wait
Espera wait segundos entre el envío de cada paquete. Por defecto se espera un segundo entre el envío de los paquetes. Esta opción es incompatible con la opción -f.

-l preload
Si se especifica preload, ping envía tantos paquetes tan rápido como le sea posible antes de volver a su comportamiento normal.
Sólo el súper-usuario puede usar esta opción.

-n Sólo salida numérica. No se realiza ningún intento de buscar nombres simbólicos para las direcciones del servidor.

-p pattern
Se pueden especificar un total de 16 bytes "pad" para completar el paquete que se envía. Esto resulta útil para el diagnóstico de problemas de red relacionados con los datos. Por ejemplo, "-p ff" hará que el paquete enviado se complete en su totalidad con unos.

-q Salida muda. No se muestra ninguna información excepto las líneas de resumen al comenzar y al terminar.

-R Registro de ruta. Incluye la opción RECORD_ROUTE en el paquete ECHO_REQUEST y muestra el buffer de ruta sobre los paquetes devueltos. Nótese que la cabecera IP tan

sólo tiene tamaño suficiente para nueve rutas de este tipo. Muchos servidores ignoran descartan esta opción.

-r Pasa por alto las tablas de encaminamiento y envía datos directamente a un ordenador en una red conectada a la propia. Si el ordenador receptor no está en una red con conexión directa, se devuelve un error. Esta opción se puede usar para hacer ping a un ordenador local a través de un interfaz que carezca de una ruta que pase por él (por ejemplo, después de que el interfaz haya sido anulado por routed (8).)

-s packetsize

Especifica el número de bytes de datos que se van a enviar. La cantidad por defecto es 56, que pasan a ser 64 bytes de datos ICMP cuando se combinan con los 8 bytes de los datos de la cabecera ICMP.

-v Aumenta la longitud de la información del programa en pantalla.

Se listan los paquetes ICMP que no sean ECHO_RESPONSE que se reciben. (54)

6.4. Prueba de la capa de red utilizando el comando trace

Comando: TRACE

Parámetros: [<servidor>]

El comando TRACE se usa para encontrar la ruta a un servidor específico. Cada servidor que procese este mensaje debe decírselo al que lo envía con una respuesta que indique que es un enlace, formando una cadena de respuestas similar a la que se obtiene al usar "traceroute". Tras enviar la respuesta, debe enviar el mensaje TRACE al siguiente servidor hasta que se llegue al servidor especificado. Si se omite el parámetro <servidor>, se recomienda que el comando TRACE envíe un mensaje al que solicita el trazado diciendo los servidores a los que el servidor actual tiene conexión directa.

Si el destino especificado por <servidor> es un servidor, el servidor de destino debe informar a todos los servidores y usuarios que están conectados a él, aunque sólo los Operadores pueden ver los usuarios. Si <servidor> es un Nick, sólo se dará la respuesta para ese Nick.

Respuestas numéricas:

ERR_NOSUCHSERVER

Si el mensaje TRACE va destinado a otro servidor, todos los servidores intermedios deben devolver una respuesta RPL_TRACELINK para indicar que el mensaje pasó por él y donde fue a continuación.

RPL_TRACELINK

Una respuesta a TRACE puede estar compuesta por un número cualquiera de las siguientes respuestas numéricas:

RPL_TRACECONNECTING	RPL_TRACEHANDSHAKE
RPL_TRACEUNKNOWN	RPL_TRACEOPERATOR
RPL_TRACEUSER	RPL_TRACESERVER
RPL_TRACESERVICE	RPL_TRACENEWTYPE
RPL_TRACECLASS	

(55)

6.5. Prueba de la capa de red utilizando el comando show ip route

Para ver la tabla de enrutamiento, debe introducirse el comando **show ip route**, desde el modo usuario o privilegiado. Las subredes que están directamente conectadas vienen marcadas por una C, las obtenidas a través de RIP vienen marcadas por una R, las obtenidas a través de IGRP vienen marcadas por una I, etc (la leyenda se muestra en pantalla junto con el resultado del comando show). Así, el comando show ip route ofrece la siguiente información:

- Lista de todas las rutas y máscaras de red que hay actualmente en la tabla de enrutamiento.
- La dirección IP del siguiente nodo y la interfaz de salida para dichas rutas.

- Si la ruta se conoce dinámicamente, también se refleja el tiempo (en segundos) que la ruta ha estado en la tabla o el tiempo transcurrido desde la última actualización, dependiendo del protocolo de enrutamiento.
- La distancia administrativa y la métrica del protocolo de enrutamiento. La distancia administrativa es el número a la izquierda de la barra que aparece entre corchetes, y la métrica es el número a la derecha de la misma barra.

La **distancia administrativa** es un valor numérico que representa la fiabilidad del origen de la actualización del enrutamiento. La **métrica** es un número que se utiliza para clasificar las rutas por preferencia cuando existe más de una ruta al mismo destino. Cada uno de los diferentes protocolos de enrutamiento dinámico posee un algoritmo distinto para calcular la métrica.

El comando show ip route también tiene parámetros opcionales que se pueden utilizar para solicitar solamente determinados tipos de rutas, como son:

- **Show ip route connected**. Muestra las rutas a interfaces directamente conectadas.
- **Show ip route static**. Muestra las rutas configuradas manualmente.
- **Show ip route 131.108.3.0**. Muestra la información la ruta especificada.

Otra herramienta que le ofrece un vistazo rápido del estado de la tabla de enrutamiento es el comando ejecutable **show ip masks**. Si se da una dirección de red como parámetro, este comando genera una lista de las máscaras que se han aplicado a dicha dirección, así como el número de rutas que tiene cada una de ellas. Un ejemplo sería **show ip masks 131.108.0.0**.

Puede utilizar el comando ejecutable **clear ip route** para eliminar un ruta específica de la tabla de enrutamiento (**clear ip route 131.108.3.0 255.255.255.128**), o todo el contenido de la tabla de enrutamiento (**clear ip route ***), teniendo en cuenta que la actualización de la información contenida en la tabla requiere un tiempo que oscila unos segundos y varios minutos.
(56)

7. Resultados

En todo sistema operativo existe una serie de comandos para verificar la correcta configuración de la red, así como mostrar algún problema posible. Los comandos utilizados se enlistan a continuación:

1. ping
2. netstat
3. trace route
4. ipconfig (winXP) e ifconfig (GNU-Linux Aurora y Solaris)

ping

En la siguiente figura se muestra le ejecución de éste comando desde la consola del SO Solaris. Esta utilidad comprueba el estado de conexión con uno o varios equipos remotos. El comando ping se ejecutó en las cuatro direcciones IPv4 de las máquinas dentro de la red.

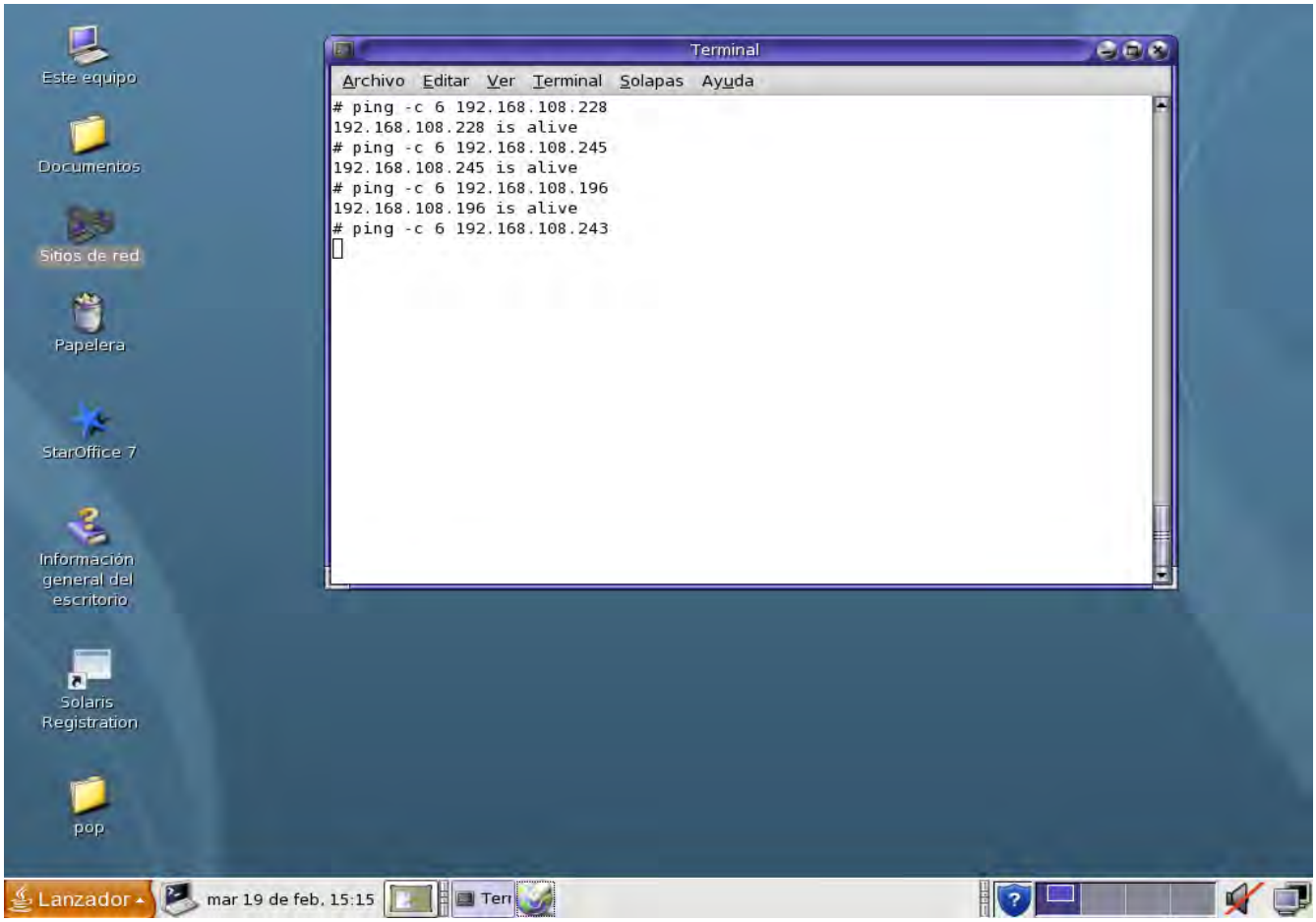

Este equipo
Documentos
Sitios de red
Papelera
StarOffice 7
Información general del escritorio
Solaris Registration
pop
Terminal
Archivo Editar Ver Terminal Solapas Ayuda
ping -c 6 192.168.108.228
192.168.108.228 is alive
ping -c 6 192.168.108.245
192.168.108.245 is alive
ping -c 6 192.168.108.196
192.168.108.196 is alive
ping -c 6 192.168.108.243
Lanzador
mar 19 de feb, 15:15

Figura 7.1

En la figura 7.1 se observa la ejecución de ping con un "is alive" lo cual nos corrobora una conexión se encuentra funcionando correctamente.

trace route Es una herramienta de diagnóstico de redes que permite seguir la pista de los paquetes que van desde un host a otro. Esta herramienta se llama traceroute en GNU-Linux , mientras que en Windows se llama tracert.

```
C:\>tracert www.unam.mx

Traza a la dirección www.unam.mx [216.239.59.147]
sobre un máximo de 30 saltos:

  1    52 ms    59 ms    59 ms  192.168.153.1
  2    55 ms    59 ms    47 ms  210.Red-81-46-52.staticIP.rima-tde.net
[81.46.52.210]
  3    78 ms    83 ms    83 ms  29.Red-81-46-5.staticIP.rima-tde.net
[81.46.5.29]
  4     *        *        *     Tiempo de espera agotado para esta
solicitud.
  5    80 ms    83 ms    83 ms  GE4-0-0-0-grtmadrr1.red.telefonica-
wholesale.net [213.140.51.9]
  6   113 ms   119 ms   107 ms  So6-0-0-0-grtlontl1.red.telefonica-
wholesale.net [213.140.38.26]
  7   197 ms   119 ms   119 ms  195.66.226.125
  8   114 ms   131 ms   119 ms  72.14.238.246
  9   138 ms   143 ms   143 ms  216.239.49.254
 10   138 ms   131 ms   131 ms  216.239.48.158
 11   138 ms   131 ms   155 ms  216.239.49.126
 12   138 ms   131 ms   143 ms  216.239.59.147
```

En GNU/Linux

```
root:/# tracert www.unam.mx


  traceroute to www.unam.mx (64.233.169.99), 64 hops max, 40 byte
packets
  1  * * *
```

```
  2  172.16.183.1 (172.16.183.1)  23 ms  23 ms  22 ms
  3  10.127.66.229 (10.127.66.229) [MPLS: Label 1479 Exp 0]  38 ms  51
ms  38 ms
  4  cnt-00-tge1-0-0.gw.cantv.net (200.44.43.85)  38 ms  38 ms  37 ms
  5  cri-00-pos1-0-0.border.cantv.net (200.44.43.50)  51 ms  43 ms  43
ms
  6  sl-st21-mia-14-1-0.sprintlink.net (144.223.245.233)  94 ms  93 ms
93 ms
  7  sl-bb20-mia-5-0-0.sprintlink.net (144.232.9.198)  95 ms  93 ms
93 ms
  8  sl-crs1-mia-0-4-0-0.sprintlink.net (144.232.2.248)  94 ms  95 ms
95 ms
  9  sl-crs1-atl-0-0-0-1.sprintlink.net (144.232.20.48)  104 ms  104
ms  103 ms
 10  sl-st20-atl-1-0-0.sprintlink.net (144.232.18.133)  104 ms  103 ms
*
 11  144.223.47.234 (144.223.47.234)  103 ms  103 ms  103 ms
 12  64.233.174.86 (64.233.174.86)  98 ms  97 ms 64.233.174.84
(64.233.174.84)  103 ms
 13  216.239.48.68 (216.239.48.68)  105 ms  104 ms  106 ms
 14  72.14.236.200 (72.14.236.200)  106 ms *  105 ms
 15  72.14.232.21 (72.14.232.21)  110 ms  109 ms  107 ms
 16  * yo-in-f99.google.com (64.233.169.99)  100 ms  99 ms
```

Traceroute en Solaris

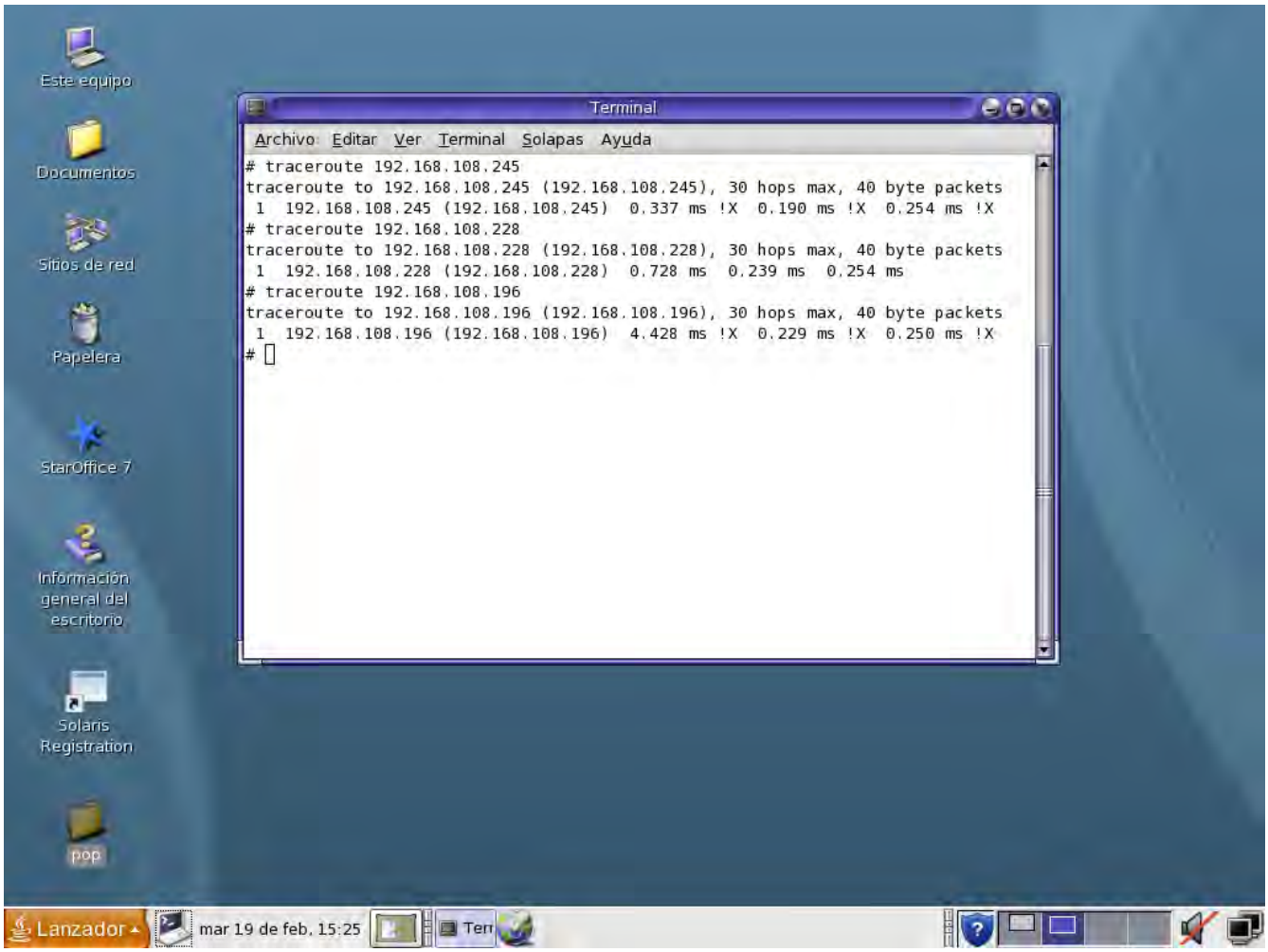


Figura 7.2. Ejecución de traceroute en SO Solaris.

netstat	Su ejecución despliega el estado de la red y estadísticas de protocolos, tales como: TCP, UDP y SCTP. También puede mostrar tablas de ruteo e información de interfaces.
netstat –i	Muestra el estado de las interfaces en red
netstat –r	Esta tabla muestra el estado de todas las rutas que el host conoce.
netstat –p	Despliega las conexiones abiertas.

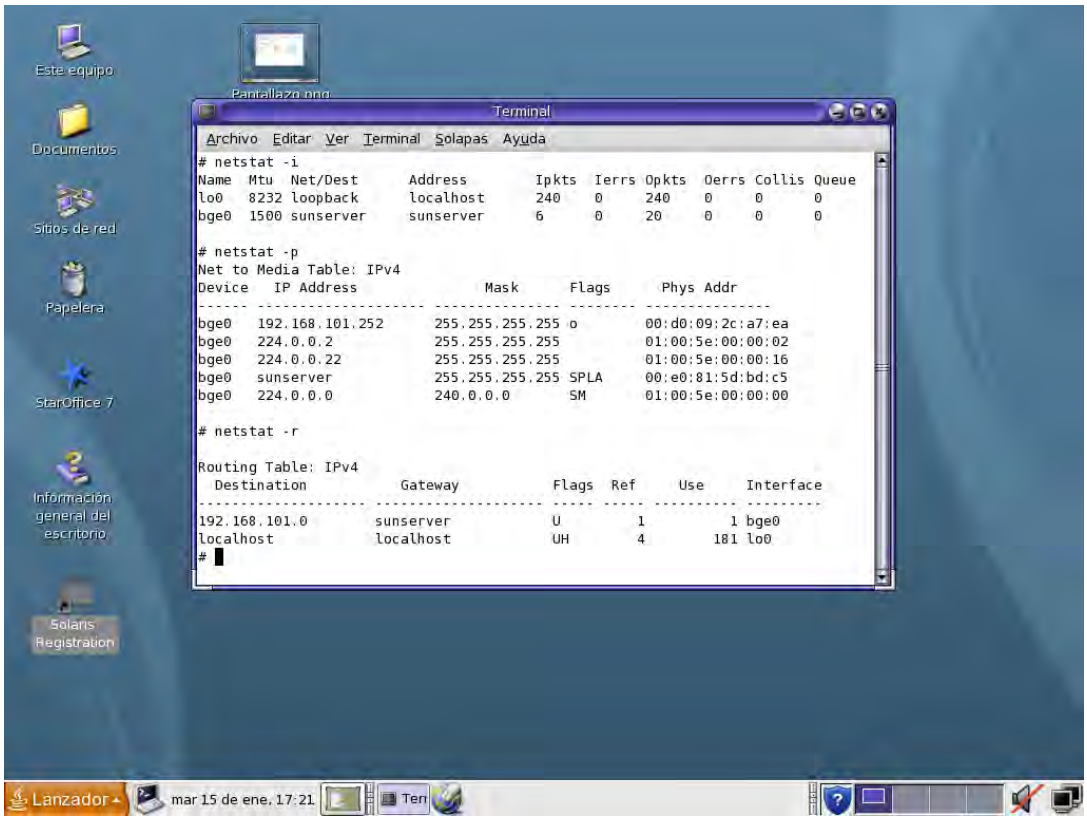


Figura 7.3 Ejecución del comando netstat.

ip route show Despliega la tabla completa/resumida de ruteo IP o de una dirección IP específica, mascara de red o protocolos.

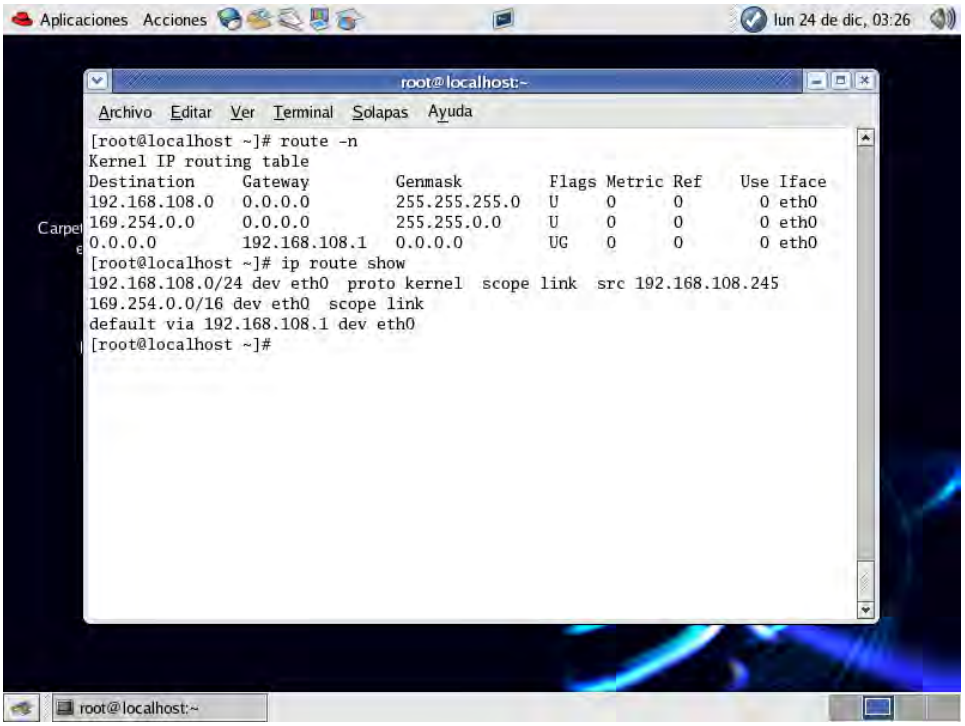


Figura 7.4 Ejecución del comando show ip route.

Router

Modo de utilización sin privilegios o user exec " **?** " (help)

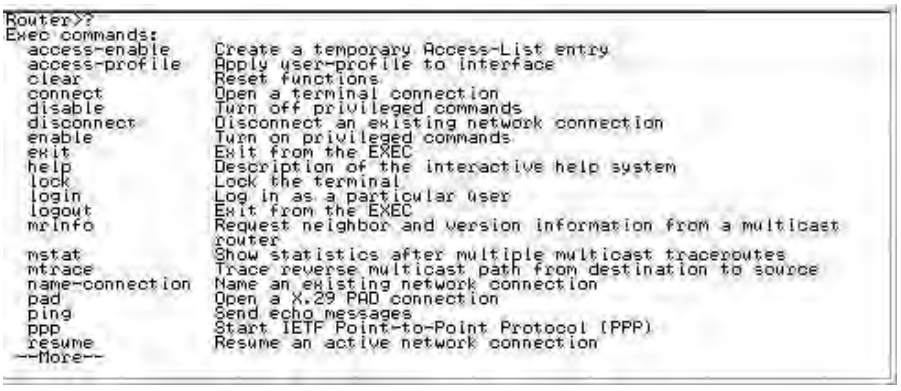


Figura 7.5 Ayuda en modo user exec.

Modo de utilización con privilegios o privileged exec " **?** " (help)

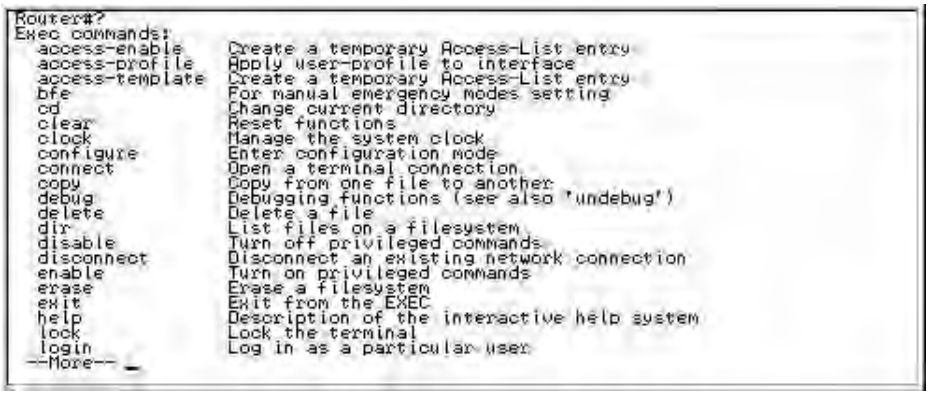


Figura 7.6 Ayuda en modo privileged exec.

Listado de comandos en el modo de ejecución privilegiado

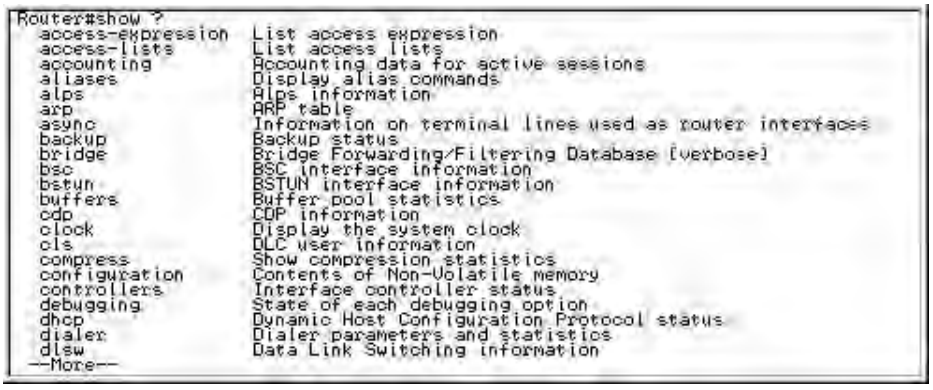


Figura 7.7 Ejecución de *show ?* en modo privilegiado.

Ejecución del comando show running config.

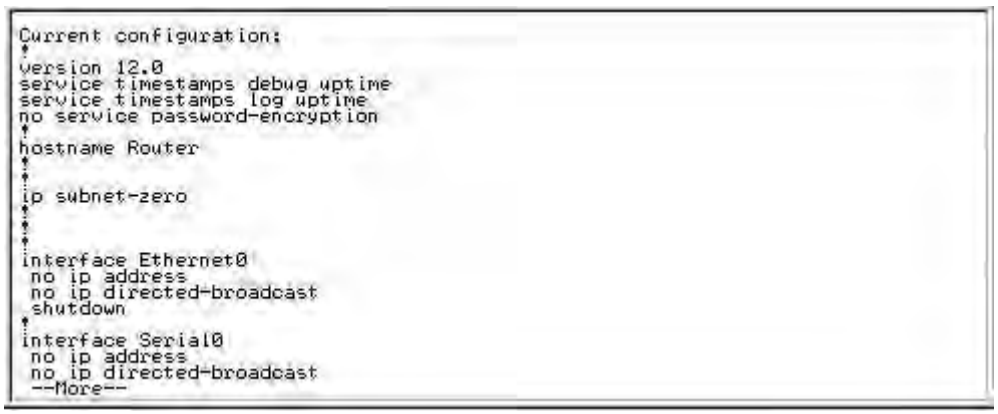


Figura 7.8 "show running config" despliega la configuración actual del router.

Configuración adicional en el servidor

El servicio DHCP se habilita por línea de comandos de la siguiente manera:

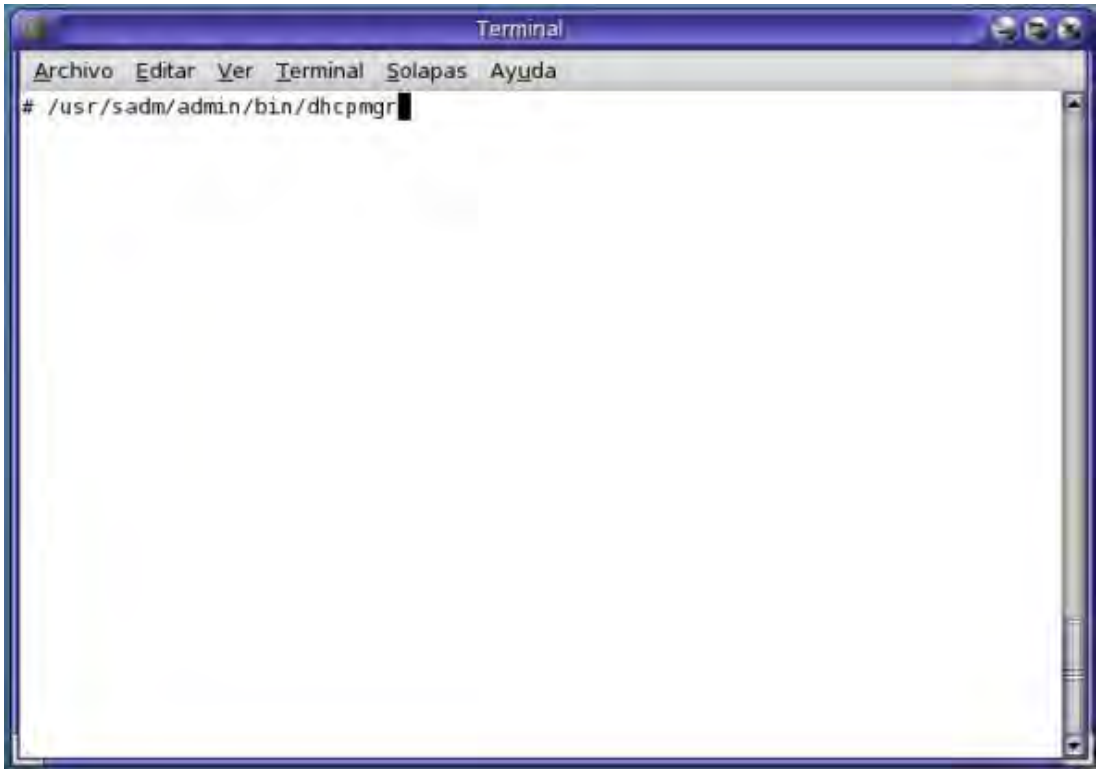


Figura X. X Lanzador de GUI DHCP por línea de comandos.

Al ejecutar el servicio, aparece la siguiente ventana. En ella, se configuró el siguiente rango de direcciones dinámicamente: 192.168.101.1:10

Además, se estableció que su dirección IP no caducará si la máquina es parte de la red. En el caso de equipos externos (como laptops personales) las direcciones caducan al terminar la sesión. En la siguiente figura observamos la ventana de configuración del gestor de DHCP Solaris.

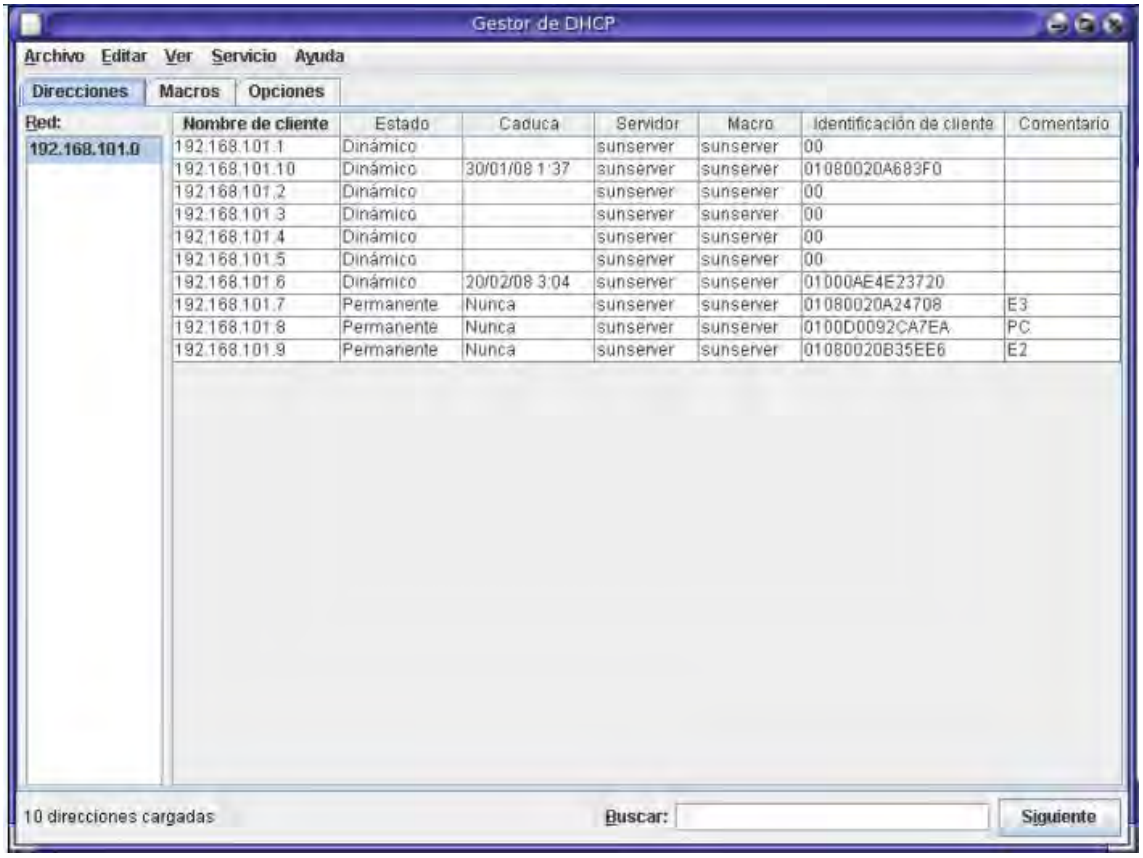


Figura X.2 Gestor DHCP

8. Conclusiones

- Para llevar a cabo la interconexión de dispositivos de red es necesario tener un sólido respaldo teórico. Éste es importante además pues nos permite detectar y reparar posibles fallas.
- Las prácticas realizadas permitirán a los alumnos introducirse en la problemática de cada uno de los pasos durante el "levantamiento de una red".
- Además, la realización de estas prácticas resaltó la importancia de contar con una parte práctica que refuerce la parte teórica.

Al término de este trabajo concluimos que la parte más complicada y tardada fue la configuración de los sistemas operativos GNU-Linux, así como la más enriquecedora. Queda en puerta el aprovechamiento de éste laboratorio para nuevos proyectos como virtualización, servidor web o terminales Java.

Apéndice 1

ÍNDICE DE ILUSTRACIONES.

Tema 1 Número de página

Tema 2.

Tema 3

Sin figuras.

Tema 4

Tema 5

Tema 7.

Apéndice 2

ÍNDICE DE FIGURAS DE PRÁCTICAS

Práctica 4.

Práctica 5.

Práctica 6.

Sin figuras.

Práctica 7.

APÉNDICE 3

ÍNDICE DE TABLAS.

Glosario

100BASE-FX: Especificación para Fast Ethernet 100Mbps sobre fibra. Similar a la especificación FDDI.

100BASE-T4: Especificación para Fast Ethernet 100Mbps sobre cableados de pares retorcidos categoría 3 o mejor. Utiliza los cuatro pares de cable. No soporta dúplex en T4

100BASE-TX: Especificación para Fast Ethernet 100Mbps sobre cableados de pares retorcidos categoría 5 o mejor. Similar a las especificaciones de CDDI.

AUI: Unidad de Interface de Enlace (Attachment Unit Interface.)

Backbone cabling: Cableado de red estructurado que corre entre marcos de distribución.

Broadcast address: Un único vector de 48 bits que se utiliza para designar todos y cada uno de los puertos conectados a la red.

CSMA/CD (Carrier Sense Multiple Access/Collision Detection): Un protocolo estándar de sensibilidad de colisión Ethernet/Fast Ethernet, que permite que múltiples dispositivos accedan a una red compartida.

Dominio de colisión: Un grupo de dispositivos Ethernet o Fast Ethernet que están directamente conectados por repetidores.

Ethernet: Red industrial estándar (IEEE 802.3) que transfiere datos a 10Mbps utilizando medios compartidos y CSMA/CD.

Dirección de destino: Un vector único de 48 bits utilizado para definir el puerto especifico al que el actual paquete se está enviando.

Fast Ethernet: Red industrial estándar que transfiere a 100Mbps utilizando medios compartidos y CSMA/CD.

Control de flujo: La habilidad de un sistema de comunicaciones o de un dispositivo de controlar el flujo de paquetes de datos.

fibra/fibras ópticas: Un tipo de cable que utiliza vidrio para cargar datos a través de impulsos de luz en lugar de corriente eléctrica. El cable de fibra óptica multimodo común es conocido como un cable de 62.5/125 micrones de diámetro, aunque también puede utilizarse el de 50/125 micrones de diámetro. El modo simple es de menor diámetro, solo aproximadamente 9/125 micrones.

dúplex: Transmisión de datos donde ambos dispositivos pueden transmitir y recibir simultáneamente.

semi-dúplex: Transmisión de datos donde un solo dispositivo transmite mientras que los otros reciben.

Cableado horizontal: Cableado de red estructurado que corre entre el marco de y el enchufe en la pared.

hub: También es llamado repetidor. Extiende una red compartida a otros hubs o estaciones mediante la retransmisión de los marcos y la propagación de las colisiones.

IEEE: Instituto de Electricidad e Ingenieros Electrónicos (Institute of Electrical and Electronics Engineers, Inc.) Un cuerpo estándar que desarrolla y publica especificaciones estándares para la industria Eléctrica y Electrónica.

NIC: Tarjeta de Interface de Red (Network Interface Card)

Control de Acceso a los Medios (Media Access Control - MAC): Layer de la red Ethernet responsable de la detección y retransmisión de colisiones así como también de otras funciones.

Mbps: Megabits por segundo: Una forma de medir el uso de la red o el ancho de banda.

MBps: Megabytes por segundo: Una forma de medir el uso de la red o el ancho de banda.

MII: Media Independent Interface: similar a AUI de Ethernet. Brinda una interface estándar específica (no medio) para Fast Ethernet.

Multimodo: Cable de fibra óptica de 62.5/125 micrones que permite la transmisión de múltiples sendas de luz.

Paquete: Un bloque de datos de entre 64 y 1526 bytes que se envía a través de los cables de red.

Repetidor: Un dispositivo de la red que acepta señales en un puerto y lo repite a todos los otros puertos. Los repetidores se utilizan para dar acceso a múltiples dispositivos a un solo dominio de colisión.

Router: Un dispositivo de la red que funciona como un switch inteligente. Es capaz de aprender no solo la dirección de origen y de destino sino también las sendas que deben utilizar los paquetes para llegar a su destino. Múltiples routers pueden ser seteados de modo de ser utilizados como respaldo en caso de una falla.

SC: Un conector locking "push/pull" para cable de fibra óptica.

ST: Un conector locking estilo bayoneta para cable de fibra óptica.

Switch: Dispositivo de la red utilizado para separar dominios de colisión o segmentos de la red. Las unidades aprenderán la dirección original y de destino de otros nodos de la red y cuando se reciben los paquetes de datos, verifica esas direcciones y decide si los paquetes deben ser redirigidos a otro puerto.

Transceptor: Los transceptores son utilizados para conectar un puerto MII de una red Ethernet o Fast Ethernet al ambiente de cableado de la red. La interface para el cableado es una interface de medios dependiente especificada por los estándares de la red.

UTP: Cable de Par Retorcido no blindado de cobre.

Wi-Fi: (Wireless Fidelity): Fidelidad inalámbrica (63).

BIBLIOGRAFÍA

LIBROS

1. Gilster R, Bienvenu J, Ulstad. (2001) "**CCNA FOR DUMMIES**" Ed: Internacional Data Group Company. Estados Unidos.

62. Academia de Networking de Cisco Systems, (2005) "**Guía del primer año: CCNA® 1, 3ª edición**" Ed.: Pearson Educación, S.A., Madrid, España.

63. Vladimirov AA, Gavrilenko KV, Mikhaivlovsky AA. (2004) "Hacking Wireless: Seguridad de redes inalámbricas". Ediciones Anaya, España. Pp: 625

INTERNET

2. http://es.wikipedia.org/wiki/Modelo_OSI
3. http://www.csi.map.es/csi/silice/Cablead6.html
4. http://es.wikipedia.org/wiki/RJ-45
5. http://sunsolve.sun.com/handbook_pub/Systems/U10/spec.html
6. http://www.dooyoo.es/switches-routers/smc-ez-switch-smc-ez1024dt/details/
7. http://en.wikipedia.org/wiki/Aurora_SPARC_Linux
8. http://en.wikipedia.org/wiki/Windows_XP
9. http://es.wikipedia.org/wiki/Telnet
10. http://es.wikipedia.org/wiki/Ping
11. http://www.rfc-es.org/rfc/rfc1459-es.txt
12. http://willie.sintax.info/cisco03.asp
13. Cisco Systems, Inc., (1997) "Cisco 2500 Access Server Series" Cisco Systems, San José California, USA
14. http://www.cisco.com
15. http://www.dooyoo.es/switches-routers/smc-ez-switch-smc-ez1024dt/details/
16. http://www.sun.com/
17. http://sunsolve.sun.com/handbook_pub/Systems/U10/spec.html
18. http://en.wikipedia.org/wiki/Aurora_SPARC_Linux
19. http://en.wikipedia.org/wiki/Windows_XP

20. http://www.sun.com/aboutsun/coinfo/history.html
21. http://www.levenez.com/unix/history.html
22. http://www.sun.com/2004-0803/feature/
23. http://www.opensolaris.org/os/
24. http://www.sun.com/cddl
25. http://www.opensource.org/licenses/gpl-license.php
26. http://www.sun.com/historico/2005/2005-0614/
27. http://www.sun.com/software/solaris/avalilability.jsp
28. http://www.sun.com/software/solaris/observability.jsp
29. http://www.sun.com/software/solaris/utilization.jsp
30. http://www.sun.com/software/solaris/data_management.jsp
31. http://www.sun.com/software/solaris/security.jsp
32. http://www.sun.com/software/solaris/support_services.jsp
33. http://www.sun.com/software/solaris/interoperability.jsp
34. http://www.linksys.com
35. http://es.wikipedia.org/wiki/IOShttp://www.opensolaris.org/os/about/faq/general_faq/#source
36. Guía del primer año ccna 1 y 2 3ª edición
37. U.P.M., Dpto. Ingeniería de Sistemas Telemáticos ETSI Telecomunicación (2002) "**Manual de Configuración de un Router CISCO**"
38. http://laespiral.org/recetas/101-200/receta111.htmlhttp://www.lab.dit.upm.es/~labrst/config/manuales-cisco.
39. http://guia-ubuntu.org/
40. www.panduitncg.com/NCG_SYSSOL/ncg_syssol_pm/ncg_syssol_pm_markets/Finar:
41. http://www.ubuntu_es.com
42. (Cisco Press, pp: 201)
43. http://www.emagister.com/manual/cursos_gratis/solicitudes/index.cfm?id_centro=445540800402496968706855707045508id_curso=450310900429524965515266555645558id_puente=450310900429677048516956675345488id_busqueda=883847&id_segmento=5&id_categ=561&id_tipocurso=17&thumbnail=http://images.emagister.com/images/snapshots/8/4/7/b883847.jpg&id_solic_emag=33272429&mail=macro15@tutopia.com&isRegistrado=YES&alta_push=0
44. http://www.emagister.com/tutorial/cursos_gratis/solicitudes/index.cfm?id_centro=611740900330666667485065496945528id_curso=705850100510484849695370546945568id_puente=7058501005105150576556567050456778id_busqueda=1019440&id_segmento=4&id_categ=561&id_tipocurso=18&thu

mbnail=http://images.emagister.com/images/snapshots/4/4/0/b1019440.jpg&id_solic_emag=33272586&mail=macro15@tutopia.com&isRegistrado=YES&alta_push=0

45. http://www.mediafire.com/?5om2londzwk
46. http://www.taringa.net/posts/videos/97675/Video--como-ponchar-un-cable-UTP-6-y-RJ45-Conector.html
47. http://secure.enterasys.com/support/techtips/tk0231-9.html
48. http://es.wikipedia.org/wiki/Cable_coaxialhttp://www.monografias.com/trabajos5/ponchado/ponchado.shtml
49. http://www.htmlweb.net/redes/tcp_ip/capa_1/fisica_6.html
50. http://www.danpex.com/faqs/cat5-conf.htm
51. http://www.alu.ua.es/f/fmba/RedesBuena_archivos/page0005.htm
52. http://www.psicofxp.com/forums/redes-informaticas.113/213533-asi-se-arma-cable-consola-cisco.html
53. http://es.wikipedia.org/wiki/Telnet
54. http://es.wikipedia.org/wiki/Ping
55. http://www.rfc-es.org/rfc/rfc1459-es.txt
56. http://willie.sintax.info/cisco03.asp
65. http://es.wikipedia.org/wiki/DHCP
66. http://www.publispain.com/adsl/que_es_dhcp.html

Artículos.

57. Sun Microsystems. (2002) "Solaris Common Desktop Environment: Guía avanzada del usuario y del administrador del sistema" Ed: Copyright Sun Microsystems, Inc. Ref: 816-4016-10, CA, USA.
58. Sun Microsystems (2006) "Man pages section 1: User Commands" Ed: Copyright Sun Microsystems, Inc. Ref: 816-5165-11, CA, USA.
59. Sun Microsystems (2006) "Man pages section 3: Networking Library Functions" Ed: Copyright Sun Microsystems, Inc. Ref: 816-5170-11, CA, USA.
60. Sun Microsystems (2006) "System Administration Guide: IP Services" Ed: Copyright Sun Microsystems, Inc. Ref: 816-4554-13, CA, USA.
61. José Mª Barceló Ordinas, (2004) "Lab 4: Introducción a la configuración de routers CISCO con IOS"
62. Fernandez LC, (2007) "¡ Hey! Emprendedores" InformationWeek, México, D.F. pp: 11 http://www.informationweek.com.mx