UAEM | Universidad Autónoma del Estado de México

MANUAL PARA PRÁCTICAS DEL LABORATORIO DE CÓMPUTO PARA LA ASIGNATURA DE REDES DE COMPUTADORAS I

IDENTIFICACIÓN DE LA UNIDAD DE APRENDIZAJE

<table>
<tr><td colspan="8">ESPACIO ACADÉMICO : Unidad Académica Profesional - Nezahualcóyotl</td></tr>
<tr><td colspan="5">PROGRAMA EDUCATIVO: LICENCIADO EN INGENIERÍA EN SISTEMAS INTELIGENTES</td><td colspan="3">Área de docencia: : INGENIERÍA Y TECNOLOGÍA</td></tr>
<tr><td colspan="3">Aprobación por los H.H. Consejos Académico y de Gobierno</td><td colspan="2">Fecha:
7 DE SEPTIEMBRE DE 2011</td><td colspan="3">Programa elaborado por:
M en C. Doricela Gutiérrez Cruz
Ing. Yaroslaf Aarón Albarrán Fernández
Mtra. en C.C.Rosa María Rodríguez Aguilar</td></tr>
<tr><td colspan="5">Nombre de la Unidad de Aprendizaje: Redes de Computadoras I</td><td colspan="3">Fecha de elaboración: 5-08-2011</td></tr>
<tr><td>Clave
L4062
2</td><td>Horas de teoría
3</td><td>Horas de práctica
2</td><td>Total de horas
5</td><td>Créditos
8</td><td>Tipo de Unidad de Aprendizaje
Curso</td><td>Carácter de la Unidad de Aprendizaje
Obligatoria</td><td>Núcleo de formación
Sustantivo</td></tr>
<tr><td colspan="2">Prerrequisitos
No se requiere de ningún curso previo, aunque es deseable contar con conocimientos básicos de computación y cualquier sistema operativo.</td><td colspan="3">Unidad de Aprendizaje Antecedente
Ninguna</td><td colspan="3">Unidad de Aprendizaje Consecuente
Redes de Computadoras II</td></tr>
</table>

ÍNDICE

UAEM | Universidad Autónoma del Estado de México

DIRECTORIO DE LA UAEM

Dr. en D. Jorge Olvera García
Rector

Dr. en Ed. Alfredo Barrera Baca
Secretario de Docencia

Dra. en Est. Lat. Ángeles Ma. del Rosario Pérez Bernal
Secretaria de Investigación y Estudios Avanzados

Dr. en D. José Benjamín Bernal Suárez
Secretario de Rectoría

Mtra. en E. P. D. Ivett Tinoco García
Secretaria de Difusión Cultural

Mtro. en C. I. Ricardo Joya Cepeda
Secretario de Extensión Vinculación

Mtro. en E. Javier González Martínez
Secretario de Administración

Dr. en C. Pol. Manuel Hernández Luna
Secretario de Planeación y Desarrollo Institucional

Mtra. en A. Ed. Yolanda E. Ballesteros Sentíes
Secretaria de Cooperación Internacional

Dr. en. D Hiram Raúl Piña Libien
Abogado General

Lic. en Com. Juan Portilla Estrada
Director General de Comunicación Universitaria

Lic. Jorge Bernaldez García
Secretario Técnico de la Rectoría

Mtro. en A. Emilio Tovar Pérez
Director General de Centros Universitarios y Unidades Académicas Profesionales

Mtro. en A. Ignacio Gutiérrez Padilla

Contralor

DIRECTORIO DE LA UAP-NEZAHUALCÓYOTL

Dr. en C.E. Luis Ramón López Gutiérrez
Coordinador

Dr. en F.M. Israel Gutiérrez González
Subdirector Académico

Lic. en E. Alfredo Ríos Flores
Subdirector Administrativo

Dra. en C. S. María Luisa Quintero Soto
Coordinadora de Investigación y Estudios Avanzados

Lic. en A. E. Víctor Manuel Durán López
Coordinador de Planeación y Desarrollo Institucional

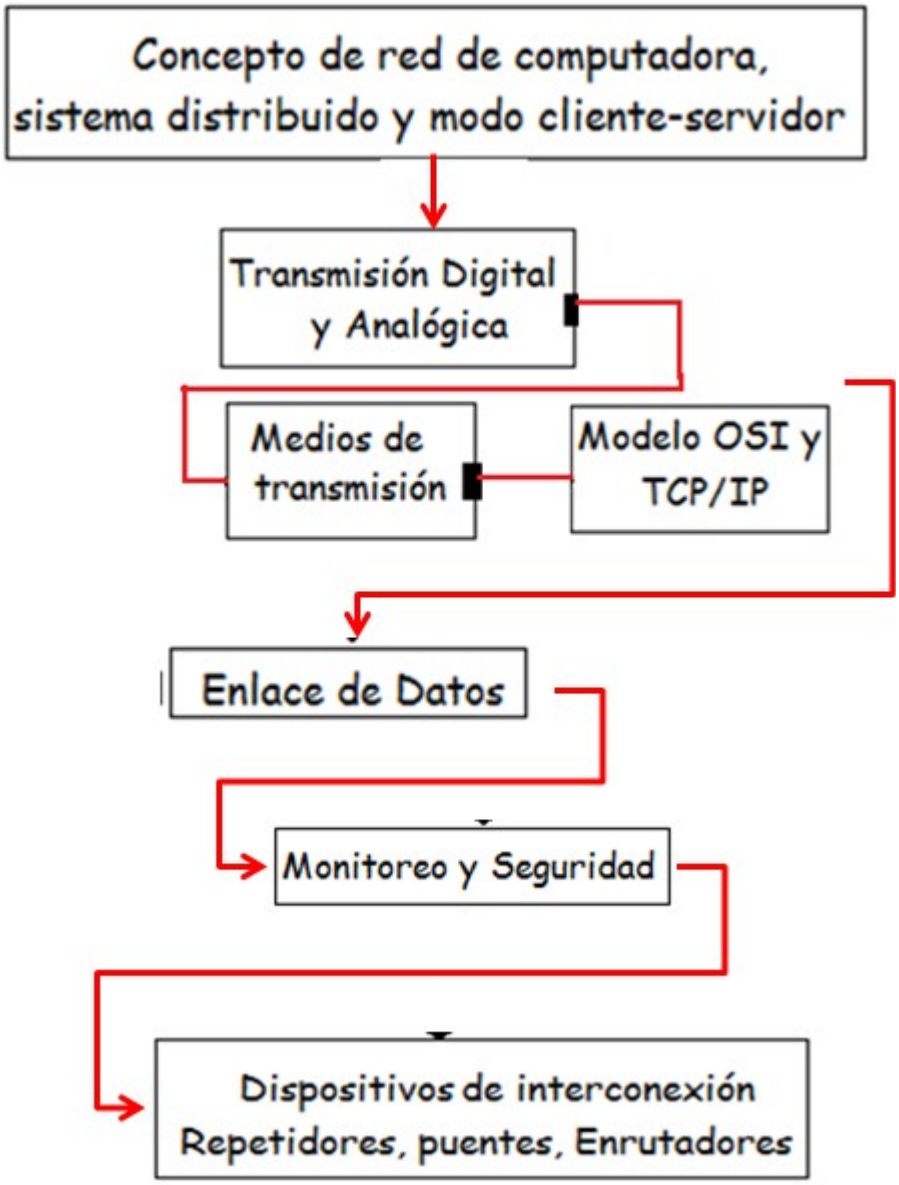
Dr. en E. Selene Jiménez Bautista
Coordinadora de la Licenciatura en Comercio Internacional

Dra. en C. Georgina Contreras Landgrave
Coordinadora de la Licenciatura en Educación para la Salud

Dra. en C. Dora María Calderón Nepamuceno
Coordinadora de Ingeniería en Sistemas Inteligentes

Mtro. en C. Juan Antonio Jiménez García
Coordinador de Ingeniería en Transporte

SECUENCIA DIDÁCTICA



PRÁCTICA 1

El Hardware de la PC

Objetivo

- Familiarizarse con los componentes periféricos básicos de un sistema de PC.
- Identificar las conexiones de PC, incluyendo la conexión de red.
- Examinar la configuración interna del PC e identificar los componentes más importantes.
- Observar el proceso de arranque para el sistema operativo Windows.
- Usar el CPU-Z para obtener información acerca del PC.

Introducción

La computadora es una máquina diseñada para facilitar el trabajo y la vida de las personas. Con ella realizamos cálculos y diseños, escribimos textos guardamos información, enviamos y recibimos mensajes, accedemos a cursos de nuestro interés, navegamos en el Internet, entre otras cosas.
Las microcomputadoras o computadoras personales (PC´s) tuvieron su origen por la necesidad de facilitar la comunicación por intermedio de una red, la más conocida se llama Internet. La parte fundamental en una computadora es su microprocesador. Un microprocesador es "una computadora en un chip", o sea un circuito integrado independiente. Las PC´s son computadoras para uso personal y actualmente se encuentran muy difundidas en todas partes: oficinas, escuelas, hogares, etc.

Hoy existen diversos tipos de micro computadoras, dependiendo del tipo de uso para el que han sido diseñadas. Por ejemplo, tenemos: la PC (Personal Computer), la Notebook, el PDA (Personal Digital Assistant) que es una microcomputadora de bolsillo.

El hardware (equipo) es la parte física de una computadora. Esta palabra se emplea para designar todos aquellos componentes de la PC que son tangibles como son el monitor, el cpu (unidad central de procesos), el “mouse”, la impresora, las unidades de almacenamiento secundario (disquete, cd, dvd), etc.

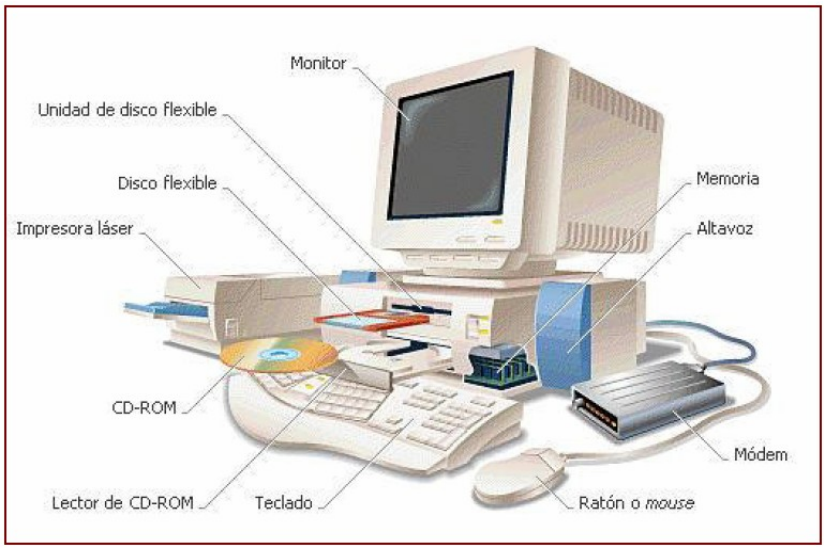


Figura 1. El Hardware de la PC.

Para poder solucionar problemas de la PC, es importante conocer sus componentes. Este conocimiento también es importante para obtener éxito en el campo de networking.

Unidad Central de Proceso.

Esta formada por la Unidad de Control, Unidad Aritmético – Lógica y la memoria principal

Unidad de Control: Dirige la ejecución del programa y controla tanto el movimiento entre memoria y ALU, como las señales que circulan entre la CPU y los Periféricos.

Unidad Aritmético – Lógica: Es la parte encargada de procesar los datos, se conoce también como ALU (Arithmetic-Logic Unit). Las operaciones que realiza son de tipo aritmético: suma, resta, multiplicación y división; y de tipo lógico: igual, mayor que o menor que.

Unidad de Almacenamiento o memoria principal: son los dispositivos donde se almacenan los datos y los programas para procesarlos. Existen dos tipos: Memoria Principal, constituida por circuitos integrados y que a su vez se subdivide en RAM y ROM; y la Memoria Secundaria, donde se almacenan otros datos que no tienen cabida en la principal, la constituyen los Discos duros (HD), CD-ROM, disquetes (FD), Unidades de cinta, memorias flash, DVD…

Unidades de entrada

Permiten introducir datos en la computadora y los principales son:

Ratón
Teclado
Escáner
Lápiz óptico
Joystick
Micrófono

Unidades de Salida

Monitor
Impresora
Plotter
Bocinas
Proyector
Audifonos

Partes internas de una computadora

a) *Tarjeta madre*: es el elemento principal de toda computadora en la cual se conectan todos los dispositivos como el procesador, la memoria el disco duro, además cuenta con ranuras de expansión, donde se puede conectar una tarjeta aceleradora de video, tarjetas de sonido, un modem, una tarjeta de red e infinidad de dispositivos.

b) *Disco Duro*: Es un dispositivo de almacenamiento magnético que la computadora utiliza para guardar datos que en un futuro volveremos a utilizar.

c) *Tarjeta de video*: es un componente electrónico requerido para generar una señal de video, que se manda a una pantalla o monitor por medio de un cable. Esta tarjeta de video puede estar integrada a la tarjeta madre o se puede colocar en una de las ranuras de la tarjeta madre.

d)*Tarjeta de sonido*: es una tarjeta electrónica que se conecta a una ranura de la tarjeta madre o puede venir integrada en la misma, su función es la salida de sonido y la introducción del mismo ya sea por micrófono o por una entrada auxiliar.

e)*Modem:* es un dispositivo de entrada y salida que se utiliza para convertir señales digitales a análogas y viceversa. Una de sus aplicaciones es la conexión a redes (Internet) a través de la línea telefónica.

f)*Tarjeta de red:* Permite la interconexión de dos o más computadoras entre si para compartir recursos en una oficina que pueden llegar a ser muy caros para tener uno por equipo, como espacio en disco duro, una impresora, Internet, o simplemente archivos de computadora. En las nuevas tarjetas madre, regularmente ya está integrada.

DESARROLLO

Paso 1. Identificación visual: Examinar la PC y componentes periféricos.

Nota: Los componentes y la configuración del PC pueden variar.

1. ¿Cuál es el fabricante y número del modelo de esta computadora?

Tabla 1.1. Datos del fabricante.

Fabricante	
Numero de modelo	

2. ¿Cuáles son los principales componentes externos del PC, incluyendo los periféricos?

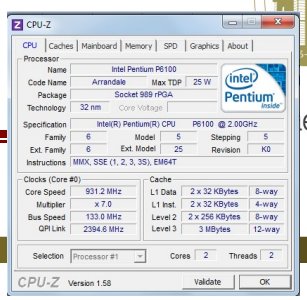
Tabla 1.2. Componentes externos.

Nombre del componente	Fabricante / Descripción / Características
1.	
2.	
3.	
4.	
5.	
6.	
7.	

Paso 2. Identificación a detalle. Información interna de la PC.

2.1 Busque, Descargue e Instale CPU-Z en su equipo.

CPU-Z es una herramienta muy interesante que sirve para el diagnóstico del CPU del ordenador, se basa en el motor de detección que provee información detallada acerca de nuestra CPU, se puede detectar la latencia de cada nivel de memoria caché, información de la placa base, procesador y su núcleo, relojes internos y externos, etc.



2.2 Una vez instalado ejecútelo en su PC y obtenga la información que a continuación se le solicita en la Tabla 1.3.

Identifique por lo menos 8 de los componentes internos más importantes que se encuentran dentro de la unidad del sistema.

Tabla 1.3

Nombre del componente	Fabricante / Descripción / Características
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	

Paso 3. Información sobre la CPU y la RAM

Recopile información básica acerca del procesador y la memoria del computador. Las instrucciones para completar este paso pueden variar levemente dependiendo de la versión de Windows.

¿Cuál es la unidad de procesamiento central (CPU)? _____

¿Cuál es la velocidad en MHz de la CPU? _____

¿Cuánta memoria RAM hay instalada? _____

Conclusiones

Anote de manera breve las principales conclusiones obtenidas al término de esta práctica

Bibliografía

CCNA 1: Conceptos básicos sobre networking v 3.1

PRÁCTICA 2
Configuración del TCP /IP

Objetivos

- Identificar las herramientas utilizadas para detectar la configuración de una red informática con varios sistemas operativos.
- Reunir información que incluya conexión, nombre de host, información de dirección MAC de Capa 2 y de dirección de red TCP/IP de Capa 3.

- Comparar la información de red con la de otras PC en la red.

Introducción

Esta práctica de laboratorio puede realizarse con cualquier versión de Windows. Esta es una práctica no destructiva que puede hacerse en cualquier máquina sin que se produzcan cambios en la configuración del sistema.
Lo ideal es que esta práctica se realice en un aula u otro entorno de LAN conectado a Internet. Esta práctica puede realizarse desde una sola conexión remota a través de un módem o conexión de tipo DSL.
Un protocolo de comunicación es un conjunto de reglas que indican cómo se debe llevar a cabo un intercambio de datos o información. Para que dos o más nodos en una red puedan intercambiar información es necesario que trabajen con el mismo conjunto de reglas, es decir, con un mismo protocolo de comunicaciones.

Debido a la gran variedad de protocolos que fueron surgiendo, se hizo necesaria su estandarización y, para ello, la ISO (*International Standards Organization*) emitió un modelo de referencia para la interconexión de sistemas abiertos, tomándose un diseño estructurado en capas que dio lugar a un modelo jerárquico conocido como modelo de referencia **OSI** (*Open Systems Interconnection*).

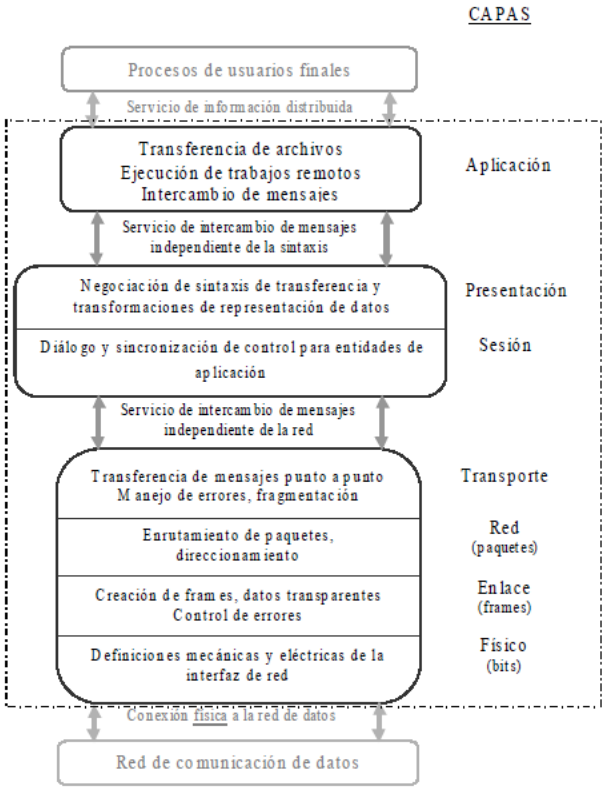


Figura 1. Capas del Modelo OSI, relaciones entre niveles y funciones.

Por otro lado, en ARPA (*Advanced Research Projects Agency*, de EEUU) definieron un conjunto de reglas bastantes robustas para establecer la interconexión de computadoras y lograr el intercambio de información, que eran capaces de soportar muchos tipos problemas o errores que surgieran en la subred. Fue así como se definió el conjunto de protocolos de TCP/IP. El modelo TCP/IP consta de 4 capas principales que se han convertido en un estándar a nivel mundial, sobre todo por su utilización en Internet.

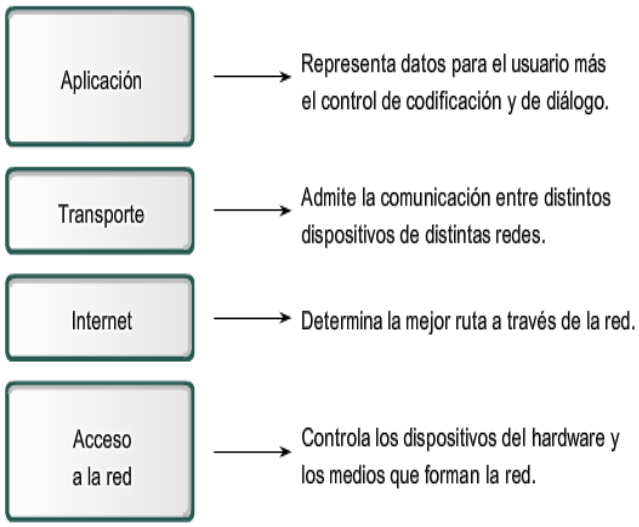


Figura 2. Capas del Modelo TCP/IP

Modelo de referencia OSI		**Suite o conjunto de protocolos TCP/IP**					
Nivel	Función	Protocolo					
7	Aplicación	Telnet	FTP	HTTP	SMTP	DNS	
6	Presentación						
5	Sesión	TCP			UDP		
4	Transporte		ICMP		RIP	OSPF	EGP
3	Red	IP			ARP		RARP
2	Enlace de datos	Ethernet		Token Ring		Otros medios	
1	Físico						

Figura 3. Correspondencia entre el modelo de referencia OSI y los protocolos de cada nivel en el modelo TCP/IP.

Las capas del modelo TCP/IP son menos que las del modelo de referencia OSI, pero son muy robustas. Normalmente, cuando se habla de TCP/IP, se relaciona automáticamente como el protocolo sobre el que funciona la red Internet. Esto, en cierta forma es cierto, ya que esta familia de protocolos está bastante extendida para la conexión a Internet y es un auténtico sistema abierto, pues los protocolos y sus implementaciones están disponibles públicamente.

El nombre TCP/IP es debido a los dos protocolos principales de esta familia:

1. El protocolo TCP, que funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.

2. El protocolo IP, que funciona en el nivel de red del modelo OSI, y permite el encaminamiento de nuestros datos hacia otras máquinas.

Hay que tener en cuenta una serie de particularidades sobre las que ha sido diseñado TCP/IP:

- Los programas de aplicación no conocen el hardware que se utiliza para realizar la comunicación (modem , tarjeta de red, ...).
- La comunicación no está orientada a la conexión de dos máquinas, es decir, que cada paquete de información es independiente y puede viajar por caminos diferentes entre dos mismas máquinas.
- El interfaz de usuario debe ser independiente del sistema, de ese modo, los programas no necesitan conocer sobre qué tipo de red trabajan.
- El uso de la red no impone ninguna topología en especial.

En definitiva, el conjunto de protocolos TCP/IP permite la comunicación entre diferentes máquinas que ejecutan sistemas operativos completamente distintos.

Direcciones IP.

El protocolo TCP/IP asigna un número único a cada máquina conectada, que consta de 32 bits y se representa en cuatro grupos de 8 bits cada uno, en formato decimal y separados por un punto, como por ejemplo, 150.217.131.78.
Las direcciones IP están constituidas por una parte que indica la dirección de la red y otra que indica la dirección de la máquina dentro de esa red.
Estas direcciones no se asignan aleatoriamente, sino que es el organismo internacional InterNIC (*Inter Network Information Centers*) el que hace las funciones de registro de direcciones Internet y de nombres de dominio. El InterNIC asigna las direcciones de red y el administrador local las de máquina.

DNS (*Domain Name Service*).

Lo habitual es que a cada equipo se le pueda conocer con un nombre del tipo maquina.dominio o maquina.subred.organizacion.pais, que es un formato más fácil de recordar que el número de las direcciones IP.
El DNS es un servicio de nombres encargado de traducir esas direcciones lógicas o textuales de máquinas a direcciones IP numéricas. Ninguna de estas direcciones se asigna arbitrariamente, sino que hay que registrar ambas en los NIC. Esto es básicamente por dos motivos:

1. Seguridad: podrían darse conflictos debidos a direcciones repetidas en distintos equipos.
2. Comodidad: permite realizar cierta correspondencia de las direcciones IP con las direcciones físicas, pues los NIC distribuyen tablas a ciertos nodos especiales de encaminamiento en la red para que consigan relacionar unas con otras.

Las consultas a un servidor DNS se realizan en modo cliente-servidor:
- Cuando una aplicación quiere "resolver" un nombre, pregunta por él a un servidor de DNS
- El servidor investiga por su cuenta y devuelve al cliente la dirección IP pedida.

A una máquina siempre hay que indicarle a qué servidores de DNS debe preguntar para resolver nombres.
A la dirección del tipo maquina.subred.organización.pais se le denomina nombre de dominio completamente cualificado y puede estar formado por un número indeterminado de subdominios separados por puntos.

Direcciones de recursos (URL, *Uniform Resource Locator*).

Esta notación permite expresar a qué servicio específico de una máquina concreta queremos acceder. El URL está formado por el nombre del protocolo (http, ftp), el dominio o nombre de la máquina donde se encuentra el servidor y el nombre del archivo al que se quiere acceder. Por ejemplo, el URL:

http://www.sita.uaemex.mx/tutoria/index_ok.html

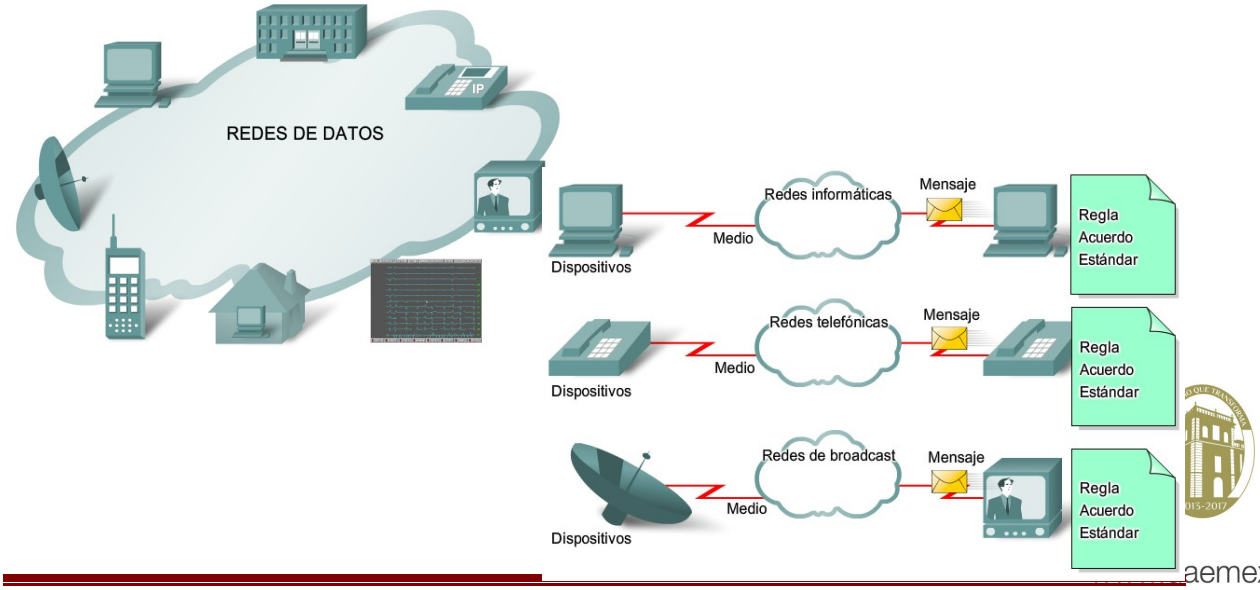
Los servicios más comunes y las acciones asociadas a cada uno de ellos en los clientes de www son:

Nombre	Función	Sintaxis[5]	Ejemplo
Ftp	Accede al servidor de FTP anónimo indicado en el URL y leer el fichero especificado	ftp://*usuario:contraseña*@maquina:*puerto*/ruta	ftp://rediris.es
http	Accede a un servidor de hipertexto y, si el fichero es una página de hipertexto, muestra su contenido, sino se pasa a una aplicación auxiliar o se almacena en disco, dependiendo del visor y del tipo de fichero	http://*usuario:contraseña*@maquina:*puerto*/*ruta?parametros*	http://www.fie.us.es/docencia/deptos/
news o nntp	Accede a un grupo de debate para leer las noticias. Aunque es necesario un servidor, si el URL no lo incluye, se usa el más próximo	news://maquina:*puerto*/nombregrupo/articulo	news://www.fie.us.es
Telnet	Establece sesiones remotas con la máquina indicada como servidor	telnet://*usuario:contraseña*@maquina:*puerto*	telnet://jaguar.pue.udlap.mx
mailto	Precede a una dirección de correo electrónico	mailto:usuario@maquina	mailto:mcromero@dte.us.es
wais	Accede a un servidor WAIS (Wide Area Information Server)	wais://maquina:*puerto/basedatos/tipoescr/rutaescr?*busqueda	wais://wais.com
File	Hace referencia a un archivo local a nuestra máquina	file://maquina/ruta	file://c:/temp/ejemplo.txt

Figura 4. Clasificación de protocolos y servicios de URL.

Software de red.

Para conectarse a Internet a través de TCP/IP es necesario un determinado software que permita a nuestro sistema y a los programas de red utilizar dicho protocolo para acceder a todos los servicios ofrecidos en Internet.
Hay diversas formas de realizar la conexión a Internet, pero las más habituales son tener cuenta en un servidor de una universidad u otra organización conectada a Internet, tener acceso desde su propia empresa, ir a un terminal público o local de conexión o tener un PC, un módem y el número de teléfono de un proveedor a través del cual conectarse.



Independientemente del tipo de conexión que se utilice, se tendrán que seguir una serie de pasos:

1. Configurar el equipo físico, que implica la instalación de la tarjeta de red o el módem, según el caso, en nuestro equipo. En función del cual, es necesario conocer algunos parámetros del hardware instalado, como el tipo de tarjeta (marca y modelo), las interrupciones que emplea, el puerto al que se conecta el módem, entre otras.

2. Instalar el software de red, es decir, los drivers de red[6]. Normalmente, este tipo de software es proporcionado junto con las tarjetas de red, con el módem o con el propio sistema operativo.

3. Configurar nuestro equipo para utilizar el protocolo TCP/IP, que implica configurar el software del sistema o de los drivers de red. Para ello se requieren una serie de parámetros que debe proporcionar el administrador de la red[7] o el proveedor de la conexión

4. Instalar programas específicos para poder acceder a los servicios: correo, sesión remota, FTP, WWW...

Hay programas de este tipo que pueden ser comerciales, shareware o freeware. Los sistemas operativos actuales incorporan todas las herramientas necesarias para la conexión, sólo es necesario instalar el hardware y el resto[9] de los elementos vienen integrados en el sistema, por lo que la configuración requerida es mínima, haciendo que los dos primeros pasos de la lista anterior sean innecesarios. Este tipo de sistemas y dispositivos son los que se denominan "plug & play".

Tabla 1. Protocolos utilizados comúnmente en internet.

Protocolo	Funcionalidad	Nivel del modelo TCP/IP
SMTP (Simple Mail Transfer Protocol)	Correo electrónico	Aplicación
TELNET (TELecommunicating NETworks)	Sesión remota	Aplicación
FTP (File Transfer Protocol)	Transferencia de archivos	Aplicación
NNTP (Network News Transfer Protocol)	Distribución de grupos de debate	Aplicación
HTTP (Hypertext Transfer Protocol)	Protocolo de transporte de ficheros de hipertexto del WWW, incluyendo documentos MIME	Aplicación
UDP (User Datagram Protocol)	Servicio de transporte de datos sin conexión (datagramas)	Transporte
TCP (Transmission Control Protocol)	Servicio de transporte de datos con conexión	Transporte
IP (Internetworking Protocol)	Envío y recepción de paquetes	Red
ICMP (Internet Control Messanges Protocol)	Regula la transmisión de mensajes de error y control entre los host y las gateways.	Red
PPP (Point to Point Protocol)	Envío de paquetes IP a través de líneas serie, es decir, conectarse a una red local para obtener acceso a Internet mediante un módem.	Enlace

DESARROLLO

Para configurar una conexión TCP/IP se necesitan una serie de datos, sea cual sea el sistema sobre el que se trabaje. La cantidad de datos requeridos depende de cómo se realice la asignación de direcciones IP del equipo, y eso va en función del tipo de conexión que se tenga:

- Manual. Si se configura de forma manual, el usuario es el encargado de introducir todos los datos necesarios para configurar el equipo dentro de una red TCP/IP. Este método se utiliza cuando el equipo posee asignada una dirección IP fija.

- Dinámica a través de un servidor. En este caso, un servidor se encarga de suministrar los datos necesarios para conectarnos a la red. Este método es el que emplean los proveedores de conexión a particulares, de modo que los usuarios llaman a un número proporcionado por el proveedor que tiene varias líneas (módems).

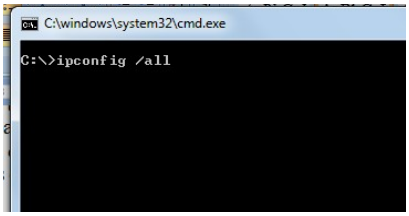
- Dinámica sin mediar un servidor. En este otro caso, el equipo adquiere una dirección IP dentro de un posible rango de direcciones posibles, pero sin conectarse con ningún servidor. Este método es útil para conexiones esporádicas y de portátiles.

Paso 1 Conectarse a Internet

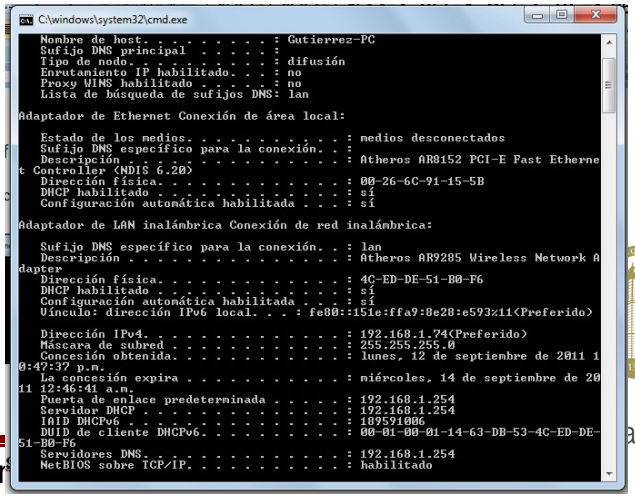
- Establezca y verifique la conectividad a Internet. Esto garantiza que la computadora tenga una dirección IP

Paso 2 Reunir información de configuración básica de TCP/IP

- En el *cmd* teclee : ipconfig /all



- Esta primera pantalla muestra la Dirección del Adaptador, o dirección MAC, en el computadora, también muestra la dirección IP, máscara de subred, y el gateway por defecto.



La dirección IP y el gateway por defecto deben estar en la misma red o subred. De lo contrario, este host no podrá comunicarse con el exterior de la red. En la figura anterior la máscara de subred indica que los primeros tres octetos deben ser los mismos para estar en la misma red.

Nota: Si este computador está en una LAN, el gateway por defecto puede no verse si se ejecuta detrás de un servidor proxy.

Registre la siguiente información representativa al equipo que esta usando:

Dirección IP: _____
Máscara de subred: _____
Gateway por defecto: _____

Paso 3 Comparar la configuración TCP/IP

Si esta computadora está en una LAN, compare la información en varias máquinas.
¿Existen similitudes? _____
¿En qué se asemejan las direcciones IP? _____
¿En qué se asemejan los gateways por defecto?
_____
¿En qué se asemejan las direcciones MAC?
_____

Las direcciones IP deben compartir la misma porción de red. Todas las máquinas en la LAN deben compartir el mismo gateway por defecto. Aunque no es obligatorio, la mayoría de los administradores de LAN intentan estandarizar los componentes como las NIC. Por lo tanto, todas las máquinas pueden compartir los primeros tres pares hexadecimales en la dirección del adaptador.

Estos tres pares identifican al fabricante del adaptador.

Registre un par de direcciones IP

_____

Paso 4 Verificar la selección del adaptador de red

- En INICIO→ Panel de Control → Administrador de Dispositivos →Adaptadores de Red→ buscar la NIC de su PC y anotar lo siguiente:

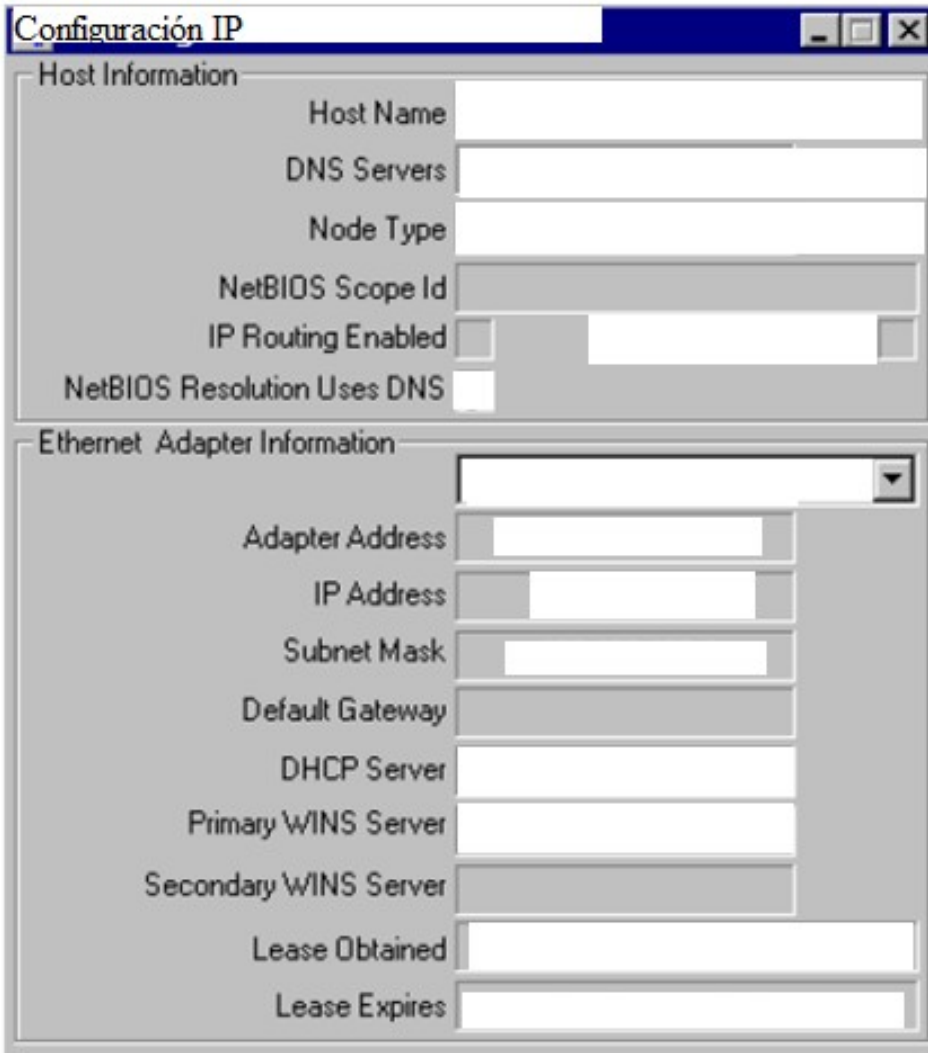
Quién es el fabricante de la NIC?_____

¿Cuál es el número de modelo de la NIC?_____

Fecha de instalación:_____

Paso 5 Reunir información adicional de configuración de TCP/IP

Complete el siguiente cuadro, ya sea que obtenga esta información en ambiente grafico o desde consola.



Es posible que se muestre el nombre de host, que incluye el nombre de la computadora y el NetBIOS. También muestra la dirección del servidor DHCP, en caso de que se use, y la fecha en que comienza y termina el alquiler de IP. Vea la información restante. También pueden aparecer las entradas de los servidores DNS y WINS. Estas entradas se usan en la resolución de nombre.
Anote las direcciones IP de cualquier servidor que aparezca:

_____

_____

Anote el nombre de host de la computadora:

_____

Anote los nombres de host de un par de otras computadoras:

¿Todos los servidores y estaciones de trabajo comparten la misma porción de red de la dirección IP que la estación de trabajo del estudiante?

Nota: No sería raro que algunos o todos los servidores y estaciones de trabajo estén en otra red. Esto significa que el gateway por defecto de este equipo va a redireccionar peticiones a la otra red.

Paso 6 Reunir información adicional de la IP

¿A que clase pertenecen las IP encontradas, en que rango se encuentran, que asignación tienen? , para ello investigue dicha asignación en las IP refiriéndose a los octetos de IPV4.

Conclusiones

Anote de manera breve las principales conclusiones obtenidas al término de esta práctica

Bibliografía

CCNA 1: Conceptos básicos sobre networking v 3.1

PRÁCTICA 3

Conversiones

Objetivo

1. El alumno conocerá la representación de datos en el sistema binario y hexadecimal

Introducción

Las computadoras manipulan y almacenan los datos usando interruptores electrónicos que están ENCENDIDOS o APAGADOS. Estas sólo pueden entender y usar datos que están en este formato binario, o sea, de dos estados. Los unos y los ceros se usan para representar los dos estados posibles de un componente electrónico de una PC. Se denominan dígitos binarios o bits. Los 1 representan el estado ENCENDIDO, y los 0 representan el estado APAGADO.

El Código americano normalizado para el intercambio de información (ASCII) es el código que se usa más a menudo para representar los datos alfanuméricos de un computador. ASCII usa dígitos binarios para representar los símbolos que se escriben con el teclado. Cuando las computadoras envían estados de ENCENDIDO/APAGADO a través de una red, se usan ondas eléctricas, de luz o de radio para representar los unos y los ceros.

Debido a que las computadoras están diseñadas para funcionar con los interruptores ENCENDIDO/APAGADO, los dígitos y los números binarios les resultan naturales. Los seres humanos usan el sistema numérico decimal, que es relativamente simple en comparación con las largas series de unos y ceros que usan los computadores. De modo que los números binarios de la computadora se deben convertir en números decimales.

A veces, los números binarios se deben convertir en números Hexadecimales (hex), lo que reduce una larga cadena de dígitos binarios a unos pocos caracteres hexadecimales. Esto hace que sea más fácil recordar y trabajar con los números.

Bits y bytes

Un número binario 0 puede estar representado por 0 volts de electricidad (0 = 0 volts).
Un número binario 1 puede estar representado por +5 volts de electricidad (1 = +5 volts).

Las computadoras están diseñadas para usar agrupaciones de ocho bits. Esta agrupación de ocho bits se denomina byte (Tabla 1). En una computadora, un byte representa una sola ubicación de almacenamiento direccionable. Estas ubicaciones de almacenamiento representan un valor o un solo carácter de datos como, por ejemplo, un código ASCII. La cantidad total de combinaciones de los ocho interruptores que se encienden y se apagan es de 256. El intervalo de valores de un byte es de 0 a 255. De modo que un byte es un concepto importante que se debe entender si uno trabaja con computadoras y redes.

Tabla 1. Unidades de información

Unidades	Definición	Bytes*	Bits*	Ejemplos
Bit (b)	Dígito binario, un 1 o un 0	1	1	Conectado/Desconectado; Abierto/Cerrado; +5 voltios o 0 voltios
Byte (B)	8 bits	1	8	Representar la letra "X" como código ASCII
Kilobyte (KB)	1 kilobyte = 1024 bytes	1000	8,000	Correo electrónico típico = 2 KB Informe de 10 páginas = 10 KB Los primeros PC = 64 KB de
Megabyte (MB)	1 megabyte = 1024 kilobytes = 1.048.576 bytes	1 millón	8 millones	Disquetes = 1,44 MB RAM típica = 32 MB CDROM = 650 MB
Gigabyte (GB)	1 gigabyte = 1024 megabytes = 1.073.741.824 bytes	Mil millones	8 mil millones	Disco duro típico = 40 GB o superior
Terabyte (TB)	1 terabyte = 1024 gigabytes = 1.099.511.627.778 bytes	1 billón	8 billones	Cantidad de datos que teóricamente se pueden transmitir por fibra óptica en un segundo

Sistema numérico de Base 10

Los sistemas numéricos están compuestos por símbolos y por las normas utilizadas para interpretar estos símbolos. El sistema numérico que se usa más a menudo es el sistema numérico decimal, o de Base 10. El sistema numérico de Base 10 usa diez símbolos: 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9. Estos símbolos se pueden combinar para representar todos los valores numéricos posibles.

El sistema numérico decimal se basa en potencias de 10. Cada posición de columna de un valor, pasando de derecha a izquierda, se multiplica por el número 10, que es el número de base, elevado a una potencia, que es el exponente. La potencia a la que se eleva ese 10 depende de su posición a la izquierda de la coma decimal. Cuando un número decimal se lee de derecha a izquierda, el primer número o el número que se ubica más a la derecha representa 10^0 (1), mientras que la segunda posición representa 10^1 (10 x 1= 10) La tercera posición representa 10^2 (10 x 10 =100). La séptima posición a la izquierda representa 10^6 (10 x 10 x10 x 10 x 10 x 10 =1.000.000).

Esto siempre funciona, sin importar la cantidad de columnas que tenga el número.

Valor posición	$\frac{}{1000}$ $\frac{}{100}$ $\frac{}{10}$ $\frac{}{1}$
Base$^{\text{Exponente}}$	$10^3 = 1000$ $10^2 = 100$ $10^1 = 10$ $10^0 = 1$
Cantidad de símbolos	10
Símbolos	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Razonamiento	Número típico de dedos igual a diez

Ejemplo:

$2134 = (2x10^3) + (1x10^2) + (3x10^1) + (4x10^0)$

Hay un 4 en la posición correspondiente a las unidades, un 3 en la posición de las decenas, un 1 en la posición de las centenas y un 2 en la posición de los miles. Este ejemplo parece obvio cuando se usa el sistema numérico decimal. Es importante saber exactamente cómo funciona el sistema decimal, ya que este conocimiento permite entender los otros dos sistemas numéricos, el sistema numérico de Base 2 y el sistema numérico hexadecimal de Base 16. Estos sistemas usan los mismos métodos que el sistema decimal.

Sistema numérico de Base 2

Las computadoras reconocen y procesan datos utilizando el sistema numérico binario, o de Base 2. El sistema numérico binario usa sólo dos símbolos, 0 y 1, en lugar de los diez símbolos que se utilizan en el sistema numérico decimal. La posición, o el lugar, que ocupa cada dígito de derecha a izquierda en el sistema numérico binario representan 2, el número de base, elevado a una potencia o exponente, comenzando desde 0. Estos valores posicionales son, de derecha a izquierda, 2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6 y 2^7, o sea, 1, 2, 4, 8, 16, 32, 64 y 128, respectivamente.

Valor posición	128 64 32 16 8 4 2 1
Base Exponente	$2^7 = 128$ $2^3 = 8$ $2^6 = 64$ $2^2 = 4$ $2^5 = 32$ $2^1 = 2$ $2^4 = 16$ $2^0 = 1$
Cantidad de símbolos	2
Símbolos	0, 1
Razonamiento	Los sistemas de voltaje de dos estados (valor binario diferenciado) creados con transistores pueden ser variados, potentes, económicos, pequeños y relativamente inmunes al ruido.

Ejemplo:

$101102 = (1 \times 2^4 = 16) + (0 \times 2^3 = 0) + (1 \times 2^2 = 4) + (1 \times 2^1 = 2) + (0 \times 2^0 = 0) = 22\ (16 + 0 + 4 + 2 + 0)$

Al leer el número binario (101102) de izquierda a derecha, se nota que hay un 1 en la posición del 16, un 0 en la posición del 8, un 1 en la posición del 4, un 1 en la posición del 2 y un 0 en la posición del 1, que sumados dan el número decimal 22.

Esto nos permite saber el número de bits que necesitamos para representar el número decimal N.

Ejemplo

$$101101{,}11 = 1x2^5 + 0x2^4 + 1x2^3 + 1x2^2 + 0x2^1 + 1x2^0 + 1x2^{-1} + 1x2^{-2}$$

En decimal se tiene: $32 + 8 + 4 + 1 + 0{,}5 + 0{,}25 = 45{,}75_{10}$

Ejercicio. Convertir los siguientes números en base binaria al correspondiente en base decimal:

1010111 =

Conversión de números decimales en números binarios de 8 bits

Existen varios métodos para convertir números decimales en números binarios. El proceso intenta descubrir cuáles de los valores de la potencia de 2 se suman para obtener el número decimal que se desea convertir en un número binario. Este es uno de varios métodos que se pueden usar. Es mejor seleccionar un método y practicarlo hasta obtener siempre la respuesta correcta.

Representación en notación decimal separada por puntos de cuatro octetos de números binarios de 32 bits

Actualmente, las direcciones que se asignan a las computadoras en Internet son números binarios de 32 bits. Para facilitar el trabajo con estas direcciones, el número binario de 32 bits se divide en una serie de números decimales. Para hacer esto, se divide el número binario en cuatro grupos de ocho dígitos binarios. Luego, se convierte cada grupo de ocho bits, también denominados octetos, en su equivalente decimal.

Binario	11001000		01110010		00000110		00110011
Decimal	200	.	114	.	6	.	51
	número	punto	número	punto	número	punto	número

Una vez que está escrito, el número binario completo se representa como cuatro grupos de dígitos decimales separados por puntos. Esto se denomina notación decimal separada por puntos y ofrece una manera compacta y fácil de recordar para referirse a las direcciones de 32 bits. Esta representación se usará frecuentemente con posterioridad durante este curso, de modo que es necesario comprenderla bien. Al realizar la conversión de binario a decimal separado por puntos, recuerde que cada grupo, que está formado por uno a tres dígitos decimales, representa un grupo de ocho dígitos binarios. Si el número decimal que se está convirtiendo es menor que 128, será necesario agregar ceros a la izquierda del número binario equivalente hasta que se alcance un total de ocho bits.

Sistema Hexadecimal

El sistema numérico hexadecimal (hex) se usa frecuentemente cuando se trabaja con computadoras porque se puede usar para representar números binarios de manera más legible. La computadora ejecuta cálculos en números binarios, pero hay varios casos en los que el resultado del computador en números binarios se expresa en números hexadecimales para facilitar su lectura.

El sistema hexadecimal es un sistema en base 16 y consta de 16 dígitos diferentes que son: del 0 al 9 y de la letra *A* a la *F*, es decir 10 dígitos numéricos y seis caracteres alfabéticos. El sistema hexadecimal se usa como forma simplificada de representación de números binarios y debido a que 16 es una potencia de $2 (2^4=16)$, resulta muy sencilla la conversión de los números del sistema binario al hexadecimal y viceversa.

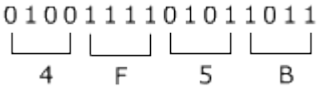
La siguiente tabla muestra los números decimales de 0 al 15 con su equivalencia en binario y hexadecimal

Decimal	Binary	Hexadecimal
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
16	00010000	10
32	00100000	20
64	01000000	40
128	10000000	80
255	11111111	FF

Para convertir un número hexadecimal en un número binario se reemplaza cada símbolo hexadecimal por un grupo de cuatro bits.

Ejemplo

El número $4F5B_{16}$ en binario equivale a



Ejercicios. Convertir a Base 16 los siguientes números binarios

10101010101010 =

101000011011 =

1111111110100001 =

Conversiones entre diferentes bases de sistemas

Las conversiones entre números de bases diferentes se efectúan por medio de operaciones aritméticas simples. Dentro de las conversiones más utilizadas se encuentran:

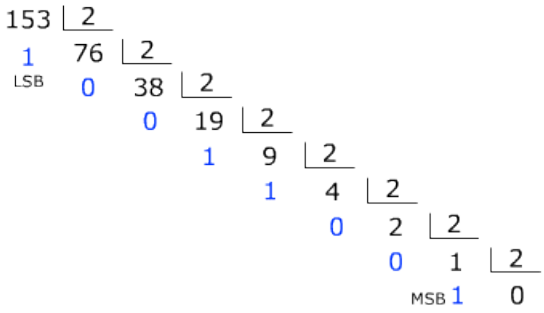
Conversión de Decimal a Binario

Para la conversión de decimal a binario se emplean dos métodos. El primero es por divisiones sucesivas y el segundo es por medio de suma de potencias de 2.

Por divisiones sucesivas

Se va dividiendo la cantidad decimal por 2, anotando los residuos, hasta obtener un cociente cero. El último residuo obtenido es el bit más significativo (*MSB*) y el primero es el bit menos significativo (*LSB*).

Por ejemplo, el número 153_{10} a binario se obtiene:.



El resultado en binario de 153_{10} es **10011001**

Por sumas de potencias de 2

Este método consiste en determinar el conjunto de pesos binarios cuya suma se equivalente al número decimal.

Ejemplo. Convertir el número 153_{10} a binario.

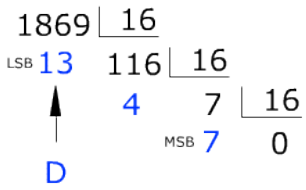
$153_{10} = \mathbf{1}x2^7 + \mathbf{0}x2^6 + \mathbf{0}x2^5 + \mathbf{1}x2^4 + \mathbf{1}x2^3 + \mathbf{0}x2^2 + \mathbf{0}x2^1 + \mathbf{1}x2^0 = 128 + 16 + 8 + 1$

$153_{10} = 10011001_2$

Conversión de Decimal a Hexadecimal

En la conversión de una magnitud decimal a hexadecimal se realizan divisiones sucesivas por 16 hasta obtener un cociente de cero. Los residuos forman el número hexadecimal equivalente, siendo el último residuo el dígito más significativo y el primero el menos significativo.

Ejemplo. Convertir el número 1869_{10} a hexadecimal.



El resultado en hexadecimal de 1869_{10} es $74D_{16}$.

EJERCICIOS. Convertir a Base 16 los siguientes números decimales

$145_{(10)}$ =

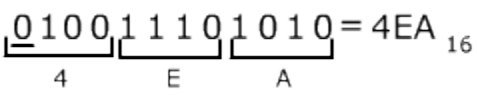
$1024_{(10)}$ =

$666_{(10)}$ =

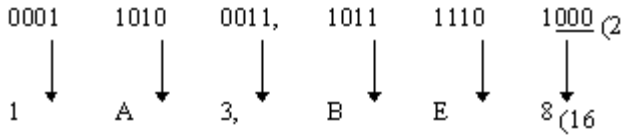
Conversión de Binario a Hexadecimal

El método consiste en conformar grupos de 4 bits hacia la izquierda y hacia la derecha del punto que indica las fracciones, hasta cubrir la totalidad del número binario. Después, se convierte cada grupo de número binario de 4 bits a su equivalente hexadecimal.

Ejemplo. Convertir el número 10011101010 a hexadecimal.



Ejemplo: Convertir el número 000110100011,101111101 $_{(2)}$ (binario) a base 16 (hexadecimal)



Conversión de Hexadecimal a Decimal

En el sistema hexadecimal, cada dígito tiene asociado un peso equivalente a una potencia de 16, entonces se multiplica el valor decimal del dígito correspondiente por el respectivo peso y realizar la suma de los productos.

Ejemplo. Convertir el número $31F_{16}$ a decimal.

$31F_{16} = 3x16^2 + 1x16 + 15 \times 16^0 = 3x256 + 16 + 15 = 768 + 31 = 799_{10}$

Conversión de Hexadecimal a Binario

La conversión de hexadecimal a binario se facilita porque cada dígito hexadecimal se convierte directamente en 4 dígitos binarios equivalentes.

Ejemplo. Convertir el número $1F0C_{16}$ a binario.

$1F0C_{16} = 0001111100001100_2$

EJERCICIOS. Convertir a Base binaria los siguientes números hexadecimales

$AF0C_{16}$ =
$23AB_{16}$ =
$980A_{16}$ =
$4BBA_{16}$ =

Binary	Hexadecimal	Binary	Hexadecimal
0000	0	1000	8
0001	1	1001	9
0010	2	1010	A
0011	3	1011	B
0100	4	1100	C
0101	5	1101	D
0110	6	1110	E
0111	7	1111	F

Binary	Hexadecimal	Decimal	Binary	Hexadecimal	Decimal
0000	0	0	1000	8	8
0001	1	1	1001	9	9
0010	2	2	1010	A	10
0011	3	3	1011	B	11
0100	4	4	1100	C	12
0101	5	5	1101	D	13
0110	6	6	1110	E	14
0111	7	7	1111	F	15

DESARROLLO.

Desarrolla las siguientes conversiones. Llenando la siguiente tabla (según corresponda) y mostrando el procedimiento realizado.

Propuesto	Decimal	Binario	Hexadecimal
1110001010101			
456			
AF89			
0101010111			
980			
345ª			
FFAF			
0101010110101			
2390			
AB56			
010101010101111			
5432			
BF908			
10101011100			
FC67			
92			
110011001110001			
FBA9			
111100011101			
128			
AB34			
569			
101010101011			

234			
CD9			
0101110001100			
127			

Bibliografía

CISCO Networking Academia. Primer año
Comunicaciones y Redes de Computadores; Stallings, William 7ª Ed. Prentice Hall, 2000. ISBN 978-84-205-4110-5
Feit, Sidnie.: TCP/IP. Arquitectura, protocolos e implementación, 2ª Ed. Mc-Graw Hill. 1998. ISBN 84-481-1531-7
Held, G.: The Complete Modem Reference, 3ª Ed. John Wiley & Sons, Inc., 1997.
Heywood, Drew: Redes con Microsoft TCP/IP. Edición Especial, 3ª Ed. Prentice Hall, 1999. ISBN 84-8322-108.

PRÁCTICA 4
CAPA FISICA: Temporización de la Red

Objetivo:

El alumno:

1. Identificara el concepto de Ancho de banda y su relación con el medio físico (cables).
2. Aplicara herramientas que le permitan mejorar y contribuir en el rendimiento del equipo: concretamente el ancho de banda.

Introducción

En esta práctica analizaremos la capa que está en la parte más baja de la jerarquía. Dicha capa define las interfaces mecánica, eléctrica y de temporización de la red. Comenzaremos con un análisis teórico de la transmisión de datos, el cual nos llevará a descubrir límites en lo que se puede enviar a través de un canal.

LA BASE TEÓRICA DE LA COMUNICACIÓN DE DATOS

Mediante la variación de algunas propiedades físicas, como el voltaje o la corriente, es posible transmitir información a través de cables. Al representar el valor de este voltaje o corriente como una función simple del tiempo, $f(t)$, podemos modelar el comportamiento de la señal y analizarlo matemáticamente.

El análisis de Fourier

A principios del siglo XIX, el matemático francés Jean-Baptiste Fourier probó que cualquier función periódica de comportamiento razonable, $g(t)$ con un periodo T, se puede construir sumando una cantidad (posiblemente infinita) de senos y cosenos:

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \operatorname{sen}(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft)$$

Donde $f = 1/T$ es la frecuencia fundamental, a_n y b_n son las amplitudes de seno y coseno de los n-ésimos (términos) **armónicos** y c es una constante. Tal descomposición se conoce como **serie de Fourier.** A partir de ella, es posible reconstruir la función, es decir, si se conoce el periodo T y se dan las amplitudes.

Una señal de datos que tenga una duración finita (la cual todas poseen) se puede manejar con sólo imaginar que el patrón se repite una y otra vez por siempre (es decir, el intervalo de T a $2T$ es el mismo que de 0 a T, etcétera). Las amplitudes a_n se pueden calcular para cualquier $g(t)$ dada multiplicando ambos lados de la ecuación (2-1) por $\operatorname{sen}(2\pi kft)$ y después integrando de 0 a T. Puesto que

$$\int_0^T \operatorname{sen}(2\pi kft)\, \operatorname{sen}(2\pi nft)dt = \begin{cases} 0 \text{ para } k \neq n \\ T/2 \text{ para } k = n \end{cases}$$

Sólo un término de la sumatoria perdura: a_n. La sumatoria de b_n desaparece por completo. De manera similar, al multiplicar la ecuación (2-1) por cos($2\pi kft$) e integrando entre 0 y T, podemos derivar b_n.

Con sólo integrar ambos lados de la ecuación como está, podemos encontrar c. Los resultados de realizar estas operaciones son los siguientes:

$$a_n = \frac{2}{T}\int_0^T g(t)\ \text{sen}(2\pi nft)\,dt \qquad b_n = \frac{2}{T}\int_0^T g(t)\ \cos(2\pi nft)\,dt \qquad c = \frac{2}{T}\int_0^T g(t)\,dt$$

Para ver cómo se relaciona todo esto con la comunicación de datos observe la Figura 2.1 muestra la salida de voltaje que produce la computadora transmisora y se muestran las amplitudes de raíz cuadrada media Estos valores son importantes porque sus cuadrados son proporcionales a la energía transmitida en la frecuencia correspondiente. Ninguna instalación transmisora puede transmitir señales sin perder cierta potencia en el proceso. Si todos los componentes de Fourier disminuyeran en la misma proporción, la señal resultante se reduciría en amplitud, pero no se distorsionaría

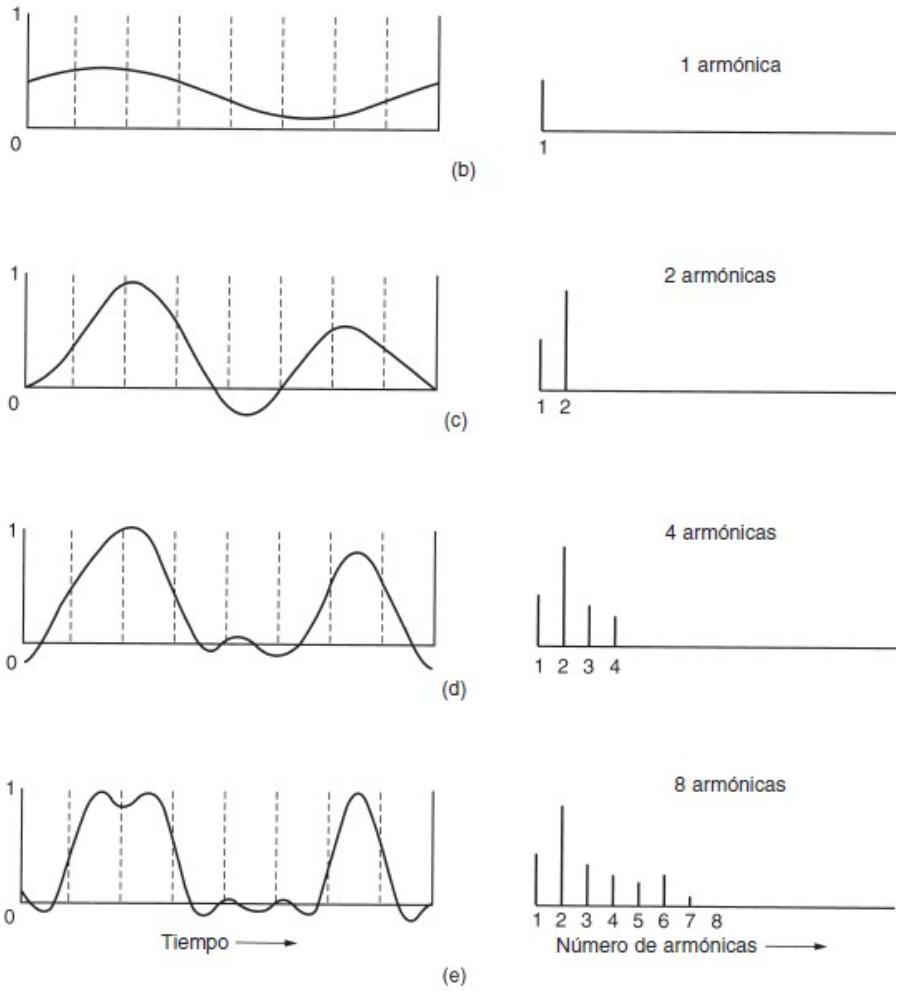
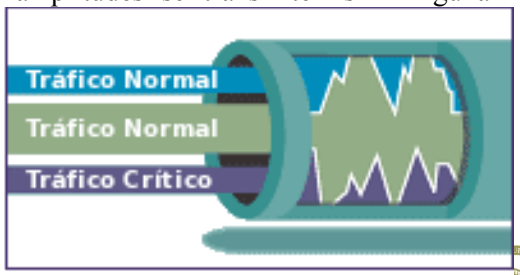
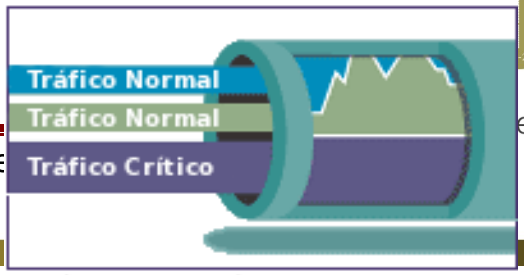


Figura 2-1. (a) Una señal binaria y sus amplitudes de raíz cuadrada media de Fourier. (b)-(e) Aproximaciones sucesivas a la señal original.

Todas las instalaciones de transmisión disminuyen los distintos componentes de Fourier en diferente grado, lo que provoca distorsión. Por lo general, las amplitudes se transmiten sin ninguna disminución desde 0 hasta cierta frecuencia f_c [medida en ciclos/seg o Hertz (Hz)], y todas las frecuencias que se encuentren por arriba de esta frecuencia de corte serán atenuadas. El rango de frecuencias que se transmiten sin atenuarse con fuerza se conoce como **ancho de banda.** En la práctica, el corte en realidad no es abrupto, por lo que con frecuencia el ancho de banda ofrecido va desde 0 hasta la frecuencia en la que el valor de la amplitud es atenuado a la mitad de su valor original.



Tráfico sin gestión de ancho de banda



Tráfico con gestión de ancho de banda

El ancho de banda es una propiedad física del medio de transmisión y por lo general depende de la construcción, grosor y longitud de dicho medio. En algunos casos, se introduce un filtro en el circuito para limitar la cantidad de ancho de banda disponible para cada cliente. Por ejemplo, un cable de teléfono podría tener un ancho de banda de 1 MHz para distancias cortas, pero las compañías telefónicas agregan un filtro que restringe a cada cliente a aproximadamente 3100 Hz. Este ancho de banda es adecuado para el lenguaje inteligible y mejora la eficiencia del sistema al limitar a los usuarios en el uso de los recursos.

Ahora consideremos cómo luciría la señal de la figura 2.1 si el ancho de banda fuera tan lento que sólo las frecuencias más bajas se transmitieran.
La señal que resulta de un canal que permite que sólo pase la primera armónica (la fundamental, f). De manera similar, se muestra el espectro y las funciones reconstruidas de canales de ancho de banda más grande.

Dada una tasa de bits de b bits/seg, el tiempo requerido para enviar 8 bits (por ejemplo) 1 bit a la vez es $8/b$ seg, por lo que la frecuencia de la primera armónica es $b/8$ Hz. Una línea telefónica normal, llamada con frecuencia **línea con calidad de voz,** tiene una frecuencia de corte introducida de manera artificial arriba de 3000 Hz. Esta restricción significa que el número de armónicas más altas que pasan es de aproximadamente $3000/(b/8)$ o $24{,}000/b$ (el corte no es abrupto).

Para algunas tasas de datos, los números resultan como se muestra en la figura 2-2. A partir de estos números, queda claro que tratar de transmitir a 9600 bps por una línea telefónica transformará la figura 2-1(a) en algo similar a lo que se muestra en la figura 2-1(c), lo que dificulta la recepción precisa del flujo de bits binarios original. Debería ser obvio que a tasas de datos mucho mayores que 38.4 kbps, no hay la menor esperanza para las señales *binarias*, aun si la transmisión se encuentra completamente libre de ruidos. En otras palabras, limitar el ancho de banda limita la tasa de datos, incluso en canales perfectos. Sin embargo, existen esquemas de codificación refinados que utilizan diferentes niveles de voltaje y pueden alcanzar tasas de datos mayores.

Bps	T (mseg)	Primera armónica (Hz)	# de armónicas enviadas
300	26.67	37.5	80
600	13.33	75	40
1200	6.67	150	20
2400	3.33	300	10
4800	1.67	600	5
9600	0.83	1200	2
19200	0.42	2400	1
38400	0.21	4800	0

Figura 2-2. Relación entre tasa de datos y armónicas.

La tasa de datos máxima de un canal

En 1924, un ingeniero de AT&T, Henry Nyquist, se dio cuenta de que incluso un canal perfecto tiene una capacidad de transmisión finita. Derivó una ecuación que expresa la tasa de datos máxima para un canal sin ruido de ancho de banda finito. En 1948, Claude Shannon continuó el trabajo de

Nyquist y lo extendió al caso de un canal sujeto a ruido aleatorio (es decir, termodinámico) (Shannon, 1948). Nyquist probó que si se pasa una señal cualquiera a través de un filtro pasa-bajas de ancho de banda H, la señal filtrada se puede reconstruir por completo tomando sólo $2H$ muestras (exactas) por segundo. No tiene sentido muestrear la línea a una rapidez mayor que $2H$ veces por segundo porque los componentes de mayor frecuencia que tal muestreo puede recuperar ya se han filtrado.

Si la señal consiste en V niveles discretos, el teorema de Nyquist establece:

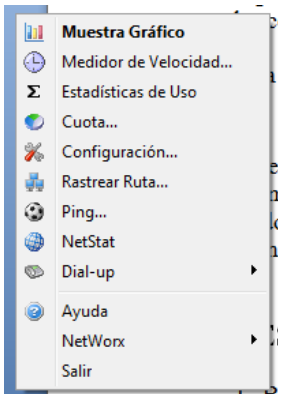
$$\text{tasa de datos máxima} = 2H \log_2 V \text{ bits/seg}$$

Si el ruido aleatorio está presente, la situación se deteriora rápidamente. Y el ruido aleatorio (térmico) siempre está presente debido al movimiento de las moléculas del sistema. La cantidad de ruido térmico presente se mide por la relación entre la potencia de la señal y la potencia del ruido, llamada **relación señal a ruido.**

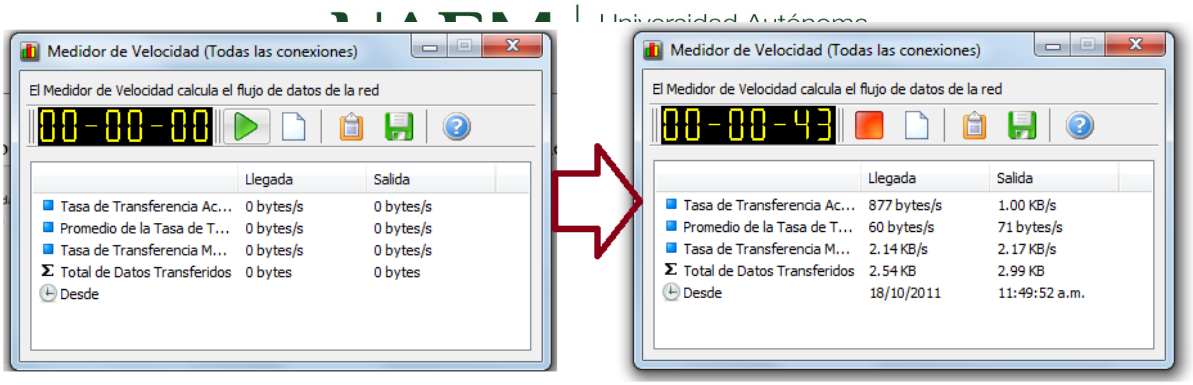
DESARROLLO

1. Busca y descarga **Networx** es una utilidad que ayuda a controlar y monitorizar el ancho de banda de la conexión, con el fin de identificar de manera oportuna, y muy sencilla, potenciales problemas, además llevar un control respecto de cuantos MB o GB llevas descargados en total.

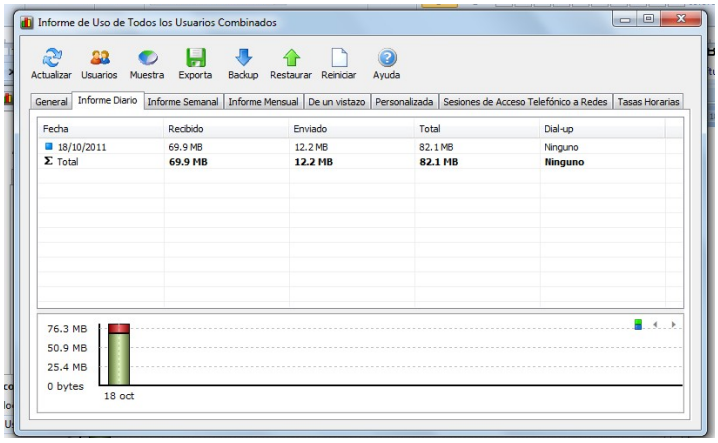
2. Trabajaremos con las aplicaciones de esta útil herramienta, entre las cuales se encuentran:



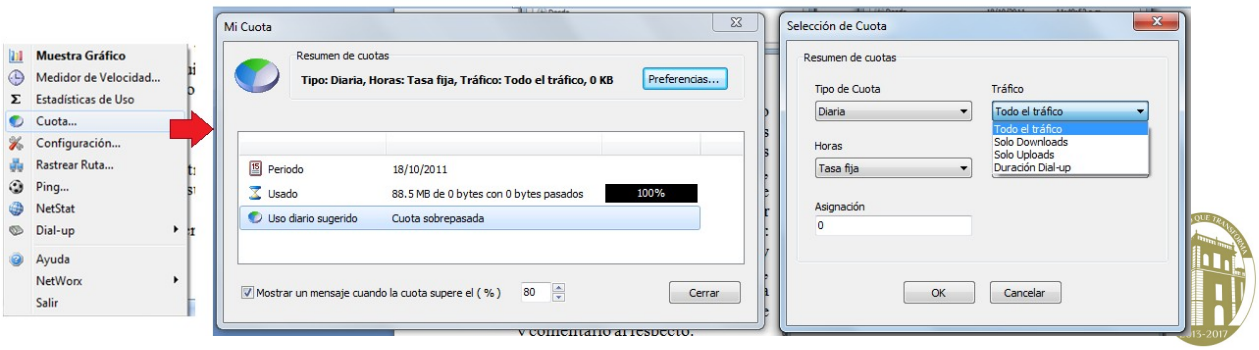
3. Desde que inicies la práctica utiliza el Medidor de velocidad el cual estará activo hasta que finalices, esta herramienta nos permitirá identificar de posibles problemas en el ancho de banda, el cual esta relacionado con el tipo de cable y la topología. Una vez que concluyas guarda el archivo resultante en un .txt para su análisis.

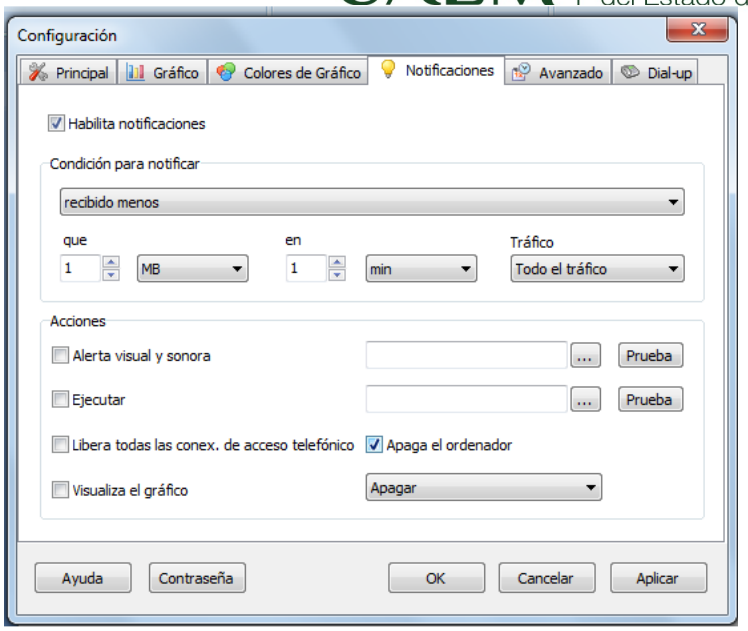


4. Ejecuta el Informe de uso diario en 3 equipos que escojas, toma los datos de inicio de cada uno de estos equipos, revísalos periódicamente, ya que entregaras un reporte de este en tres semanas y debes tener evidencia de lo elaborado, es decir: evidencia de inicio, a la semana y un día antes de entregar tu reporte, en total 3 evidencias por cada equipo, y deberás analizar el reporte y comentarlo al respecto.



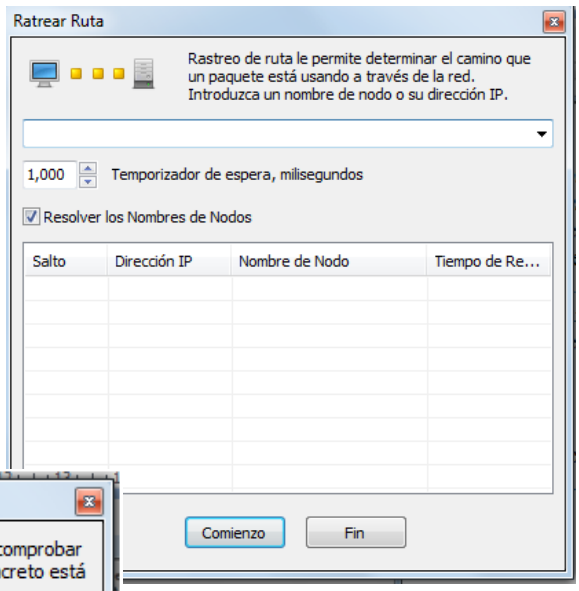
5. Para complementar el paso 4 deberás ejecutar *cuota* e implementar medidas que controlen el consumo de ancho de banda, en los tres equipos deberás al menos implementar una restricción y mostrar la evidencia de lo implantado y del mismo modo analizar que ocurre al final de tu monitoreo cuando apliques dicha restricción . Es importante tener evidencia de todo lo aplicado y contar con el registro correspondiente.

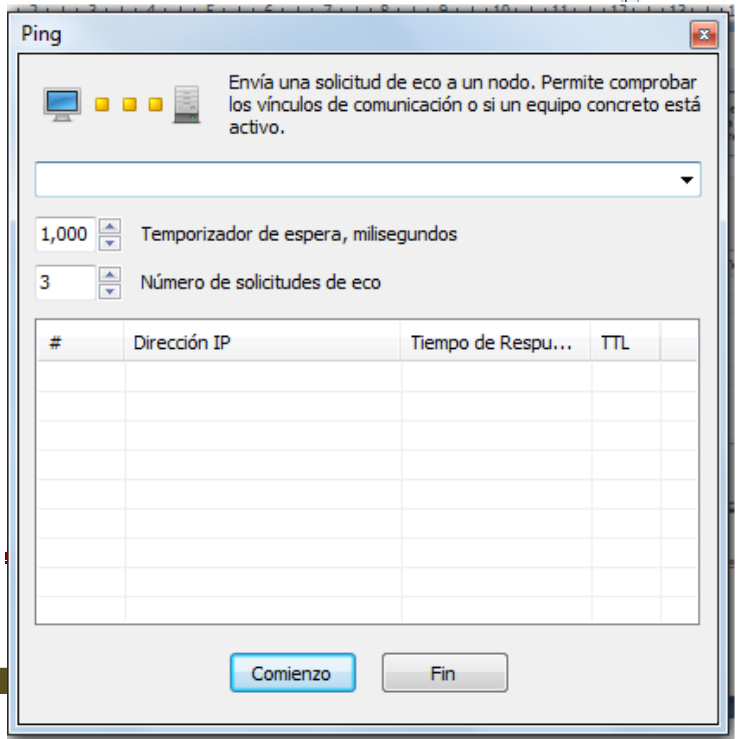




6. Al utilizar *configuración* →*notificaciones*; habilita las notificaciones e implementa alguna de ellas en cada uno de los equipos a tu cargo, se cuidadoso y mantén el registro de lo que realizas en cada estación de trabajo.

7. obtén la dirección IP de las tres maquinas a tu cargo; ejecuta *rastrea ruta* y envía esa IP entre las maquinas, obtén el nombre del nodo por donde pasa y el tiempo, de este construye un GRAFO que represente este enrutamiento.

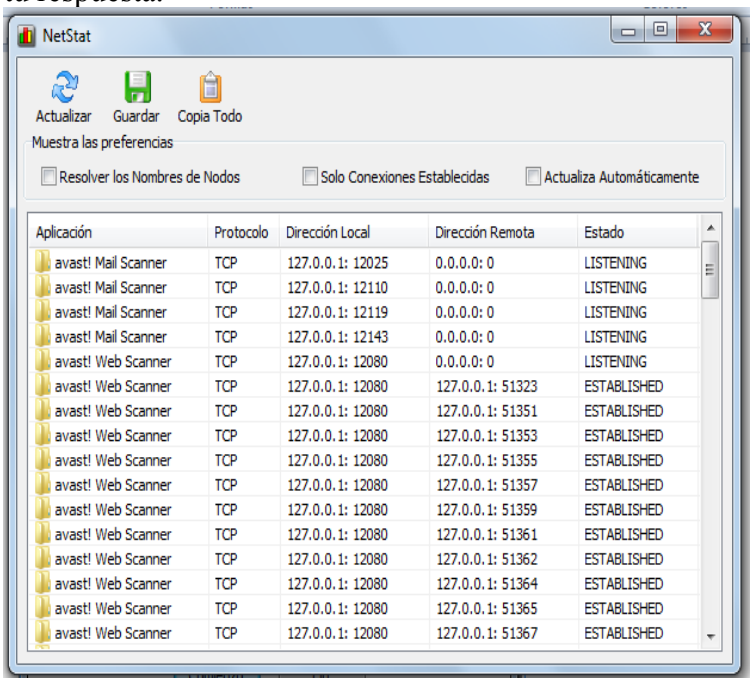




8. Comprueba el estado de la conexión del host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes ICMP de solicitud y de respuesta. Mediante esta utilidad puede diagnosticarse el

estado, velocidad y calidad de una red determinada. El PING se utiliza para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos. Envía tres PING a tres equipos diferentes y analiza los resultados obtenidos. Modifica el tiempo de espera y el numero de *ecos*. Analiza lo obtenido y muestra evidencia de lo realizado.

9. Muestra un listado de las conexiones activas del equipo, tanto entrantes como salientes, mediante NETSTAT; que tipo de protocolos intervienen y a que capa pertenecen, justifica tu respuesta.



Aplicación	Protocolo	Dirección Local	Dirección Remota	Estado
avast! Mail Scanner	TCP	127.0.0.1: 12025	0.0.0.0: 0	LISTENING
avast! Mail Scanner	TCP	127.0.0.1: 12110	0.0.0.0: 0	LISTENING
avast! Mail Scanner	TCP	127.0.0.1: 12119	0.0.0.0: 0	LISTENING
avast! Mail Scanner	TCP	127.0.0.1: 12143	0.0.0.0: 0	LISTENING
avast! Web Scanner	TCP	127.0.0.1: 12080	0.0.0.0: 0	LISTENING
avast! Web Scanner	TCP	127.0.0.1: 12080	127.0.0.1: 51323	ESTABLISHED
avast! Web Scanner	TCP	127.0.0.1: 12080	127.0.0.1: 51351	ESTABLISHED
avast! Web Scanner	TCP	127.0.0.1: 12080	127.0.0.1: 51353	ESTABLISHED
avast! Web Scanner	TCP	127.0.0.1: 12080	127.0.0.1: 51355	ESTABLISHED
avast! Web Scanner	TCP	127.0.0.1: 12080	127.0.0.1: 51357	ESTABLISHED
avast! Web Scanner	TCP	127.0.0.1: 12080	127.0.0.1: 51359	ESTABLISHED
avast! Web Scanner	TCP	127.0.0.1: 12080	127.0.0.1: 51361	ESTABLISHED
avast! Web Scanner	TCP	127.0.0.1: 12080	127.0.0.1: 51362	ESTABLISHED
avast! Web Scanner	TCP	127.0.0.1: 12080	127.0.0.1: 51364	ESTABLISHED
avast! Web Scanner	TCP	127.0.0.1: 12080	127.0.0.1: 51365	ESTABLISHED
avast! Web Scanner	TCP	127.0.0.1: 12080	127.0.0.1: 51367	ESTABLISHED

Responde lo siguiente

1. Que es el ancho de banda?
2. Que relación establece el ancho de banda y el medio físico?
3. Que relación hay entre procesos y ancho de banda?
4. Como se puede controlar los procesos, mejorando asi el consumo del ancho de banda?
5. Explica por lo menos 3 aplicaciones que utilizaste y que beneficios puede tener para el administrador de redes.

Conclusiones.

Que aprendizaje obtuvo al realizar esta práctica y que dudas le quedaron para una posterior discusión?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Bibliografía

CISCO Networking Academia. Primer año
Comunicaciones y Redes de Computadores; Stallings, William 7ª Ed. Prentice Hall, 2000. ISBN 978-84-205-4110-5
Feit, Sidnie.: TCP/IP. Arquitectura, protocolos e implementación, 2ª Ed. Mc-Graw Hill. 1998. ISBN 84-481-1531-7
Held, G.: The Complete Modem Reference, 3ª Ed. John Wiley & Sons, Inc., 1997.
Heywood, Drew: Redes con Microsoft TCP/IP. Edición Especial, 3ª Ed. Prentice Hall, 1999. ISBN 84-8322-108.

PRÁCTICA 5

MEDIOS DE TRANSMISIÓN: CABLEADO UTP

Objetivos

El alumno:

1. Fabricara un cable Ethernet de conexión directa según los estándares T568-B ó T568-A, para conexión desde una estación de trabajo a un hub/switch o de un panel de conexión a un hub/switch, y fabricar también cables cruzados para conectar dos estaciones de trabajo o dos hubs/switches de forma directa, y de consola, para conectar una estación de trabajo a un switch o router para tareas de configuración.
2. Usara la función de Prueba del analizador para detectar circuitos abiertos y cortocircuitos en el cable UTP.
3. Comprenderá el uso de la función de identificación de cable.

Introducción

Hasta hace poco había una mezcla confusa de normalizaciones que regían los medios de red. Existen distintas organizaciones que desarrollan estándares de red, entre ellas la TIA/EIA (Telecommunications Industry Association/Electronic Industries Association) que tiene el mayor impacto en las normas relacionadas con los medios de red. Los estándares TIA/EIA (Figura 5.1) especifican los requisitos mínimos para entornos de múltiples productos y de múltiples fabricantes. Permiten la planificación y la instalación de sistemas LAN sin dictar el uso de equipos específicos, de modo que dan a los diseñadores de LANs la libertad de crear opciones de mejora y expansión.

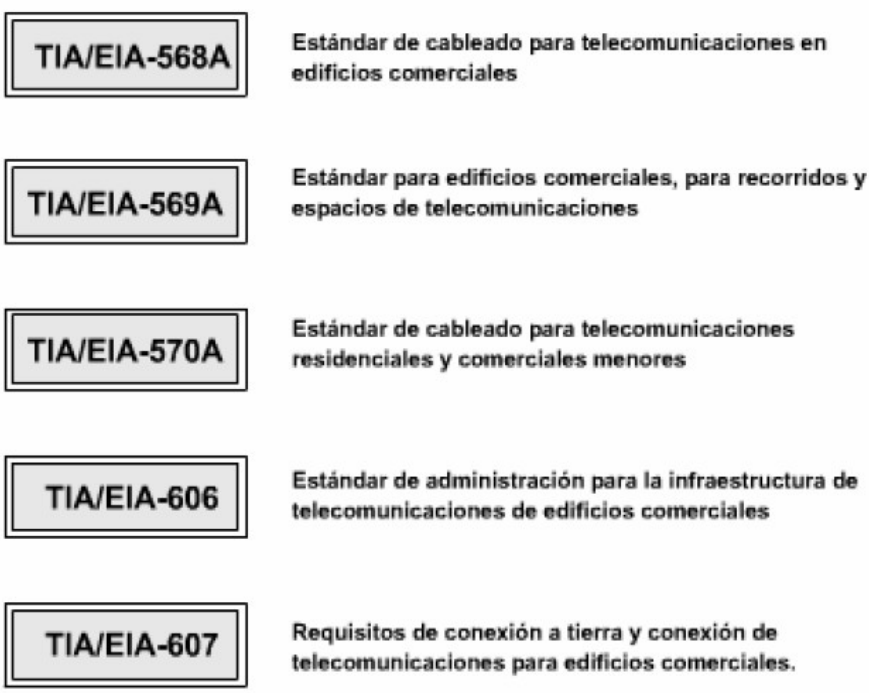


Figura 5.1 Estándares para cableado.

El estándar TIA/EIA- 568A describe el cableado horizontal, es decir, el cableado que se extiende desde el armario para el cableado hasta la estación de trabajo.

Los medios de red reconocidos son STP (Par Trenzado Blindado), UTP (Par Trenzado no Blindado), cable coaxial y fibra óptica. En UTP se distinguen 5 categorías, en función de la calidad del cable. Las categorías 1 y 2 no se aceptan para LAN y las categorías 3, 4 y 5 sí se aceptan. En Ethernet 10BASET se suelen utilizar dos pares UTP CAT 3/4/5. El estándar especifica el tipo de cable, la longitud máxima y el modo de conectar los cables en los conectores RJ- 45 y en los jacks. Según los dispositivos a conectar hay tres tipos de cables: recto, cruzado y consola.

En esta práctica de laboratorio se aprenderá a fabricar un cable de conexión de red Ethernet de par trenzado no blindado (UTP) Categoría 5 (CAT 5) y probarlo para verificar la calidad de las conexiones (continuidad) y salidas de pin correctas (color correcto de los hilos en el pin correcto). El cable será de 4 pares (8 hilos) de conexión directa, lo que significa que el color del hilo en el pin 1 en un extremo del cable será el mismo que el del pin 1 en el otro extremo. El pin 2 será el mismo que el pin 2 y así sucesivamente.

Este cable de conexión se puede usar en un área de estación de trabajo para conectar la NIC de la estación de trabajo al jack de datos de la placa de pared o bien se pueden usar en el centro de cableado para conectar el panel de conexión (conexión cruzada horizontal) a un hub o switch Ethernet. Los cables de conexión se encuentran alambrados como cables de conexión directa, ya que el cable desde la estación de trabajo hasta el hub o switch se cruza normalmente de forma automática en el switch o hub. Se debe observar que los puertos en la mayoría de los hubs tienen una X al lado.

Esto significa que los pares de emisión y recepción se cruzarán cuando el cableado llegue al switch. A fin de verificar las pruebas de la calidad de los cables se usan dos tipos de instrumentos de medida: el **polímetro** y un **analizador de cables**. El polímetro digital es un dispositivo versátil de prueba y de diagnóstico de fallos. Relacionada denominada continuidad. La resistencia se mide en ohms (Ω). Los cables de cobre como, por ejemplo, los que se utilizan comúnmente en el cableado de red (UTP y cable coaxial) por lo general tienen una resistencia muy baja o "buena" continuidad (el cable es continuo), si se los verifica de extremo a extremo. Si hay una interrupción en el cable, se le denomina "abierto", lo que crea una resistencia muy alta (el aire tiene una resistencia prácticamente infinita que se indica mediante el símbolo de infinito). El polímetro tiene una batería que utiliza para verificar la resistencia de un conductor (cable) o aisladores (revestimiento del cable). Cuando se aplican las sondas en los extremos de un conductor, la corriente de la batería fluye y el medidor mide la resistencia detectada.

En esta práctica de laboratorio, se verificarán los cables comunes de networking para poder familiarizarse con ellos y sus características de resistencia. En primer lugar, se debe aprender a usar la configuración de resistencia del polímetro, es decir se debe tener en cuenta la característica de continuidad.

Las pruebas de cables básicas pueden resultar de gran ayuda en el diagnóstico de problemas de cableado para el cable UTP y coaxial. Se aprenderá a usar un analizador de cables para

verificar la calidad de una instalación con cable de par trenzado no blindado (UTP) para una red Ethernet. Probarás diferentes cables para determinar algunos problemas emergentes de la instalación y terminación incorrectas de los cables.

Se supone que la infraestructura de cableado (o planta de cables) de un edificio debe durar por lo menos 10 años. Los problemas de cableado son una de las causas más comunes de fallos de las redes. La calidad de los componentes de cableado utilizados, el enrutamiento e instalación del cable y la calidad de las terminaciones de los conectores serán los factores principales en la determinación de la calidad del cableado.

Herramientas / Preparación:

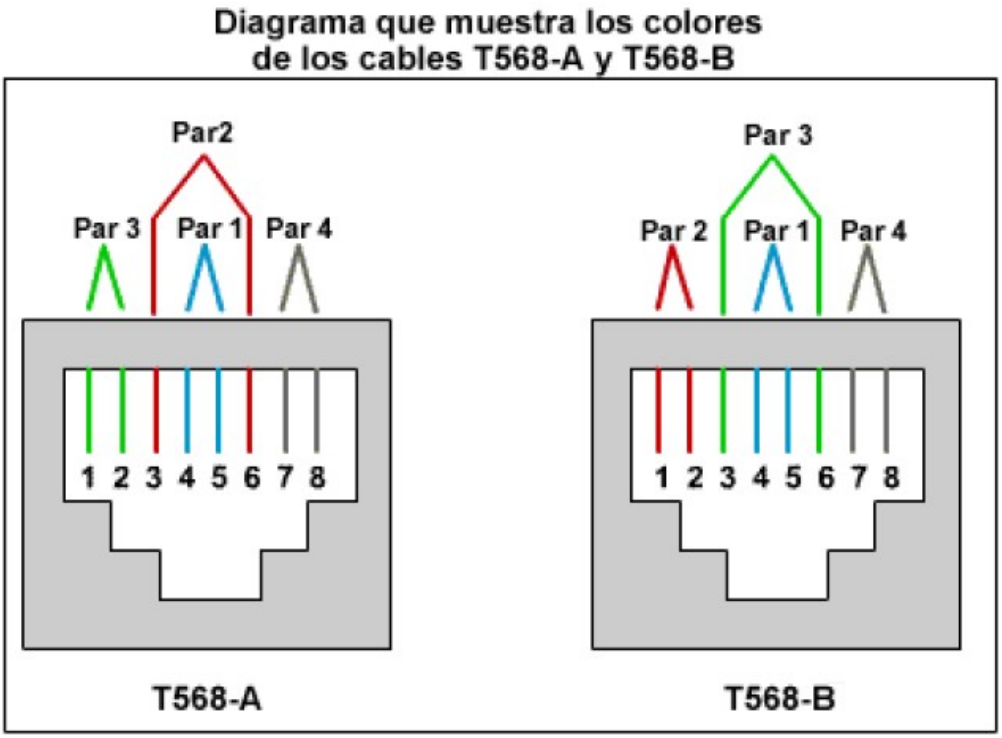
Antes de empezar la práctica de laboratorio es necesario que el alumno cuente con el cable de par trenzado no blindado (UTP) Cat 5, conectores RJ45 (de 8 pins) y una tenaza engarzadora RJ-45. También se deben suministrar varios cables CAT 5 con problemas para probar. Los cables deben estar numerados, para simplificar el proceso de prueba y mantener la coherencia. Se debe proporcionar un analizador de cables que pueda realizar por lo menos pruebas básicas para cables UTP. Se trabaja de forma individual. Para ello, se necesitarán los siguientes recursos:

1. Cable CAT 5 de entre 40 y 90 cm de longitud (uno por persona o por equipo)
2. Cuatro conectores RJ-45
3. Tenazas engarzadoras RJ-45 para colocar los conectores RJ-45 en los extremos del cable
4. Pinzas para cortar hilos.

Paso 1 - Información de cableado.

En esta sección se proporcionan instrucciones para fabricar un cable T568-A o T568-B.

Cualquiera de estos cables se pueden usar siempre y cuando todas las conexiones desde la estación de trabajo hasta el centro de cableado y los dispositivos electrónicos de terminación (hubs o switches) sean coherentes. Si se fabrican cables para una red existente, es importante mantener el mismo estándar ya existente. Un cable de conexión armado en forma de conexión directa debe tener el mismo color de hilo en el mismo pin (1 - 8) en ambos extremos. Un cable de conexión directa se puede usar para conectar un PC a una placa de pared en un área de trabajo o se puede usar para conectar un panel de conexión en un centro de cableado con un hub o switch. También se puede utilizar este cable para conectar directamente un PC a un puerto de un hub o switch.



Cableado T568-B

Nro. de pin	Nro. de par	Función	Color de hilo	¿Se usa con Ethernet 10/100 BASE-T?	¿Se usa con Ethernet 100 BASE-T4 y 1000 BASE-T?
1	2	Transmitir	Blanco/Anaranjado	Sí	Sí
2	2	Transmitir	Anaranjado/Blanco	Sí	Sí
3	3	Recibir	Blanco/Verde	Sí	Sí
4	1	No se utiliza	Azul/Blanco	No	Sí
5	1	No se utiliza	Blanco/Azul	No	Sí
6	3	Recibir	Verde/Blanco	Sí	Sí
7	4	No se utiliza	Blanco/Marrón	No	Sí
8	4	No se utiliza	Marrón /Blanco	No	Sí

Paso 2 - Fabricar un cable de panel de conexión directa (straight-through) T568-B.

a) Material necesario

CABLE PAR TRENZADO 	Se necesitará un rollo de cable de par trenzado no apantallado UTP de categoría 5 [8 hilos] para ir cortando trozos e ir realizando cables de los tres tipos posibles: de consola, directo y cruzado.
CRIMPADORA 	Se usará una crimpadora para realizar las siguientes acciones: a) Cortar trozos de cable b) Quitar revestimiento del cable en los extremos para dejar los pares de hilos al descubierto c) Engarzar el cable a los conectores a través de los hilos [crimpar]
CONECTORES RJ45 	Harán falta varios conectores RJ45 de 8 pines para poder crear los extremos de los cables directo, cruzado y de consola.

b) Proceso de creación de un cable

Ambos extremos del cable deben estar armados de la misma manera cuando se observan los conductores. En Ethernet 10BASE-T o 100BASE-TX sólo se usan cuatro hilos:


Trozo de Cable

1. **Cortar un trozo de cable de par trenzado no blindado Cat 5 de una longitud establecida**: se usará el cable trenzado para cables de conexión ya que tiene una duración más prolongada cuando se dobla repetidas veces. El alambre sólido es perfecto para tendidos de cable que se colocan a presión en los jacks.

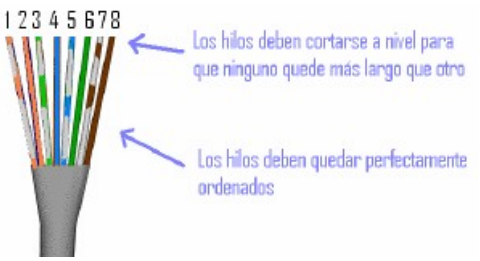

Cable pelado: los 8 hilos quedan al descubierto

2. Retirar 4 ó 5 cm de la envoltura de uno de los extremos del cable: hay que pelar el cable para que en el extremo los hilos queden al descubierto para poder manejarlos e introducirlos en el conector RJ45.

3. **Separar los pares de hilos**: en este punto hay que tratar de separar los pares de hilos pero manteniendo las trenzas todas lo que sea posible, ya que esto es lo que proporciona la anulación del ruido, (par anaranjado, par verde, par azul, par marrón). El estándar de colocación de los hilos se especifica en el **Anexo A.**

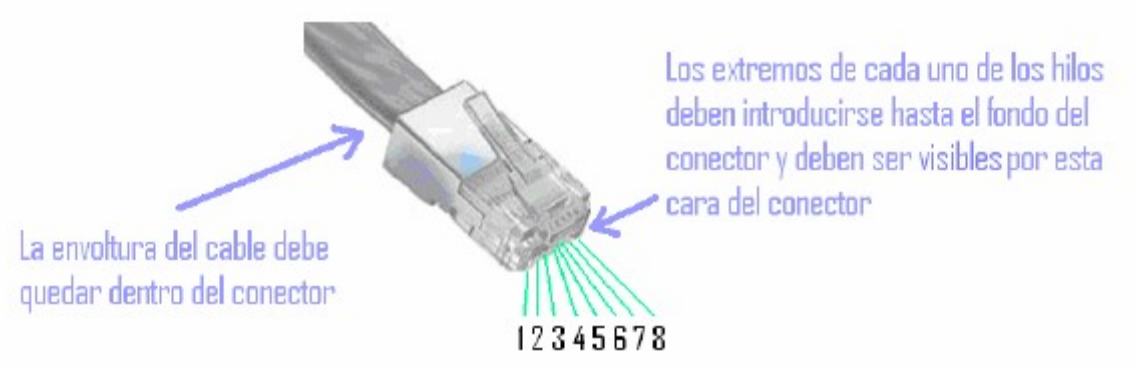
4. **Destrenzar los hilos para cumplir con el estándar**: Sostener la envoltura y el cable con una mano, destrenza un pequeño tramo de los pares verde y azul y reorganízalos de modo que cumplan con el diagrama de color. Destrenzar y ordenar el resto de los pares de hilos según el diagrama de color.

5. **Aplanar, enderezar y alinear los hilos, y recortarlos en línea recta a alrededor de 1,20 cm - 1,90 cm del borde de la envoltura**: Hay que asegurarse de no soltar la envoltura y los hilos que ahora están ordenados, y se debe reducir al mínimo la longitud de los cables no trenzados ya que las secciones excesivamente largas ubicadas cerca de los conectores constituyen una fuente importante de ruido eléctrico. *Al final de este paso, los hilos tienen que estar organizados y cortados a nivel, para que no queden hilos más largos que otro, lo que provocaría un mal engarzamiento en el conector ya que los hilos más cortos no harían contacto.*



6. **Colocar un conector RJ-45 en el extremo del cable:** con la lengüeta hacia abajo y el par anaranjado en la parte izquierda del conector, *siguiendo el esquema del anexo A.*

7. **Empujar suavemente los hilos dentro del conector hasta que se puedan ver los extremos de cobre de los hilos a través del extremo del conector**: Hay que asegurarse de que el extremo de la envoltura esté ubicado dentro del conector y de que todos los hilos estén en el orden correcto y que lleguen hasta el fondo de los carriles del conector para que al crimpar hagan contacto. Si la envoltura no está ubicada dentro del conector, no estará correctamente protegida contra los tirones y con el tiempo esto causará problemas. Si todo está en orden, engarza el conector con la suficiente fuerza como para forzar los contactos a través del aislamiento en los hilos, completando así el camino conductor.



8. **Crimpar o engarzar los hilos:** Se introduce el conector con el cable en la crimpadora, en la zona habilitada para crimpar o engarzar los hilos al conector, que como se puede observar es una especie de molde donde encaja el conector RJ45. Se aprietan las manillas de la crimpadora hasta oir un pequeño clic, y en ese momento harán contacto las patillas del conector con los hilos, quedando fijo el cable al conector.

9. **Repetir los pasos 2-7 para terminar el otro extremo del cable, usando el mismo diagrama para terminar el cable de conexión directa**.

Efectuar las pruebas de cable básicas -Función Aprobado/No aprobado

Efectúa una prueba de cable básica en cada uno de los cables suministrados y/o que hayas creado, y llena la siguiente tabla según los resultados para cada cable que hayas probado. Para cada cable, apunta el número e indica si el cable es de conexión directa o de interconexión cruzada. Incluye

Cable Nro.	Resultados de la prueba en la pantalla del analizador	Descripción del problema
1		
2		
3		
4		
5		

también los resultados mostrados en pantalla por el analizador y tu idea de cuál puede ser el problema (en caso de que exista).

Anexo A
Cable UTP

Esquema-Secuencia de colores

PATCH CABLE: Straing-Through o Cable directo

Cable de conexión directa: conecta un PC/Panel al Hub/Switch

Ambos conectores (Estandar T568-B):

EXTREMO	1	2	3	4	5	6	7	8
(1) T568B	BlancoNaranja	Naranja	BlancoVerde	Azul	BlancoAzul	Verde	BlancoMarrón	Marrón
(2) T568B	BlancoNaranja	Naranja	BlancoVerde	Azul	BlancoAzul	Verde	BlancoMarrón	Marrón

Prueba visual: Se colocan los conectores uno contra el otro y los colores están totalmente opuestos.

La conexión de pines entre extremos es: [1.1- 2.2 - 3.3 - 4.4 - 5.5 - 6.6 -7.7 -8.8]

ROLLOVER o cable de consola

Cable consola: conecta un PC al Router-Cable Consola.

EXTREMO	1	2	3	4	5	6	7	8
(1) T568B	BlancoNaranja	Naranja	BlancoVerde	Azul	BlancoAzul	Verde	BlancoMarrón	Marrón
(2) T568B	Marrón	BlancoMarrón	Verde	BlancoAzul	Azul	BlancoVerde	Naranja	BlancoNaranja

Prueba visual: Se colocan los conectores uno contra el otro y los colores coinciden totalmente.

La conexión de pines entre extremos es [1.8-2.7-3.6-4.5-5.4-6.3-7.2-8.1]

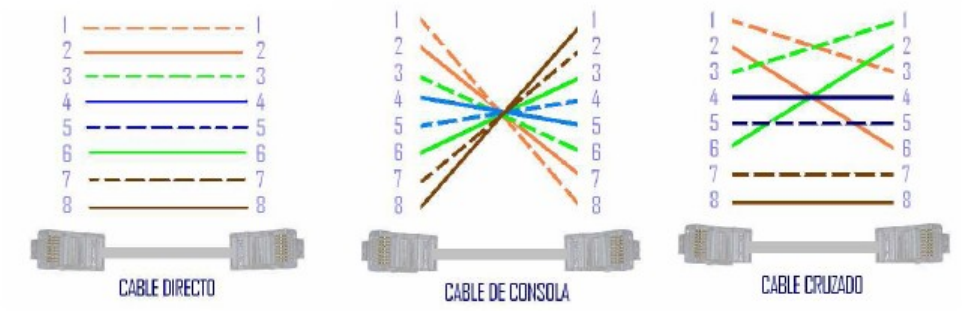
CROSS-OVER o cable cruzado

Cable de conexión cruzada: Conecta nodo a nodo (PC con PC, hub con hub, hub con switch)

Prueba visual: Se colocan los conectores uno al lado del otro y los colores coinciden con los pines correspondientes.

EXTREMO	1	2	3	4	5	6	7	8
(1) T568A	BlancoVerde	Verde	BlancoNaranja	Azul	BlancoAzul	Naranja	BlancoMarrón	Marrón
(2) T568B	BlancoNaranja	Naranja	BlancoVerde	Azul	BlancoAzul	Verde	BlancoMarrón	Marrón

Pines: (1.3-2.6-3.1-4.4-5.5-6.2-7.7-8.8)



Preguntas

¿Cuál es la función de la capa Física?

¿Qué importancia tiene esta capa en el Tx y Rx de datos?

¿Qué diferencia existe entre un cable directo y uno cruzado?

¿Qué estándares intervienen en esta capa?

Elabora una tabla comparativa de tipos de cables: velocidad, costo, utilidad, entre otras características.

Conclusiones.

¿Que aprendizaje obtuvo al realizar esta práctica y que dudas le quedaron para una posterior discusión?

_____
_____
_____
_____
_____
_____
_____

Bibliografía

CISCO Networking Academia. Primer año
Comunicaciones y Redes de Computadores; Stallings, William 7ª Ed. Prentice Hall, 2000. ISBN 978-84-205-4110-5
Feit, Sidnie.: TCP/IP. Arquitectura, protocolos e implementación, 2ª Ed. Mc-Graw Hill. 1998. ISBN 84-481-1531-7
Held, G.: The Complete Modem Reference, 3ª Ed. John Wiley & Sons, Inc., 1997.
Heywood, Drew: Redes con Microsoft TCP/IP. Edición Especial, 3ª Ed. Prentice Hall, 1999. ISBN 84-8322-108.

PRÁCTICA 6

Conexión Punto a Punto

PRÁCTICA 6

Conexión Punto a Punto

Nombre: _____

Fecha de Elaboración:_____ **Firma:**_____

Objetivo

Al término de esta práctica el alumno será capaz de:

- Identificar correctamente los cables que se utilizan en la red.
- Cablear físicamente una red conmutada punto a punto.
- Verificar la conectividad básica en cada red.

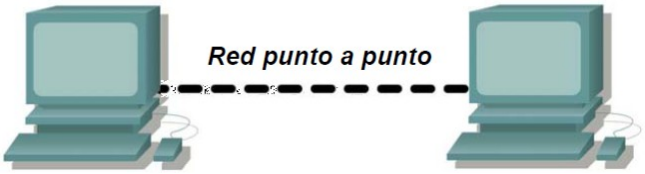
Introducción

Varios de los problemas de red se pueden solucionar en la capa Física de una red. Por esta razón, es importante saber exactamente cuáles son los cables que se utilizan para las conexiones de red. En la capa Física (Capa 1) del modelo OSI, los dispositivos finales se deben conectar por medios (cables). Los tipos de medios requeridos dependen de los tipos de dispositivos que se conecten.

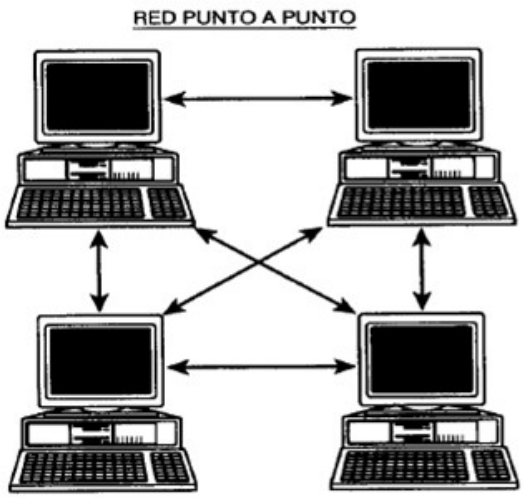
Las computadoras pueden desarrollar dos funciones: como servidores o estaciones de trabajo. Los elementos de conexión son los cables, tarjetas de red y los dispositivos de interconectividad como los hubs. Dentro de los cables de conexión se tienen: el cable UTP, que consiste en dos hilos trenzados en forma independiente y recubiertos de una capa aislante, y que es considerado de fácil instalación; el cable STP, consistente en dos hilos trenzados en forma independiente y recubiertos de una malla metálica que ofrece una protección contra las interferencias externas; el cable coaxial, hilo de cobre envuelto en una malla trenzada, separados por un material aislante; y, finalmente, la fibra óptica, formada por un núcleo de material transparente fino cuyo funcionamiento se basa en la transmisión de las refracciones de luz.

En la actualidad, en el mundo de los sistemas de cableado estructurado existen diferentes tipos de servicios, por ejemplo, voz, datos, video, monitoreo, control de dispositivos, etc.; éstos pueden transmitirse sobre un mismo tipo de cable. El estándar más conocido de cableado estructurado está definido por la EIA/TIA, y específicamente sobre cable de par trenzado UTP de categoría 5, estos estándares son: EIA/TIA 568A y EIA/TIA 568B.

Los dispositivos de interconexión proporcionan la capacidad de extender la distancia de cobertura de una LAN, interconectar redes distantes o distintas y acceder a recursos centralizados; de la misma manera, reducen los dominios de colisión y mejoran el rendimiento de las redes.



Un paquete puede visitar varias computadoras antes de llegar a su destino, con la posibilidad de seguir varias rutas al destino cuyo objetivo es buscar la ruta más cercana y menos congestionada, por lo tanto; son necesarios algoritmos de ruteo (encaminamiento).



Los servidores no dedicados pueden acceder a los recursos compartidos de cualquier otro servidor no dedicado a la red

En una red con Punto a Punto la administración de los recursos es más flexible; la administración de los recursos de red puede estar más distribuida, pues cada computadora 'en la red puede ser servidor y cliente al mismo tiempo, con lo cual, se evita "perder" un cliente

Los sistemas de Punto a Punto permiten que las PC's sean tanto clientes como servidores al mismo tiempo (Esto los hace funcionalmente equivalentes a los sistemas de servidor de archivos.) Los sistemas de Punto a Punto ofrecen controles de acceso similares a los a los de los sistemas Cliente-Servidor y soportan aplicaciones de usuarios múltiples, como productos de base de datos, al igual que los sistemas de servidor de archivos. También es posible compartir impresoras, de manera que la impresora de una PC queda a la disposición de cualquier usuario.

Los sistemas de punto apunto también son más baratos que los sistemas basados en servidor de archivos, pero sus capacidades están más restringidas, no sólo en rendimiento sino también en el número de usuarios que pueden tener acceso simultáneo a una PC con funciones de servidor. Una red de Punto a Punto generalmente no tiene más de 20 PC's, aunque es posible construir redes de más de 300 PC's. (Por supuesto, cada 30 días habrá un nuevo administrador de red).
Si bien las redes de Punto a Punto ofrecen muchos beneficios, su bajo costo redunda en un rendimiento más bajo, disminución del manejo y menor seguridad (son aspectos muy importantes en cualquier red).

En un sistema de Punto a Punto, se corre el riesgo que la gente tenga acceso a datos de cualquier parte de la red. Aun si se construye un sistema de este tipo, es difícil evitar que una persona con conocimientos tenga acceso a la PC de otro usuario cuando no hay nadie cerca. La seguridad en Sistemas Punto a Punto es muy débil; ya que aun cuando se asigne seguridad a los recursos propios, sin embargo por el hecho de estar punto a punto: cualquier persona si lo desea, puede tener acceso.

Desarrollo

En esta práctica de laboratorio se utilizarán cables de conexión directa y cruzada. Además, dos o más dispositivos se comunican a través de una dirección. La capa de Red (Capa 3) requiere una dirección única (que se conoce también como una dirección lógica o Direcciones IP), que permite que los datos alcancen el dispositivo destino correcto. En esta práctica de laboratorio se aplicará el direccionamiento a las estaciones de trabajo y se utilizará para permitir la comunicación entre los dispositivos.

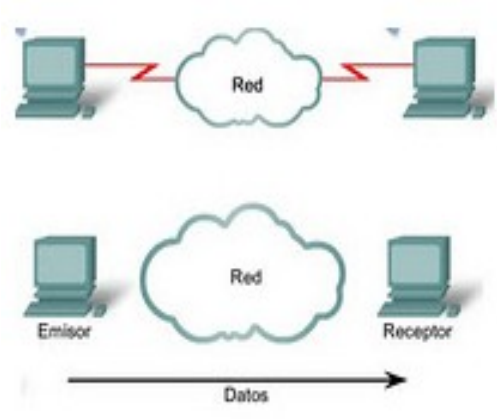
Esta práctica de laboratorio comienza con la conexión de red más simple (punto a punto) y finaliza con la práctica de conexión a través de un switch (con el *Paket Tracer*).

Creación de una red punto a punto

Obtenga el equipo y los recursos para la práctica de laboratorio.
Equipo necesario:
2 estaciones de trabajo
1 cable de conexión directa (patch).
1 cable de conexión cruzada
1 switch (o hub) (con el *Paket Tracer)*

Identificar los cables que se utilizan en una red

Antes de que los dispositivos puedan conectarse, se necesitará identificar los tipos de medios que se utilizarán. Los cables que se utilizarán en esta práctica de laboratorio son de conexión cruzada y de conexión directa.



Utilice un **cable de conexión cruzada** para conectar dos estaciones de trabajo entre sí a través de los puertos Ethernet de su NIC. Éste es un cable Ethernet. Cuando mire el conector notará que los cables naranja y verde están en posiciones opuestas al final de cada cable.

Utilice un **cable de conexión directa** para conectar el puerto Ethernet del router a un puerto del switch o una estación de trabajo a un puerto del switch. Éste, también, es un cable Ethernet. Cuando mire el conector notará que ambos extremos del cable son exactamente iguales en cada posición del pin.

Conectar una red punto a punto.

Conecte dos estaciones de trabajo.

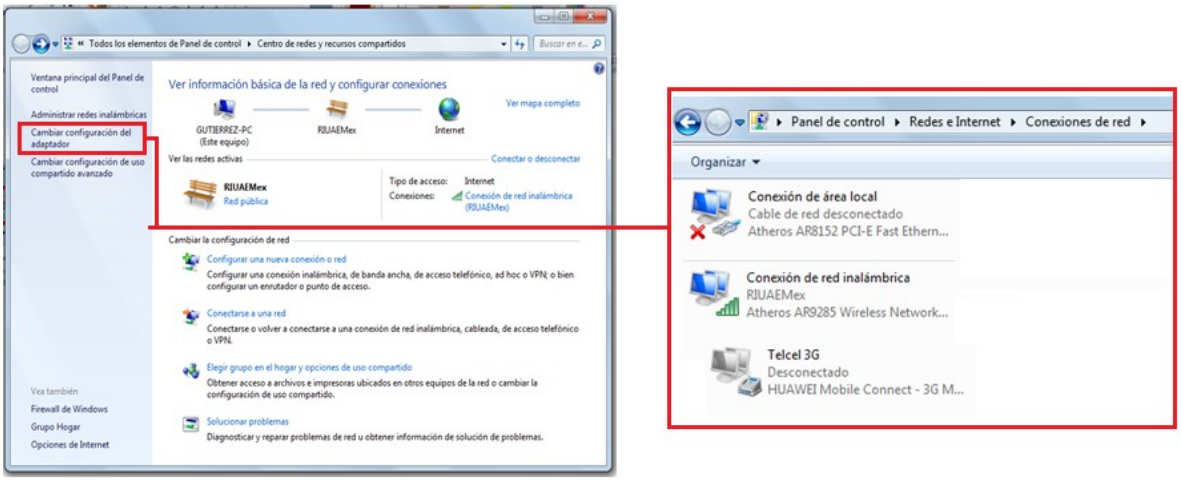
Con el cable Ethernet correcto, conecte dos estaciones de trabajo. Conecte un extremo del cable al puerto de la NIC en la PC1 y el otro extremo del cable a la PC2.
¿Qué cable usó? _____

Aplique una dirección de Capa 3 a las estaciones de trabajo.

Para completar esta tarea, deberá seguir las siguientes instrucciones paso a paso.

Nota: *Estos pasos se deben completar en cada estación de trabajo. Las instrucciones son para Windows XP. Los pasos pueden diferir si se utiliza otro sistema operativo.*

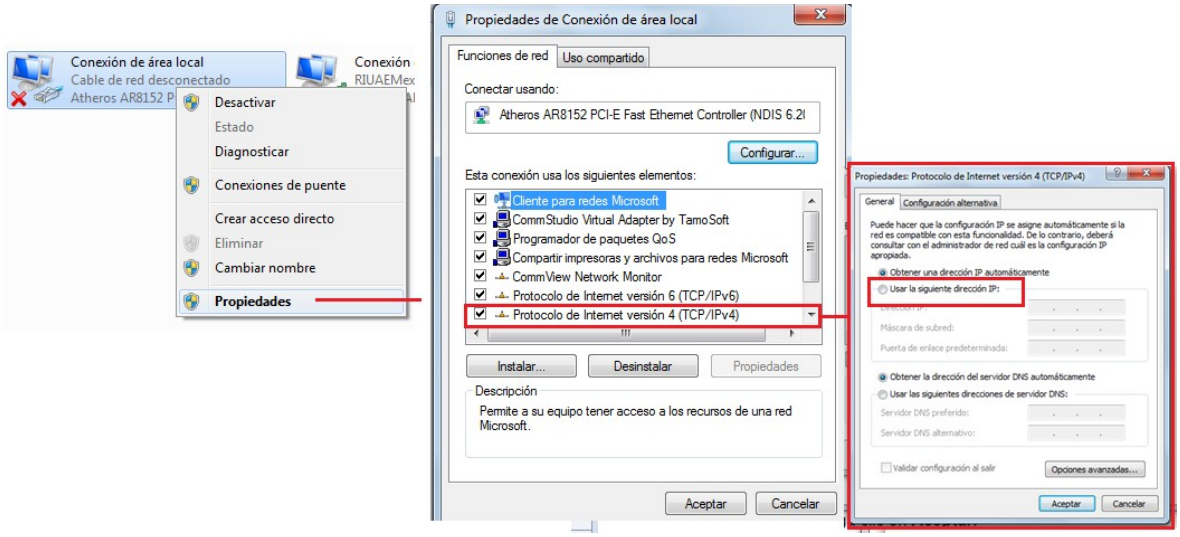
1. En su computadora, haga clic en **Inicio**, haga clic con el botón derecho en **Mis sitios de red** y luego un último clic en **Propiedades.** Debe mostrarse la ventana Conexiones de red, con íconos que muestren las diferentes conexiones de red.



2. Haga clic con el botón derecho en **Conexión de área local** y haga clic en **Propiedades**.
3. Seleccione el **Protocolo de Internet (TCP/IP)** y haga clic en el botón **Propiedades**.
4. En la ficha General de la ventana Propiedades del Protocolo de Internet (TCP/IP), seleccione la opción **Usar la siguiente dirección IP.**
5. En la casilla **Dirección IP**, ingrese la dirección IP 192.168.1.2 para PC1. (Ingrese la dirección IP 192.168.1.3 para PC2.) o bien UBIQUE la IP del equipo en uso, recuerde este es un ejemplo.

6. Presione la tecla de tabulación y la máscara de subred se ingresará automáticamente. La dirección de subred debe ser 255.255.255.0. Si esa dirección no ingresa automáticamente, ingrésela de manera manual.

7. Haga clic en **Aceptar**.

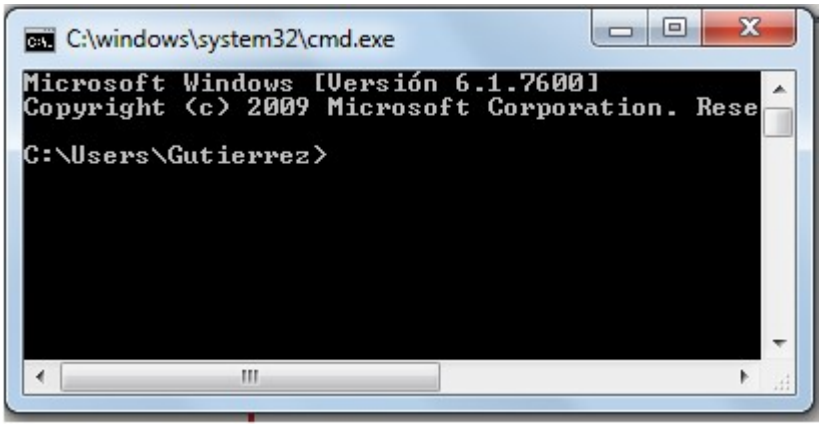


8. Cierre la ventana Propiedades de Conexión de área local.

Paso 3: Verifique la conectividad.

1. En su computadora, haga clic en **Inicio** y después en **Ejecutar.**
2. Escriba **cmd** en la casilla Abrir y haga clic en **Aceptar.**

Se mostrará la ventana de comando DOS (cmd.exe). Se pueden ingresar comandos DOS mediante esta ventana. Para ayudar al propósito de esta práctica de laboratorio, se ingresarán comandos de red básicos para permitirle probar conexiones de computadoras.



El comando **ping** es una herramienta de red de computadoras que se utiliza para probar si un host (estación de trabajo, router, servidor, etc.) es alcanzable a través de una red IP.

3. Utilice el comando **ping** para verificar que PC1 puede alcanzar PC2 y que PC2 puede alcanzar PC1. Desde la petición de entrada de comandos PC1 DOS, escriba **ping 192.168.1.3.** Desde la petición de entrada de comandos PC2 DOS, escriba **ping 192.168.1.2.**

¿Cuál es el resultado del comando **ping**?

_____
_____
_____
_____

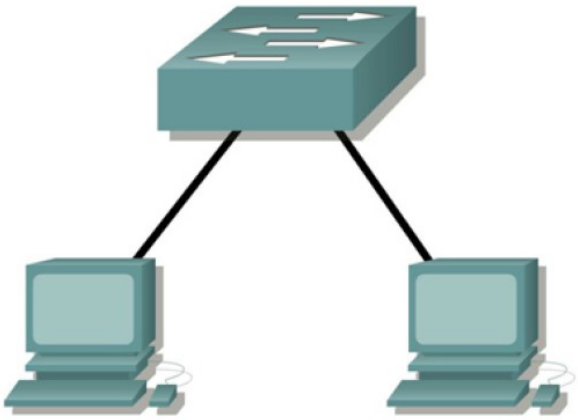
Si el comando **ping** muestra un mensaje de error o no recibe una respuesta de la otra estación de trabajo, realice un diagnóstico de fallas. Las áreas que pueden fallar incluyen:

• Verificación de la dirección IP correcta en ambas estaciones de trabajo
• Comprobación de que se utilizó el tipo de cable correcto entre las estaciones de trabajo

¿Cuál es el resultado del comando **ping** si se desconecta el cable de red y hace ping en la otra estación de trabajo?

_____
_____

Conectar las estaciones de trabajo al switch de laboratorio (Packet Tracer).



Tome el cable correcto y conecte uno de los extremos del mismo al puerto NIC de la estación de trabajo y el otro extremo al puerto del switch.

Repita este proceso con cada estación de trabajo de la red.

¿Qué cable usó?

Verifique la conectividad.

Verifique la conectividad de la red utilizando el comando **ping** para alcanzar las otras estaciones de trabajo conectadas al switch.

¿Cuál es el resultado del comando **ping**?

¿Cuál es el resultado del comando **ping** si se hace ping en una dirección que no está conectada a esta red?

_____
_____
_____

Comparta un documento con otras PC.

1. En el escritorio, cree una carpeta nueva y denomínela **prueba**.
2. Haga clic con el botón derecho en la carpeta y haga clic en Compartir archivos.
3. Ubique un archivo en la carpeta.
4. En el escritorio, haga doble clic en **Mis sitios de red** y luego en **Computadoras cercanas**.
5. Haga doble clic en el ícono estación de trabajo. Debe mostrarse la carpeta **prueba.** Podrá tener acceso a esta carpeta a través de la red. Una vez que pueda verla y trabajar con el archivo, tendrá acceso a través de las 7 capas del modelo OSI.

¿Qué podría evitar que un ping se envié entre las estaciones de trabajo cuando éstas están directamente conectadas?

_____
_____
_____
_____

¿Qué podría evitar que un ping se envié a las estaciones de trabajo cuando éstas están conectadas a través del switch?

_____
_____
_____
_____

Conclusiones.

¿Qué aprendizaje obtuvo al realizar esta práctica y que dudas le quedaron para una posterior discusión?

_____
_____
_____
_____
_____
_____
_____

Bibliografía

CISCO Networking Academia. Primer año
Comunicaciones y Redes de Computadores; Stallings, William 7ª Ed. Prentice Hall, 2000. ISBN 978-84-205-4110-5
Feit, Sidnie.: TCP/IP. Arquitectura, protocolos e implementación, 2ª Ed. Mc-Graw Hill. 1998. ISBN 84-481-1531-7
Held, G.: The Complete Modem Reference, 3ª Ed. John Wiley & Sons, Inc., 1997.
Heywood, Drew: Redes con Microsoft TCP/IP. Edición Especial, 3ª Ed. Prentice Hall, 1999. ISBN 84-8322-108.

PRÁCTICAS 7 y 8

Montaje de Redes y Arquitectura de Capas

Objetivo

Al término de la práctica el alumno será capaz de:

1. Realizar diferentes diseños de una Red de Área Local (LAN).
2. Conocer el funcionamiento básico de una LAN.
3. Identificar la utilización específica de cada equipo de interconexión empleado en el montaje.
4. Familiarizarse con la arquitectura en capas del modelo TCP/IP mediante las utilidades de simulación que proporciona el programa *Packet Tracer*.

Introducción

Equipos de interconexión y equipos a interconectar
Antes de realizar y estudiar ningún diseño de red LAN, necesitamos conocer qué tipo de equipos pueden integrar este tipo de redes:

· Equipos de interconexión: hub, switch, router
· Equipos a interconectar: PCs, impresoras, servidores…
Esto quiere decir que el objetivo de montar una red LAN (en una habitación, en un edificio…) suele ser tener conectados entre sí una serie de equipos: PCs, impresoras, servidores… y, para gestionar estas conexiones necesitamos lo que llamamos equipos de interconexión.

Equipos de interconexión

- **Hub**: es un repetidor multipuerto. Cualquier información recibida por uno de sus puertos la "repetirá" hacia el resto de puertos. De esta manera, si varios equipos conectados a un mismo hub intentan transmitir paquetes simultáneamente, se producirá una colisión de estos paquetes en el hub y no llegarán correctamente a su destino. El hub es, por tanto, un dispositivo muy sencillo que sólo trabaja a **nivel físico**.

- **Switch**: es un hub con "cierta inteligencia". La información que le llega por un puerto sólo la "repetirá" hacia el puerto donde sabe que tiene conectado el equipo al que va dirigida la información. Para ello, necesita tener información de la **dirección MAC** de los equipos que tiene conectados en cada uno de sus puertos. Una dirección MAC identifica unívocamente la tarjeta de red de un equipo (**nivel de enlace**) y viene impuesta por el fabricante, no se puede cambiar. Por tanto, el switch nos sirve para interconectar equipos pertenecientes a una misma red sin que sus paquetes colisionen entre sí.

- **Router**: lo necesitamos cuando queremos interconectar equipos pertenecientes a redes diferentes. Cada uno de los equipos de una misma red tienen una **dirección IP** (**nivel de red**) perteneciente al rango de direcciones asignado a esa red, diferente del de otras redes. Por tanto, el router, en función de la dirección IP destino del paquete de información que le llega, es capaz de calcular la mejor ruta que tiene que seguir este paquete hacia su destino y enviarlo hacia la red correspondiente.

Para darle conectividad a un equipo en una red IP, necesitamos definir al menos tres cosas en cada uno de ellos:

- **Dirección IP**: dirección binaria de 32 bits que identifica a un equipo dentro de la red a la que pertenece. Una primera parte de la dirección identifica a la red a la que pertenece el equipo y otra parte al equipo dentro de esa red. Se suele representar mediante la codificación decimal de cada uno de sus 4 bytes separados por puntos: 192.168.100.1

- **Máscara de subred**: es también una dirección binaria de 32 bits que sirve para identificar qué parte de la dirección IP identifica a la red (con 1s) y qué parte identifica al equipo (con 0s): 11111111 11111111 11111111 00000000 = 255.255.255.0

- Con esta máscara sabemos que los primeros 24 bits de la dirección IP identifican a la red y los últimos 8 bits al equipo dentro de la red.

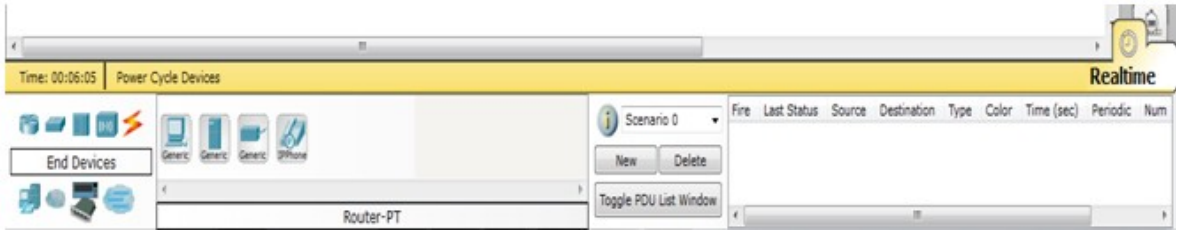
- **Puerta de Enlace** (Gateway): dirección IP del equipo de interconexión (router) a través de la cual podremos salir a otras redes.

Desarrollo

Una vez conocidos los equipos que pueden pertenecer a nuestra Red LAN y sus características, veamos cómo se pueden representar y estudiar su comportamiento en el programa de simulación que vamos a utilizar.

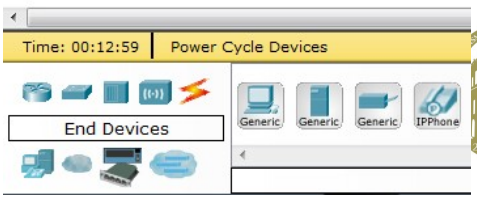
Creación y conexión de equipos en Packet Tracer 5.1

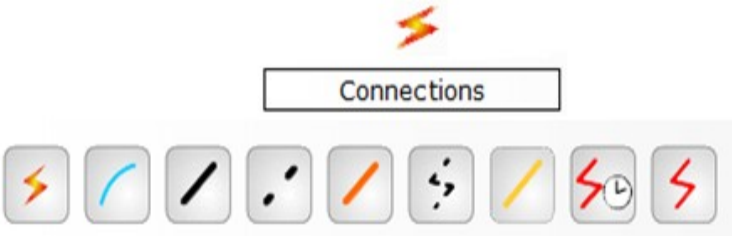
Cuando iniciamos el programa tenemos tres posibles pestañas para seleccionar: “Simulation” y “Realtime”. Si nos quedamos en la primera de ellas, podemos ver todos los posibles equipos que podemos integrar en nuestra red:



Para añadir un nuevo equipo a nuestra red, simplemente tenemos que dar clic en uno de los símbolos disponibles y luego llevarlo al área de trabajo y dar clic donde lo queremos colocar:

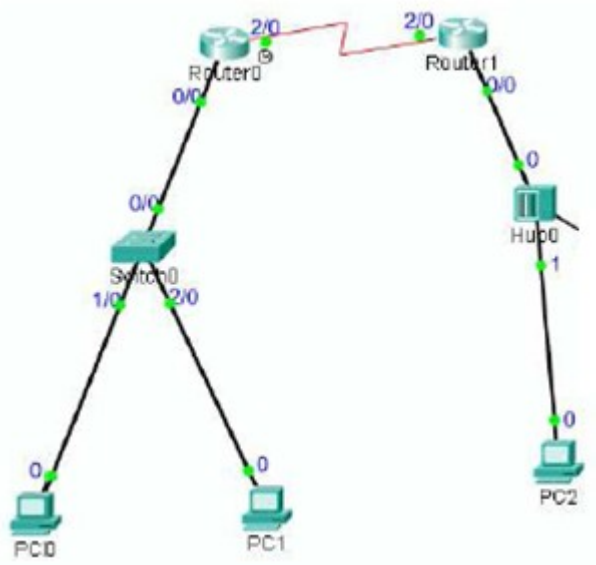
Una vez colocados los equipos, es el momento de conectarlos entre sí. Para ello tenemos el botón:





Si damos clic sobre él y luego sobre cada par de equipos que se quieran interconectar, vamos haciendo las conexiones entre equipos. Al igual que para colocar equipos, si hacemos doble click sobre "Connect", podemos hacer varias conexiones seguidas. El programa escoge automáticamente el tipo de conexión y puerto que se necesita, según el par de equipos que se estén interconectando (router-router, router-switch…).

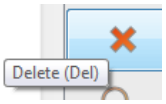
Vamos a interconectar entonces los equipos mostrados, cada PC con un equipo de interconexión adecuado y los equipos de interconexión entre sí, de manera que creemos dos subredes de dos PCs cada una y podamos comunicar ambas redes:



Es importante guardar cada cierto tiempo el trabajo que vamos haciendo (File _ Save).

De esta manera, se crea un archivo con extensión .pkt con nuestro diseño de red.

Si en algún momento necesitamos eliminar un equipo o conexión utilizaremos el botón:



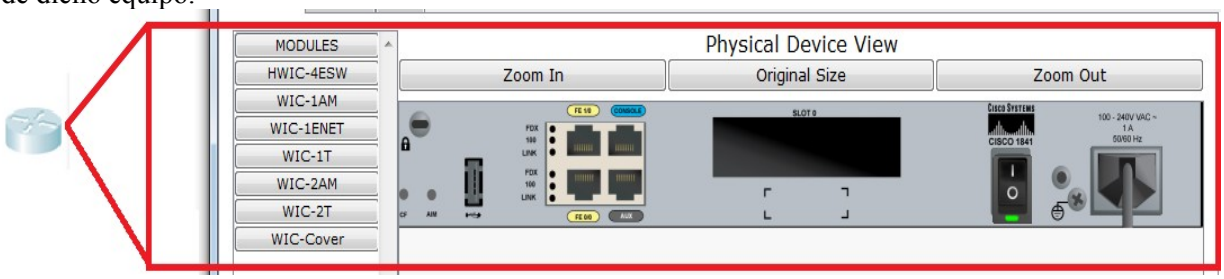
Dar clic sobre él y a continuación sobre el equipo o conexión a eliminar, vamos borrando los elementos que queramos.

Como en ocasiones anteriores, si hacemos doble click sobre el botón "Delete" podremos borrar varios elementos seguidos, hasta que asi sea necesario, dar clic en "Cancel". Hay que tener en cuenta que si borramos un equipo, automáticamente se borrarán todas las conexiones conectadas a él.

Otra cosa importante que hay que saber para trabajar en la pestaña "Real time" con los equipos, es como mover éstos o aumentar una parte de la zona de trabajo donde queramos trabajar. Esto es útil sobre todo cuando tengamos redes muy grandes con muchos equipos y conexiones. Para mover un equipo, basta con dar clicr sobre él y arrastrarlo a donde queramos. Esto supone mover también las conexiones asociadas.

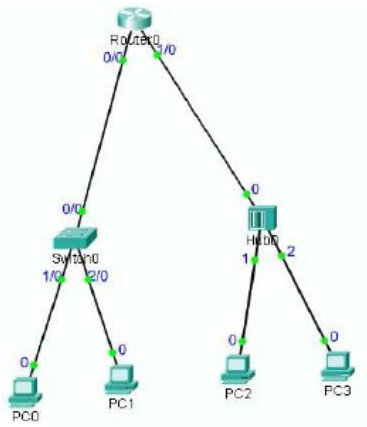
Configuración de equipos en Packet Tracer

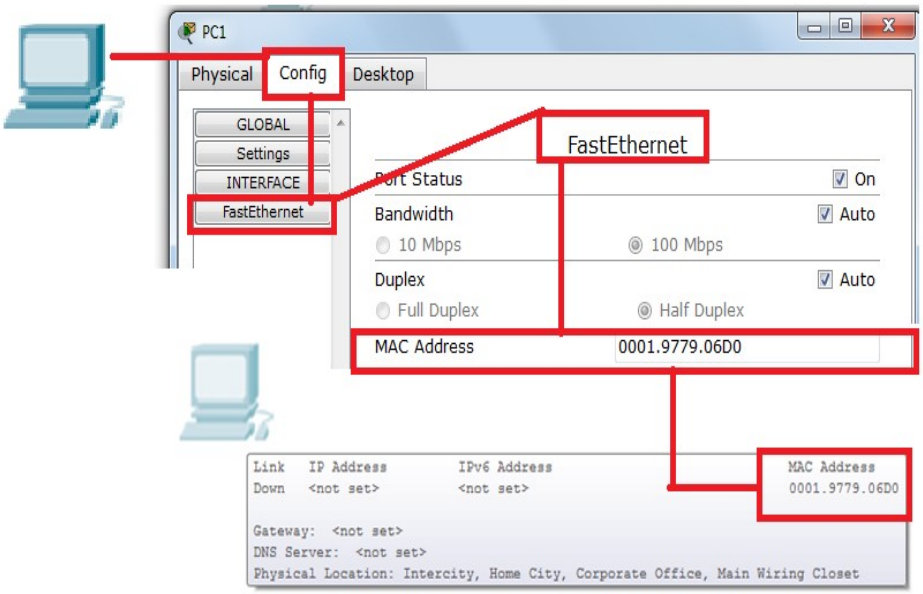
Una vez colocados y conectados todos los equipos (en la pestaña “Real time”) que necesitemos en nuestra red, hay que configurarlos adecuadamente para que los PCs sean capaces de intercambiarse paquetes.
Si damos clic sobre cualquier equipo colocado, nos aparecerá una nueva ventana de configuración de dicho equipo.



En ella, se pueden configurar por ejemplo cada uno de los puertos disponibles en el equipo, dando clic sobre cada recuadro que lo representa.

Los equipos que pueden trabajar a nivel de enlace como los switches, routers y los diversos equipos a interconectar (PCs, servidores, impresoras), tienen sus puertos configurados con una dirección MAC (que decíamos que en un sistema real viene impuesta por el fabricante y no se puede cambiar). Para ver las direcciones MAC de cada puerto no hace falta abrir la ventana de configuración, basta colocar el mouse sobre el equipo y ya aparece un cuadro gris con todos los puertos disponibles en él y sus MAC asociadas.

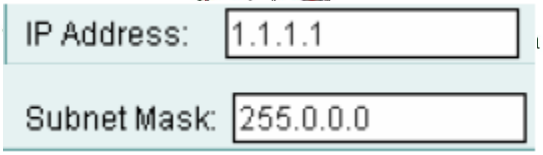




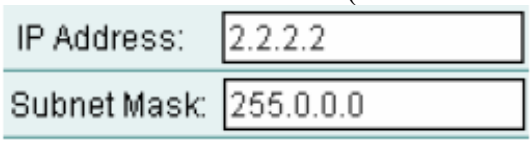
Si el equipo además trabaja a nivel IP (nivel de red), como los routers y los equipos a interconectar, habría que configurar también las tres cosas que comentábamos que eran

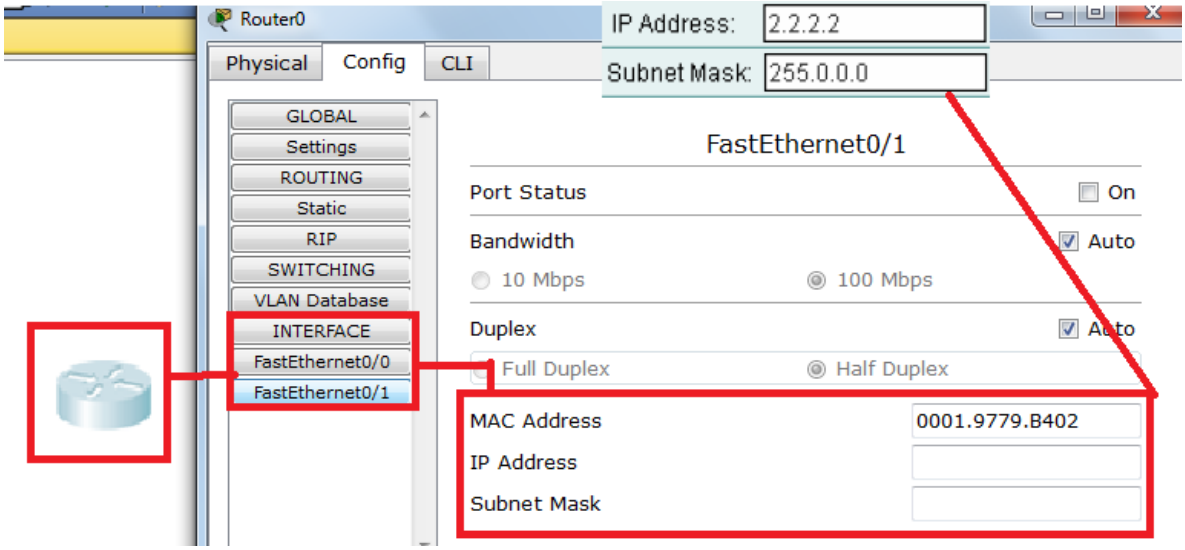
necesarias para dar conectividad a un equipo en una red IP: dirección IP, máscara de subred y puerta de enlace.

En un router, por ejemplo, habría que definir en cada uno de sus puertos dirección IP y máscara adecuados al rango de direcciones asignado a cada una de las redes a las que esté conectado. Por ejemplo, el Router 0 interconecta dos subredes. En el puerto 0/0, el cual tiene conectado a la subred 1 (a través del switch) configuramos lo siguiente:



y en el puerto 1/0, que tiene conectado a la subred 2 (a través del hub) configuramos:





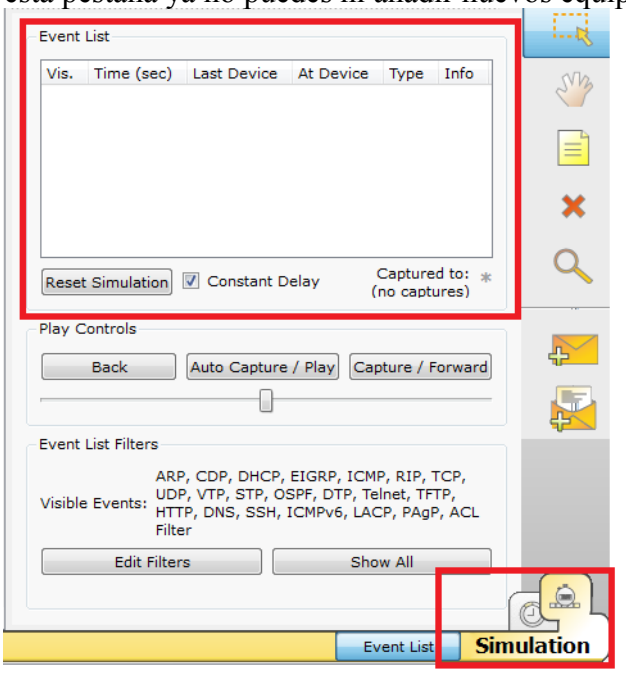
Antes de cerrar la ventana de configuración del Router0 es recomendable guardar su configuración, para que si apagáramos el router, no perdiéramos su configuración. Vamos a configurar ahora cada uno de los PCs. Como hemos descrito para usarlo en el siguiente apartado.

Antes de pasar al apartado de simulación, veamos un aspecto más que podemos configurar en los equipos: número y tipo de puertos disponibles. Si en la ventana de configuración de un equipo nos aparecen cuadraditos vacíos en la representación de los puertos: podremos dar clic sobre uno de ellos para añadir un nuevo puerto. Podemos elegir entre varios tipos de puertos: de cobre, de fibra… Si, por el contrario, queremos borrar o cambiar un puerto, clic dos veces sobre un cuadradito lleno (una para seleccionar el puerto que queremos

borrar o cambiar y la segunda para que aparezca la opción “Delete”). De esta manera, nos quedará un cuadradito vacío en el que podremos añadir el tipo de puerto que queramos.

Simulación de transmisión de paquetes entre equipos

Vamos a partir del diseño de red creado y configurado en el apartado anterior. Para simular el intercambio de paquetes entre los PCs, tenemos que pasar a la pestaña “Simulation”. En esta pestaña ya no puedes ni añadir nuevos equipos, ni configurar los existentes.

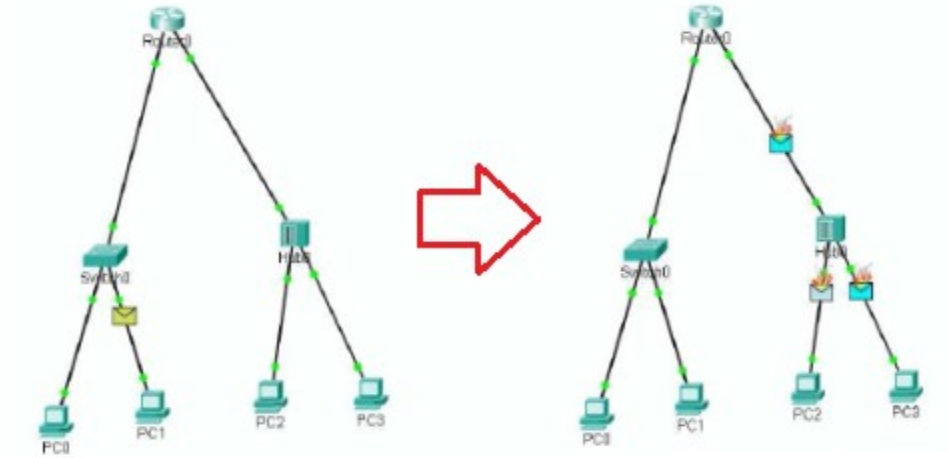


Lo que vamos a añadir en esta pestaña son los paquetes que queramos que se intercambien los PCs.

Indicar primero en el PC origen (el que va a enviar el paquete) y luego en el PC destino (el que tiene que recibir el paquete).

Una vez creado el paquete, si pulsamos el botón “ Auto capture -play ” , veremos como se desplaza el paquete a través de la red, desde su origen a su destino. En el instante que queramos crear nuevos paquetes y así vamos generando nuestro escenario de simulación de intercambio de paquetes entre equipos.

PC0, al llegar al switch sólo se reenvía hacia su destino (PC1) y no hacia todos los puertos del switch. Si seguimos avanzando, veremos como en el instante 4 comienzan a enviarse los paquetes originados en PC2 y PC3. Cuando estos paquetes lleguen al hub colisionarán al intentar reenviarlos por todos los puertos y no llegarán bien a su destino.



Si cuando termina el proceso descrito anteriormente, creamos un nuevo paquete enviado por el PC0 al PC2 y simulamos el envío, veremos como el switch reenvía el paquete sólo por donde sabe que va a llegar a su destino y el router continúa encaminando este paquete

hacia la red destino. Sin embargo, el hub repetirá el paquete a todos los puertos, por lo que al final llegará a PC2 y PC3, pero el destinatario sólo es PC2.

Diseño de una red LAN

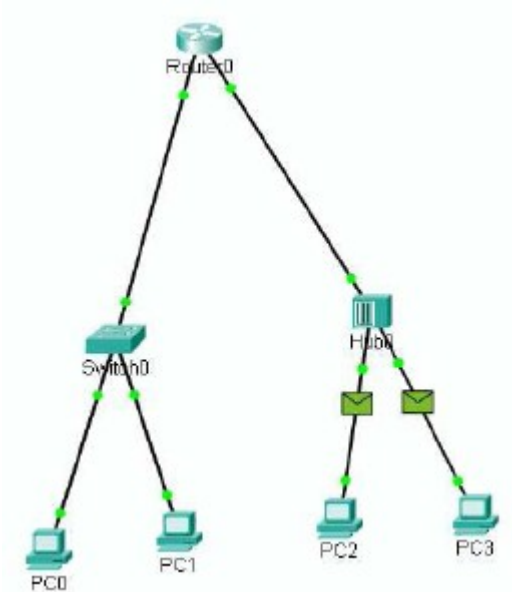
En este apartado vamos ya a diseñar una red LAN utilizando los elementos de interconexión típicos en estas redes, de modo que se van a formar dos escenarios distintos:

- Una red LAN utilizando un hub
- Una red LAN utilizando un switch

A partir de los diseños realizados se deben contestar cada uno de los apartados de la **hoja de resultados**.

Cumplir con las características de los dos escenarios:

Escenario 1	Escenario 2
Hub	Switch
PC0	PC2
PC1	PC3
Servidor	Servidor



Una vez situados los equipos de cada escenario, realiza la conexión de los mismos uniendo los PCs y el servidor al elemento de interconexión de cada escenario.

Una vez situados y conectados los equipos, es necesario comenzar la configuración de los mismos de acuerdo a los datos de la siguiente tabla:

Escenario 1		Escenario 2	
Hub	Puertos utilizados: Fast Ethernet Nombre: Hub0	Switch	Puertos utilizados: Fast Ethernet Nombre: Switch0
PC0	Puerto 0:Fast Ethernet Dirección IP:192.168.100.2 Máscara: 255.255.255.0 Nombre: Sistema A1	PC2	Puerto 0: Fast Ethernet Dirección IP: 10.0.0.2 Máscara: 255.255.255.0 Nombre: Sistema A2
PC1	Puerto 0: Fast Ethernet Dirección IP:192.168.100.3 Máscara: 255.255.255.0 Nombre: Sistema B1	PC3	Puerto 0: Fast Ethernet Dirección IP: 10.0.0.3 Máscara: 255.255.255.0 Nombre: Sistema B2
Servidor	Puerto 0: Fast Ethernet Dirección IP: 192.168.100.4 Máscara: 255.255.255.0 Nombre: Servidor FTP	Servidor	Puerto 0: Fast Ethernet Dirección IP: 10.0.0.4 Máscara: 255.255.255.0 Nombre: Servidor DNS

Anotar en la hoja de resultados las direcciones MAC de los equipos (sólo puertos activos o "up") Asi como que puerto del elemento de interconexión está unido a qué equipo.

Comprueba si la configuración es correcta. Para ello pasa a la ventana de simulación. En este punto crea paquetes de unos equipos a otros según la tabla siguiente y rellena los campos correspondientes de la hoja de resultados.

Escenario 1		Escenario 2	
Comunicación 1	Paquete entre Sistema A1 y Sistema B1	Comunicación 5	Paquete entre Sistema A2 y Sistema B2
Comunicación 2	Paquete entre Sistema A1 y Servidor FTP	Comunicación 6	Paquete entre Sistema A2 y Servidor DNS
Comunicación 3	Paquete entre Sistema B1 y Hub	Comunicación 7	Paquete entre Sistema B2 y Switch
Comunicación 4	1 Paquete entre Sistema B1 y Sistema A1 1 Paquete entre Sistema A1 y Servidor FTP (Simultáneamente)	Comunicación 8	1 Paquete entre Sistema B2 y Sistema A2 1 Paquete entre Sistema A2 y Servidor DNS (Simultáneamente)

Una vez llevados a cabo los pasos anteriores para los dos escenarios, pasa de nuevo a la ventana de topología para añadir una impresora a la red en la que hay un switch. Configúrala con los siguientes parámetros:

Nombre: Impresora2, Dirección IP: 10.0.1.5, Máscara: 255.255.255.0

Pasa a simulación y comprueba el correcto funcionamiento de la red enviando un paquete desde el Sistema A2 a la Impresora2. Contesta a la pregunta de la hoja de resultados.

Realiza los cambios necesarios para solucionar el problema anterior.

En base a los resultados obtenidos en los pasos anteriores intentar determinar las principales diferencias entre el montaje de una red de área local con un hub y con un switch. Para ello, debes fijarte en los siguientes aspectos y a continuación contestar las cuestiones de la hoja de resultados:

_ Nº paquetes que atraviesan los equipos
_ Actividad en los enlaces
_ Equipos que reciben la información
_ Colisiones

Comunicación entre redes LAN

En este apartado se va estudiar uno de los posibles casos de conectividad entre redes LAN, puesto que habitualmente no se montan redes aisladas, sino que se requiere la comunicación con otras redes.

Escenario 3.

Supón que los escenarios 1 y 2 son dos redes de área local de una empresa, la primera correspondiente al área comercial y la otra al área técnica. Se trata de dos redes que se encuentran en el mismo edificio por lo que es posible conectarlas mediante un router sin tener que pedir licencias ni contratar circuitos terceros. Sigue los pasos siguientes para conectar ambas redes.

Si has borrado los escenarios anteriores vuelve a crearlos y configúralos según lo indicado en los apartados anteriores.

Sitúa un router entre ambas redes y conéctalo al hub y al switch mediante conexiones Fast Ethernet. Configura las interfaces de cada router según la tabla, sabiendo que el puerto del router que se conecta al hub debe tener una dirección IP de la red que forma el hub y lo mismo para el switch:

Router	
Interfaz Router –Hub (Conexión con LAN escenario 1)	**Interfaz Router – Switch (Conexión con LAN escenario 2)**
Dirección IP: 192.168.100.1 Máscara: 255.255.255.0	Dirección IP: 10.0.0.1 Máscara: 255.255.255.0

Pasa a la ventana de simulación y envía los siguientes paquetes para comprobar que el router tiene bien configuradas las direcciones IP:

Escenario 3	
Comunicación 9	Paquete entre Sistema A1 y Router
Comunicación 10	Paquete entre Servidor DNS y Router

Comprobaremos que no podemos realizar con éxito la Comunicación 10. El problema es que, al tener activado “Simple Mode” y tener conectado el hub al puerto 0/0 del router,

cualquier paquete que se intente enviar al router (aunque sea desde la red conectada al switch), el simulador lo enviará al primer puerto activo del router (0/0), que tiene una dirección IP del rango de la red conectada al hub. Por eso falla el envío al enviar un paquete desde un equipo conectado a la red del switch. Para solucionar el problema, habría que desactivar la opción "Simple Mode", eliminar el paquete creado en la Comunicación 10 y crear uno nuevo. Cuando demos clic en el equipo origen, nos aparecerá una nueva ventana para definir los datos del equipo destino. En esta ventana, introduciremos como "IP Address", nuestra dirección IP destino, es decir la dirección IP del puerto del router conectado a la red del switch (10.0.0.1). Comprobaremos que se ha podido enviar correctamente el paquete entre el Servidor DNS y el router.

Conexión de dos sistemas

En este apartado veremos cómo se deben conectar dos equipos iguales directamente entre sí (sin utilizar elementos de interconexión).

1. Sitúa dos PCs en la zona de trabajo y ponles un nombre. A continuación, pon direcciones IP y máscaras a cada equipo, sabiendo que deben ser direcciones de la misma red (del mismo rango).

2. Une los equipos mediante un cable de par trenzado. En primer lugar, utiliza la opción "Copper Straight Through" (cable normal en comunicaciones). Cuando pregunte el tipo de puerto, escoger "Copper Fast Ethernet".

3. Pasa a la ventana de simulación y comprueba su funcionamiento enviando un paquete de un equipo a otro.

4. Regresa a la ventana de topología, borra el cable de unión y ahora conéctalos con la opción "Copper Cross-Over" (cable cruzado en comunicaciones). Tipo de puerto: "Copper Fast Ethernet".

5. Comprueba su funcionamiento como hiciste en el paso 4 y responde a la pregunta planteada en la hoja de resultados.

Hoja de Resultados

Dibuja el esquema de las redes que has implementado:

Escenario 1	Escenario 2

Anota las direcciones MAC de los equipos que has empleado en cada escenario:

Escenario 1		**Escenario 2**	
Hub		Switch	
PC_Sistema A1		PC_Sistema A2	
PC_Sistema B1		PC_Sistema B2	
Servidor FTP		Servidor DNS	

Puertos de conexión:

Escenario 1		**Escenario 2**	
Conexión	**Puerto**	**Conexión**	**Puerto**
Hub-PC_Sistema A1		Switch-PC_Sistema A2	
Hub-PC Sistema B1		Switch-PC_Sistema B2	
Hub-Servidor		Switch-Servidor	

Comprobación de funcionamiento.

Para cada comunicación, observando el paquete de datos en cada uno de los puntos indicados en la columna “posición”, completa la tabla siguiente:

Escenario 1					
Comunicación	**Posición**	Dirección IP origen	Dirección IP destino	Dirección MAC origen	Dirección MAC destino
Comunicación 1	Origen				
	Hub				
	Destino				
Comunicación 4	Origen				
	Hub				
	Destino				

Escenario 2					
Comunicación	**Posición**	Dirección IP origen	Dirección IP destino	Dirección MAC origen	Dirección MAC destino
Comunicación 5	Origen				
	Switch				
	Destino				
Comunicación 8	Origen paquete 1				
	Origen paquete 2				
	Switch (paquete 1)				
	Switch (paquete 2)				
	Destino paquete 1				
	Destino paquete 2				

¿Cuál es el problema que se da en la Comunicación 4? ¿Por qué no sucede lo mismo en la Comunicación 8?

Después de añadir la impresora tal y como se pidió en la práctica. ¿Ha sido posible la comunicación? ¿Cuál crees que ha sido el problema? ¿Cómo solucionaste el problema?

Completa la siguiente tabla con los datos obtenidos de la tabla MAC del switch (clic sobre switch en la pestaña simulación):

MAC Address	Port

¿Cómo y para qué utiliza el switch dicha tabla?

Estudio de las diferencias entre un hub y un switch.

En base a los resultados obtenidos en las simulaciones anteriores:

1. ¿Qué elemento de conexión es más eficiente? ¿Por qué?
2. ¿Por qué se producen las colisiones?

Comunicación entre redes LAN
Escenario 3
Dibuje el esquema de la red que ha implementado:

Anota las direcciones MAC del router:

Escenario 3	
Router Interfaz Conexión hub	
Router Interfaz Conexión switch	

Observa paso a paso el envío del paquete de la Comunicación 14 y anota en el siguiente cuadro los resultados de todo el proceso de comunicación, a nivel MAC e IP.

Comunicación	**Posición**	Dirección IP origen	Dirección IP destino	Dirección MAC origen	Dirección MAC destino
Comunicación 14	Origen				
	Switch				
	Router				
	Hub				
	Destino				

Compara el resultado con las Comunicaciones 1-8. ¿Por qué son diferentes?
Para comprender mejor los resultados, comenta las capas TCP/IP activas en cada nodo por que pasa el mensaje en la simulación de la comunicación 14. Razone especialmente las capas activas en los extremos de la comunicación así como el cambio que se produce a nivel de enlace el router que une ambas subredes.

Bibliografía

CISCO Networking Academia. Primer año
Comunicaciones y Redes de Computadores; Stallings, William 7ª Ed. Prentice Hall, 2000. ISBN 978-84-205-4110-5
Feit, Sidnie.: TCP/IP. Arquitectura, protocolos e implementación, 2ª Ed. Mc-Graw Hill. 1998. ISBN 84-481-1531-7
Held, G.: The Complete Modem Reference, 3ª Ed. John Wiley & Sons, Inc., 1997.
Heywood, Drew: Redes con Microsoft TCP/IP. Edición Especial, 3ª Ed. Prentice Hall, 1999. ISBN 84-8322-108.

PRÁCTICA 9

WIRESHARK® PARA VER LAS UNIDADES DE DATOS DEL PROTOCOLO

Objetivos

• Explicar el propósito de un analizador de protocolos (Wireshark).
•Realizar capturas básicas de la unidad de datos del protocolo (PDU) mediante el uso de Wireshark.
• Elaborar un análisis básico de la PDU en un tráfico de datos de red simple.
•Experimentar con las características y opciones de Wireshark, como captura de PDU y visualización de filtrado.

Introducción

Wireshark es un analizador de protocolos de software o una aplicación "husmeador de paquetes" que se utiliza para el diagnóstico de fallas de red, verificación, desarrollo de protocolo y software y educación.

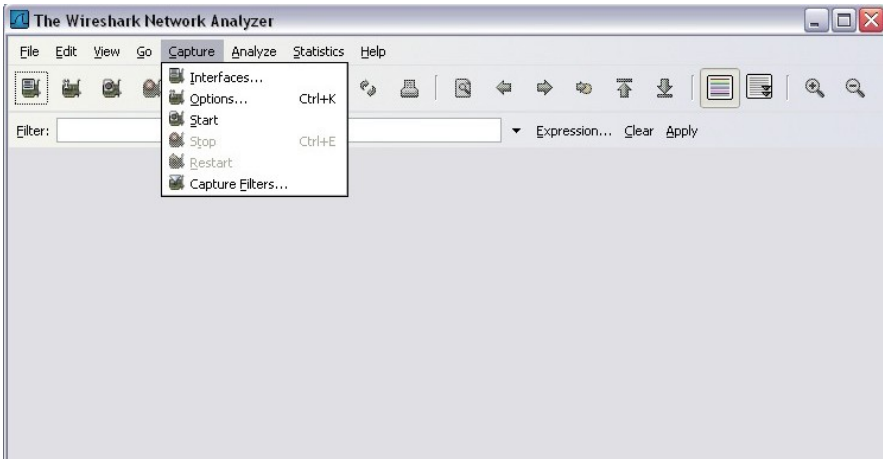
Antes de junio de 2006, Wireshark se conocía como Ethereal. Un husmeador de paquetes (también conocido como un analizador de red o analizador de protocolos) es un software informático que puede interceptar y registrar tráfico de datos pasando sobre una red de datos. Mientras el flujo de datos va y viene en la red, el husmeador "captura" cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo a la RFC correcta u otras especificaciones.

Programado para reconocer la estructura de los diferentes protocolos de red. Esto le permite mostrar la encapsulación y los campos individuales de una PDU e interpretar su significado. Es una herramienta útil para cualquiera que trabaje con redes y se puede utilizar en la mayoría de las prácticas de laboratorio en los cursos CCNA para el análisis de datos y el diagnóstico de fallas. Para obtener más información y para descargar el programa visite: http://www.Wireshark.org

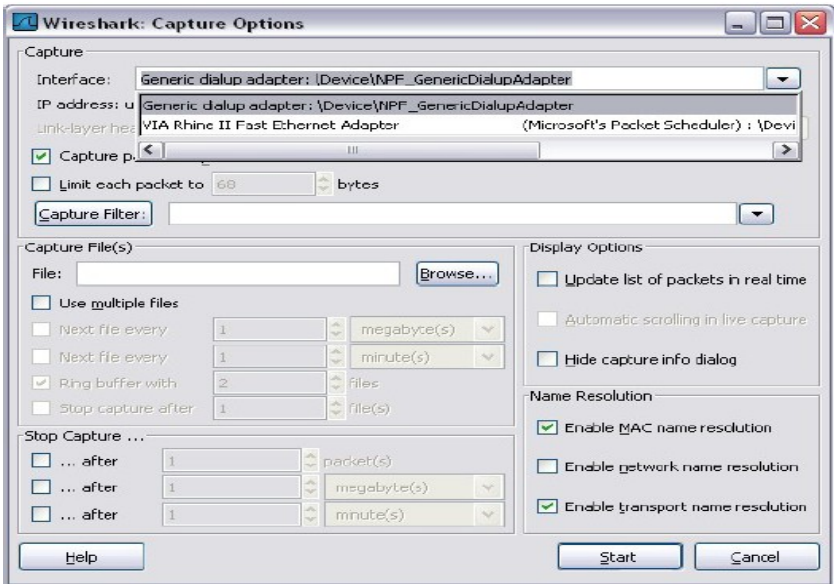
Desarrollo

Para capturar las PDU, la computadora donde está instalado Wireshark debe tener una conexión activa a la red y Wireshark debe estar activo antes de que se pueda capturar cualquier dato.

Cuando se inicia Wireshark, se muestra la siguiente pantalla.

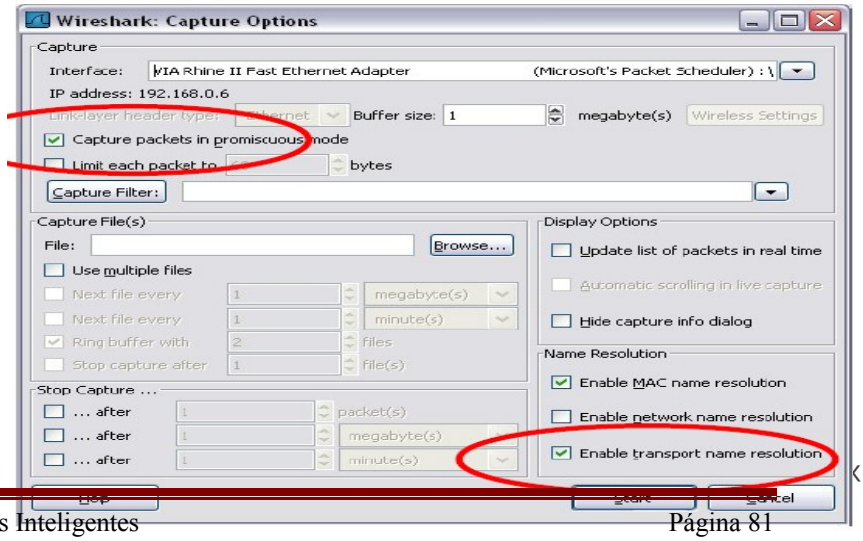


Para empezar con la captura de datos es necesario ir al menú **Captura** y seleccionar **Opciones**. El cuadro de diálogo **Opciones** provee una serie de configuraciones y filtros que determinan el tipo y la cantidad de tráfico de datos que se captura.



Primero, es necesario asegurarse de que Wireshark está configurado para monitorear la interfaz correcta. Desde la lista desplegable **Interfaz**, seleccione el adaptador de red que se utiliza.

Generalmente, para una computadora, será el adaptador Ethernet conectado. Luego se pueden configurar otras opciones. Entre las que están disponibles en **Opciones de captura,** merecen examinarse las siguientes dos opciones resaltadas.



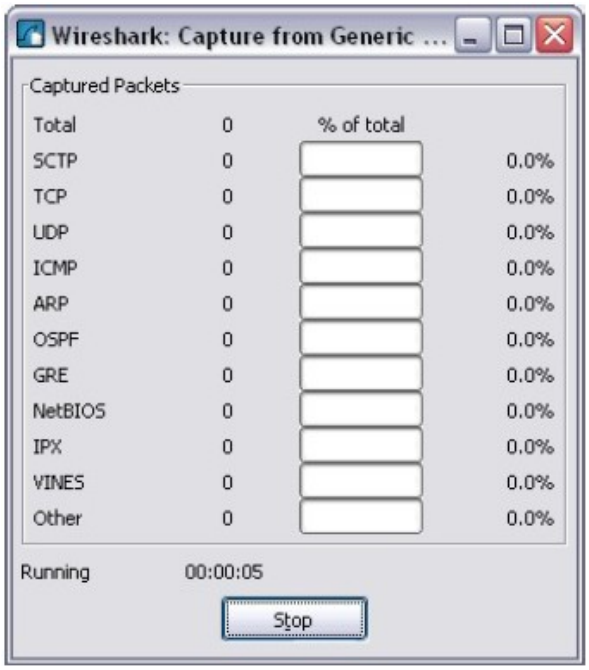
Configurar Wireshark para capturar paquetes en un modo promiscuo.

Si esta característica NO está verificada, sólo se capturarán las PDU destinadas a esta computadora.

Si esta característica está verificada, se capturarán todas las PDU destinadas a esta computadora Y todas aquellas detectadas por la NIC de la computadora en el mismo segmento de red (es decir, aquellas que "pasan por" la NIC pero que no están destinadas para la computadora).
Nota: La captura de las otras PDU depende del dispositivo intermediario que conecta las computadoras del dispositivo final en esta red. Si utiliza diferentes dispositivos intermediarios (hubs, switches, routers) durante estos cursos, experimentará los diferentes resultados de Wireshark.

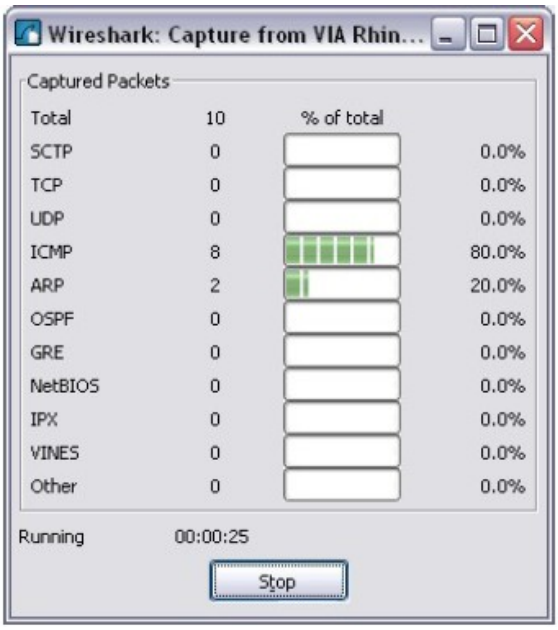
Configurar Wireshark para la resolución del nombre de red

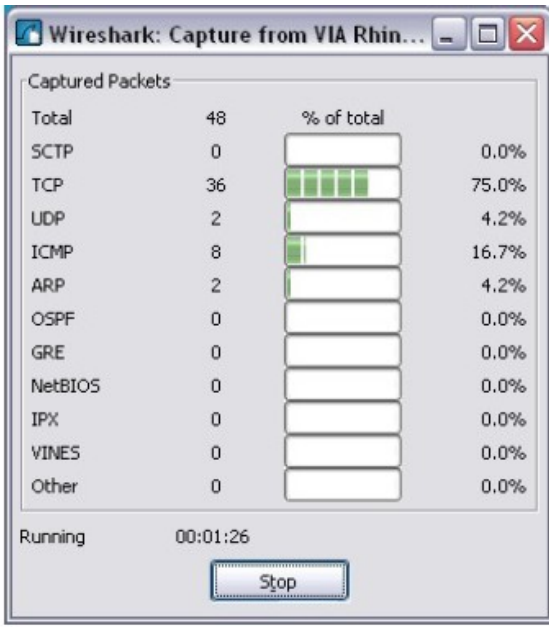
Esta opción le permite controlar si Wireshark traduce a nombres las direcciones de red encontradas en las PDU. A pesar de que esta es una característica útil, el proceso de resolución del nombre puede agregar más PDU a sus datos capturados, que podrían distorsionar el análisis. También hay otras configuraciones de proceso y filtrado de captura disponibles. Haga clic en el botón **Iniciar** para comenzar el proceso de captura de datos y una casilla de mensajes muestra el progreso de este proceso.

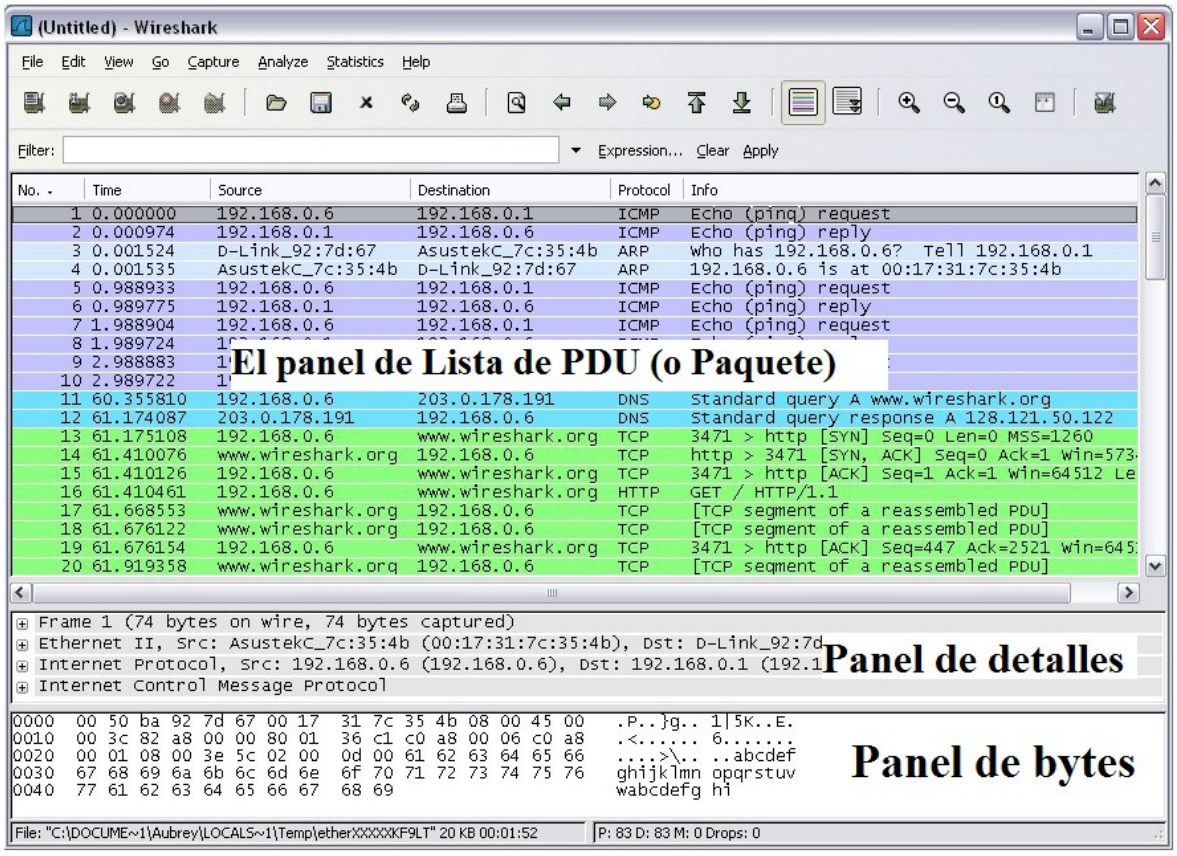


Mientras se capturan las PDU, los tipos y números se indican en la casilla de mensajes. Los ejemplos de abajo muestran la captura de un proceso ping y luego el acceso a una página Web.

Si hace clic en el botón **Detener**, el proceso de captura termina y se muestra la pantalla principal.


Wireshark: Capture from VIA Rhin...
Captured Packets
Total 10 % of total
SCTP 0 0.0%
TCP 0 0.0%
UDP 0 0.0%
ICMP 8 80.0%
ARP 2 20.0%
OSPF 0 0.0%
GRE 0 0.0%
NetBIOS 0 0.0%
IPX 0 0.0%
VINES 0 0.0%
Other 0 0.0%
Running 00:00:25
Stop


Wireshark: Capture from VIA Rhin...
Captured Packets
Total 48 % of total
SCTP 0 0.0%
TCP 36 75.0%
UDP 2 4.2%
ICMP 8 16.7%
ARP 2 4.2%
OSPF 0 0.0%
GRE 0 0.0%
NetBIOS 0 0.0%
IPX 0 0.0%
VINES 0 0.0%
Other 0 0.0%
Running 00:01:26
Stop


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.0.6 192.168.0.1 ICMP Echo (ping) request
2 0.000974 192.168.0.1 192.168.0.6 ICMP Echo (ping) reply
3 0.001524 D-Link_92:7d:67 AsustekC_7c:35:4b ARP Who has 192.168.0.6? Tell 192.168.0.1
4 0.001535 AsustekC_7c:35:4b D-Link_92:7d:67 ARP 192.168.0.6 is at 00:17:31:7c:35:4b
5 0.988933 192.168.0.6 192.168.0.1 ICMP Echo (ping) request
6 0.989775 192.168.0.1 192.168.0.6 ICMP Echo (ping) reply
7 1.988904 192.168.0.6 192.168.0.1 ICMP Echo (ping) request
El panel de Lista de PDU (o Paquete)
11 60.355810 192.168.0.6 203.0.178.191 DNS Standard query A www.wireshark.org
12 61.174087 203.0.178.191 192.168.0.6 DNS Standard query response A 128.121.50.122
13 61.175108 192.168.0.6 www.wireshark.org TCP 3471 > http [SYN] Seq=0 Len=0 MSS=1260
14 61.410076 www.wireshark.org 192.168.0.6 TCP http > 3471 [SYN, ACK] Seq=0 Ack=1 Win=573
15 61.410126 192.168.0.6 www.wireshark.org TCP 3471 > http [ACK] Seq=1 Ack=1 Win=64512 Le
16 61.410461 192.168.0.6 www.wireshark.org HTTP GET / HTTP/1.1
17 61.668553 www.wireshark.org 192.168.0.6 TCP [TCP segment of a reassembled PDU]
18 61.676122 www.wireshark.org 192.168.0.6 TCP [TCP segment of a reassembled PDU]
19 61.676154 192.168.0.6 www.wireshark.org TCP 3471 > http [ACK] Seq=447 Ack=2521 Win=645
20 61.919358 www.wireshark.org 192.168.0.6 TCP [TCP segment of a reassembled PDU]
Frame 1 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: AsustekC_7c:35:4b (00:17:31:7c:35:4b), Dst: D-Link_92:7d
Internet Protocol, Src: 192.168.0.6 (192.168.0.6), Dst: 192.168.0.1 (192.1
Panel de detalles
Internet Control Message Protocol
0000 00 50 ba 92 7d 67 00 17 31 7c 35 4b 08 00 45 00 .P..}g.. 1|5K..E.
0010 00 3c 82 a8 00 00 80 01 36 c1 c0 a8 00 06 c0 a8 .<...... 6.......
0020 00 01 08 00 3e 5c 02 00 0d 00 61 62 63 64 65 66 ....>\.. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
Panel de bytes
File: "C:\DOCUME~1\Aubrey\LOCALS~1\Temp\etherXXXXXKF9LT" 20 KB 00:01:52
P: 83 D: 83 M: 0 Drops: 0

El panel de Lista de PDU (o Paquete) ubicado en la parte superior del diagrama muestra un resumen de cada paquete capturado. Si hace clic en los paquetes de este panel, controla lo que se muestra en los otros dos paneles.
El panel de detalles de PDU (o Paquete) ubicado en el medio del diagrama, muestra más detalladamente el paquete seleccionado en el panel de Lista del paquete.

El panel de bytes de PDU (o paquete) ubicado en la parte inferior del diagrama, muestra los datos reales (en números hexadecimales que representan el binario real) del paquete seleccionado en el panel de Lista del paquete y resalta el campo seleccionado en el panel de Detalles del paquete.

Cada línea en la Lista del paquete corresponde a una PDU o paquete de los datos capturados.
Si seleccionó una línea en este panel, se mostrarán más detalles en los paneles "Detalles del paquete" y "Bytes del paquete". El ejemplo de arriba muestra las PDU capturadas cuando se utilizó la utilidad ping y cuando se accedió a http://www.Wireshark.org. Se seleccionó el paquete número 1 en este panel.

El panel Detalles del paquete muestra al paquete actual (seleccionado en el panel "Lista de paquetes") de manera más detallada. Este panel muestra los protocolos y los campos de protocolo de los paquetes seleccionados. Los protocolos y los campos del paquete se muestran con un árbol que se puede expandir y colapsar.
El panel Bytes del paquete muestra los datos del paquete actual (seleccionado en el panel "Lista de paquetes") en lo que se conoce como estilo "hexdump". En esta práctica de laboratorio no se examinará en detalle este panel. Sin embargo, cuando se requiere un análisis más profundo, esta información que se muestra es útil para examinar los valores binarios y el contenido de las PDU.

La información capturada para las PDU de datos se puede guardar en un archivo. Ese archivo se puede abrir en Wireshark para un futuro análisis sin la necesidad de volver a capturar el mismo tráfico de datos. La información que se muestra cuando se abre un archivo de captura es la misma de la captura original. Cuando se cierra una pantalla de captura de datos o se sale de Wireshark se le pide que guarde las PDU capturadas.

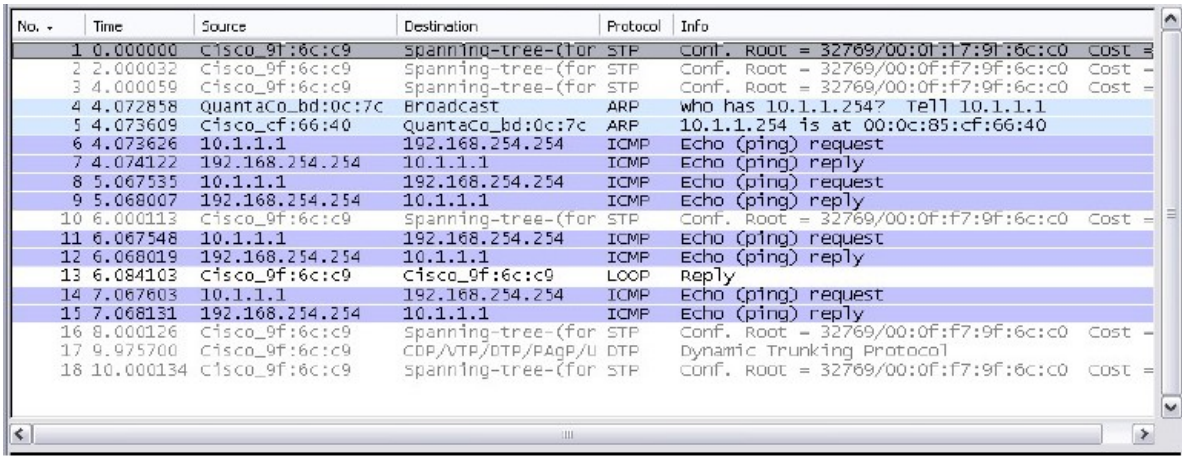
Después de asegurarse de que la topología y configuración de laboratorio estándar son correctas, inicie Wireshark en un equipo en un módulo de laboratorio.

Configure las opciones de captura como se describe arriba en la descripción general e inicie el proceso de captura.

Desde la línea de comando del equipo, haga ping en la dirección IP de otra red conectada y encienda el dispositivo final en la topología de laboratorio. En este caso, haga ping en Eagle Server utilizando el comando ping **192.168.254.254**.

Después de recibir las respuestas exitosas al ping en la ventana de línea de comandos, detenga la captura del paquete.

Examine el panel Lista de paquetes.
El panel Lista de paquetes en Wireshark debe verse ahora parecido a éste:



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	Who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAgP/U	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Observe los paquetes de la lista de arriba. Nos interesan los números de paquetes 6, 7, 8, 9, 11, 12, 14 y 15. Localice los paquetes equivalentes en la lista de paquetes de su equipo.

Responda lo siguiente desde la lista de paquetes Wireshark:

¿Qué protocolo se utiliza por ping? _____ _____
¿Cuál es el nombre completo del protocolo? _____
¿Cuáles son los nombres de los dos mensajes ping? ____ _____
¿Las direcciones IP de origen y destino que se encuentran en la lista son las que esperaba? Sí / No
¿Por qué? _____

Los detalles de cada sección y protocolo se pueden expandir más. Tómese el tiempo para leer esta información. En esta etapa del curso, puede ser que no entienda completamente la información que se muestra, pero tome nota de la que sí reconozca.

Localice los dos tipos diferentes de "Origen" y "Destino". ¿Por qué hay dos tipos?
_____

¿Cuáles son los protocolos que están en la trama de Ethernet?
_____

Si selecciona una línea en el panel de Detalles del paquete, toda o parte de la información en el panel de Bytes del paquete también quedará resaltada.

Considere lo que puede proveer Wireshark sobre la información de encapsulación referida a los datos de red capturados. Relacione esto a los modelos de la capa OSI y TCP/IP. Es importante que pueda reconocer y relacionar tanto los protocolos representados como la capa de protocolo y los tipos de encapsulación de los modelos con la información provista por Wireshark.
_____
_____
_____

Analice cómo podría utilizar un analizador de protocolos como Wireshark para:
(1) diagnosticar fallas de una página Web para descargar con éxito un navegador en un equipo

(2) identificar el tráfico de datos en una red requerida por los usuarios.

_____
_____
_____
_____
_____

Bibliografía

CISCO Networking Academia. Primer año
Comunicaciones y Redes de Computadores; Stallings, William 7ª Ed. Prentice Hall, 2000. ISBN 978-84-205-4110-5
Feit, Sidnie.: TCP/IP. Arquitectura, protocolos e implementación, 2ª Ed. Mc-Graw Hill. 1998. ISBN 84-481-1531-7
Held, G.: The Complete Modem Reference, 3ª Ed. John Wiley & Sons, Inc., 1997.
Heywood, Drew: Redes con Microsoft TCP/IP. Edición Especial, 3ª Ed. Prentice Hall, 1999. ISBN 84-8322-108.
http://www.Wireshark.org