

SISTEMAS DE COMUNICACIÓN Y REDES INFORMÁTICAS



Ing. Jorge Bladimir Rubio Peñaherrera, Mgs
GI-CIR

“Grupo de investigación en Ciencias informáticas
y Redes”

UTC



Autores

Ing. Mgs. Jorge Bladimir Rubio Peñaherrera
PhD. Gustavo Rodríguez Bárcenas
Mgs. Fausto Alberto Viscaíno Naranjo
Mgs. Alex Santiago Cevallos Culqui
Mgs. Segundo Humberto Corrales Beltrán

Dirección Editorial

Comité Editorial
Universidad Técnica de Cotopaxi

Diagramación

José Eduardo Cócheres Sandoval
Cristian José Iza Caguana

Todos los derechos reservados © 2017.

Se autoriza a los interesados para copiar, distribuir o modificar cualquier parte de este manual siempre y cuando se cite la fuente y se envíe una notificación por escrito o vía correo electrónico al autor o autores.

Primera edición.

ISBN Digital: 978-9978-395-41-7

DE LOS AUTORES



jorge.rubio@utc.edu.ec

Ing. Mgs. Jorge Bladimir Rubio Peñaherrera.

Ingeniero en Informática y Sistemas Computacionales
Diploma Superior en Gerencia Informática
Magister en Gerencia Informática mención Desarrollo de Software y Redes.
Certificación Internacional de Experto en Seguridad Informática y Etical Hacking
Docente de la Universidad Técnica de Cotopaxi



gustavo.rodriguez@utc.edu.ec

PhD. Gustavo Rodríguez Bárcenas

Ingeniero Mecánico
Master en Nuevas Tecnologías para La Educación
Master en Bibliotecología y Ciencia de la Información
DOCTOR (Programa de Doctorado Bibliotecología y Documentación Científica)
Docente de la Universidad Técnica de Cotopaxi



fausto.viscaino@utc.edu.ec

Mgs. Fausto Alberto Viscaíno Naranjo

Ingeniero en Sistemas e Informática
Magister en Gerencia Informática mención Desarrollo de Software y Redes.
Magister en Docencia de las Ciencias Informáticas
Docente de la Universidad Técnica de Cotopaxi



alex.cevallos@utc.edu.ec

Mgs. Alex Santiago Cevallos Culqui

Ingeniero en Sistemas e Informática
Magister en Tecnologías de la Información
Docente de la Universidad Técnica de Cotopaxi



segundo.corrales@utc.edu.ec

Mgs. Segundo Humberto Corrales Beltrán

Ingeniero en Informática y Sistemas Computacionales
Magister en Sistemas Informáticos Educativos
Docente de la Universidad Técnica de Cotopaxi

A mi esposa Bertha Mila y mis hijos

Mirely Rafaela y Daniel Antonio.

*Quienes representan la razón de ser de mi existencia,
son mi fuente permanente de
inspiración y deseo de superación.*

A mis padres: Gerardo y Julia.

A mis hermanas, cuñados, sobrino y sobrina.

*Juntos formamos ilusiones en la vida
y las estamos viendo cristalizadas como familia.*

Gracias.

A mis amigos y compañeros de trabajo Gustavo Rodríguez,

*Fausto Viscaino, Alex Cevallos, Segundo Corrales, que además
de la amistad, compartimos la honorífica vocación de la
docencia, mil gracias por su valiosa aportación de conocimientos,
experiencia y voluntad para el desarrollo de este libro.*

Tabla de Contenido

De los autores	
Tabla de contenido	
Índice de figuras	
Índice de tablas	
Prólogo	14
Capítulo I	16
Sistemas de comunicación	16
Transmisión de datos	18
Transmisión por radiofrecuencia	18
Asignación de bandas y frecuencias.	19
Sistemas infrarrojos	20
Características de los sistemas de comunicación infrarrojos.	20
Clasificación de los sistemas de comunicación infrarrojos.	21
Modos de transmisión infrarroja	22
• Sistemas punto a punto	22
• Sistema casi -difuso	23
• Sistemas difusos.	23
Sistemas satelitales	24
Capítulo II	26
Comunicación de datos con redes informáticas	26
Redes informáticas	27
Tipos de redes.	28
Redes Lan	28
Redes Man	29
Redes Wan	30

Ventajas de la red Wan	30	Clases de redes	45
Desventajas de la red Wan	30	Máscara de subred	47
Topologías de redes informáticas	32	Restricciones del direccionamiento Ip	49
Topología en estrella.	32	Cableado y conexión de red	50
Ventajas de la topología estrella:	33	Cable de par trenzado sin apantallar	
Inconvenientes de la topología de estrella.	33	Unshielded Twisted Pair (Utp).	50
Topología de Bus	34	Estándares para la conexión de redes	52
Ventajas de la topología de Bus:	34	Cable cruzado	53
Desventajas de la topología de Bus:	34	Transmisión inalámbrica:	54
Topología de árbol	35	Conectarse a una red inalámbrica (Wi-Fi)	55
Ventajas de la topología de árbol:	35	Dispositivos bluetooth	55
Desventajas de la topología de árbol:	35	Subneteo clase A, B, C.	55
Capítulo III	36	Convertir bits en números decimales	57
Transmisión de datos en redes informáticas	36	Calcular la cantidad de subredes y hosts por subred	58
Protocolos de red	36	Capítulo IV	59
Modelos de referencia de capas de red	39	Cisco Packet Tracer 7.0 – Manual paso a paso	59
Modelo Osi	39	Iniciamos en packet tracer	60
Modelo Tcp/Ip.	40	Posicionamiento de los dispositivos	64
Hardware de conexión de redes	42	Despliegue de información de dispositivos	65
Tarjeta de red	42	Configuración de equipos	66
La dirección Mac	42	Configurando un Pc	66
Concentradores: switch y hub	43	Configurando un Switch	67
Hub	43	Configurando un Router	70
Switch	43	Primera aplicación	73
Hardware de conexión a Internet: Módem y Router	44	Packet tracer y las redes inalámbricas	82
Direccionamiento Ip	44	Uso de la herramienta packet tracer, simulando una red	
Jerarquía de redes	45	híbrida controlada por un router inalámbrico.	85

Uso del protocolo wep en redes inalámbricas	89	2. En la empresa XYZA,	110
Capítulo V	92	3. Su red utiliza	110
Seguridad en redes	92	4. Usted planea la migración	110
Amenazas externas	93	5. Una red esta dividida	112
Amenazas internas	93	Practicas de configuración de servidores en packet tracer.	111
Ataques informáticos	94	Glosario	140
Ataques de denegación de servicios (Dos)	94	Referencia bibliográficas	147
Man in the Middle (Mitm)	95	Citada:	147
Ataques de replay:	95	Consultada	148
Los cortafuegos	95	Direcciones web de referencia.	149
Listas de control de acceso (Acl) y filtrado de paquetes.	98	Índice de Figuras	
Lista de control de acceso en routers.	98	Figura 1. Diagrama de bloques de un	
Iptables.	99	Sistema de comunicación	17
Redes inalámbricas.	100	Figura 2. Modelo simplificado de un	
Consejos de seguridad.	101	Sistema de comunicación	17
Capítulo VI	103	Figura 3. Transmisión de la información a distancia	18
Ejercicios propuestos, prácticas y laboratorios.	103	Figura 4. Longitud de onda	19
Práctica #1	103	Figura 5. Comunicación por infrarrojo	22
Práctica #2	103	Figura 6. Sistema de comunicación satelital	25
Práctica #3	104	Figura 7. Ejemplo de una red de computadores	27
Práctica # 4	104	Figura 8. Red lan	28
Taller práctico # 1	105	Figura 9. Red man	29
Taller práctico # 2	106	Figura 10. Red wan	32
Ejercicios de subneteo	106	Figura 11. Red con topología estrella	33
En la empresa XYZ se encuentra	106	Figura 12. Red con topología bus	35
Ejercicios propuestos	109	Figura 13. Red con topología árbol	35
1. En la empresa ABC	109	Figura 14. Red con topología árbol	36

Figura 15. Capas del modelo osi	39	Figura 39. Estándar t568b	54
Figura 16. Capas del modelo tcp/ip	41	Figura 40. Código de colores para la norma t568a y t568b	54
Figura 17. Envio y recepcion de paquetes en los modelos de capas tcp/ip	41	Figura 41. Componentes para comunicaciones inalámbricas	54
Figura 18. Tarjetas de red	42	Figura 42. Porción de red y host de una dirección ip	56
Figura 19. Conección de red con un hub	43	Figura 43. Posiciones y valores de los bits	57
Figura 20. Hubs	43	Figura 44. Transformación de binario a decimal	57
Figura 21. Conexión de una red con un switch	44	Figura 45. Ejemplos de la transformación de binario a decimal	58
Figura 22. Switchs	44	Figura 46. Portada de cisco packet tracer 7.0	59
Figura 23. Routers	44	Figura 47. Interfaz principal de packet tracer	60
Figura 24. Estructura de una dirección ip en sistema binario	44	Figura 48. Barra de menus de packet tracer	60
Figura 25. Estructura de una dirección ip en sistema decimal	45	Figura 49. Pantalla de preferencias de packet tracer	61
Figura 26. Estructura jerárquica de una dirección ip	45	Figura 50. Preferencias administrativas de packet tracer	61
Figura 27. Dirección ip, clase a	46	Figura 51. Insertar descripciones de la red en packet tracer	62
Figura 28. Dirección ip, clase b	46	Figura 52. Descripción de la barra de herramientas	62
Figura 29. Dirección ip, clase c	47	Figura 53. Barra de herramientas de dispositivos	63
Figura 30. Máscara de red, clase a	48	Figura 54. Opciones de simulación	63
Figura 31. Máscara de red, clase b	48	Figura 55. Opciones de vistas	64
Figura 32. Máscara de red, clase c	48	Figura 56. Barra de herramientas de dispositivos	64
Figura 33. Rango global de direcciones ip	49	Figura 57. Vista de diseño	65
Figura 34. Cable stp	51	Figura 58. Despliegue de información de dispositivos	65
Figura 35. Cable utp	51	Figura 59. Pantalla de configuración de un pc	66
Figura 36. Fibra óptica	52	Figura 60. Pantalla del command prompt en packet tracer	67
Figura 37. Cable de fibra óptica	52	Figura 61. Pantalla de configuración de un switch	67
Figura 38. Estándar t568a	53	Figura 62. Configuración de un switch	68

Figura 63. Configuración de interfaces en un switch	69	Figura 87. Conexión entre una red cableada y una inalámbrica (switch - access point)	84
Figura 64. Pantalla de los command - línea de comandos	69	Figura 88. Diagrama de una red hibrida	85
Figura 65. Configuración de interfaces en un router	70	Figura 89. Asignación de direcciones ip	86
Figura 66. Definición de ruteo estático	71	Figura 90. Configuración del gateway	86
Figura 67. Definición de ruteo dinámico rip	72	Figura 91. Configuración de la red inalámbrica	87
Figura 68. Configuración del router		Figura 92. Configuración del wireless router	88
Por línea de comandos	72	Figura 93. Ejecución del comando ping	89
Figura 69. Esquema de una red	73	Figura 94. Esquema de red para la sección inalámbrica	89
Figura 70. Selección de dispositivos en packet tracer	73	Figura 95. Configuración wep en wireless settings	90
Figura 71. Selección de dispositivos de red	74	Figura 96. Conexión del switch con el router	90
Figura 72. Selección de puertos de conexión	75	Figura 97. Configuración de uno de los pcs	91
Figura 73. Selección de puertos en dispositivos	75	Figura 98. Configuración del segundo pc.	91
Figura 74. Conexión de una pc a un switch	76	Figura 99. Esquema final de la red cuando ya existe conexión	91
Figura 75. Apariencia física de un computador		Figura 100. Cortafuegos o firewall de una red	97
En packet tracer	76	Figura 101. Red perimetral o zona desmilitarizada	98
Figura 76. Pantalla de ip configuration	77	Índice de tablas	
Figura 77. Asignación de direcciones ip	78	Tabla 1. Distribución de frecuencias	5
Figura 78. Asignación de direcciones ip	79	Tabla 2. Medios y tipos de transmisión	50
Figura 79. Pantalla de command prompt		Tabla 3. Categorías y uso de los cables	50
Para utilizar el comando ipconfig	79		
Figura 80. Resultado del comando ipconfig	80		
Figura 81. Resultado de ipconfig/all	80		
Figura 82. Utilización del comando ping	81		
Figura 83. Conexión de un pc y un access point	82		
Figura 84. Conexión de una pc y un access point	83		
Figura 85. Utilización del comando ping	83		
Figura 86. Conexión de redes cableadas e inalámbricas	84		

PRÓLOGO

La obra Sistemas de Comunicación y Redes, pretende orientar al lector en el campo de las redes de computadores de forma práctica. Para ello se analizará el estudio de una Red de Área Local (LAN) que emplea la arquitectura de red TCP/IP. Esta arquitectura de red se ha convertido en un estándar para los sistemas de transmisión de datos actuales y proporciona la tecnología base para multitud de aplicaciones: correo electrónico, servidores www, servidores FTP, IRC, comercio electrónico, acceso a bases de datos remotas, tecnología WAP, etc.

Este libro contiene información actualizada y un conjunto de prácticas de laboratorio que servirán como guía para el estudio de las asignaturas de Sistemas de Comunicación, Redes I, Redes II y Seguridad Informática.

La presente guía estará estructurada de seis (6) capítulos, distribuidos de la siguiente manera: en el **Capítulo I, Sistemas de Comunicación**, aquí analizaremos los distintos avances tecnológicos que se fueron sucediendo a lo largo de la historia en el campo de los Sistemas de Comunicación.

El **Capítulo II, Comunicación de Datos con Redes Informáticas**, en este capítulo se analiza el procesamiento de la información y la distribución de la misma a través de medios técnicos que permitan se realice una comunicación a grandes distancias, en el **Capítulo III, Transmisión de Datos en Redes Informática**. Se analiza el proceso que se realiza dentro de una red para transmitir datos de un computador a otro.

Capítulo IV, Cisco Packet Tracer. Esta sección está dedicada específicamente al análisis de la herramienta de simulación Packet Tracer V 7.0. En el **Capítulo V, Seguridad en Redes Informáticas**. Se realiza el análisis de algunos factores importantes en la seguridad de las redes informáticas debido a los constantes ataques que estas sufren los mismos que pueden ser devastadores y ocasionar muchas pérdidas económicas.

El **Capítulo VI**, consiste en una serie de ejercicios con los que se pretende reforzar los conocimientos adquiridos por los lectores de esta obra.

CAPÍTULO I

SISTEMAS DE COMUNICACIÓN

Los sistemas de comunicación actualmente se han convertido en un medio más que necesario, el mundo en el que habitamos se basa precisamente de los principios de la comunicación; es así que, si analizamos los distintos avances tecnológicos que se fueron sucediendo a lo largo de la historia encontraremos que la mayoría de ellos están vinculados a la comunicación.

Entre los años 1970 y 1980 se puede decir que surgió una unión bien notada entre los campos de los ordenadores y los sistemas de comunicaciones, el mismo que desencadenó con un cambio drástico en las TIC's, las empresas y los productos que se derivaban de estos elementos.

Para poder definir un sistema de comunicación como un conjunto de dispositivos interconectados entre sí; es necesario que retomemos un poco de historia al sistema más antiguo de comunicación que tuvo como lugar una oficina de correos, en donde la correspondencia y encomiendas se almacenaban, clasificaba y distribuían hacia sus correspondientes destinos. Se puede decir que esta fue la primera forma de comunicación material que, por su puesto, evolucionó hasta convertirse en lo que hoy conocemos como correo electrónico o e-mail. [1]

El surgimiento de tecnologías emergentes dio paso a que los sistemas de comunicación a través de la www sean hoy los más utilizado por todos: e-mails, chats, mensajes, correo de voz, telefonía IP, foros, etc.; se los puede utilizar a través de una simple máquina, desde la comodidad de nuestros hogares nos comunicamos a cualquier parte del mundo, esta es la razón por la que se asegura que fue el

Internet el fenómeno que logró los avances más significativos en los Sistemas de Comunicación. [2]

Para comenzar con el presente estudio, es necesario considerar un modelo básico de comunicación, el mismo que se representa en un diagrama de bloques, tal como se muestra en la figura 1.



Figura 1. Diagrama de Bloques de un Sistema de Comunicación

El objetivo principal de todo sistema de comunicaciones es intercambiar información. La figura 2, nos presenta un ejemplo en particular de un proceso de comunicación entre una estación de trabajo y un servidor utilizando una red telefonía pública. Los elementos que intervienen en este modelo de comunicación son los siguientes:



Figura 2. Modelo simplificado de un Sistema de Comunicación

Los elementos que forman parte de este modelo de comunicación son:

- **La Fuente:** Es el dispositivo que genera los datos que se van a transmitir, por ejemplo: puede ser un servidor o una estación de trabajo.

- **El Transmisor:** Originalmente los datos generados por la fuente no se transmiten tal y como son generados. Ahí es cuando entra a funcionar el transmisor, el mismo que transforma y codifica la información, generando señales electromagnéticas susceptibles de ser transmitidas a través de algún medio o canal. Por ejemplo, el módem: convierte los diferentes grupos de bits generadas por un

computador personal (señal digital) y las transforma en señales analógicas que pueden ser transmitidas a través de la red de telefónica.

- **El sistema de transmisión:** Este sistema puede ser desde la más sencilla línea de transmisión (un cable) hasta una compleja red que conecte a la fuente con el destino.
- **El receptor:** Acepta la señal proveniente del sistema de transmisión y la transforma de tal manera que pueda ser manejada por el dispositivo de destino. Por ejemplo, un módem captará la señal analógica de la red o línea de transmisión y la convertirá en una cadena de bits.
- **El Destino:** Recibe los datos del receptor.

TRANSMISIÓN DE DATOS¹

La comunicación es un concepto amplio que engloba a cualquier sistema de transferencia de información entre dos puntos, en este caso la información está contenida en algunos de los parámetros (amplitud, frecuencia) de una señal eléctrica. [3]

Los medios más habituales de un sistema de comunicación son:

- Cables eléctricos (par trenzado, coaxial)
- Ondas electromagnéticas (Radio, enlaces de microondas)
- Señales Ópticas (infrarrojas)

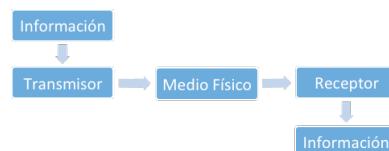


Figura 3. Transmisión de la Información a Distancia

TRANSMISIÓN POR RADIOFRECUENCIA

La transmisión de datos por radio frecuencia es un modelo de telecomunicación que se realiza a través de ondas radioeléctricas. Se entiende por radiofrecuencia al conjunto de frecuencias situadas

¹ El tema más amplio se lo puede encontrar en el libro "Comunicaciones y Redes de Computadoras" de MANGAÑA, Lizarrondo Eduardo, Person Education, Mexico, Cap. II, Páginas 9-12.

entre los 3hz y los 300 Ghz, correspondiente a la parte menos energética del espectro electromagnético. [10]

Los elementos más sobresalientes en un proceso de radiocomunicación son:

- **Frecuencia:** es la magnitud que mide el número de veces que una señal se repite en una cantidad de tiempo y su unidad es Hz.
- **Longitud de onda:** es la distancia que una señal recorre en un intervalo de tiempo comprendido entre dos máximos consecutivos y que es inversamente proporcional a la frecuencia de la señal.

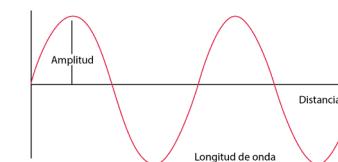


Figura 4. Longitud de onda

Asignación de bandas y frecuencias.

En base a su frecuencia y longitud de onda se asignan algunas bandas para los sistemas de radiocomunicación.

VLF	LF	MF	HF	VHF	UHF	SHF	EHF
Muy Baja Frecuencia	Baja Frecuencia	Media Frecuencia	Alta Frecuencia	Muy Alta Frecuencia	Ultra Alta Frecuencia	Super Alta Frecuencia	Extrema Alta Frecuencia
Rangos de Frecuencia							
3 - 30	30 - 300	300 - 3000	3 - 30	30 - 300	300 - 3000	3 - 30	30 - 300
Radionavegación Servicio Móvil Marítimo	Frecuencias Patrón	Radiodifusión Sonora en AM	Telefonía Fija y Móvil Radioaficionados Radiodifusión en Onda Corta	Telefonía Fija y Móvil Radioaficionados Radio difusión Sonora FM Televisión Abierta Radionavegación	Telefonía Fija y Móvil Televisión abierta Radiolocalización	Telefonía Fija y Móvil Radiodifusión por Satélite Radionavegación	Telefonía Fija

Tabla 1. Distribución de frecuencias

SISTEMAS INFRARROJOS

Los Sistemas de comunicación Infrarrojos, radiación infrarroja o radiación térmica es un tipo de radiación electromagnética de mayor longitud de onda que la luz visible, pero menor que la de las microondas.

El nombre de infrarrojo, quiere decir “por debajo del rojo”, se origina al dividir la luz solar en diferentes colores por medio de un prisma que separa la luz en su espectro de manera que a ambos extremos aparecen visibles. Aunque estas experiencias fueron realizadas por Isaac Newton, William Herschel quienes en el año 1800 observaron que se podía recibir radiación debajo del rojo al situar medidores de calor en las diferentes zonas no visiblemente irradiadas por el espectro de luz. Su longitud de onda, entre 700 nanómetros y un milímetro, es la siguiente en longitud al rojo, el color de longitud de onda más larga de la luz visible. [10]

Si queremos hablar de comunicaciones inalámbricas lo primero que pensamos es en señales de radio y nos olvidamos que realmente la comunicación se realiza con equipos electrónicos que utilizan una tecnología muy común y sofisticada, un ejemplo muy común lo tenemos cuando operamos un control remoto, lo que en realidad hace es comunicarse por medio de luz en gama de los infrarrojos.

Este tipo de enlaces puede servir también para enviar datos a un robot desde los sensores, establecer y detectar balizas en el entorno o para que una persona pueda dar órdenes utilizando un aparato convencional sea este radio o televisión.

Características de los sistemas de comunicación infrarrojos.

Los sistemas de comunicaciones infrarrojos ofrecen muchas ventajas significativas con respecto a los sistemas de radio frecuencia. Al ser su medio de comunicación la luz, los sistemas Infrarrojos de comunicaciones cuentan con un canal con un ancho de banda es muy grande sin ningún tipo de regulación, algo que también debemos considerar es que los sistemas de comunicación infrarrojos son inmunes a interferencias y ruido de tipo radioeléctrico. [9]

La luz infrarroja no puede atravesar paredes, se puede manejar al menos un enlace en cada habitación de un edificio sin que existe interferencia con lo demás, esto permite una alta densidad de recursos del sistema, lo que permite obtener una gran capacidad por unidades de área, lo que hace que las señales infrarrojas sean difíciles de captar por escuchas clandestinas; la única manera de que las señales infrarrojas pudieran ser captadas si permiso, es atravesar las ventanas de una habitación, pero si estas están cubiertas por con persianas o cortinas se evitara este problema de inseguridad.

Clasificación de los sistemas de comunicación infrarrojos

En general, los sistemas Infrarrojos (IR), se pueden clasificar de acuerdo a dos criterios:

- El primer criterio: es el grado de direccionalidad del transmisor y del receptor, así podemos encontrar enlaces dirigidos y enlaces no dirigidos.

Los enlaces dirigidos son aquellos que emplean transmisores y receptores altamente direccionales, los cuales deben apuntar uno al otro o hacia un área común (generalmente suele ser el techo de la habitación) para establecer el enlace.

Los enlaces no dirigidos son aquellos en los que emplean transmisores y receptores de gran ángulo, lo que permite disminuir la necesidad de tal apuntamiento directo. En los enlaces directos se maximiza la eficiencia de potencia, ya que esta se dirige en un rango muy pequeño de direcciones, y por lo mismo se minimizan las pérdidas de propagación y la recepción de ruido causado por la luz ambiental. Al ser mínima la necesidad de apuntamiento, en un enlace no dirigido se facilita su reconfiguración.

- El segundo criterio de clasificación está relacionado con la existencia o no de una línea de vista entre el transmisor y el receptor.

En los enlaces de línea o punto de vista, la luz emitida por el transmisor llega directamente al receptor. En los enlaces sin línea o punto de vista, la luz que sale del transmisor para llegar al receptor generalmente después de haberse reflejado difusamente en una o varias superficies.

En un enlace de línea o punto de vista, se utiliza con mayor eficiencia la potencia de las señales y se minimiza la distorsión por multitrayectorias. Y, con un enlace sin línea de vista, se obtiene una mayor facilidad de uso, mayor movilidad, y robustez, o sea que el sistema siga operando aun cuando existan obstrucciones causadas por personas u objetos que se interpongan entre el transmisor y el receptor. [6]



*Figura 5. Comunicación por infrarrojo
Fuente: www.drajonjar.com*

Modos de transmisión infrarroja

A la hora de realizar una transmisión infrarroja, las estaciones pueden utilizar tres métodos para ello, estos son: punto a punto, casi-difuso y difuso.

• Sistemas punto a punto

Un enlace punto a punto, consiste en que el transmisor concentra su potencia en una pequeña región del espacio, de esta manera, el receptor capta luz infrarroja, produciéndose así un mínimo de distorsión por multitrayectorias y de ruido causado por las fuentes de luz de ambiente.

Las combinaciones de estas características dan como resultado altas razones de transmisión y grandes alcances. Además de esto, los sistemas punto a punto son relativamente baratos y simples.

Un ejemplo de sistemas infrarrojos punto a punto son los enlaces intersatelitales, en donde las condiciones del ambiente permiten

que con potencias relativamente pequeñas se tengan muy grandes alcances de transmisión.

• Sistema casi-difuso

En el modo casi-difuso, el tipo de emisión es radial; lo que quiere decir que la emisión se produce en todas las direcciones, al contrario que en el modo punto a punto. Para conseguir esto, lo que se hace es transmitir hacia distintas superficies reflectantes, las cuales redirigirán el haz de luz hacia las estaciones receptoras. De esta forma, se rompe la limitación impuesta en el modo punto a punto de la direccionalidad del enlace.

En función de cómo sea la superficie reflectante, se podrán distinguir dos tipos de reflexión: pasiva y activa. **En la reflexión pasiva**, la superficie reflectante refleja la señal, debido a las cualidades reflexivas del material. **En la reflexión activa**, por el contrario, el medio reflectante no sólo refleja la señal, sino que además la amplifica. En este caso, el medio reflectante se conoce como satélite. Se debe destacar que, mientras la reflexión pasiva es más flexible y barata, esta requiere de una mayor potencia de emisión por parte de las estaciones, debido al hecho de no contar con etapa repetidora. [5]

• Sistemas difusos

Los sistemas difusos tienen más altas perdidas de propagación de señal que sus contrapartes de línea de vista, ya que se requiere de altas potencias de transmisión y un receptor que tenga una gran área de colección de luz.

Los transmisores difusos típicos emplean varios LEDs, los cuales son orientados en diferentes direcciones, lo que permite proveer una diversidad de trayectorias de propagación de la señal. Cuando transmiten, por lo general emiten una potencia óptica promedio en el intervalo de 100 a 500 mW, esto causa un consumo de potencia eléctrica más alto que el de un transmisor típico IrDA. Los receptores difusos típicos emplean como detectores diodos pin de silicio encapsulado en lentes hemisféricos, los cuales concentran la luz y tienen un amplio campo visual. [5]

SISTEMAS SATELITALES²

Los Sistemas de comunicación satelital que antes era inalcanzable para el común de las personas, ahora son mucho más accesible por la demanda del público, debido a la movilidad y autonomía que esta presta al usuario en cualquier lugar del mundo por más remoto que este sea, lo que permite liberar al cliente de las restricciones.

Desde el año 1970 la comunicación satelital o por satélite, ha ido tomando fuerza; inicialmente no fue muy popular debido a su elevado costo y por tanto su uso eran con fines gubernamentales, científicos o militares; pero a medida que las comunicaciones fueron tomando importancia y popularidad, se empezaron a enviar más satélites al espacio ya con fines comunicativos, permitiendo un gran avance en el tema de las telecomunicaciones o comunicaciones a distancia, permitiendo que se transmitiera información de un lugar de la tierra a otro lejano en segundos. [3]

Un satélite actúa básicamente como un repetidor situado en el espacio: recibe las señales enviadas desde la estación terrestre y las reemite a otro satélite o de vuelta a los receptores terrestres. Existen dos tipos de satélites de comunicaciones, los mismos que son:

- **Satélites pasivos.**- Se limitan a reflejar la señal recibida sin llevar a cabo ninguna otra tarea.
- **Satélites activos.**- Amplifican las señales que reciben antes de reemitirlas hacia la Tierra. Son los más habituales.

Los satélites son puestos en órbita mediante cohetes espaciales que los sitúan circundando la Tierra a distancias relativamente cercanas fuera de la atmósfera. Los tipos de satélites según sus órbitas son:

- **Satélites LEO.**- (Low Earth Orbit, que significa órbitas bajas). Orbitan la Tierra a una distancia de 160-2000 km y su velocidad les permite dar una vuelta al mundo en 90 minutos. Se usan para proporcionar datos geológicos sobre movimiento de placas terrestres y para la industria de la telefonía por satélite.
- **Satélites MEO.**- (Medium Earth Orbit, órbitas medias). Son satélites con órbitas medianamente cercanas, de unos 10.000 km.

²"Comunicaciones y Redes de Computadoras" de MANGAÑA, Lizarrondo Eduardo, Person Education, Mexico, Cap. IV, Paginas 28-31.

Su uso se destina a comunicaciones de telefonía y televisión, y a las mediciones de experimentos espaciales.

• **Satélites HEO.**- (Highly Elliptical Orbit, órbitas muy elípticas). Estos satélites no siguen una órbita circular, sino que su órbita es elíptica. Esto supone que alcanzan distancias mucho mayores en el punto más alejado de su órbita. A menudo se utilizan para cartografiar la superficie de la Tierra, ya que pueden detectar un gran ángulo de superficie terrestre.

• **Satélites GEO.**- Tienen una velocidad de traslación igual a la velocidad de rotación de la Tierra, lo que supone que se encuentren suspendidos sobre un mismo punto del globo terrestre. Por eso se llaman satélites geoestacionarios. Para que la Tierra y el satélite igualen sus velocidades es necesario que este último se encuentre a una distancia fija de 35.800 km sobre el Ecuador. Se destinan a emisiones de televisión y de telefonía, a la transmisión de datos a larga distancia, y a la detección y difusión de datos meteorológicos.



Figura 6. Sistema de comunicación satelital
Fuente: www.warnyu.info

CAPÍTULO II

COMUNICACIÓN DE DATOS CON REDES INFORMÁTICAS

El procesamiento de la información y la distribución de la misma convergen, ambas hacia las telecomunicaciones, las mismas que corresponden al conjunto de medios técnicos que permiten se realice una comunicación a grandes distancias para poder transmitir información sea esta sonora o visual por ondas electromagnéticas o a través de otros medios, los cuales permiten que la transmisión se realice de forma analógica, digital o mixta, pero la misma se realiza siempre de forma transparente para el usuario. [3]

Para 1940, los computadores eran grandes dispositivos electromecánicos que eran propensos a sufrir fallas. En 1947, la invención del transistor semiconductor permitió la creación de computadores más pequeños y confiables. Para los años de 1950 los computadores mainframe, funcionaban con programas en tarjetas perforadas, los mismos que comenzaron a ser utilizados habitualmente por las grandes instituciones especialmente privadas. A fines de esta década, se crea el circuito integrado, que combinaba muchos y, en la actualidad, millones de transistores en un pequeño semiconductor.

Para la década de 1960, los mainframes con terminales o estaciones de trabajo eran comunes, y los circuitos integrados comenzaron a ser utilizados de forma generalizada. Hacia la década de 1970, se inventaron computadores mucho más pequeños, denominados minicomputadores. Sin embargo, estos seguían siendo muy voluminosos en comparación con los equipos que conocemos en la actualidad. Ya para 1977, la Compañía Apple Computer presentó el microcomputador, conocido también como computador personal, de uso sencillo, de arquitectura abierta y la posterior microminiaturización de los circuitos integrados dieron como

resultado el uso difundido de los computadores personales en hogares y empresas. [2]

A mediados de los 80 los usuarios con computadores autónomos comenzaron a usar dispositivos “módem” para conectarse con otros computadores y compartir archivos. Esta forma de conexión se denominaba comunicación punto-a-punto o de acceso telefónico. El concepto se expandió a través del uso de computadores que funcionaban como punto central de comunicación en una conexión de acceso telefónico. La desventaja de este tipo de sistema era la necesidad de un módem por cada conexión al computador. Si cinco personas se conectaban simultáneamente, hacían falta cinco módems conectados a cinco líneas telefónicas diferentes.

A medida que crecía el número de usuarios interesados, el sistema no pudo soportar la demanda. Es así que a partir de la década de 1960 y durante las décadas de 1970, 1980 y 1990, el Departamento de Defensa de Estados Unidos desarrolló redes de gran extensión y alta confiabilidad, para uso militar y científico. Esta tecnología era diferente de la comunicación punto-a-punto ya que permitía la Internetworking de varios computadores mediante diferentes rutas. La red en sí determinaba la forma de transferir datos de un computador a otro. En lugar de poder comunicarse con un solo computador a la vez, se podía acceder a varios computadores mediante la misma conexión. [2]

REDES INFORMÁTICAS

Las redes informáticas son un conjunto de ordenadores y otros dispositivos, conectados entre sí, por un medio físico (cable) o de forma inalámbrica (Wi-Fi o Bluetooth). El objetivo principal de una red es compartir sus archivos o recursos (impresoras, etc.)

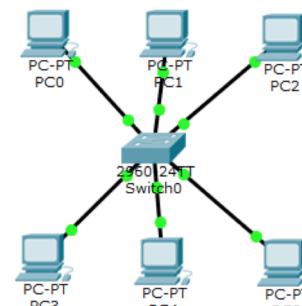


Figura 7. Ejemplo de una red de computadores

TIPOS DE REDES³.

Según la dimensión de la red, podemos distinguir los siguientes tipos de redes:

- **LAN** (Local Área Network): Red de Área Local.
- **MAN** (Metropolitan Area Network)
- **WAN** (Wide Area Network)

REDES LAN

Una LAN (Local Area Network, red de área local) es un grupo de equipos pertenecientes a una misma organización y conectados dentro de un área geográfica pequeña a través de una red, generalmente con la misma tecnología, la más utilizada es Ethernet.

Una red de área local es una red en su versión más simple. La velocidad de transferencia de datos en una red de área local puede alcanzar hasta 10 Mbps (por ejemplo, en una red Ethernet) y 1 Gbps (por ejemplo, en FDDI o Gigabit Ethernet). Una red de área local puede contener 100, o incluso 1.000 usuarios.

Según los servicios que proporciona, se pueden distinguir dos modos de funcionamiento de una LAN: en una red “de igual a igual” (P2P), en la que la comunicación se establece de un equipo a otro sin la necesidad de un equipo central y donde cada equipo tiene la misma función; y en un entorno “cliente/servidor”, en el que un equipo central se encarga de brindar los servicios de red a los usuarios.

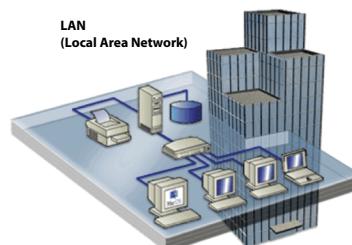


Figura 8. Red LAN

Fuente: <http://redesdedatosinfo.galeon.com>

REDES MAN

Son las siglas de **Metropolitan Area Network**, que puede traducirse como **Red de Área Metropolitana**. Una red MAN es aquella que, a través de una conexión de alta velocidad, ofrece cobertura en una zona geográfica extensa (como una provincia, ciudad o cantón).

Con una red MAN es posible compartir e intercambiar todo tipo de datos (texto, vídeos, audio, etc.) mediante cable de par trenzado o fibra óptica. Este tipo de red supone una evolución de las redes LAN, ya que favorece la interconexión en una región más amplia, cubriendo una mayor superficie.

Las redes MAN pueden ser públicas o privadas. Estas redes se desarrollan con dos buses unidireccionales, lo que quiere decir que cada uno actúa independientemente del otro respecto a la transferencia de datos. Cuando se utiliza fibra óptica, la tasa de error es menor que si se usa cable de cobre, siempre que se comparan dos redes de iguales dimensiones. Cabe mencionar que ambas opciones son seguras dado que no permiten la lectura o la alteración de su señal sin que se interrumpa el enlace físicamente.

Entre los usos de las redes MAN, puede mencionarse la interconexión de oficinas dispersas en una ciudad, pero pertenecientes a una misma corporación, el desarrollo de un sistema de videovigilancia y el despliegue de servicios de VoIP.

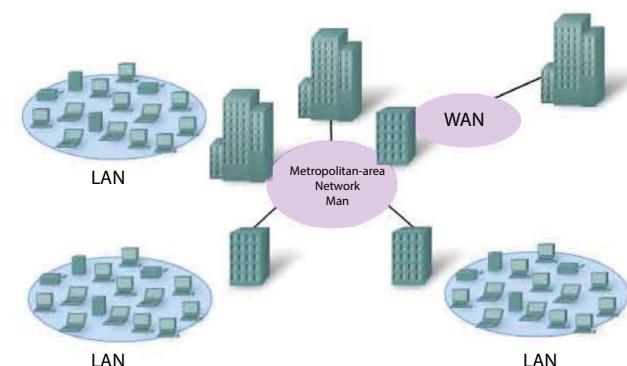


Figura 9. Red MAN

Fuente: <http://redesdedatosinfo.galeon.com>

³ Tennenbaum Andrew, Redes de Computadoras, 5ta edición Person Education.

REDES WAN

WAN es la sigla de Wide Area Network, una expresión en lengua inglesa que puede traducirse como Red de Área Amplia. Esto quiere decir que la red WAN es un tipo de red que cubre distancias de entre unos 100 y unos 1.000 kilómetros, lo que le permite brindar conectividad a varias ciudades o incluso a un país entero.

Las redes WAN pueden ser desarrolladas por una empresa o una organización para un uso privado, o incluso por un proveedor de Internet (ISP, Internet Service Provider) para brindar conectividad a todos sus clientes.

Por lo general, las redes WAN funcionan punto a punto, por lo que puede definirse como una red de paquete commutado. Estas redes, por otra parte, pueden utilizar sistemas de comunicación de radio o satelitales.

Entre los componentes de la red WAN aparecen los equipos que se dedican a ejecutar los programas de usuario y que reciben el nombre de hosts; los enruteadores que concretan la división entre las líneas de transmisión y los elementos de commutación; y las subredes formadas a partir de la interconexión de varios hosts.

Su velocidad de transmisión se encuentra entre 1 Mbps y 1 Gbps, aunque este último límite puede cambiar drásticamente con los avances tecnológicos. La red WAN se utiliza para establecer comunicaciones privadas y los principales medios de transmisión en los que se basa son la fibra óptica y el cable de teléfono. Ofrece una gran versatilidad para hacer modificaciones en el software y en el hardware de los equipos que vincula y además permite establecer conexiones con otras redes.

Ventajas de la red WAN

- Permite usar un software especial para que entre sus elementos de red coexistan mini y macrocomputadoras;
- No se limita a espacios geográficos determinados;
- Ofrece una amplia gama de medios de transmisión, como ser enlaces satelitales.

Desventajas de la red WAN

- Se deben emplear equipos con una gran capacidad de memoria, ya que este factor repercute directamente en la velocidad de acceso a la información;
- No se destaca por la seguridad que ofrece a sus usuarios. Los virus y la eliminación de programas son dos de los males más comunes que sufre la red WAN.

Existen varios tipos de red WAN, y tres de ellos se agrupan bajo la clasificación de red commutada (en física, la commutación consiste en el cambio del destino de una señal o de una corriente eléctrica):

• Por circuitos

Para establecer una comunicación, este tipo de red WAN exige que se realice una llamada y recién cuando la conexión se efectúa cada usuario dispone de un enlace directo.

• Por mensaje

Sus commutadores suelen ser computadoras que cumplen la tarea de aceptar el tráfico de cada terminal que se encuentre conectado a ellas. Dichos equipos evalúan la dirección que se encuentra en la cabecera de los mensajes y pueden almacenarla para utilizarla más adelante. Cabe mencionar que también es posible borrar, redirigir y responder los mensajes en forma automática.

• Por paquetes

Se fracciona cada mensaje enviado por los usuarios y se transforman en un número de pequeñas partes denominadas paquetes, que se vuelven a unir una vez llegan al equipo de destino, para reconstruir los datos iniciales. Dichos paquetes se mueven por la red independientemente, y esto repercute positivamente en el tráfico, además de facilitar la corrección de errores, ya que en caso de fallos sólo se deberán reenviar las partes afectadas.

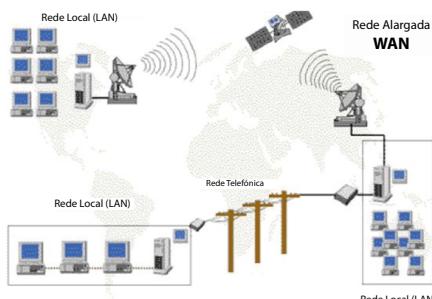


Figura 10. Red WAN

Fuente: <http://redesdedatosinfo.galeon.com>

TOPOLOGÍAS DE REDES INFORMÁTICAS

Las topologías de redes informáticas se definen como un mapa físico o lógico de una red para intercambiar datos, es la forma en que está diseñada la red, sea en el plano físico o lógico. [1]

En función de la disposición física de los cables y las conexiones, podemos tener diferentes topologías de red, en la actualidad las más comunes y utilizadas son:

Topología en estrella

Se considera una topología tipo estrella cuando todos y cada uno de los nodos de la red, se conectan a un concentrador switch o hub. Los datos en estas redes fluyen del emisor hasta el concentrador, este realiza todas las funciones de la red, además actúa como amplificador de los datos.

Todos los elementos de la red se encuentran conectados directamente mediante un enlace punto a punto al nodo central de la red, quien se encarga de gestionar las transmisiones de información por toda la estrella. Obviamente, todas las tramas de información que circulen por la red deben pasar por el nodo principal, con lo cual un fallo en él provoca la caída de todo el sistema.

Por otra parte, un fallo en un determinado cable sólo afecta al nodo asociado a él; si bien esta topología obliga a disponer de un cable propio para cada terminal adicional de la red. La topología de Estrella es una buena elección siempre que se tenga varias

unidades dependientes de un procesador, esta es la situación de una típica mainframe, donde el personal requiere estar accesando frecuentemente esta computadora. En este caso, todos los cables están conectados hacia un solo sitio, esto es, un panel central.

Equipos como: unidades de multiplexaje, concentradores y pares de cables, solo reducen los requerimientos de cableado sin eliminarlos y produce una reducción en los costos para esta topología. Resulta económico la instalación de un nodo cuando se tiene bien planeado su establecimiento, ya que este requiere de un cable desde el panel central, hasta el lugar donde se desea instalarlo.

Ventajas de la topología estrella:

- Gran facilidad de instalación
- Posibilidad de desconectar elementos de red sin causar problemas.
- Facilidad para la detección de fallo y su reparación.

Inconvenientes de la topología de estrella.

- Requiere más cable que la topología de BUS.
- Un fallo en el concentrador provoca el aislamiento de todos los nodos a él conectados.
- Se requiere la compra de hubs o concentradores (switch o routers).

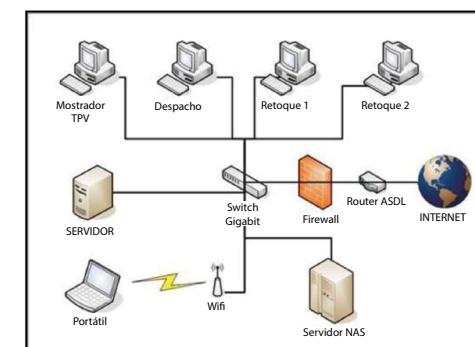


Figura 11. Red con topología estrella

Fuente: <http://redesdedatosinfo.galeon.com>

Topología de BUS

Esta topología, consiste en un cable con un terminador en cada extremo del que se conectan los nodos de la red, ya que todos están unidos por un único cable. Este cable recibe el nombre de “Backbone Cable”. Tanto Ethernet como LocalTalk pueden utilizar esta topología.

En esta topología, los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable. Las tramas de información emitidas por un nodo (terminal o servidor) se propagan por todo el bus (en ambas direcciones), alcanzado a todos los demás nodos. Cada nodo de la red se debe encargar de reconocer la información que recorre el bus, para así determinar cuál es la que le corresponde, la destinada a él.

Es el tipo de instalación más sencillo y un fallo en un nodo no provoca la caída del sistema de la red. Por otra parte, una ruptura del bus es difícil de localizar (dependiendo de la longitud del cable y el número de terminales conectados a él) y provoca la inutilidad de todo el sistema.

El bus es la parte básica para la construcción de redes Ethernet y generalmente consiste de algunos segmentos de bus unidos ya sea por razones geográficas, administrativas u otras.

Ventajas de la topología de BUS:

- Es más fácil conectar nuevos nodos a la red.
- Requiere menos cable que una topología estrella.

Desventajas de la topología de BUS:

- Toda la red se caería si hubiera una ruptura en el cable principal.
- Se requiere terminadores.
- Es difícil detectar el origen de un problema cuando toda la red cae.
- No se debe utilizar como única solución en un gran edificio.

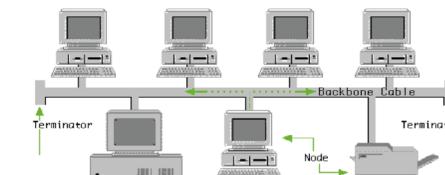


Figura 12. Red con topología bus
Fuente: <http://www.cintel.org.com.co>

Topología de Árbol

La topología tipo árbol, combina las características de la topología estrella con la topología tipo bus. Consiste en un conjunto de subredes estrella conectadas a un bus. Esta topología facilita el crecimiento de la red. Esta estructura de red se utiliza en aplicaciones de televisión por cable, sobre la cual podrían basarse las futuras estructuras de redes que alcancen los hogares. También se ha utilizado en aplicaciones de redes locales analógicas de banda ancha.

Ventajas de la topología de árbol:

- Cableado punto a punto para segmentos individuales.
- Soportado por multitud de vendedores de software y de hardware.

Desventajas de la topología de árbol:

- La medida de cada segmento viene determinada por el tipo de cable utilizado.
- Si se viene abajo el segmento principal todo el segmento se viene abajo con él.
- Es más difícil su configuración.

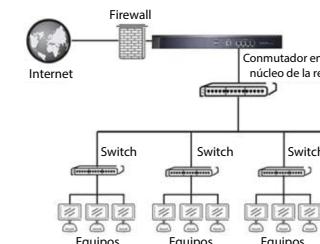


Figura 13. Red con topología árbol
Fuente: <http://www.cintel.org.com.co>

CAPÍTULO III

TRANSMISIÓN DE DATOS EN REDES INFORMÁTICAS

Para que se pueda realizar una transmisión de datos de un computador a otro, estos datos son empaquetados y depositados en la red para que estos puedan ser leídos en la estación destino, las estaciones destino deben estar siempre a la escucha para identificar el momento exacto en el que llega un paquete, ya que existen casos en los que dos o más estaciones de trabajo intentan enviar un paquete de datos al mismo tiempo, lo que produce un error llamado colisión, y obliga a que las dos terminales intenten enviar de nuevo el paquete cuando la red este libre. [3]



Figura 14. Red con topología árbol
Fuente: <http://www.cintel.org.com.co>

PROTOCOLOS DE RED

Los protocolos de red son reglas y especificaciones técnicas que siguen los dispositivos conectados en red para poder comunicarse y transferir información unos a otros (es el lenguaje de comunicación común que utilizan para entenderse).

El protocolo más utilizado actualmente tanto en redes locales como en comunicación a través de Internet, es el TCP/IP. Este protocolo es en realidad un conjunto de protocolos que son los que realmente proporciona los servicios.

Dentro de las redes informáticas se conoce bajo el nombre de protocolo al lenguaje, que es un conjunto de reglas formales, que permiten la comunicación de distintas computadoras entre sí, entre ellos tenemos:

- **TCP / IP:** Protocolo definido como el conjunto de protocolos básicos para la comunicación de redes y es por medio de él que se logra la transmisión de información entre computadoras pertenecientes a una red. Gracias al protocolo TCP/IP los distintos ordenadores de una red se logran comunicar con otros diferentes y así enlazar a las redes físicamente independientes en la red virtual conocida bajo el nombre de Internet. Este protocolo es el que provee la base para los servicios más utilizados como por ejemplo transferencia de ficheros, correo electrónico y login remoto.
- **TCP (Transmision Control Protocol):** este es un protocolo orientado a las comunicaciones y ofrece una transmisión de datos confiable. El TCP es el encargado del ensamblaje de datos provenientes de las capas superiores hacia paquetes estándares, asegurándose que la transferencia de datos se realice correctamente.
- **HTTP (Hypertext Transfer Protocol):** este protocolo permite la recuperación de información y realizar búsquedas indexadas que permiten saltos intertextuales de manera eficiente. Por otro lado, permiten la transferencia de textos de los más variados formatos, no sólo HTML. El protocolo HTTP fue desarrollado para resolver los problemas surgidos del sistema hipermedial distribuidos en diversos puntos de la red.
- **FTP (File Transfer Protocol):** este es utilizado a la hora de realizar transferencias remotas de archivos. Lo que permite es enviar archivos digitales de un lugar local a otro que sea remoto o al revés. Generalmente, el lugar local es la PC mientras que el remoto el servidor.
- **SSH (Secure Shell):** este fue desarrollado con el fin de mejorar la seguridad en las comunicaciones de internet. Para lograr esto el SSH elimina el envío de aquellas contraseñas que no son cifradas y codificando toda la información transferida.

- **UDP (User Datagram Protocol):** el protocolo de datagrama de usuario está destinado a aquellas comunicaciones que se realizan sin conexión y que no cuentan con mecanismos para transmitir datagramas. Esto se contrapone con el TCP que está destinado a comunicaciones con conexión. Este protocolo puede resultar poco confiable excepto si las aplicaciones utilizadas cuentan con verificación de confiabilidad.
- **SNMP (Simple Network Management Protocol):** este usa el Protocolo de Datagrama del Usuario (PDU) como mecanismo para el transporte. Por otro lado, utiliza distintos términos de TCP/IP como agentes y administradores en lugar de servidores y clientes. El administrador se comunica por medio de la red, mientras que el agente aporta la información sobre un determinado dispositivo.
- **TFTP (Trivial File Transfer Protocol):** este protocolo de transferencia se caracteriza por su sencillez y falta de complicaciones. No cuenta con seguridad alguna y también utiliza el Protocolo de Datagrama del Usuario como mecanismo de transporte.
- **SMTP (Simple Mail Transfer Protocol):** este protocolo está compuesto por una serie de reglas que rige la transferencia y el formato de datos en los envíos de correos electrónicos. SMTP suele ser muy utilizado por clientes locales de correo que necesiten recibir mensajes de e-mail almacenados en un servidor cuya ubicación sea remota.
- **ARP (Address Resolution Protocol):** por medio de este protocolo se logran aquellas tareas que buscan asociar a un dispositivo IP, el cual está identificado con una dirección IP, con un dispositivo de red, que cuenta con una dirección de red física. ARP es muy usado para los dispositivos de redes locales Ethernet. Por otro lado, existe el protocolo RARP y este cumple la función opuesta a la recién mencionada.
- **POP (Post Office Protocol):** protocolo que almacena los mensajes de correo electrónico en un servidor de correo para su posterior lectura.

- **TELNET:** permite la conexión a una aplicación remota desde otro ordenador.

MODELOS DE REFERENCIA DE CAPAS DE RED

A la hora de describir la estructura y función de los protocolos de comunicación se suele recurrir a modelos de arquitectura de redes, entre los más comunes tenemos OSI y TCP/IP.

Modelo OSI⁴

Este modelo está constituido por 7 capas las mismas que definen las funciones de los protocolos de comunicaciones. Cada capa del modelo representa una función realizada cuando los datos son transferidos entre aplicaciones cooperativas a través de una red intermedia.

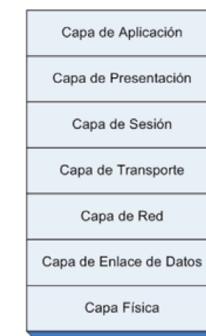


Figura 15. Capas del modelo OSI

En una capa no se define un único protocolo sino una función de comunicación de datos que puede ser realizada por varios protocolos. Por ejemplo, un protocolo de transferencia de ficheros y otro de correo electrónico facilitan, ambos, servicios de usuario y son los dos partes de la capa de aplicación.

Cada protocolo se comunica con su igual en la capa equivalente de un sistema remoto.

⁴ Tennenbaum Andrew, Redes de Computadoras, 5ta Edición, Editorial Person

Cada protocolo solo ha de ocuparse de la comunicación con su gemelo, sin preocuparse de las capas superior o inferior. Sin embargo, también debe haber acuerdo en cómo se envían los datos de capa en capa dentro de un mismo sistema, ya que cada capa está implicada en el envío de datos.

Las capas superiores delegan en las inferiores para la transmisión de los datos a través de la red subyacente. Los datos descenden por la pila, de capa en capa, hasta que son transmitidos a través de la red por los protocolos de la capa física. En el sistema remoto, irán ascendiendo por la pila hasta la aplicación correspondiente.

La ventaja de esta arquitectura es que, al aislar las funciones de comunicación de la red en capas, minimizamos el impacto de cambios tecnológicos en el juego de protocolos, es decir, podemos añadir nuevas aplicaciones sin cambios en la red física y también podemos añadir nuevo hardware a la red sin tener que reescribir el software de aplicación.

Modelo TCP/IP.

Este modelo de arquitectura de protocolos es más simple que el modelo OSI, como resultado de la agrupación de diversas capas en una sola o bien por no usar alguna de las capas propuestas en dicho modelo de referencia.

Así, por ejemplo, la capa de presentación desaparece debido a que las funciones a definir en ellas se incluyen en las propias aplicaciones. Lo mismo sucede con la capa de sesión, cuyas funciones son incorporadas a la capa de transporte en los protocolos TCP/IP. Finalmente, la capa de enlace de datos no suele usarse en dicho paquete de protocolos.

De esta forma nos quedamos con una modelo en cuatro capas, tal y como se ve en la siguiente figura:



Figura 16. Capas del modelo TCP/IP

Al igual que en el modelo OSI, los datos descenden por la pila de protocolos en el sistema emisor y la escalan en el extremo receptor. Cada capa de la pila añade a los datos a enviar a la capa inferior, información de control para que el envío sea correcto. Esta información de control se denomina cabecera, pues se coloca precediendo a los datos. A la adición de esta información en cada capa se le denomina encapsulación. Cuando los datos se reciben tiene lugar el proceso inverso, es decir, según los datos ascienden por la pila, se van eliminando las cabeceras correspondientes. [4]

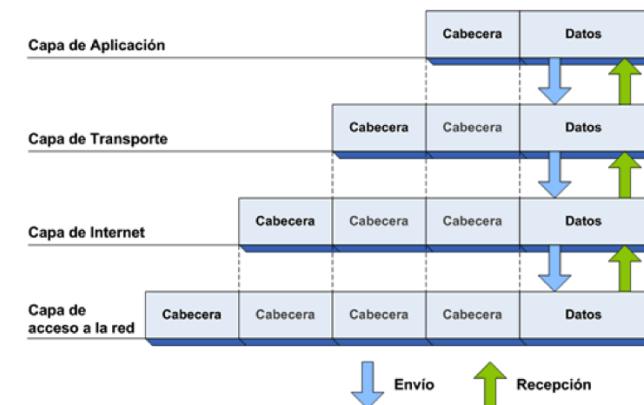


Figura 17. Envío y recepción de paquetes en los modelos de capas TCP/IP

HARDWARE DE CONEXIÓN DE REDES

TARJETA DE RED

Para poder trabajar en red, es necesario instalar, en todos los ordenadores, unas tarjetas de red, también llamadas adaptadores de red o NIC (Network Interface Card). Normalmente se instalan en las ranuras de expansión de la placa madre del ordenador. Cada tarjeta de red permite configurar el ordenador donde se instala y añadirlo a la red de área local, independientemente del sistema operativo que tenga.



Figura 18. Tarjetas de red

Una vez instalada y configurada la tarjeta de red, podremos comunicar nuestro computador con otros computadores a través de los medios de transmisión. Estos medios de transmisión pueden ser cables o bien pueden ser inalámbricos. Una conexión de red nos permite enlazar nuestro computador con otra red existente o al Internet. Por cada tarjeta de red instalada en nuestro ordenador, dispondremos de una conexión de red.

LA DIRECCIÓN MAC

La dirección MAC (Media Access Control) es el identificador único de 6 bytes (48 bits) que corresponde a una tarjeta de red, es individual, cada dispositivo tiene su propia dirección MAC, de tal manera que no pueda haber dos tarjetas con el mismo identificador MAC.

Los primeros 24 bits de la MAC viene determinada y configurada por el IEEE (Institute of Electrical and Electronics Engineers) y se denominan OUI y los últimos 24 bits, denominados NIC son puestos por el fabricante.

Se la conoce también como la dirección física en cuanto identificar dispositivos de red.

CONCENTRADORES: SWITCH Y HUB

Los concentradores son dispositivos que nos permiten conectar varios dispositivos de red (ordenadores, impresoras de red, etc.), así como crear topologías del tipo estrella y árbol. Disponen de una serie de puertos a las que se conectan todos los dispositivos de red. Pueden tener de 4 a 48 puertos.

Hub

El “Hub” transmite toda la información a todos los puertos que contenga, esto es, si el “Hub” tiene 4 puertos, todas las computadoras que estén conectadas al “Hub” recibirán la misma información, y en ocasiones esto puede resultar innecesario y excesivo (lento).

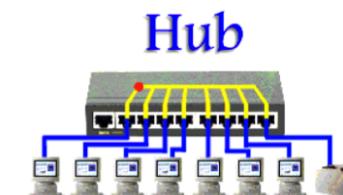


Figura 19. Conección de red con un HUB



Figura 20. Hubs

Switch

Un “**Switch**” es considerado un “**Hub Inteligente**”, reconoce las direcciones “MAC” que generalmente son enviadas por cada puerto, y permite enviar la información de un elemento de red a otro haciendo una comprobación previa de adónde va la información y seleccionando para ello sólo el dispositivo de red de destino. Mejora el rendimiento del ancho de banda.

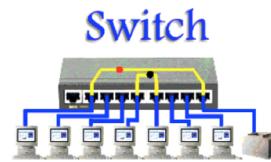


Figura 21. Conexión de una red con un SWITCH



Figura 22. Switchs

HARDWARE DE CONEXIÓN A INTERNET: MÓDEM Y ROUTER

El router es un dispositivo que permite conectar nuestro ordenador o nuestra red de área local a Internet. Los routers tienen dos direcciones IP, una que pertenece a la red local a la que da servicio (IP privada) y otra externa, única en el mundo, con la que navega por Internet y que se conoce como IP pública (estática o dinámica).

Es dinámica cuando cada vez que nos conectamos el servidor de Internet nos da una IP diferente, y es estática cuando siempre es la misma.



Figura 23. Routers

DIRECCIONAMIENTO IP⁵

La dirección IP está formada por cuatro grupos de números entre 0 y 255 que identifican de forma única nuestro computador en la Red.

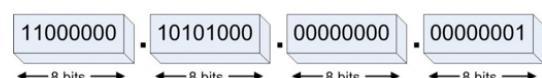


Figura 24. Estructura de una dirección IP en sistema binario

⁵ http://www.revistasbolivianas.org.bo/scielo.php?pid=S1729-75322015000100005&script=sci_arttext

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



Figura 25. Estructura de una dirección IP en sistema decimal

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

JERARQUÍA DE REDES

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

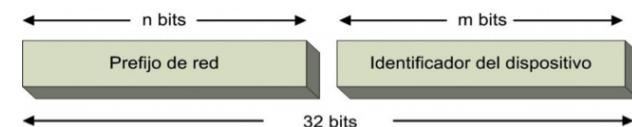


Figura 26. Estructura jerárquica de una dirección IP

Como se puede ver en la figura, de los 32 bits que forman la dirección IP, algunos de ellos forman el prefijo de red y el resto identificarán el dispositivo, de forma que todos los dispositivos conectados a la misma red tendrán sus primeros n bits (prefijo de red) iguales. El número de bits n que forman el prefijo de red y el número de bits que identifican los dispositivos lo establece el administrador de la red para el caso de redes privadas, o el organismo de gestión de direcciones públicas para el caso de direcciones públicas. [3]

CLASES DE REDES

Existen tres principales clases de redes, las mismas que se clasifican acorde al número de bits que utilizan, hay valores de n y m que facilitan muchas cosas. Por ejemplo:

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

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

84.	34.245. 12
110.	62. 0. 1
10.	20. 30. 40

Figura 27. Dirección IP, clase A

n=16 y **m=16**. A las redes que utilizan los 16 primeros bits para identificarse se denominan redes de **clase B**. Una red de clase B tiene $2^{16} = 65.534$ direcciones IP.

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

128. 7.	14.100
172. 20.	2. 3
181.255.	255. 99

Figura 28. Dirección IP, clase B

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

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

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

Figura 29. Dirección IP, clase C

Las clases fueron la primera forma de organización de las direcciones IP públicas, aunque debido al gran crecimiento que experimentó Internet esta organización de las direcciones IP se volvió bastante ineficaz y en la actualidad sólo se sigue empleando para redes con direccionamiento privado. Para el direccionamiento público el uso de clases se sustituyó por otro mecanismo conocido como CIDR. (Classless Inter-Domain Routing o CIDR / enrutamiento entre dominios sin clases).

Máscara de subred

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

La máscara de subred es un número binario de 32 bits y que se representa en formato punto decimal. Por tanto, su "apariencia" es similar a una dirección IP, sin embargo, NO ES UNA DIRECCIÓN IP. La máscara de subred es un número binario que está siempre asociado con una dirección IP y que nos indica qué parte de esa dirección IP es el prefijo de red y qué parte de esa dirección IP es el identificador de dispositivo.

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

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



Figura 30. Máscara de red, clase A

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

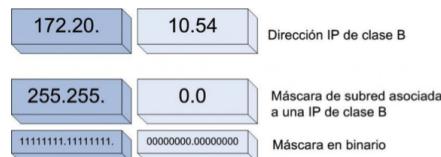


Figura 31. Máscara de red, clase B

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

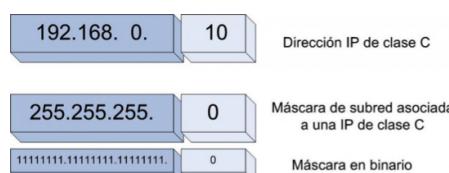


Figura 32. Máscara de red, clase C

Restricciones del direccionamiento IP

- El primer octeto **no puede ser 255** (11111111), ya que eso es **Broadcast**.
- El primer octeto **no puede ser 0** (00000000). Esto es “**solo esta red**”.
- El primer octeto **no puede ser 127** (01111111). **Loop back**.
- La IP de red debe ser única en Internet.
- La de un host debe ser única en un Red.
- El último octeto (dir. del host) **no puede ser 255** (11111111), ya que eso es **Broadcast**.
- El último octeto (dir. del host) **no puede ser 0** (00000000). **Esto es local host**.

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

Clases	Primer dirección	Última dirección	Uso	Número de direcciones
A	0.0.0.0	0.255.255.255	Reservado	16.777.216
	1.0.0.0	9.255.255.255	Direcciones públicas	150.994.944
	10.0.0.0	10.255.255.255	Direcciones privadas	16.777.216
	11.0.0.0	126.255.255.255	Direcciones públicas	1.946.157.056
	127.0.0.0	127.255.255.255	Reservada	16.777.216
B	128.0.0.0	169.253.255.255	Direcciones públicas	721.289.216
	169.254.0.0	169.254.255.255	Reservado	65.536
	169.255.0.0	171.15.255.255	Direcciones públicas	17.891.328
	172.16.0.0	172.31.255.255	Direcciones privadas	1.048.576
	172.32.0.0	191.255.255.255	Direcciones públicas	333.447.168
C	192.0.0.0	192.167.255.255	Direcciones públicas	11.010.048
	192.168.0.0	192.168.255.255	Direcciones privadas	65.536
	192.169.0.0	223.255.255.255	Direcciones públicas	525.795.328

Figura 33. Rango global de direcciones IP

Fuente: <http://www.cintel.org.com.co>

CABLEADO Y CONEXIÓN DE RED⁶

El cable es el medio más común para las conexiones de red debido a que a través de él fluye la información para toda la red. Una red puede utilizar uno o más tipos de cables, aunque el tipo de cable que se vaya a utilizar siempre estará acorde a la topología a utilizar, el tipo de red y el tamaño de esta.

MEDIO	NOMBRE	TIPO DE TRANSMISIÓN	VELOCIDAD DE TRANSMISIÓN
FÍSICO	Par Trenzado	Señales eléctricas	Hasta 1 GB/s
	Fibra óptica	Haz de luz	Hasta 1 TB/s
SIN CABLE	WIFI	Ondas Electromagnéticas	Hasta 100 MB/s
	Bluetooth	Ondas Electromagnéticas	Hasta 3 MB/s

Tabla 2. Medios y tipos de transmisión

Cable de par trenzado sin apantallar / Unshielded Twisted Pair (UTP).

Este tipo de cable es el más utilizado, tiene una variante con apantallamiento, pero la variante sin apantallamiento suele ser la mejor opción para una PYME.

La calidad del cable será lo que el que influya directamente en la calidad de los datos que transcurra por los cables. Las calidades de los cables van desde el cable de telefónico (par de cables para voz), al cable de nivel 5 que es capaz de transferir tasas de 100 MBit/s.

TIPO	USO
Categoría 1 – Cat 1	VOZ – Cable telefónico
Categoría 2 – Cat 2	DATOS a 4 Mbps (LocalTalk)
Categoría 3 – Cat 3	DATOS a 10 Mbps (Ethernet)
Categoría 4 – Cat 4	DATOS a 20 Mbps / 16 Mbps (Token Ring)
Categoría 5 – Cat 5	DATOS a 100 Mbps (Fast Ethernet)
Categoría 6 – Cat 6	DATOS a 1000 Mbps (Giga Ethernet)

Tabla 3. Categorías y uso de los cables

⁶<http://www.nacio.unlp.edu.ar/archivos/concursos/cableado-red-datos-telefonia-11820.pdf>

La diferencia entre las distintas categorías es la tensión. A mayor tensión mayor capacidad de transmisión de datos. Se recomienda el uso de cables de Categoría 3 o 5 para la implementación de redes en PYMES (pequeñas y medianas empresas).

Cable STP (Par trenzado blindado)

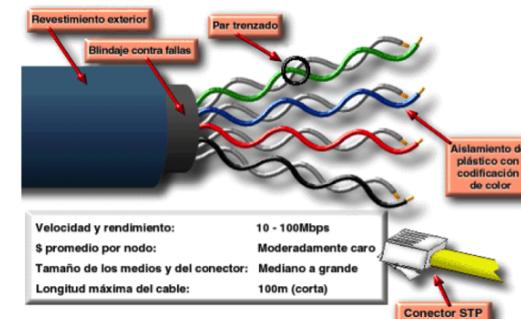


Figura 34. Cable STP

El cable de par trenzado es el más utilizado. Está formado por cuatro pares de hilos, trenzados entre sí. En los extremos del cable es necesario un conector, denominado RJ45, capaz de conectar el cable con los equipos, el switch y el router. La información se transmite por señales eléctricas.

Cable UTP (par trenzado no blindado)

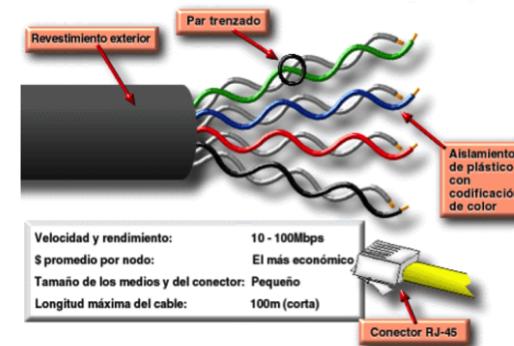


Figura 35. Cable UTP

También se puede transmitir la información por Cable de Fibra Óptica. La Fibra Óptica (FO) Está formado por filamentos de vidrio transparentes (de cristal natural o de plástico), tan finos como un cabello humano, y que son capaces de transportar los paquetes de información como haces de luz producidos por un láser. Existen dos tipos de Fibra Monomodo y Multimodo.

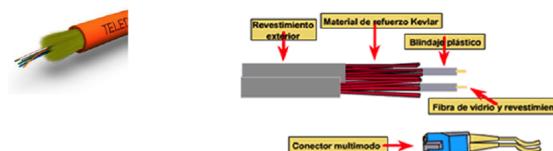


Figura 36. Fibra óptica

Fibra Óptica

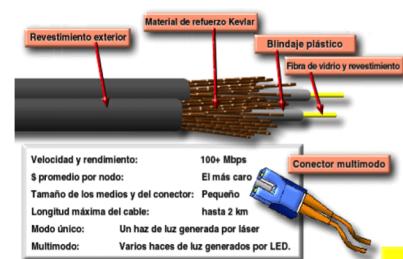


Figura 37. Cable de fibra óptica

ESTÁNDARES PARA LA CONEXIÓN DE REDES

Las redes Ethernet o 100 Base T, necesita conectar los pares sobre un conector RJ45. Si deseamos conectar más de dos estaciones es necesario hacerlo a través de un Hub, Switch o Router para ello necesitamos implementar la conexión que se indica a continuación en cada uno de los cables que conectan a la estación con el Hub, Switch o Router. Para poder realizar esta conexión utilizaremos las normas TIA/EIA-568, Esta norma establece dos standars (A y B) para el cableado Ethernet 10Base-T, determinando qué color corresponde a cada pin del conector RJ-45. [7]

El estándar 568-B, también llamado especificación AT&T es usado más frecuentemente, pero muchas instalaciones están diseñadas con el estándar 568-A, también denominado ISDN.

Normalmente, un patch está armado respetando el mismo estándar (A o B) en ambos extremos del cable. Estos cables se utilizan para:

- Conectar una estación de trabajo a la roseta de una instalación de cableado estructurado.
- Conectar la patchera con un hub o un switch en el armario de cableado.
- Conectar directamente una estación de trabajo a un hub o un switch.
- Conectar un hub con el puerto “crossover” de otro dispositivo.

Cable cruzado

Se denomina así al patch armado utilizando el estándar A en un extremo y el B en el otro. Estos cables responden al estándar 568, y se utilizan para:

- Conectar hubs o switch entre sí.
- Conectar dos estaciones de trabajo aisladas, a modo de una mini-LAN.
- Conectar una estación de trabajo y un servidor sin necesidad de un hub.

Pin#	Par #	Función	Color del Cable	10/100 Base-T Ethernet	100 Base-T4 y 1000 Base-T Ethernet
1	3	Transmite	Blanco/Verde	Si	Si
2	3	Recibe	Verde/Blanco	Si	Si
3	2	Transmite	Blanco/Naranja	Si	Si
4	1	Telefonía	Azul/Blanco	No	Si
5	1	Telefonía	Blanco/Azul	No	Si
6	2	Recibe	Naranja/Blanco	Si	Si
7	4	Respaldo	Blanco/Marrón	No	Si
8	4	Respaldo	Marrón/Blanco	No	Si

Figura 38. Estándar T568A

Pin #	Par #	Función	Color del Cable	10/100 Base-T Ethernet	1000 Base-T4 y Ethernet
1	2	Transmite	Blanco/Naranja	Si	Si
2	2	Recibe	Naranja/Blanco	Si	Si
3	3	Transmite	Blanco/Verde	Si	Si
4	1	Telefonía	Azul/Blanco	No	Si
5	1	Telefonía	Blanco/Azul	No	Si
6	3	Recibe	Verde/Blanco	Si	Si
7	4	Respaldo	Blanco/Marrón	No	Si
8	4	Respaldo	Marrón/Blanco	No	Si

Figura 39. Estándar T568B

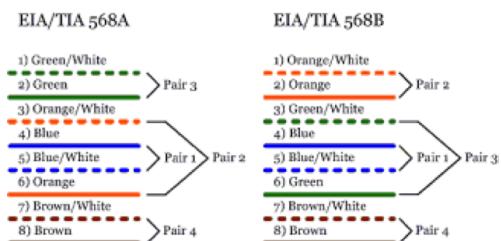


Figura 40. Código de colores para la norma T568A y T568B

TRANSMISIÓN INALÁMBRICA:

Si decidimos usar como medio de comunicación “el aire”, es necesario instalar dos componentes hardware en nuestra red. Por un lado, una tarjeta de red inalámbrica (interna o externa) a través del puerto USB y, además, un punto de acceso inalámbrico conectado a un switch, o un switch inalámbrico, que se encargará de recoger todas las señales y distribuirlas por la red.



Figura 41. Componentes para comunicaciones inalámbricas

CONECTARSE A UNA RED INALÁMBRICA (WI-FI)

Wi-Fi significa Wireless-Fidelity (fidelidad sin hilos). Las redes locales inalámbricas se llaman WLAN. En estas redes la transmisión de datos es mediante ondas de radio. La distancia de transmisión puede llegar a 100-150 m, aunque la distancia va aumentando según avanza la tecnología.

La conexión puede hacerse mediante IP automática o mediante IP fija, al igual que en las redes con cables. Aunque lo más frecuente es mediante IP automática. En estos casos, al ir al menú Conectarse a una red inalámbrica y elegir la red que queremos, se nos pedirá la contraseña de red (que nos proporciona el fabricante). La contraseña se coloca para evitar que otro equipo con conexión Wi-Fi pueda conectarse a nuestra red. [7]

DISPOSITIVOS BLUETOOTH

Se utilizan en Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante radiofrecuencia. Permite comunicaciones a distancias de hasta 10 m. [7]

Los principales objetivos que se pretenden conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas.

SUBNETEO CLASE A, B, C⁷.

La función del Subneteo o Subnetting es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de estas trabaje a nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio.

⁷ <https://es.scribd.com/document/88650064/Manual-Subneteo>

El Subneteo permite una mejor administración, control del tráfico y seguridad al segmentar la red por función. También, mejora la performance de la red al reducir el tráfico de broadcast de nuestra red. Como desventaja, su implementación desperdicia muchas direcciones, sobre todo en los enlaces seriales. [4]

Ejemplos:

Si tenemos la dirección IP Clase C 192.168.1.0/24 y la pasamos a binario, los primeros 3 octetos, que coinciden con los bits “1” de la máscara de red (fondo bordó), es la dirección de red, que va a ser común a todos los hosts que sean asignados en el último octeto (fondo gris). Con este mismo criterio, si tenemos una dirección Clase B, los 2 primeros octetos son la dirección de red que va a ser común a todos los hosts que sean asignados en los últimos 2 octetos, y si tenemos una dirección Clase A, el 1 octeto es la dirección de red que va a ser común a todos los hosts que sean asignados en los últimos 3 octetos.

Porción de Red				Porción de Host			
192	.	168	.	1	.	0	
11000000	.	10101000	.	00000001	.	00000000	
255	.	255	.	255	.	0	
11111111	.	11111111	.	11111111	.	00000000	=/24

Figura 42. Porción de RED y HOST de una dirección IP

Si en vez de tener una dirección con Clase tenemos una ya subneteada, por ejemplo, la 132.18.0.0/22, la cosa es más compleja. En este caso los 2 primeros octetos de la dirección IP, ya que los 2 primeros octetos de la máscara de red tienen todos bits “1” (fondo bordo), es la dirección de red y va a ser común a todas las subredes y hosts. Como el 3º octeto está dividido en 2, una parte en la porción de red y otra en la de host, la parte de la dirección IP que corresponde a la porción de red (fondo negro), que tienen en la máscara de red los bits “1”, se va a ir modificando según se vayan asignando las subredes y solo va a ser común a los hosts que son parte de esa subred. Los 2 bits “0” del 3º octeto en la porción de host (fondo gris) y todo el último octeto de la dirección IP, van a ser utilizados para asignar direcciones de host.

CONVERTIR BITS EN NÚMEROS DECIMALES

Como sería casi imposible trabajar con direcciones de 32 bits, es necesario convertirlas en números decimales. En el proceso de conversión cada bit de un intervalo (8 bits) de una dirección IP, en caso de ser “1” tiene un valor de “2” elevado a la posición que ocupa ese bit en el octeto y luego se suman los resultados.

Posición y Valor de los Bits								
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binario	1	0	0	0	0	0	0	0
Decimal	128	0	0	0	0	0	0	0
Binario	0	1	0	0	0	0	0	0
Decimal	0	64	0	0	0	0	0	0
Binario	0	0	1	0	0	0	0	0
Decimal	0	0	32	0	0	0	0	0
Binario	0	0	0	1	0	0	0	0
Decimal	0	0	0	16	0	0	0	0
Binario	0	0	0	0	1	0	0	0
Decimal	0	0	0	0	8	0	0	0
Binario	0	0	0	0	0	1	0	0
Decimal	0	0	0	0	0	4	0	0
Binario	0	0	0	0	0	0	1	0
Decimal	0	0	0	0	0	0	2	0
Binario	0	0	0	0	0	0	0	1
Decimal	0	0	0	0	0	0	0	1

Figura 43. Posiciones y valores de los bits

1	1	1	1	1	1	1	1	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	+ 64	+ 32	+ 16	+ 8	+ 4	+ 2	+ 1	= 255
1	1	0	0	0	0	0	0	
2^7	2^6							= 192
128	+ 64							
1	0	1	0	1	1	0	0	
2^7	2^6			2^3	2^2			= 172
128	+ 32			+ 8	+ 4			

Figura 44. Transformación de binario a decimal

La combinación de 8 bits permite un total de 256 combinaciones posibles que cubre todo el rango de numeración decimal desde el 0 (00000000) hasta el 255 (11111111). Algunos ejemplos.

00000000 = 0	00010100 = 20	10100000 = 160
00000001 = 1	00011110 = 30	10110100 = 180
00000010 = 2	00101000 = 40	11010000 = 200
00000011 = 3	00110010 = 50	11011100 = 220
00000100 = 4	00111100 = 60	11110000 = 240
00000101 = 5	01000110 = 70	11111010 = 250
00000110 = 6	01010000 = 80	11111011 = 251
00000111 = 7	01011010 = 90	11111100 = 252
00001000 = 8	01100100 = 100	11111101 = 253
00001001 = 9	01111000 = 120	11111110 = 254
00001010 = 10	10001100 = 140	11111111 = 255

Figura 45. Ejemplos de la transformación de binario a decimal

CALCULAR LA CANTIDAD DE SUBREDES Y HOSTS POR SUBRED

Cantidad de Subredes es igual a: 2^N , donde “N” es el número de bits “robados” a la porción de Host. Cantidad de Hosts x Subred es igual a: $2^M - 2$, donde “M” es el número de bits disponible en la porción de host y “-2” es debido a que toda subred debe tener su propia dirección de red y su propia dirección de broadcast.

Aclaración: Originalmente la fórmula para obtener la cantidad de subredes era $2^N - 2$, donde “N” es el número de bits “robados” a la porción de host y “-2” porque la primer subred (subnet zero) y la última subred (subnet broadcast) no eran utilizables ya que contenían la dirección de la red y broadcast respectivamente.

Actualmente para obtener la cantidad de subredes se utiliza y se enseña con la fórmula 2^N , que permite utilizar tanto la subred zero como la subnet broadcast para ser asignadas.

CAPÍTULO IV

CISCO PACKET TRACER 7.0 – Manual paso a paso

“El manual base de este Capítulo fue desarrollado por el Profesor Miguel Rebollo, para la versión 5.0 de Packet Tracer, en esta ocasión se ha tomado como referencia dicho manual y se lo ha traducido y actualizado a la versión 7.0.”

[17], [22], [23].

Cisco Packet Tracer es un software propiedad de Cisco System, Inc., diseñado para la simulación de redes, es la principal herramienta de trabajo para pruebas y simulación de prácticas en los cursos de formación de Cisco System.

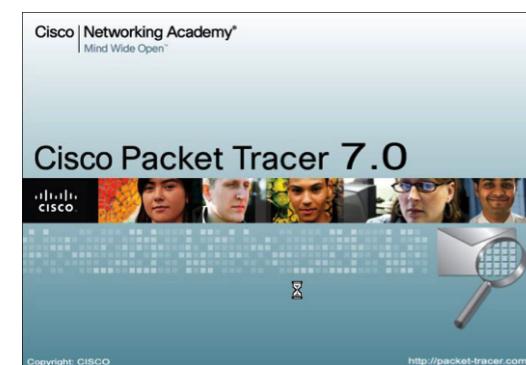


Figura 46. Portada de Cisco Packet Tracer 7.0

INICIAMOS EN PACKET TRACER

En esta primera fase se hablará de la interfaz que tiene la herramienta con los usuarios.

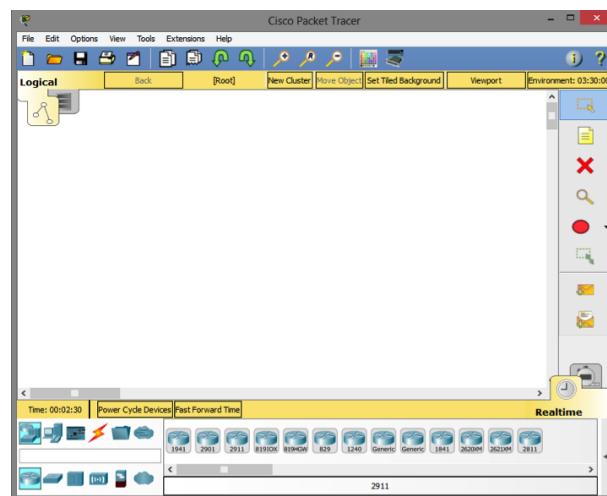


Figura 47. Interfaz principal de Packet Tracer

Esta como otras herramientas dispone de sus menús principales, entre los cuales están FILE, OPTIONES y HELP; además de contar con una barra de uso rápido que contiene las opciones de nuevo escenario (NEW), abrir un escenario (OPEN), guardar cambios en un escenario (SAVE), imprimir un escenario (PRINT) y un asistente de actividades (ACTIVITY WIZARD).

En el menú FILE, se encuentran las opciones descritas en la barra de uso rápido, con la única diferencia que aparece la opción de guardar como (SAVE AS).

En el menú OPTIONS, se encuentra la opción PREFERENCES, que maneja la personalización de la herramienta, Packet Tracer.

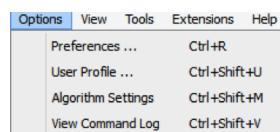


Figura 48. Barra de menus de Packet Tracer

Al seleccionar esta opción se despliega un cuadro de dialogo, el cual dispone de 7 pestañas, una de las cuales tiene el título INTERFACE en donde se puede habilitar o deshabilitar las opciones de Animación, Sonido y Etiquetas. Además de seleccionar el idioma que dispone la herramienta.

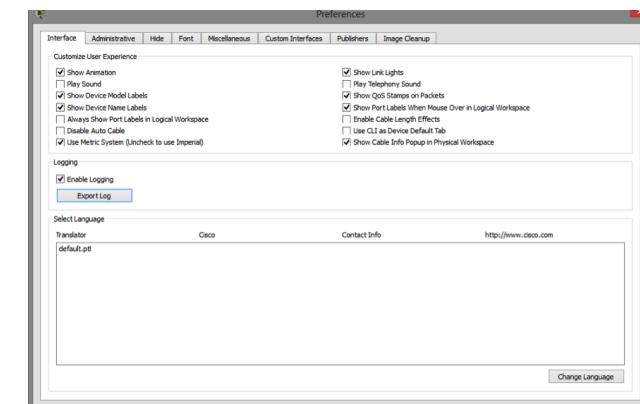


Figura 49. Pantalla de preferencias de Packet Tracer

La otra, con el título ADMINISTRATIVE provee opciones adicionales de administración. Entre las cuales dispone de un password y su confirmación para futuras entradas a la herramienta, al igual que la habilitación y deshabilitación de éste. También da la opción de agregar o remover distintos fondos.

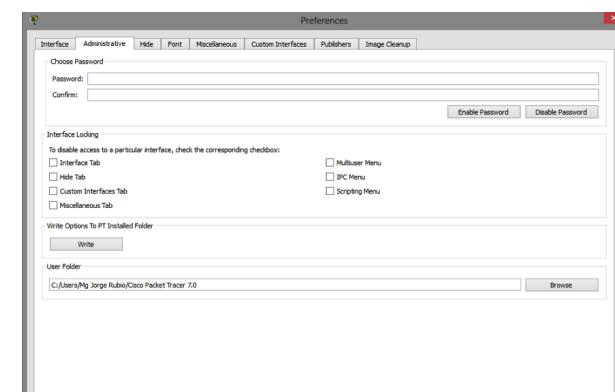


Figura 50. Preferencias administrativas de Packet Tracer

Una forma esencial de agregar información relativa a la red que se ha de construir, está disponible en el cuadro de información, en la parte derecha de la barra de acceso rápido.

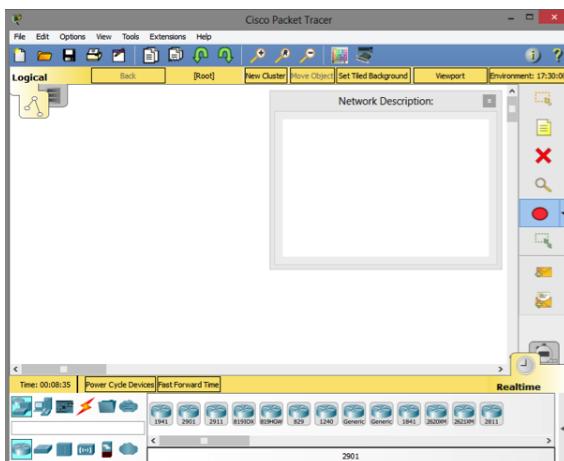


Figura 51. Insertar descripciones de la red en Packet Tracer

La barra de acceso común provee herramientas para la manipulación de los dispositivos, las cuales se detallan a continuación. El orden de descripción es el mismo en que aparecen los iconos de la barra.

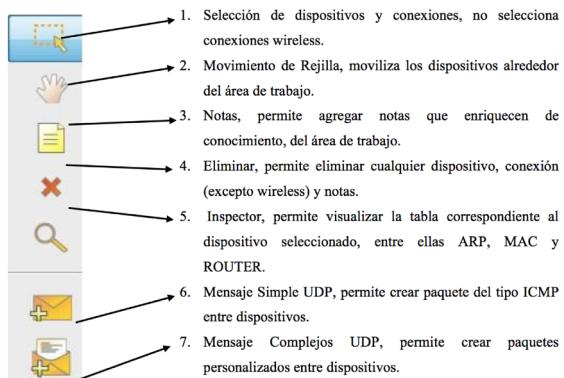


Figura 52. Descripción de la barra de herramientas

En la parte inferior izquierda, aparecen una serie de dispositivos que pueden ser agregados. Por ejemplo, se selecciona el router, a la par aparece una serie de routers, entre ellos destacan los específicos de CISCO y un genérico.

Las conexiones tienen todas las conocidas, desde automáticas, que detectan el tipo correcto entre dispositivos, hasta punto a punto (Cooper Straight - through), cruzadas (Cooper Cross - over), consola (console), fibra óptica (fiber), teléfono (telephone), Serial DCE y Serial DTE. Entre los últimos por mencionar se tiene a los dispositivos que van conectados entre sí, es decir pc's, servidores, impresoras, siendo genéricas todas estas.



Figura 53. Barra de herramientas de dispositivos

Hay dos modos en las redes concretadas, un el modo real, en donde se crean las configuraciones y se dispone la posición de los dispositivos; y el modo simulación en el cual se pone a andar la o las redes armadas. Se puede cambiar entre los diferentes modos, esto está en la parte inferior derecha. El modo real (Realtime) es representado por un reloj, y el modo simulación (Simulation) es representado con un cronómetro.

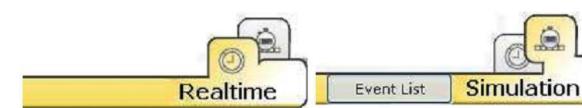


Figura 54. Opciones de simulación

Existen dos vistas, la lógica y la física. En la vista lógica se agregan todos los dispositivos, y en la vista física la disposición de las redes, una vista de ciudad, departamento y oficina. Estas pueden ser alternadas por las opciones que aparecen en la barra. Estas vistas pueden ser cambiadas en la barra que aparece en la parte de debajo de la barra de acceso rápido.

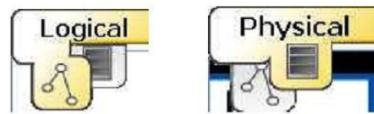


Figura 55. Opciones de vistas

POSICIONAMIENTO DE LOS DISPOSITIVOS

Como se mencionó anteriormente, para poder agregar un dispositivo, tal como un router, switch, computador, etc.; es necesario únicamente dar un clic simple sobre el que deseamos y colocarlo en el área de trabajo. Notaremos que al dar un clic sobre el dispositivo el cursor cambia de una flecha a un signo más, si deseamos colocar más de un dispositivo del mismo tipo, la tarea puede volverse tediosa, pero para ello únicamente debe presionar la tecla CTRL antes de seleccionar el dispositivo, notará que ahora el cursor permanece con el signo más, después de agregar el primero. En ese momento se podrá agregar cuantos dispositivos se desee. Para terminar, debemos pulsar la tecla ESC, o bien dando un clic sobre el botón del dispositivo que selecciono.



Figura 56. Barra de Herramientas de dispositivos

Después de agregar el primer router genérico, el cursor cambia a una flecha y el botón seleccionado se coloca con la figura del router. Esto se muestra en la siguiente ilustración. Ahora si se agregan los dispositivos, en este caso routers, el cursor queda en forma de signo más y el botón con una diagonal invertida en forma indeterminada, hasta que oprimamos el mismo botón que seleccionamos para agregar el dispositivo o pulsando la tecla ESC.

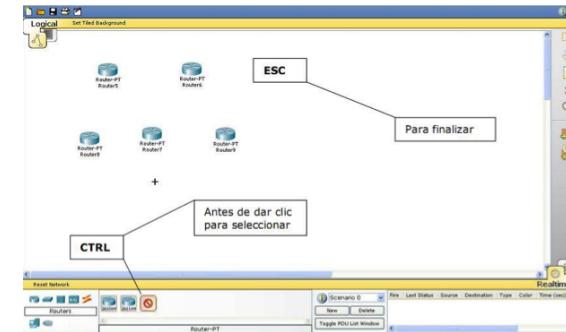


Figura 57. Vista de diseño

Para eliminar cualquier dispositivo, es necesario seleccionarlo y luego dirigirnos a la barra común, dar un clic en el botón identificado con una equis. Nota: La barra común se encuentra en la parte derecha central de la ventana. Otra forma de eliminar algún dispositivo es oprimiendo la tecla DEL; el cursor tendrá el aspecto del signo más, y luego podrá seleccionar el dispositivo que deseé. También puede seleccionar un grupo de dispositivos, y repetir cualquier de los dos pasos mencionados anteriormente.

DESPLIEGUE DE INFORMACIÓN DE DISPOSITIVOS

Existen dos formas en que es posible mostrar la información de los estados de cada uno de los dispositivos, una de ellas es utilizar el inspector, que sirve para visualizar las tablas ARP, MAC y ROUTING. De un clic sobre esta herramienta situada en la barra de herramientas comunes, en la parte central derecha de la ventana, y el cursor tendrá la apariencia de una lupa, entonces seleccione con un clic simple el dispositivo y se le preguntará por el tipo de tabla, debe seleccionar la que necesite, y entonces se desplegará un cuadro de texto con la información de la tabla.

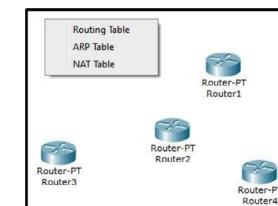


Figura 58. Despliegue de información de Dispositivos

La otra forma es posicionar el cursor sobre el dispositivo y esperar que se despliegue la información, la cual desaparecerá una vez que el usuario saque el mouse del equipo.

CONFIGURACIÓN DE EQUIPOS

Como se mencionó anteriormente, este manual no tiene como objetivo enseñar como armar una red y los protocolos que corren detrás de este procedimiento, sino que el uso básico de Packet Tracer, para que el alumno pueda ir explorando a medida que va acostumbrándose al software e ir reconociendo nuevas funcionalidades de ésta potente herramienta.

En esta sección se enseñará la configuración en el programa de los dispositivos más utilizados en el laboratorio. Entre ellos, Routers, Switches, PCs y conexiones cableadas.

CONFIGURANDO UN PC

Se ingresa dirección IP, máscara de subred y puerta de enlace o Gateway: Se da un click sobre PCx (donde x representa número de pc en la red), desplegándose un cuadro en la parte central derecha con nombre Edit PCx.

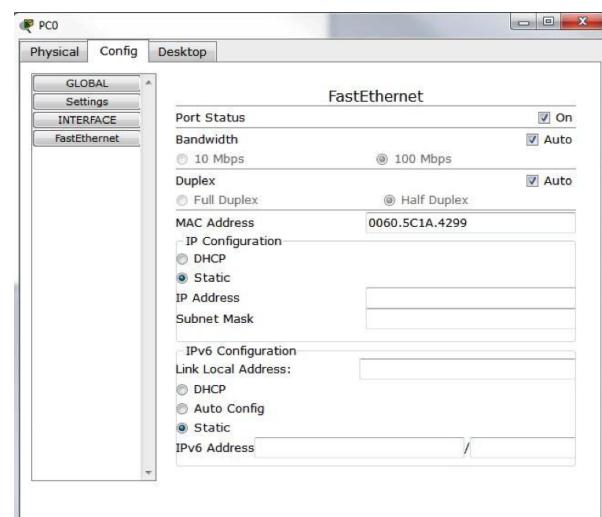


Figura 59. Pantalla de configuración de un Pc

En la figura anterior se puede apreciar, que en la pestaña Config, es posible el ingreso de los datos antes mencionados. Fijarse que también da la opción de configurar por DHCP, pero afectos del curso no se utilizará.

También en la pestaña **Desktop>Command Prompt**, se pueden realizar pruebas de conexión con los demás dispositivos usando ping por ejemplo.

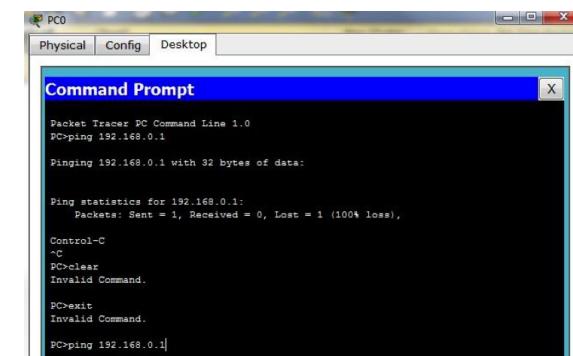


Figura 60. Pantalla del Command Prompt en Packet Tracer

CONFIGURANDO UN SWITCH

Dentro de las configuraciones básicas de los switches para las experiencias del curso, va en lo que es la creación de VLANs (Virtual Local Area Network), la cual permite ir separando redes dentro de una topología, con fines de diferenciación de servicios dentro de una empresa o institución.

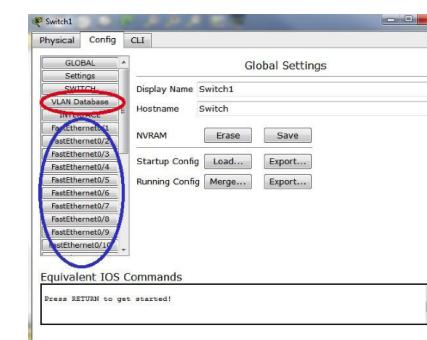


Figura 61. Pantalla de configuración de un Switch

La figura anterior muestra los botones de importancia para la configuración de un switch (VLAN y FastEthernet 0/x que corresponde a las bocas del equipo). También se puede cambiar el nombre por efectos de orden en la topología.

1. Se procede a configurar VLAN: Para ello es necesario seguir los pasos de la figura, la cual indica con rojo donde dirigirse para el proceso de creación. Además, cabe mencionar que por omisión vienen creadas las vlan 1, 1002, 1003, 1004, 1005. En este caso se creó la VLan elo y telo, con número 2 y 3 respectivamente.

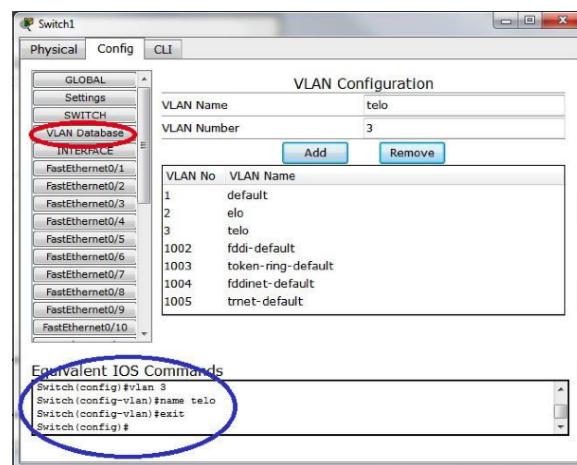


Figura 62. Configuración de un Switch

2. Configuración de una interfaz: Como se sabe que en un switch no se configura IP, el manejo de cada una de las interfaces es para la asignación de VLAN, la que puede ser de modo Access o Trunk. En la figura se muestra que la interfaz 0/1 se le asigna la VLAN telo de modo Access.

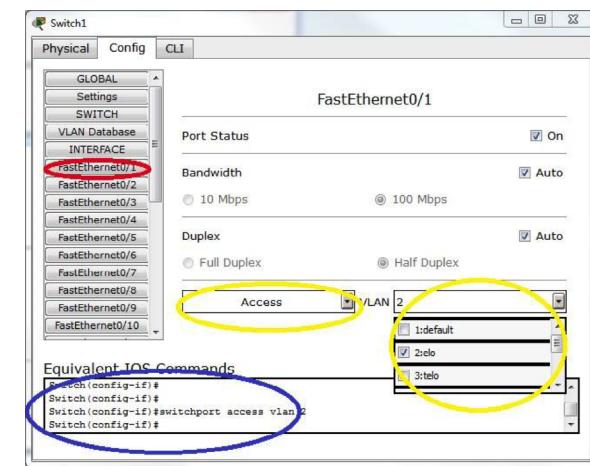


Figura 63. Configuración de interfaces en un switch

3. Manejo de IOS: Finalmente es posible realizar modificaciones a la configuración del switch de forma directa en el IOS, lo cual permite que el usuario se familiarice potencialmente con el equipo.

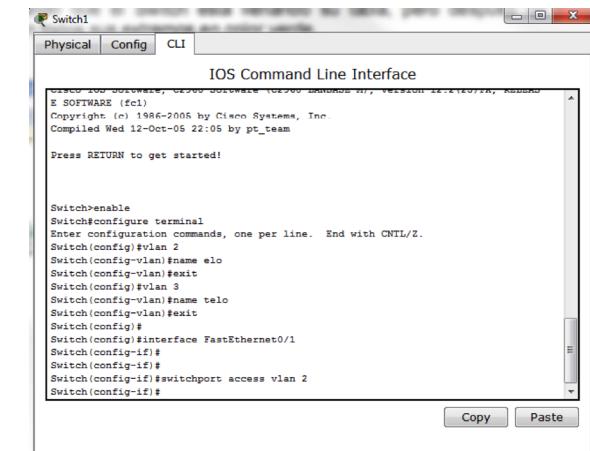


Figura 64. Pantalla de IOS Command - linea de comandos

CONFIGURANDO UN ROUTER

Este equipo posee muchas más características de configuración que el switch, dado que se comporta en capas superiores. Es posible tratar el tema de enrutamientos, que puede ser estático o dinámico (RIP), los que se pueden configurar explícitamente a través de la interfaz gráfica.

1. Configurar Interfaces: Es de vital importancia que como primer paso sea el encender la interfaz, ya que en el caso real (router físico) generalmente están apagadas produciendo conflictos de conectividad. Además, se procede a la configuración de IP que pasará a ser el Gateway de la red.

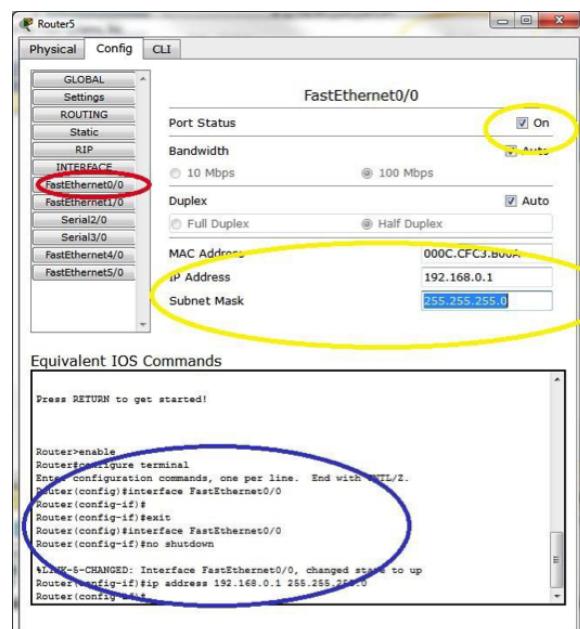


Figura 65. Configuración de interfaces en un router

2. Definición de ruteo estático: Este es el tipo de enrutamiento en donde el usuario tiene que definir las redes que no están conectadas al router. Asumiendo que una de las bocas del router tiene la red 192.168.3.0, a través de ésta trata de conectarse a la red 192.168.10.0.

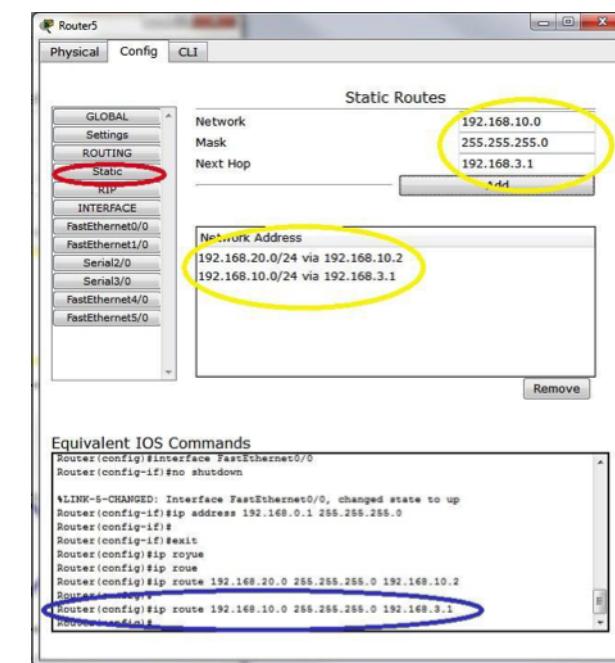


Figura 66. Definición de ruteo estático

3. Definición de Ruteo Dinámico RIP: Este es el más simple, ya que le indica al router cuáles son las demás rutas que están compartiendo el resto de los dispositivos.

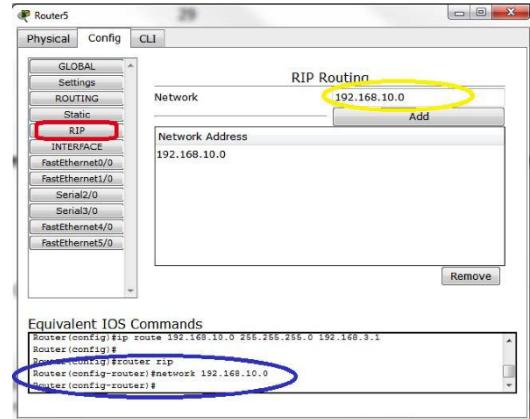


Figura 67. Definición de ruteo dinámico RIP

4. Manejo de IOS: Finalmente es posible realizar modificaciones a la configuración del router de forma directa en el IOS, lo cual permite que el usuario se familiarice potencialmente con el equipo.

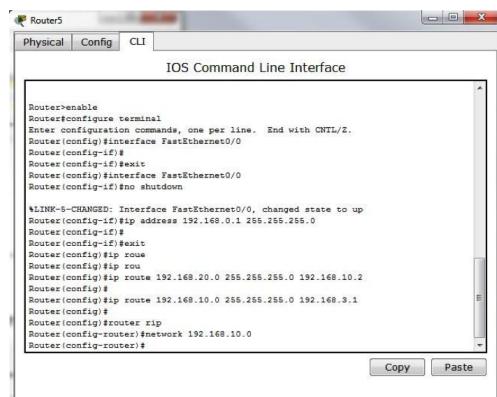


Figura 68. Configuración del router por línea de comandos

PRIMERA APlicación

Utilizando la herramienta de simulación PACKET TRACER 7.0, se desea implementar la siguiente estructura de red.

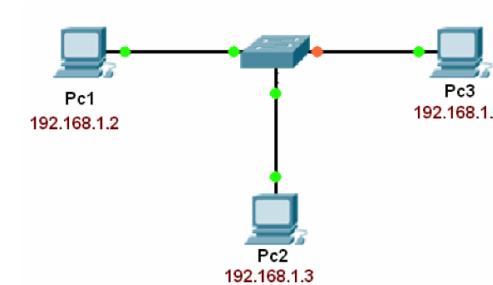


Figura 69. Esquema de una red

Paso 1: Ingresar a la herramienta Packet Tracer y seleccionar la referencia de Switch 2960-24 el cual se encuentra en el menú Switches.

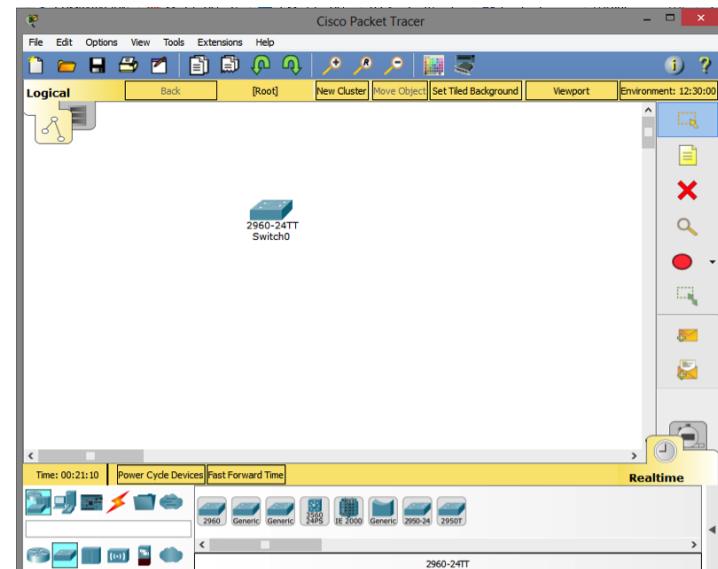


Figura 70. Selección de dispositivos en Packet Tracer

Paso 2: En el menú **End Devices**, seleccionar la opción **PC-PT** y dibujar el primer PC.

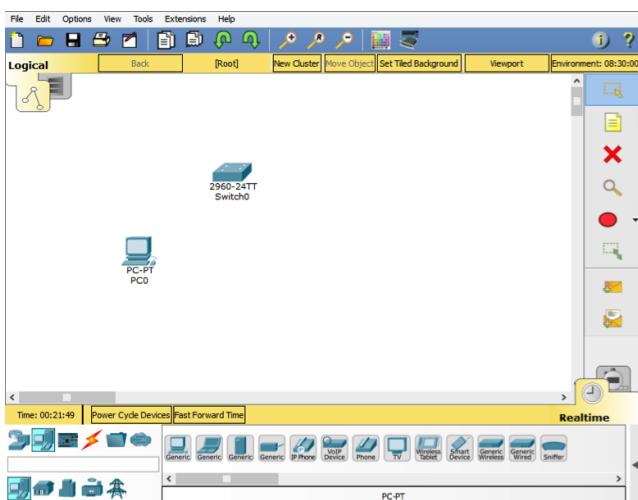


Figura 71. Selección de dispositivos de red

Repetir el paso anterior dos veces, completando con ello los tres Pcs requeridos en el esquema.

Paso 3:

En la opción **Connections** del menú de elementos, escoger la opción **Copper Straight through**, la cual corresponde a un cable de conexión directa requerido en éste caso para conectar un Pc a un Switch.

Hecho esto, se debe seleccionar el primer PC, hacer clic con el botón derecho del Mouse y escoger la opción Fastethernet, indicando con ello que se desea establecer una conexión a través de la tarjeta de red del equipo.

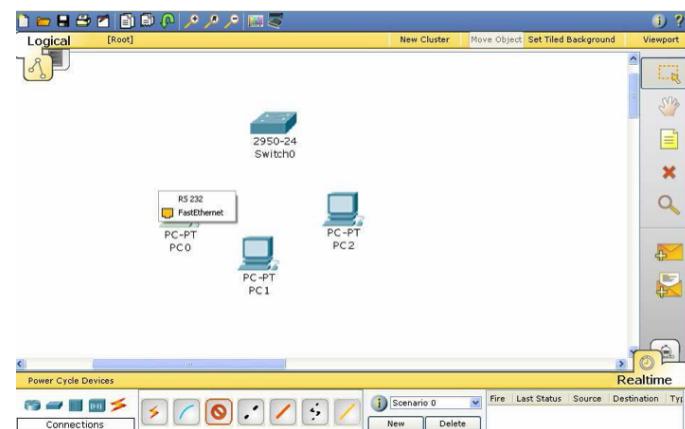


Figura 72. t

Paso 4: Despues de seleccionar la opción Fast Ethernet en el primer Pc, arrastrar el mouse hasta el Switch, hacer clic sobre él y seleccionar el puerto sobre el cual se desea conectar el Pc1, en nuestro caso corresponde al puerto Fast Ethernet 0/1.

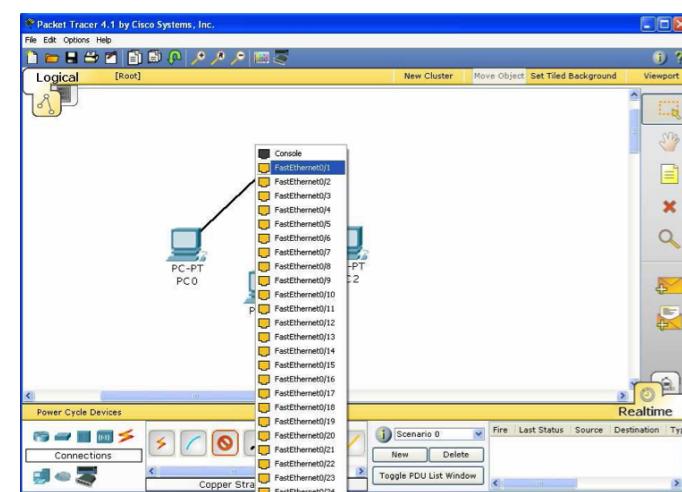


Figura 73. Selección de puertos en dispositivos

El resultado de lo anterior se refleja en la siguiente figura, lo cual se debe repetir con cada uno de los PCs que hacen parte del diseño.

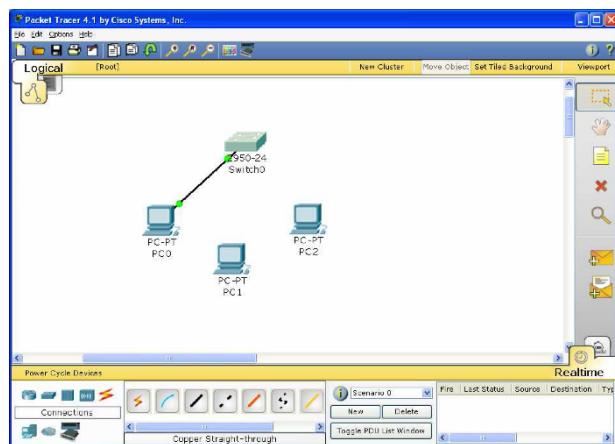


Figura 74. Conexión de una Pc a u Switch

Paso 5: Despues de realizar cada una de las conexiones, se deben configurar las direcciones IP según los criterios de diseño. Para ello, se selecciona el primer PC y se hace doble clic sobre él. Apareciendo el formulario que se ilustra en la siguiente figura, el cual corresponde a la apariencia física de un computador.

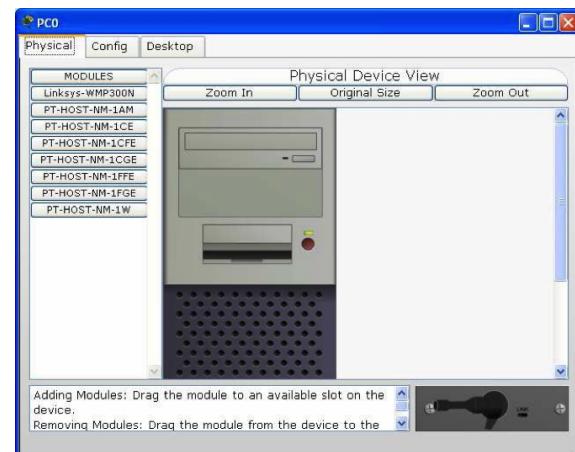


Figura 75. Apariencia física de un computador en Packet Tracer

En la parte superior aparecen tres opciones, las cuales permiten realizar diversas funciones sobre el equipo en particular. La primera opción **Physical**, permite configurar parámetros físicos del PC, tales como la inclusión o exclusión de componentes hardware propios de red. La segunda opción **Config**, permite configurar parámetros globales tales como un direccionamiento estático o dinámico y la tercera opción **Desktop**, permite realizar operaciones de funcionamiento y configuración de la red tales como:

Dirección IP, máscara de red, dirección de gateway, dirección DNS, ejecutar comandos como PING, TELNET, IPCONFIG, entre otras funciones más.

Como en éste paso se requiere la configuración de los parámetros lógicos de red tales como la dirección IP, máscara de red y dirección Gateway se escoge la opción 3 (**Desktop**), en donde posteriormente se selecciona la opción **IP Configuration**.

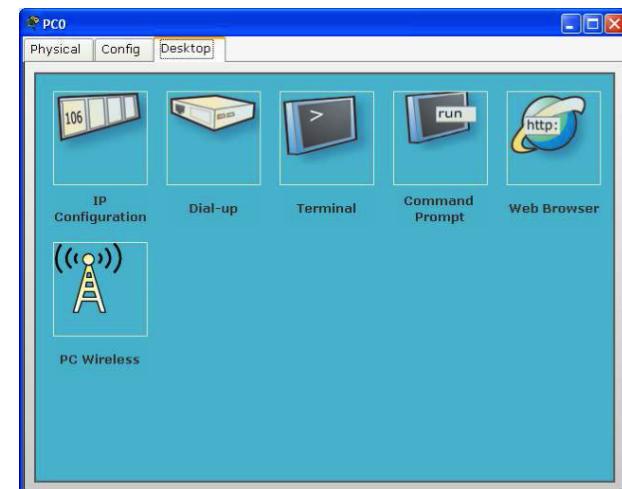


Figura 76. Pantalla de IP Configuration

Aquí se definen la dirección IP del computador, la cual corresponde a la dirección 192.168.1.2; se toma como máscara de subred la máscara por defecto para una clase C la cual corresponde al valor 255.255.255.0 y finalmente se define la dirección de gateway o puerta de enlace, ésta dirección corresponde a la dirección sobre la cual los computadores de la red tratarán de acceder cuando requieran establecer comunicación con otras redes a través de un dispositivo **capa 3 (Router)**, la cual por criterios de diseño corresponde a la primera dirección IP de la red: 192.168.1.1

Adicionalmente, en este caso se desea trabajar bajo el modelo de configuración IP estática y no bajo la alternativa del protocolo DHCP, el cual establece en forma automática la dirección IP a un host o computador de la red, acorde con la disponibilidad de direcciones IP existentes en la red a fin de optimizar su uso; ésta alternativa es muy utilizada en redes inalámbricas Wifi.

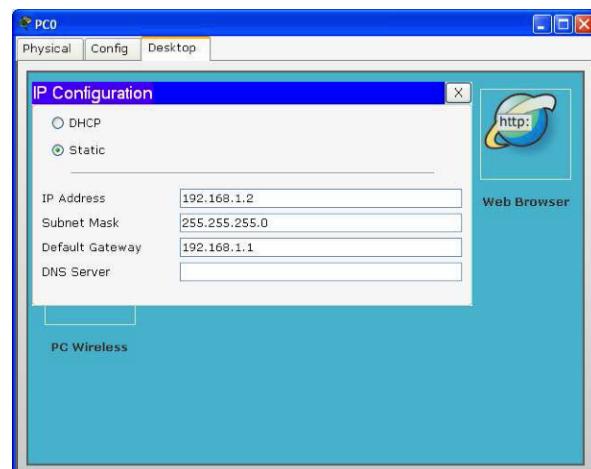


Figura 77. Asignación de direcciones IP

Este paso se repite para cada uno de los host o computadores que hacen parte del diseño, teniendo en cuenta que, en cada uno de ellos, el único parámetro que varía será la dirección IP; la máscara de subred y la dirección de Gateway permanecen constantes debido a que todos los equipos pertenecen a la misma subred. En las dos figuras siguientes se evidencia claramente esto.

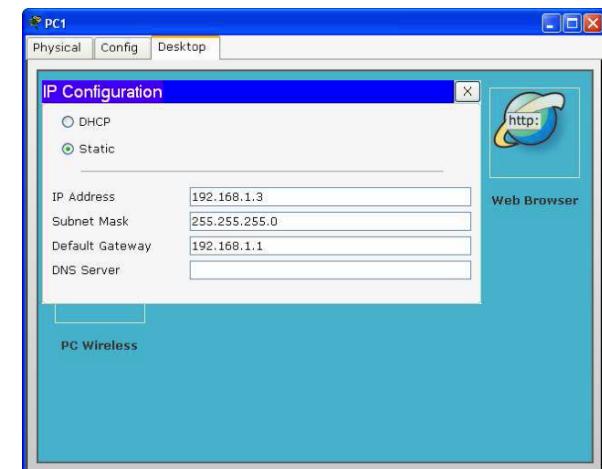


Figura 78. Asignación de direcciones IP

Paso 6:

Si se desea verificar la configuración de un computador en particular, simplemente se selecciona el Host, se escoge la opción Desktop, seleccionamos la opción **Command prompt**, la cual visualiza un ambiente semejante al observado en el sistema operativo DOS. Allí escribimos **IPCONFIG** y pulsamos enter.

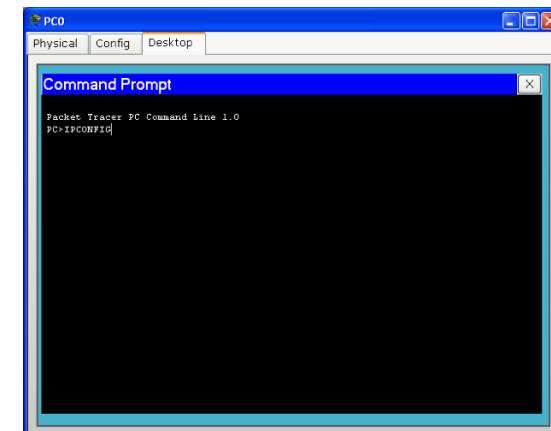


Figura 79 Pantalla de Command Prompt para utilizar el comando Ipconfig

El resultado de ello se visualiza claramente en la siguiente figura, en donde se identifican los parámetros del host correspondientes a la dirección IP, la máscara de Subred y la dirección de Gateway.

```

PC0 Physical Config Desktop
Command Prompt
Packet Tracer PC Command Line 1.0
PC>IPCONFIG

IP Address.....: 192.168.1.2
Subnet Mask....: 255.255.255.0
Default Gateway.: 192.168.1.1

PC>
  
```

Figura 80. Resultado del comando *Ipconfig*

Si el comando introducido es **IPCONFIG/ALL**, el resultado es el observado en la siguiente figura.

```

PC0 Physical Config Desktop
Command Prompt
Packet Tracer PC Command Line 1.0
PC>IPCONFIG

IP Address.....: 192.168.1.2
Subnet Mask....: 255.255.255.0
Default Gateway.: 192.168.1.1

PC>IPCONFIG /ALL

Physical Address.....: 000A.F393.150A
IP Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.0
Default Gateway....: 192.168.1.1
DNS Servers.....: 0.0.0.0

PC>
  
```

Figura 81. Resultado de *Ipconfig/all*

En donde se evidencia no solo los parámetros mencionados anteriormente, sino que además incluye la dirección física del equipo conocida como MAC y la dirección del servidor de dominio DNS.

Paso 7: Para verificar que existe una comunicación entre los diferentes equipos que hacen parte de la red, simplemente se selecciona uno de ellos; Para esto se ejecuta el comando **PING** acompañado de la dirección IP de la maquina a la que queremos conectarnos.

```

PC2 Physical Config Desktop
Command Prompt
Packet Tracer PC Command Line 1.0
PC>PING 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=182ms TTL=128
Reply from 192.168.1.2: bytes=32 time=72ms TTL=128
Reply from 192.168.1.2: bytes=32 time=83ms TTL=128
Reply from 192.168.1.2: bytes=32 time=94ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 72ms, Maximum = 182ms, Average = 107ms

PC>
  
```

Figura 82. Utilización del comando ping

El resultado de ello se observa en la siguiente figura, en donde se constata claramente que se enviaron 4 paquetes de información y 4 paquetes fueron recibidos a satisfacción.

PACKET TRACER Y LAS REDES INALÁMBRICAS

Anteriormente se utilizó Packet Tracer como herramienta de simulación de redes de datos en forma cableada; sin embargo, también es posible utilizarlo como herramienta de simulación para redes inalámbricas. A continuación, se hará un montaje bastante básico de una red inalámbrica.

Ejercicio: Se desea implementar una red LAN en forma inalámbrica, constituida por dos equipos mediante el uso de un **Access Point**. Para ello, lo primero es dibujar el access point, el cual se encuentra en el menú **Wireless**.

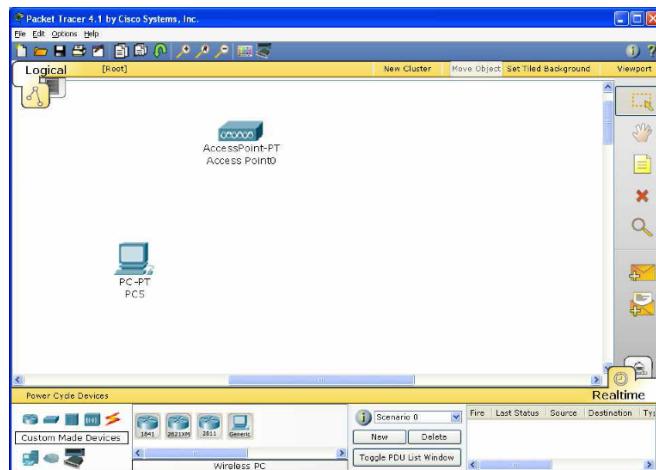


Figura 83. Conexión de un PC y un Access Point

Posteriormente se dibujan **los dos PCs con tarjeta inalámbrica**, los cuales se encuentran ya configurados en la opción **Custom Made Devices**, el cual al dibujarlo comienza a negociar con el **access point** hasta establecer una conexión inalámbrica con él.

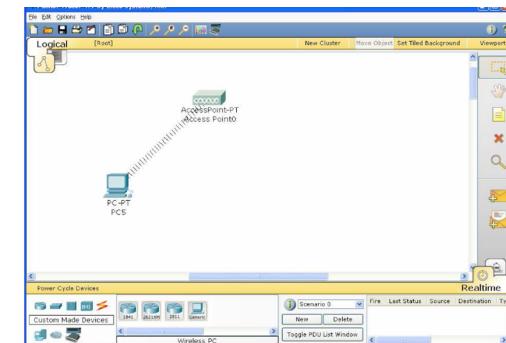


Figura 84. Conexión de una PC y un Access Point

Se realiza el mismo proceso incluyendo ahora el nuevo PC, sin embargo, el hecho de que existe una conexión no significa que exista una comunicación completa.

Por tal razón es indispensable definir en cada uno de los PCs una dirección IP, la cual por el momento se harán de manera estática. A los PCs se les configurará con las direcciones IP 192.168.1.11 y 192.168.1.12, utilizando máscara por defecto y dirección de Gateway 192.168.1.1, a fin de verificar la comunicación entre los equipos, realizamos un **PING** a la dirección 192.168.1.11 y listo.

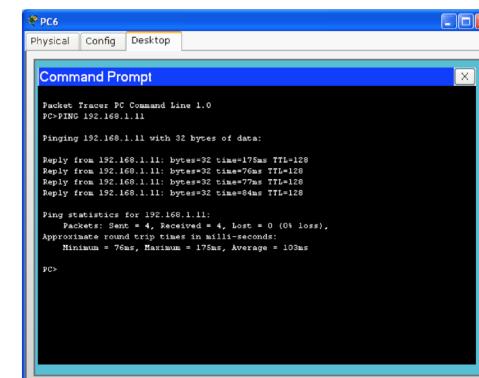


Figura 85. Utilización del comando Ping

Hasta aquí simplemente se ha implementado una red inalámbrica básica, sin embargo, muchas veces es necesario interconectar redes inalámbricas cableadas con redes inalámbricas.

A continuación, un ejemplo al respecto.

Integrando el ejemplo anterior junto con el primer ejemplo de interconexión de host en forma cableada y utilizando las mismas direcciones IP, se obtiene el esquema.

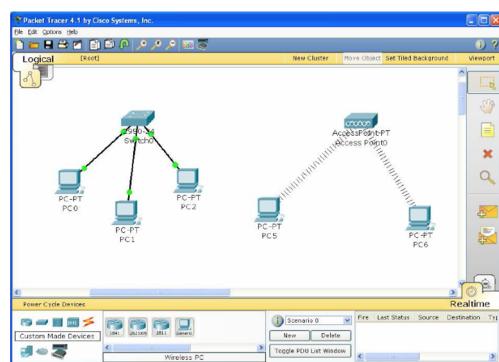


Figura 86. Conexión de redes cableadas e inalámbricas

Sin embargo, para que exista comunicación entre los equipos de la red cableada y los equipos de la red inalámbrica, debe existir una conexión física entre los equipos concentradores, es decir, entre el Switch y el Acces point. Por tal razón, es necesario conectar a éstos dos dispositivos mediante un cable de conexión directa.

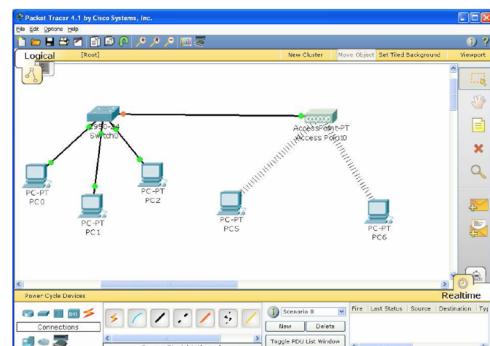


Figura 87. Conexión entre una red cableada y una inalámbrica (switch - access point)

USO DE LA HERRAMIENTA PACKET TRACER, SIMULANDO UNA RED HÍBRIDA CONTROLADA POR UN ROUTER INALÁMBRICO.

En prácticas anteriores se realizó el montaje de una red híbrida en donde se utilizaba como dispositivos concentradores un switch y un Access Point. Sin embargo, este sistema presentaba una limitante la cual consistía en que solamente se podían comunicar entre sí siempre y cuando los equipos pertenezcan a la misma subred.

En este caso, los equipos que hacen parte de la red cableada pertenecen a una dirección de subred diferente a los equipos que pertenecen a la red inalámbrica. Adicionalmente, se aprovechará la oportunidad para configurar los equipos de tal forma que los host pertenecientes a la LAN cableada utilicen direccionamiento IP estático y los hosts de la WLAN (Wireless LAN) utilicen direccionamiento IP dinámico bajo el uso del protocolo DHCP.

El esquema topológico es el siguiente:

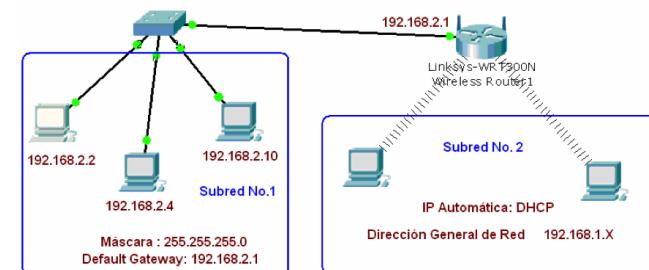


Figura 88. Diagrama de una red híbrida

En la figura se indica claramente las direcciones IP requeridas para la subred cableada, las cuales pertenecen a la dirección de subred: 192.168.2.0; la subred inalámbrica trabajará bajo el uso del protocolo DHCP distribuyendo las direcciones IP a los host propios de la dirección de subred: 192.168.1.0.

En vista de lo anterior, lo primero que se debe hacer es configurar las direcciones IP, máscara de Subred y Default Gateway en cada uno de los equipos que hacen parte de la red cableada, según los criterios de diseño.

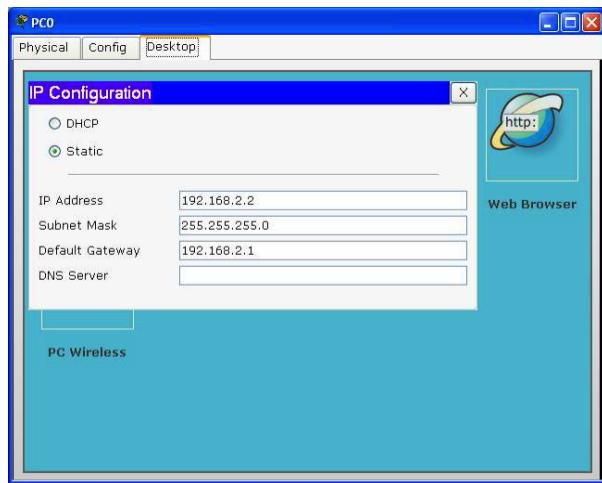


Figura 89. Asignación de direcciones IP

Como en este caso se hace uso de un Router Inalámbrico, hay necesidad de configurar la dirección de gateway, la cual es la aquella dirección que utilizarán los hosts para acceder a otras subredes, en éste caso, para acceder a la subred 192.168.1.0

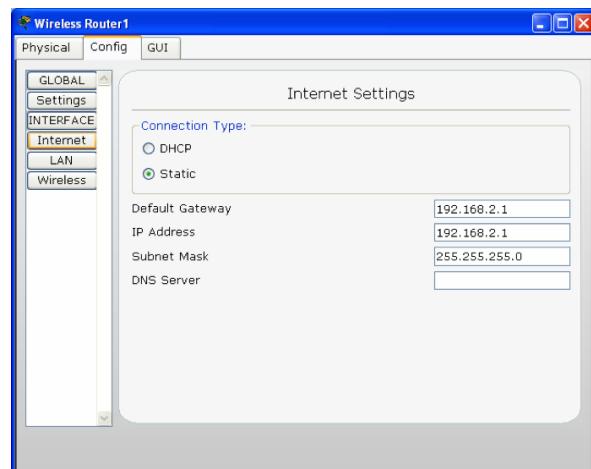


Figura 90. Configuración del Gateway

Cuando se realizar la conexión física entre el Switch y el Router Inalámbrico, se hace a través de la interfaz de INTERNET; sobre la cual se debe configurar la dirección de Gateway. Despues de configura los parámetros correspondientes a la red cableada, se inicia la configuración de la red inalámbrica de la siguiente forma:

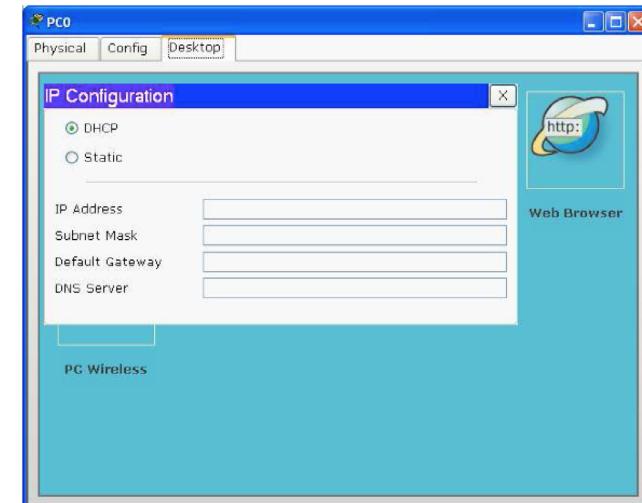


Figura 91. Configuración de la red inalámbrica

Cada uno de los hosts que hacen parte de la red inalámbrica se deben configurar utilizando el protocolo DHCP, tal como se ilustra en la figura anterior, el cual se encargará de adjudicar según sus criterios las direcciones IP a cada uno de los Host.

Sin embargo, es importante comprender en qué lugar se deben definir aquellos parámetros que rigen la distribución de direcciones IP, propias de la red inalámbrica.

Se selecciona el Router inalámbrico, se escoge la opción GUI sobre la cual de definen los siguientes parámetros:

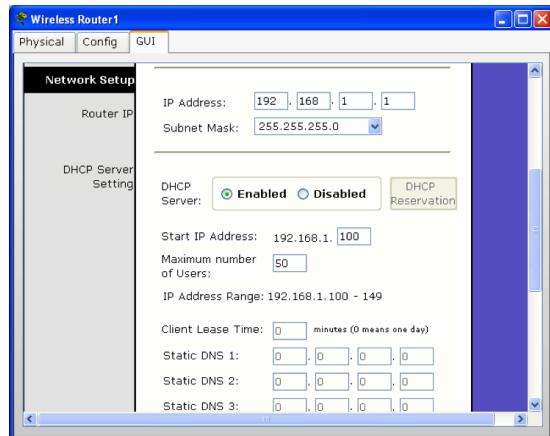


Figura 92. Configuración del Wireless Router

- IP Address: 192.168.1.1 (Gateway subred inalámbrica)
- Subnet Mask (Máscara de subred): 255.255.255.0
- DHCP Enabled: Indicando que se utilizará el protocolo DHCP
- Start IP Address: 192.168.1.100 (Dirección inicial para la adjudicación de direcciones IP en forma automática)
- Número máximo de usuarios: 50
- Rango de direcciones IP para distribución: 192.168.1.100 – 192.168.1.149

A continuación, se verifica la comunicación entre un equipo de la red cableada y un host inalámbrico, específicamente, desde la dirección 192.168.2.2 (LAN Cableada) a la dirección 192.168.1.102 (LAN Inalámbrica)

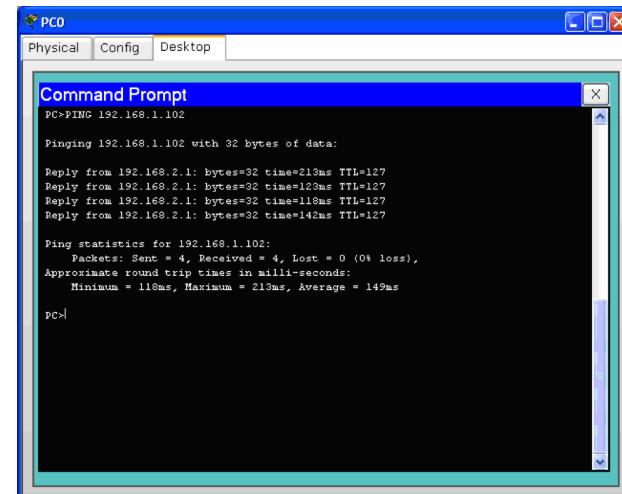


Figura 93. Ejecución del comando Ping

USO DEL PROTOCOLO WEP EN REDES INALÁMBRICAS

Utilizando el mismo esquema de red anterior, tal como se ilustra en la figura, seleccionamos el router inalámbrico y nos ubicamos en la sección Config. Allí se encuentra establecido el modo de Seguridad a utilizar, el cual por defecto se encuentra deshabilitado.

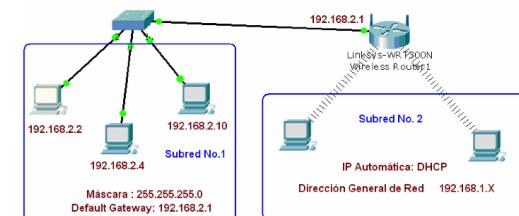


Figura 94. Esquema de red para la sección inalámbrica

En éste caso en particular, seleccionamos WEP y establecemos la contraseña o Key, la cual será utilizada por el router inalámbrico y los PCs para encriptar su información bajo el uso de éste protocolo. Vale la pena mencionar que ésta contraseña deberá ser de al menos 10 caracteres.

Existen herramientas software especializadas en generar este tipo de contraseñas teniendo en cuenta criterios de seguridad mayores a los que usualmente poseen las contraseñas convencionales.



Figura 95. Configuración WEP en Wireless Settings

Se puede observar que, si activamos el protocolo WEP en el router, los equipos o host no establecerán comunicación con él hasta que en cada uno de ellos no se defina que se utilizará este protocolo y se defina la misma contraseña de encriptación configurada en el router. En la siguiente figura se ilustra claramente esta situación. En la primera figura se evidencia que ninguno de los host inalámbricos presenta comunicación con el Router, y tan pronto esta configuración se realiza en uno de los PCs, automáticamente inicia el proceso de comunicación demostrado en la tercera figura.

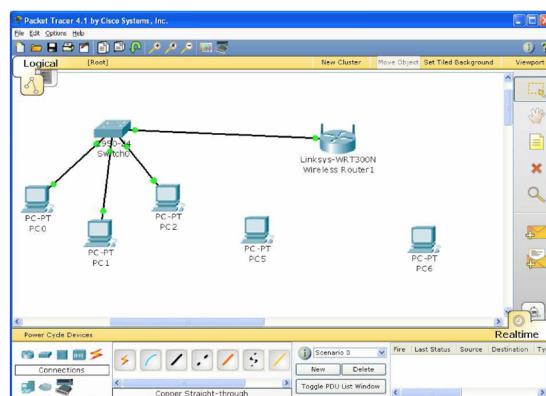


Figura 96. Conexión del switch con el router

En la siguiente figura se ilustra la configuración en uno de los PCs

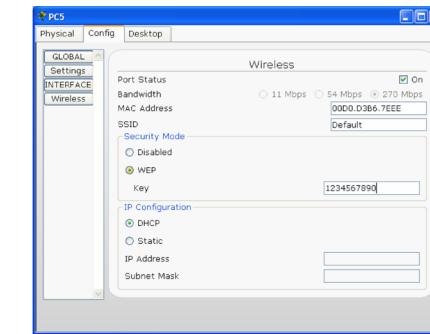


Figura 97. Configuración de uno de los PCs

Configurando el segundo PC inalámbrico.

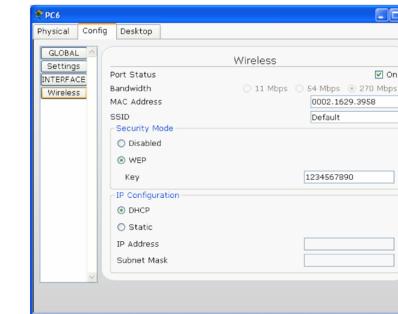


Figura 98. Configuración del segundo PC.

En donde finalmente queda configurada la red de la siguiente forma:

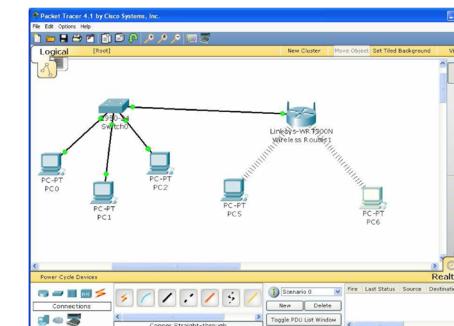


Figura 99. Esquema final de la red cuando ya existe conexión

CAPÍTULO V

SEGURIDAD EN REDES⁸

Sin importar que las redes informáticas en la actualidad, estén conectadas por cables o de manera inalámbrica, cada vez se vuelven más primordiales para nuestras actividades diarias. Tanto las personas como las organizaciones dependen de sus computadoras y de sus redes para funciones como: correo electrónico, contabilidad, organización y administración de archivos, etc.

Las intromisiones de personas no autorizadas pueden causar problemas costosos en la red y pérdidas de trabajo, los ataques a una red pueden ser devastadores y pueden causar pérdida de tiempo y de dinero debido a los daños o robos de información o de archivos importantes. [14]

A los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se les denominan “Piratas Informáticos o Hackers”. Una vez que un hacker tiene el acceso a una red pueden surgir 4 tipos de amenazas consideradas como primordiales:

- Robo de información
- Robo de identidad
- Perdida y manipulación de datos
- Interrupción del servicio.

Las amenazas de seguridad causadas por intrusos en la red pueden originarse tanto en forma interna como externa, así tenemos que:

Amenazas externas

Provienen de personas que no tienen autorización para acceder al sistema o a la red. Logran introducirse principalmente desde Internet, enlaces inalámbricos o servidores de acceso.

Amenazas internas

Por lo general, conocen información valiosa y vulnerable o saben cómo acceder a esta. Sin embargo, no todos los ataques internos son intencionados.

Con la evolución de los tipos de amenazas, ataques y explotaciones se han acuñado varios términos para describir a las personas involucradas

- **Hacker:** un experto en programación. Recientemente este término se ha utilizado con frecuencia con un sentido negativo para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- **Hacker de sombrero blanco:** una persona que busca vulnerabilidades en los sistemas o en las redes y a continuación informa a los propietarios del sistema para que lo arreglen.
- **Hacker de sombrero negro:** utilizan su conocimiento de las redes o los sistemas informáticos para beneficio personal o económico, un cracker es un ejemplo de hacker de sombrero negro.
- **Cracker:** es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- **Phreaker:** persona que manipula la red telefónica para que realice una función que no está permitida. Por lo general, a través de un teléfono público para realizar llamadas de larga distancia gratuitas.
- **Spammer:** persona que envía grandes cantidades de mensajes de correo electrónico no deseado, por lo general, los spammers utilizan virus para tomar control de las computadoras domésticas y utilizarlas para enviar mensajes masivos.

⁸ <https://www.certsuperior.com/SeguridadRedes.aspx> <https://www.mcafee.com/es/products/network-security/index.aspx>

- **Estafador:** utiliza el correo electrónico u otro medio para engañar a otras personas para que brinden información confidencial como número de cuenta o contraseñas.

Algunos de los **delitos informáticos** más frecuentes en la red son:

- Abuso del acceso a la red por parte de personas que pertenecen a la organización.
- Virus.
- Suplantación de identidad.
- Uso indebido de la mensajería instantánea.
- Denegación de servicio, caída de servidores.
- Acceso no autorizado a la información.
- Robo de información de los clientes o de los empleados.
- Abuso de la red inalámbrica
- Penetración en el sistema.
- Fraude financiero.
- Detección de contraseñas.
- Registro de claves.
- Alteración de sitios web.
- Uso indebido de una aplicación web pública.

Ataques informáticos

Existen diversos tipos de ataques informáticos en redes, algunos de ellos son:

Ataques de denegación de servicios (DOS)

Es un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red por el consumo

del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. [15]

Man in the middle (MITM)

Es una situación donde un atacante supervisa (generalmente mediante un rastreador de puertos) una comunicación entre las 2 partes y falsifica los intercambios para hacerse pasar por una de ellas.

Ataques de replay:

Una forma de ataque de red en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o recalcada, es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite posiblemente como parte de un ataque enmascarado.

LOS CORTAFUEGOS

En el Protocolo TCP/IP el puerto es una numeración lógica que se asigna a las conexiones tanto en origen como en destino sin significación física. El permitir o denegar acceso a los puertos es importante porque las aplicaciones servidoras deben escuchar en un puerto conocido de antemano para que un cliente pueda conectarse. Esto quiere decir que cuando el sistema operativo recibe una petición a ese puerto la pasa a la aplicación que escucha en él (si hay alguna) y a ninguna otra. Los servicios más habituales tienen asignados los llamados puertos bien conocidos, por Ejemplo: 80 para Servidor web, 21: Puerto FTP, 23: TELNET etc. [15]

Es así que cuando se pide acceso a una página web su navegador pide acceso al puerto 80 del servidor web y si este número no se supiera de antemano o estuviera bloqueado no podría recibir la página.

Un puerto puede estar en varios estados:

- **ABIERTO:** Acepta conexiones hay una aplicación escuchando en este puerto. Esto no quiere decir que se tenga acceso a la aplicación solo que hay posibilidades de conectarse.

- **CERRADO:** se rechaza la conexión. Probablemente no hay aplicación escuchando en este puerto o no se permite acceso por alguna razón. Este es el comportamiento normal del sistema operativo.

- **BLOQUEADO O SIGLOSO:** no hay respuesta, este es el estado real para un cliente en Internet. De esta forma ni siquiera se sabe si el ordenador está conectado. Normalmente este comportamiento se debe a un cortafuego o a que el ordenador está apagado. Para controlar el estado de los puertos de conexión a redes TCP-IP y por tanto las aplicaciones que lo usan emplearemos un cortafuego (firewall).

El cortafuegos o Firewall es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos pueden ser hardware o software o una combinación de ambos y se utilizan con frecuencia para que una serie de usuarios autorizados se conecten a una red privada o Intranet.

Firewall: Todos los paquetes de la red pasan por el cortafuego que examina y bloquea los que no cumplen los criterios de seguridad especificados. Algunos cortafuegos muestran un mensaje al usuario mostrando el programa o proceso que solicita la comunicación preguntándole si la permite o la deniega. El problema surge cuando el nombre del proceso que muestran no lo reconocemos o que tiene el mismo que un proceso confiable conocido, en este caso hay que tener en cuenta varias cosas: si deniego el acceso a un programa este puede no funcionar, la siguiente vez que me pregunte le permitiré el acceso y en caso de funcionar la próxima vez que me pregunte le permitiré acceso permanentemente es importante leer siempre los mensajes para permitir o denegar acceso.

- **Ventajas de un cortafuego:**

- Protege de intrusiones, el acceso a ciertos segmentos de la red sólo se permite a máquinas autorizadas de otros segmentos o de Internet.

- Protección de la información privada: permite definir distintos niveles de acceso a la información de manera que cada grupo de usuarios definido tenga solo acceso a los servicios e información que les son estrictamente necesarios.

- Optimización de acceso: Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa.

- **Limitaciones de un cortafuego:**

- Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuego o que sencillamente no use la red seguirá constituyendo una amenaza.

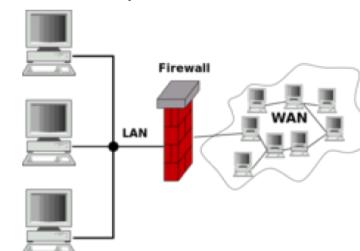


Figura 100. Cortafuegos o firewall de una red

Una red perimetral o zona desmilitarizada es un área local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa. Los equipos en la DMZ no pueden conectar con la red interna. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, servidores Web y DNS.[14].

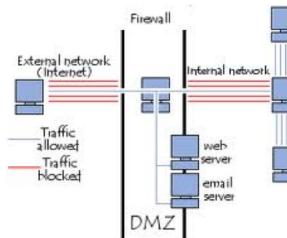


Figura 101. Red Perimetral o zona desmilitarizada

Fuente: <http://www.cintel.org.com.co>

Listas de control de acceso (ACL) y filtrado de paquetes

Una lista de control de acceso o ACL, es una forma de determinar los permisos de acceso apropiados a un determinado objeto dependiendo de diferentes aspectos del proceso que hace el pedido. Las ACL permiten controlar el flujo del tráfico en equipos de redes como routers y switches, su principal objetivo es filtrar tráfico permitiendo o denegando el tráfico de red de acuerdo a alguna condición, sin embargo, también tienen usos adicionales como por ejemplo distinguir tráfico prioritario.

Las listas de control de acceso pueden configurarse para controlar el tráfico entrante y saliente y en este contexto son similares a un cortafuego. Se pueden considerar como cada una de las reglas individuales que controlan y configuran un cortafuego.

Lista de control de acceso en routers

Son listas de condiciones que se aplican al tráfico que viaja a través de una interfaz del router y se crean según el protocolo la dirección o el puerto a filtrar.

Estas listas indican al router qué tipos de paquetes se deben aceptar o desplazar en las interfaces del router, ya sea a la entrada o a la salida.

Las razones principales para crear las ACL son:

- Limitar el tráfico de la red.
- Mejorar el rendimiento de la red.
- Controlar el flujo del tráfico decidiendo qué flujo de tráfico se bloquea y cual se permite ya sea por direccionamiento o por servicios de la red.
- Proporcionar un nivel básico de seguridad para el uso de la red.

Existen 2 tipos de ACL:

- **ACL estándar:** Especificamos una sola dirección de origen.
- **ACL extendida:** Especificamos una dirección de origen y de destino, se utilizan más que las estándar porque ofrecen un mayor control, verifica las direcciones de paquetes de origen y destino y también protocolos y números de puertos.

IPTABLES

El cortafuegos utilizado para gestionar las conexiones de red de los sistemas GNU Linux desde la versión 2.4 del núcleo es IPTABLES, las posibilidades de IPTABLES son prácticamente infinitas y un administrador que quiera sacarle el máximo provecho puede realizar configuraciones extremadamente complejas, para simplificar, diremos que básicamente IPTABLES permite crear reglas que analizarán los paquetes de datos que entran, salen o pasan por nuestra máquina y en función de las condiciones que mantengamos, tomaremos una decisión que normalmente será permitir o denegar que dicho paquete siga su curso. El cortafuego controla las comunicaciones entre la red y el exterior para crear las reglas podemos analizar muchos aspectos de los paquetes de datos, podemos filtrar paquetes en función de: [14]

- Tipo de paquete de datos:
 - INPUT (paquetes que llegan a nuestra maquina).
 - OUTPUT (paquetes que salen de nuestra maquina).
 - FORWARD (paquetes que pasan por nuestra maquina).

- Interfaz por la que entran (-i) o salen (-o) los paquetes: ETH0, wlan1.

- IP origen de los paquetes (-s): IP concreta (10.0.1.3), rango de red (10.0.1.0/8)

- IP destinada a los paquetes (-d): IP concreta, 2 rango de red.

- Protocolo de los paquetes (-t): TCP, UDP, CMP...

Una forma sencilla de trabajar con IPTABLES es permitir las comunicaciones que interesen y luego denegar el resto de la comunicación, lo que se suele hacer es definir la política por defecto, aceptar, después crear reglas concretas para permitir las comunicaciones que nos interesen y finalmente denegar el resto de comunicaciones, lo mejor será crear un script en el que dispondremos de la secuencia de reglas que queremos aplicar a nuestro sistema.

Redes inalámbricas

Los cables que se suelen usar para construir redes locales van desde el cable telefónico hasta la fibra óptica. Algunos edificios se construyen con los cables instalados para evitar gasto de tiempo y dinero posterior y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental. Los riesgos más comunes para el cableado se pueden resumir en los siguientes.

- **Interferencias:** estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración por acción de campos eléctricos, por tanto, son más seguros.

- **Corte del cable:** la conexión establecida se rompe lo que impide que el flujo de datos circule por el cable.

- **Daños en el cable:** los daños normales con el uso pueden dañar el aislamiento que preserva la integridad de los datos transmitidos o dañar al propio cable lo que hace que las comunicaciones dejen de ser fiables.

La mayoría de las organizaciones clasifican estos problemas como daños naturales sin embargo también se puede ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

Consejos de seguridad

- Asegurar el punto de acceso por ser un punto de control de las comunicaciones de todos los usuarios y por tanto críticos en las redes inalámbricas:

* Cambia la contraseña por defecto: todos los fabricantes ofrecen un password por defecto de acceso a la administración del punto de acceso, al usar un fabricante la misma contraseña para todos sus equipos es fácil o posible que el observador la conozca.

* Aumentar la seguridad de los datos transmitidos: usar encriptación WEP o WPA, las redes inalámbricas basan su seguridad en la encriptación de los datos que viajan a través de aire. El método habitual es la encriptación WEP pero no podemos mantener WEP como única estrategia de seguridad ya que no es del todo seguro, existen aplicaciones para Linux o Windows que escaneando suficientes paquetes de información son capaces de obtener las claves WEP y permitir acceso de intrusos en nuestra red. Activa la encriptación de 128bits WEP mejor que la de 64bits. Algunos puntos de acceso más recientes soportan también encriptación WPA y WPA2, encriptación dinámica y más segura que WEP, si activas WPA en el punto de acceso tanto los accesorios como los dispositivos WLAN de tu red como tu sistema operativo debe de soportar.

*Ocultar tu red WIFI: cambia el SSID por defecto en lugar de mi AP o Apmanolo o el nombre de la empresa es preferible coger algo menos atractivo como wroken, down o desconectado, si no llamamos la atención del observador hay menos posibilidades de que este intente entrar en nuestra red.

* Desactiva también el broadcasting SSID o identificador de la red inalámbrica. El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red wifi identifiquen automáticamente el nombre y los datos de la red inalámbrica evitando así la tarea de configuración manual. Al desactivarlo tendrás que introducir manualmente el SSID en la configuración de cada nuevo equipo que quieras conectar.

- Evitar que se conecten:

* Activa el filtrado de direcciones mac: para activar el filtrado mac dejaras que solo los dispositivos con las direcciones mac especificadas se conecten a tu red wifi. Por un lado, es posible conocer las direcciones mac de los equipos que se conectan a la red con tan solo escuchar con el programa adecuado ya que las direcciones mac se transmiten en abierto sin encriptar entre el punto de acceso y el equipo, además, aunque en teoría las direcciones mac son únicas a cada dispositivo de red y no pueden modificarse hay comando o programas que permiten simular temporalmente por software una nueva dirección mac para una tarjeta de red.

* Establece el número máximo de dispositivos.

* Desactiva DHCP en el router o en el punto de acceso en la configuración de los dispositivos o accesorios WIFI, tendrás que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y los DNS. Si el observador conoce el rango de IP que usamos en nuestra red no habremos conseguido nada con este punto.

* Desconecta el AP cuando no lo uses: el AP almacena la configuración y no necesitarás introducirla de nuevo cuando lo conectes.

* Cambia las claves regularmente: puede ser necesario entre 1 y 4 GB de datos para romper una clave WEP dependiendo de la complejidad de las claves de manera que cuando llegue a este caudal de información transmitida es recomendable cambiar las claves.

CAPÍTULO VI

EJERCICIOS PROPUESTOS, PRÁCTICAS Y LABORATORIOS.

Práctica # 1

PRÁCTICA # 1

Encuentra la dirección MAC de tu tarjeta de red de dos maneras diferentes:

- Para ello debemos irnos al centro de redes y consulta el estado y detalles de tu tarjeta de red (dirección física).
- Ejecuta el comando “cmd” en el menú Inicio de Windows y escribe el comando “**getmac**”.
- En gran parte de los sistemas con kernel Linux, está el comando “**ifconfig**”
- Con los tres primeros bytes (por ejemplo 00-1C-BF), averigua quien es el fabricante de tu tarjeta.

Práctica #2

PRÁCTICA # 2

Vamos a encontrar la dirección IP pública y privada de nuestro computador.

- IP pública: Ingrese a Internet y en cualquier navegador escriba mi ip, cual es mi ip, etc.
- IP privada:

- Ejecute la instrucción “**cmd**” en el menú Inicio de Windows y escribe el comando “**ipconfig/all**” (verás la configuración de todos los dispositivos o tarjetas de red de tu equipo).

- Para ello debemos ir al centro de redes y consulta el estado y detalles de tu tarjeta de red (dirección física).

Práctica #3

PRÁCTICA # 3

- Consulte que es un Proxy.
 - Consulte las funciones tiene el Firewall o cortafuegos.
 - Consulte que son los puertos 80 y 25?

Práctica # 4

PRÁCTICA # 4

- Compruebe que clase de red es la que tenemos en el Laboratorio de Investigación en Redes Informáticas.
- Para saber qué IP corresponde a un nombre de dominio, podemos usar el comando “**ping**”. Debemos ir al CMD en Windows o Una terminal en Linux y escribir el comando ping, seguido de un espacio y la dirección (IP o nombre de dominio) que nos interesa. Por ejemplo:

“**ping www.utc.edu.ec**” sin comillas.

- Rellena la siguiente tabla usando el comando ping. Añada 10 dominios más de páginas a las que suelas entrar.

Nombre	IP	Clase de Red
www.utc.edu.ec	181.112.224.98	Es de clase B

Taller Práctico # 1

TALLER PRÁCTICO – DIRECCIONAMIENTO IP

¿A qué clase pertenecen las siguientes direcciones IP?. ¿Qué máscara de red usaría para las siguientes direcciones?

IP	Clase de red	Red pública/privada	Máscara de red
214.258.23.35			
47.25.36.14			
3.21.25.41			
125.369.65.21			
45.69.68.24			
192.168.0.1			
11.25.36.54			
192.168.24.58			
210.25.36.84			
177.100.18.4			
119.18.45.0			
223.23.223.109			
10.10.250.1			
126.123.23.2			
220.90.130.1			

¿Cuál de las siguientes direcciones IP no pertenecen a la misma red?

IP	Máscara de red	IP de otros equipos
172.26.0.1	255.255.0.0	172.26.0.100 172.26.10.100 172.26.10.50 172.26.0.300 172.25.0.100 10.12.1.67 12.10.1.67
10.12.1.1	255.0.0.0	1.1.1 10.13.1.1 10.13.1.255 192.189.189.0 192.168.200.257
192.168.200.1	255.255.255.0	192.168.1.1 194.10.10.10 192.168.200.5

Taller Práctico # 2

TALLER PRÁCTICO - CABLEADO BÁSICO DE REDES

OBJETIVOS:

- Identificar la diferencia entre conexión cruzada y conexión directa para el cableado utilizando las normas EIA/TIA T568A y EIA/TIA T568B
- Realizar el cableado básico de las tomas de red Categoría 5.
- Realizar una red LAN empleando conductores de cuatro pares, un Router Switch de cuatro puertos y dos computadores.

EJERCICIOS DE SUBNETEO

En la Empresa XYZ se encuentra una serie de equipos con la misma máscara de subred (255.255.255.224) y cuyas direcciones IP son las que se exponen a continuación. Indicar cuántas redes existen y cuántas subredes y equipos existen y cuántas son posibles.

192.168.1.1

192.168.1.34

192.168.1.67

192.168.1.100

192.168.1.2

192.168.1.36

192.168.1.70

192.168.1.104

192.168.1.3

192.168.1.37

192.168.1.69

192.168.1.103

192.168.1.4

192.168.1.40

192.168.2.71

192.168.2.111

192.168.2.5

192.168.2.44

SOLUCIÓN

En **primer lugar**, observamos que todas las direcciones empiezan por 192, por lo que deducimos que la red o redes que existen son de clase C, por lo tanto, la dirección viene definida por los tres primeros bytes.

En **segundo lugar**, comprobamos que sólo hay dos tipos de direcciones con los tres primeros bytes diferentes: 192.168.1 y 192.168.2. Esto implica que en la instalación hay dos redes.

En tercer lugar, como las dos redes son clase C y la máscara de red es 255.255.255.224 que en binario es: 11111111.11111111.11111111.11100000, y dado que los tres primeros bytes indican la red, la subred dentro de la red vendrá determinada por los tres primeros bits del último byte. Fijándonos en esos bits, verificamos que hay las siguientes direcciones diferentes:

a) Para la red 192.168.1 encontramos:

192.168.1.[000XXXXX] ;

192.168.1.[001XXXXX] ;

192.168.1.[010XXXXX] y

192.168.1.[011XXXXX].

Es decir, **cuatro subredes**

b) Para la red 192.168.2 encontramos:

192.168.2.[000XXXXX] ;

192.168.2.[001XXXXX] ;

192.168.2.[010XXXXX] y

192.168.2.[011XXXXX]

Es decir, **cuatro subredes**

En total existen **ocho subredes**.

En cuanto al número de equipos vemos que, clasificados por subred, hay los siguientes:

Subred: 192.168.1.0 - **cuatro equipos**

192.168.1.1

192.168.1.2

192.168.1.3

192.168.1.4

Subred: 192.168.1.32 - **cuatro equipos**

192.168.1.34

192.168.1.36

192.168.1.37

192.168.1.40

Subred: 192.168.1.64 - **tres equipos**

192.168.1.67

192.168.1.69

192.168.1.70

Subred: 192.168.1.96 - **tres equipos**

192.168.1.100

192.168.1.103

192.168.1.104

Subred: 192.168.2.0 - **un equipo**

192.168.2.5

Subred: 192.168.2.32 - **un equipo**

192.168.2.44

Subred: 192.168.2.64 - **un equipo**

192.168.2.71

Subred: 192.168.2.96 - **un equipo**

192.168.2.111

En total **18 equipos**

El número de subredes posibles es, dado que hay tres bits para definirlas, **ocho (dos elevado a tres) subredes por red, es decir, 16 subredes.**

El número de equipos posibles es **32 por subred**, ya que hay cinco bits para definir la estación y dos elevado a cinco son 32. En total, serán posibles 8 subredes por 32 equipos/subred, es decir, **256 equipos.**

Pero si atendemos al número de redes existentes, entonces, como hay dos redes clase C (que permiten 256 equipos), habrá 2 redes por 256 equipos/red, es decir, **512 equipos.**

RESULTADOS

Redes existentes: 2

Subredes existentes: 8

Equipos existentes: 18

Subredes posibles: 16 (8 por red)

Equipos posibles en función de las subredes existentes: 256 (32 por subred)

Equipos posibles en función de las redes existentes: 512 (256 por red)

EJERCICIOS PROPUESTOS

1. **En la empresa ABC** encontramos una serie de equipos con la misma máscara de subred (255.255.255.224) y cuyas direcciones IP son las que se exponen a continuación. **Indicar cuántas redes existen y cuántas subredes y equipos existen y cuántas son posibles?.**

192.168.1.129 ; 192.168.1.162 ; 192.168.1.195 ; 192.168.1.228

192.168.1.130 ; 192.168.1.164 ; 192.168.1.198 ; 192.168.1.232

192.168.1.131 ; 192.168.1.165 ; 192.168.1.197 ; 192.168.1.233

192.168.1.132 ; 192.168.1.168 ; 192.168.2.199 ; 192.168.2.239

192.168.2.133 ; 192.168.2.172

2. En la empresa XYZA, encontramos una serie de equipos con la misma máscara de subred (255.255.255.224) y cuyas direcciones IP son las que se exponen a continuación. Indicar cuántas redes existen y cuántas subredes y equipos existen y cuántas son posibles.

10.0.1.129 ; 10.0.1.162 ; 10.1.1.195 ; 10.1.1.228

10.0.1.130 ; 10.0.1.164 ; 10.1.1.198 ; 10.1.1.232

10.0.1.131 ; 10.0.1.165 ; 10.1.1.197 ; 10.1.1.233

10.0.1.132 ; 10.0.1.168 ; 10.1.2.199 ; 10.1.2.239

10.0.2.133 ; 10.0.2.172

3. Su red utiliza la dirección IP 172.30.0.0/16. Inicialmente existen 25 subredes

Con un mínimo de 1000 hosts por subred. Se proyecta un crecimiento en los próximos años de un total de 55 subredes. ¿Qué máscara de subred se deberá utilizar?

A. 255.255.240.0

B. 255.255.248.0

C. 255.255.252.0

D. 255.255.254.0

E. 255.255.255.0

4. Usted planea la migración de 100 ordenadores de IPX/SPX a TCP/IP y que puedan establecer conectividad con Internet. Su ISP le ha asignado la dirección IP 192.168.16.0/24. Se requieren 10 Subredes con 10 hosts cada una. ¿Qué máscara de subred debe utilizarse?

a. 255.255.255.224

b. 255.255.255.192

c. 255.255.255.240

d. 255.255.255.248

5. Una red está dividida en 8 subredes de una clase B. ¿Qué máscara de subred se deberá utilizar si se pretende tener 2500 host por subred

a. 255.248.0.0

b. 255.255.240.0

c. 255.255.248.0

d. 255.255.255.255

e. 255.255.224.0

f. 255.255.252.0

g. 172.16.252.0

PRACTICAS DE CONFIGURACIÓN DE SERVIDORES EN PACKET TRACER.

PRÁCTICAS DE LABORATORIO

Fecha:		Practica #	1
Tema o Descripción:	SERVIDOR DHCP		
Nombre del alumno:			
Ciclo:			

INTRODUCCIÓN:

SERVIDOR DHCP

DHCP (siglas en inglés de *Dynamic Host Configuration Protocol*, en español (protocolo de configuración dinámica de host) es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente. Este protocolo se publicó en octubre de 1993.

DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si fuera el caso en que el dispositivo es conectado en un lugar diferente de la red.

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

- **Asignación manual o estática.** - Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.
- **Asignación automática.** - Asigna una dirección IP a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.
- **Asignación dinámica.** - El único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada dispositivo conectado a la red está configurado para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes.

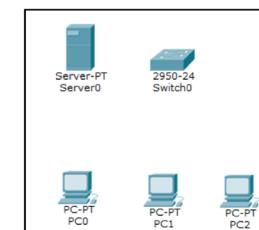
DESARROLLO DE LA PRÁCTICA

Para la resolución de este ejercicio, se utilizará el software Cisco Packet Tracer 7.

1. Materiales y equipos a utilizar

- 1 servidor genérico
- 3 PCs genéricos

- 1 switch

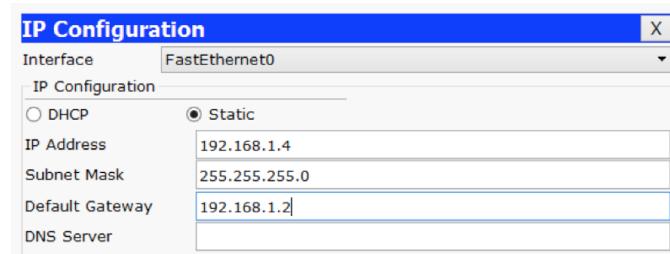


3 Definir rangos de IPs

- Gateway 192.168.1.2
- DNS 192.168.1.3
- DHCP 192.168.1.4
- WEB 192.168.1.5
- CORREO 192.168.1.6
- PCs Desde la 192.168.1.10

4 Procedimiento:

- El primer paso consiste en asignar nombres al Servidor.
- Seleccionamos el Servidor, ingresamos a configuraciones y le asignamos la dirección IP, en este caso es 192.168.1.4, mascara de 255.255.255.0 y **Gateway** 192.168.1.2.



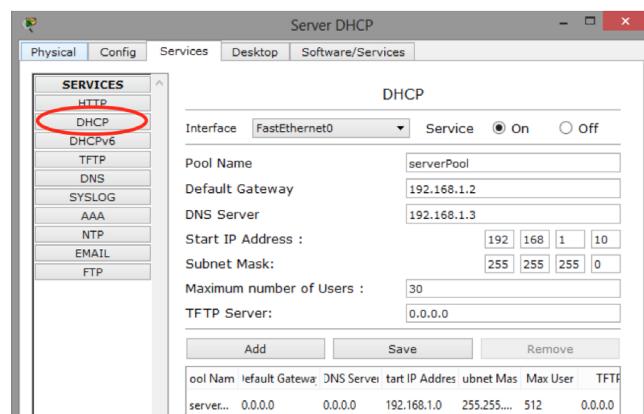
- Ingresamos a la opción **CONFIG** y buscamos el submenú **SERVICE** y ahí **DHCP**.

o Service DHCP
 o Default Gateway 192.168.1.2
 o Server DNS 192.168.1.3

Asignar IP

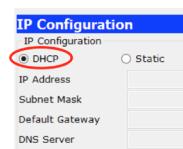
o Star 192.168.1.10
 255.255.255.0
 o # max Usuarios 30

o Levantar el Servidor seleccionando la opción ON



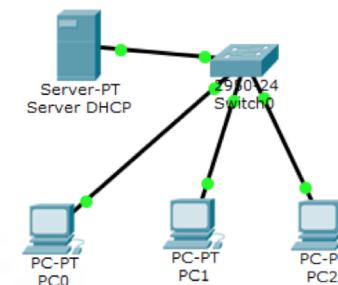
Cerrar la Ventana

- Seleccionamos una de las PCs e ingresamos a su ventana de configuración y cambiamos de Static a DHCP.



El servidor armado y configurado quedaría de la siguiente manera:

IPs	
Gateway	192.168.1.2
DNS	192.168.1.3
DHCP	192.168.1.4
WEB	192.168.1.5
Correo	192.168.1.6
PCs	192.168.1.10



PRÁCTICAS DE LABORATORIO

Fecha:		Practica #	2
Tema o Descripción:	SERVIDOR WEB		
Nombre del alumno:			
Ciclo:			

INTRODUCCIÓN:

SERVIDOR WEB

Un **servidor web** o **servidor HTTP** es un programa informático que procesa una aplicación del lado del servidor, realizando conexiones bidireccionales y/o unidireccionales y síncronas o asíncronas con el cliente y generando o cediendo una respuesta en cualquier lenguaje o Aplicación del lado del cliente.

El código recibido por el cliente es renderizado por un navegador web. Para la transmisión de todos estos datos suele utilizarse algún protocolo. Generalmente se usa el protocolo HTTP para estas comunicaciones, perteneciente a la capa de aplicación del modelo

OSI. El término también se emplea para referirse al ordenador que ejecuta el programa.

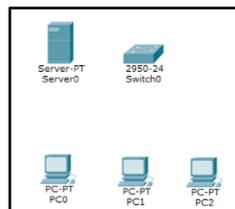
Un servidor web opera mediante el protocolo HTTP, de la capa de aplicación del Modelo OSI. Al protocolo HTTP se le asigna habitualmente el puerto TCP 80. Las peticiones al servidor suelen realizarse mediante HTTP utilizando el método de petición GET, en el que el recurso se solicita a través de la URL al servidor Web.

DESARROLLO DE LA PRÁCTICA

Para la resolución de este ejercicio, se utilizará el software Cisco Packet Tracer 6.3.

5. Materiales y equipos a utilizar

- 1 servidor genérico
- 3 PCs genéricos
- 1 switch



6. Definir rangos de IPs

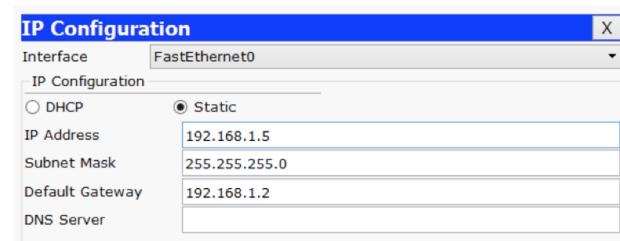
- Gateway 192.168.1.2
- DNS 192.168.1.3
- DHCP 192.168.1.4
- WEB 192.168.1.5
- CORREO 192.168.1.6
- PCs Desde la 192.168.1.10

7. Procedimiento:

- El primer paso consiste en asignar nombres al Servidor.
- Configurar los equipos

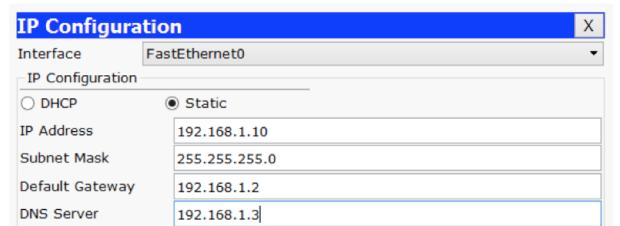
Server

IP 192.168.1.5
Mascara 255.255.255.0
Gateway 192.168.1.2



PC

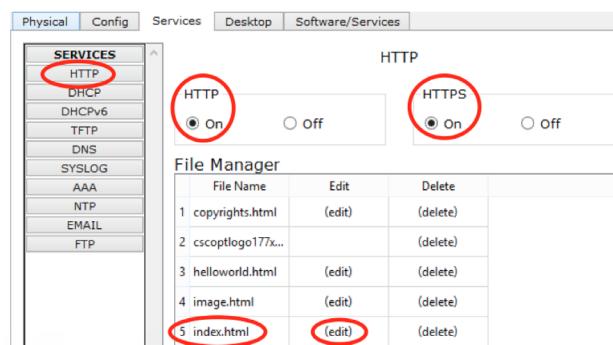
IP 192.168.1.10
Mascara 255.255.255.0
Gateway 192.168.1.2
DNS 192.168.1.3



•CONFIGURACIÓN DEL SERVER:

Ingresamos a configuraciones y seleccionamos SERVICES, ahí buscamos HTTP, Manipulamos el código Fuente para poder comprobar los cambios, el código fuente con el que debemos trabajar se encuentra en [index.html](#), ahí escogemos la opción editar.

Nos aparece el siguiente código fuente, lo que esta con rojo es los que se ha editado para el ejemplo.



```

<html>
<center><font size='2' color='blue'>PRUEBA DEL SERVIDOR</font></center>

<hr>Bienvenidos a mi Sitio Web

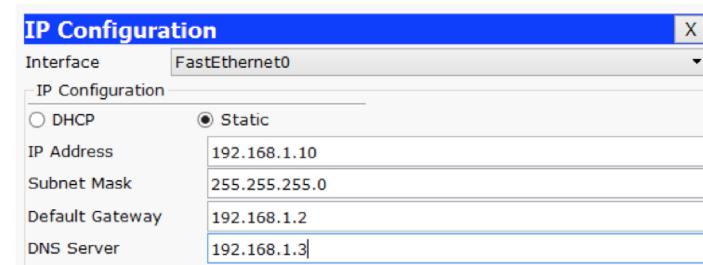
<p>Quick Links:</p>
<br><a href='helloworld.html'>A small page</a>
<h1><font color='red'> Mi nombre es Jorge</font></h1>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscptlogo177x111.jpg'>Image</a>
</html>

```

- Regresamos a la opción HTTP y nos fijamos que se encuentre en ON HTTP y HTTPS, caso contrario el servidor no funcionará.

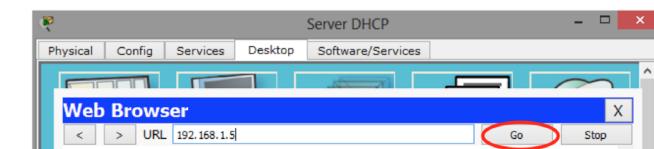
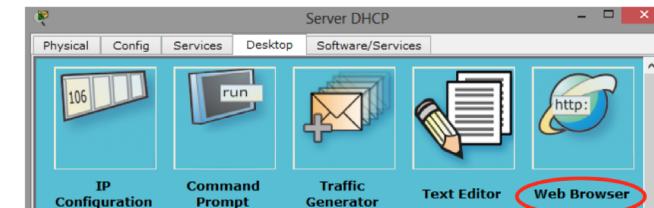
CONFIGURACIÓN DE LAS PCS

- Seleccionamos la PC y entramos a sus configuraciones
- Asignamos las direcciones IP, Mascara, Gateway y DNS que se nos pida, en base a la tabla realizada anteriormente.



- En las mismas configuraciones buscamos la opción Web Browser, ingresamos a la opción y en la barra de direcciones escribimos la IP del Servidor 192.168.1.5 y presionamos GO.

Como se puede ver ya se nos despliega la página web que hemos creado.



Como complemento de esta práctica es necesario que se configure también un servidor DNS, para no tener que ingresar la dirección IP del Servidor, sino el nombre de dominio del sitio.

PRÁCTICAS DE LABORATORIO

Fecha:		Practica #	3
Tema o Descripción:	SERVIDOR DNS.		
Nombre del alumno:			
Ciclo:			

INTRODUCCIÓN:

SERVIDOR DNS

El Sistema de Nombres de Dominio o DNS es un sistema de nomenclatura jerárquico que se ocupa de la administración del espacio de nombres de dominio (Domain Name Space). Su labor primordial consiste en resolver las peticiones de asignación de nombres. Esta función se podría explicar mediante una comparación con un servicio telefónico de información que dispone de datos de contacto actuales y los facilita cuando alguien los solicita. Para ello, el sistema de nombres de dominio recurre a una red global de servidores DNS, que subdividen el espacio de nombres en zonas administradas de forma independiente las unas de las otras. Esto permite la gestión descentralizada de la información de los dominios.

Cuando se quiere acceder a una página web en Internet se necesita la **dirección IP** del servidor donde está almacenada, pero, por regla general, el usuario solo conoce el nombre del dominio. La razón no es otra que la dificultad de recordar las series numéricas del tipo **93.184.216.34** que las componen, que son las que, precisamente, constituyen la base de la comunicación en Internet. Es por este motivo por el que las direcciones IP se “traducen” en nombres que podamos recordar, los llamados dominios:

Dirección IP: 93.184.216.34

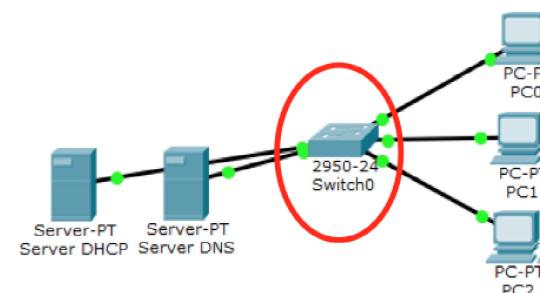
Dominio: www.ejemplo.es

DESARROLLO DE LA PRÁCTICA

Para la resolución de este ejercicio, se utilizará el software Cisco Packet Tracer 6.3.

2. Materiales y equipos a utilizar

- 1 servidor genérico.
- Se utilizará la misma red del Servidor Web.

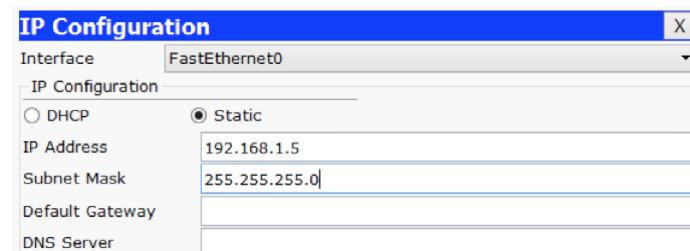


Configuración del Servidor

- Asignamos la Dirección IP y Mascara. NINGUNA MAS.

IP 192.168.1.5

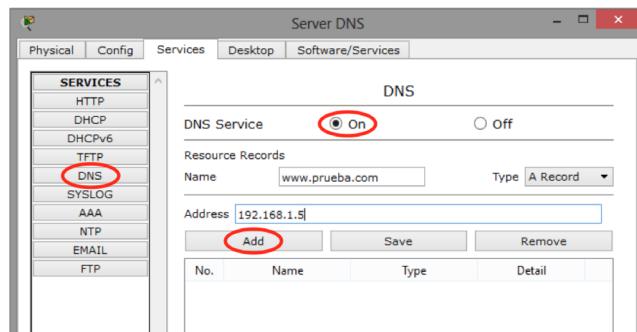
Mascara 255.255.255.0



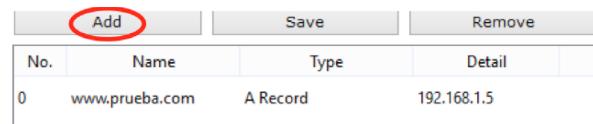
Ingresamos a Configuraciones y en Servicios seleccionamos DNS, en donde vamos a realizamos lo siguiente:

Name: **www.prueba.com**

Address: **192.168.1.5**



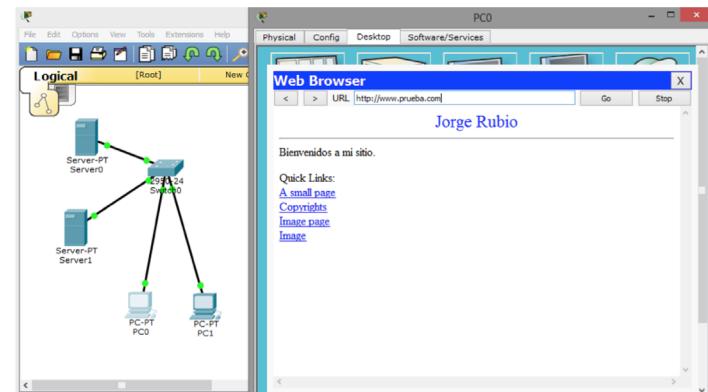
y hacemos clic en ADD para agregar la configuración



Nos fijamos que los servicios se encuentren **ON** y cerramos la ventana.

Desde la PC ingresamos a Configuraciones buscamos la opción Web Browser, ingresamos a la opción y en la barra de direcciones escribimos ya no la IP del Servidor sino la dirección de dominio que en este caso es **www.prueba.com** y presionamos **GO**.

Como se puede ver ya se nos despliega la página web que hemos creado.



PRÁCTICAS DE LABORATORIO

Fecha:		Practica #	4
Tema o Descripción:	SERVIDOR DE CORREO ELECTRÓNICO (MAIL)		
Nombre del alumno:			
Ciclo:			

INTRODUCCIÓN:

SERVIDOR CORREO (MAIL)

Un servidor de correo es una aplicación que nos permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta:

- **SMTP, Simple Mail Transfer Protocol:** Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.
- **POP, Post Office Protocol:** Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

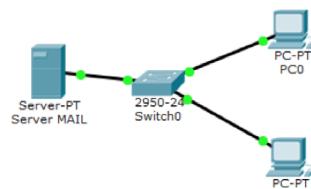
- **IMAP, Internet Message Access Protocol:** Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.
- Así pues, un servidor de correo consta en realidad de dos servidores: **un servidor SMTP** que será el encargado de enviar y recibir mensajes, y **un servidor POP/IMAP** que será el que permita a los usuarios obtener sus mensajes.

DESARROLLO DE LA PRÁCTICA

Para la resolución de este ejercicio, se utilizará el software Cisco Packet Tracer 6.3.

8. Materiales y equipos a utilizar

- 1 servidor genérico
- 2 PCs genéricos
- 1 switch



9. Definir rangos de IPs

- Gateway 192.168.1.2
- DNS 192.168.1.3
- DHCP 192.168.1.4
- WEB 192.168.1.5
- CORREO 192.168.1.6
- PCs Desde la 192.168.1.10

10. Procedimiento:

- El primer paso consiste en asignar nombres al Servidor.
- Configurar los equipos

Server Mail

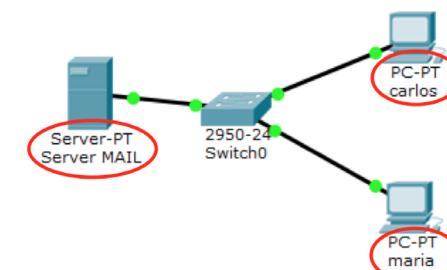
IP	192.168.1.6
Mascara	255.255.255.0
Gateway	192.168.1.2

PC 1 Carlos

IP	192.168.1.10
Mascara	255.255.255.0
Gateway	192.168.1.2
DNS	192.168.1.3

PC2 María

IP	192.168.1.11
Mascara	255.255.255.0
Gateway	192.168.1.2
DNS	192.168.1.3

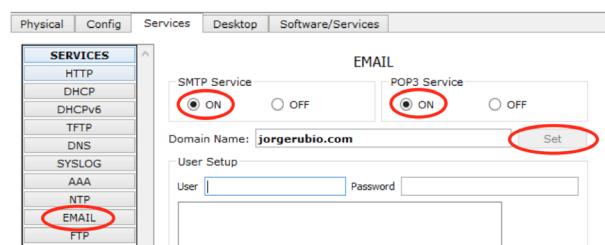


• CONFIGURACIÓN DEL SERVER

Ingresamos a configuraciones y seleccionamos **SERVICES**, ahí en primer lugar revisamos que todos los servicios se encuentren apagados **OFF**, para evitar conflictos con los servicios.

Ahora revisamos que el **servicio Email**, se encuentre encendido **ON**.

En la pantalla que se nos presenta ingresamos un nombre de dominio. Ejm. **www.jorgerubio.com** y presionamos el botón **SET**.

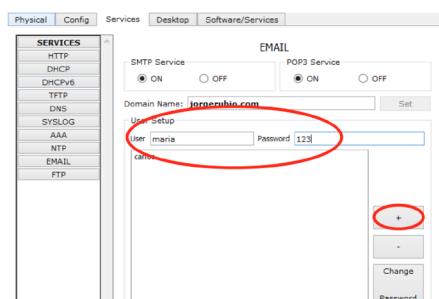


En el siguiente formulario ingresamos los datos que nos piden **USER SETUP** para asignar usuarios.

User: carlos Password:123

User: maria Password:123

presionamos **el icono +** para agregar más usuarios, una vez ingresados todos los usuarios, solo cerramos la ventana.



• CONFIGURACIÓN DEL USUARIOS:

Ingresamos a configuraciones y seleccionamos **DESKTOP**, seleccionamos la **opción EMAIL** y como es la primera vez que ingresamos tenemos que llenar el formulario con el dato de los clientes, cuando llenamos los datos de los usuarios debemos tener en cuenta que el correo deberá ir con el nombre del dominio que pusimos, Ejm: **carlos@jorgerubio.com**, en este caso es la maquina PC1 de Carlos

Lo más importante es seleccionar el servidor de entrada y de salida del correo:

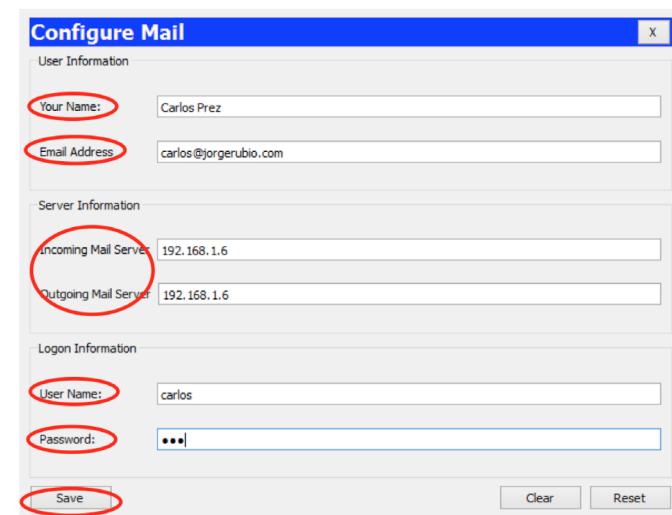
Incoming mail Server 192.168.1.6 (es la misma IP del Servidor)

Outgoing Server 192.168.1.6 (es la misma IP del Servidor)

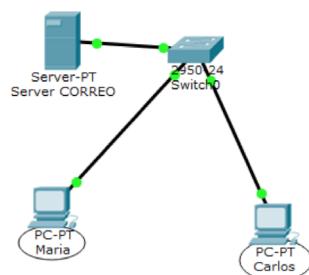
Volvemos a ingresar el nombre de usuario y la contraseña

User Namer Carlos

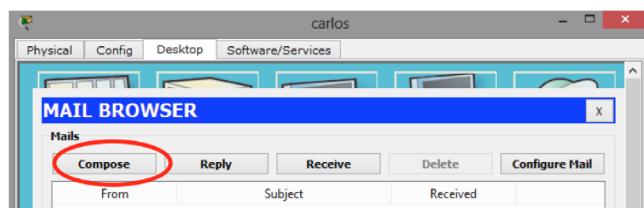
Password 123 y SAVE (Guardar)



Repetimos el mismo procedimiento a la Maquina PC2 María, en este caso con los datos de ella.



Para comprobar el funcionamiento ingresamos a las configuraciones DESKTOP y buscamos **Configure Mail** y se abrirá la opción **Mail Browser**, ahí en la opción **compose**, se escribirá un correo desde la máquina de Carlos a la máquina de maría.



Y redactamos el correo y presionamos Send.



Luego nos vamos a la máquina de María ingresamos a las configuraciones DESKTOP y buscamos **Configure Mail** y se abrirá la opción **Mail Browser**, ahí en la opción **RECEIVE** para poder leer el correo que se envió desde Carlos.

PRÁCTICAS DE LABORATORIO

Fecha:		Practica #	5
Tema o Descripción:	Configuración básica de un Router Cisco		
Nombre del alumno:			
Ciclo:			

INTRODUCCIÓN:

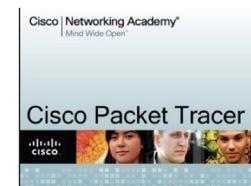
Configurar un router, al principio, parece una tarea complicada. Con el paso del tiempo, aprendiendo los comandos, sus funciones y configurando, nos vamos a dar cuenta que no lo es para nada, todo lo contrario, termina siendo un proceso simple, mecánico.



Este tutorial solo contiene la configuración básica de un router, la que deberemos realizar siempre, sin importar que protocolos de enrutamiento o servicios que se configuren después.

ACTIVIDAD

Vamos a explicar los pasos básicos para configurar un Router Cisco, para lo cual utilizaremos el programa de simulación Packet Tracer 6.3.



COMENCEMOS LA CONFIGURACIÓN:

Los routers tienen varios Modos y Submodos de configuración.

- **Modo Exec Usuario:** Este modo solo permite ver información limitada de la configuración del router y no permite modificación alguna de ésta.
- **Modo Exec Privilegiado:** Este modo permite ver en detalle la configuración del router para hacer diagnósticos y pruebas. También permite trabajar con los archivos de configuración del router (Flash - NVRAM).
- **Modo de Configuración Global:** Este modo permite la configuración básica de router y permite el acceso a submodos de configuración específicos.

CONFIGURACIONES BÁSICA DE UN ROUTER

• NOMBRAR AL ROUTER

```
router> enable  
router# configure terminal  
router(config)# hostname RouterA (nombra al router como)  
RouterA(config)#{}
```

• CONFIGURAR CONTRASEÑAS “ENABLE SECRET” Y “ENABLE PASSWORD”

```
RouterA> enable  
RouterA# configure terminal  
RouterA(config)# enable secret contraseña * (configura contraseña Enable  
Secret)  
RouterA(config)# enable password contraseña (configura  
contraseña Enable)
```

Password)

```
RouterA(config)#
```

* Es recomendable configurar Enable Secret ya que genera una clave global cifrada en el router.

•CONFIGURAR CONTRASEÑA DE CONSOLA RouterA> enable

```
RouterA# config terminal  
RouterA(config)# line con 0 (ingresa a la Consola)  
RouterA(config-line)# password contraseña (configura contraseña)  
RouterA(config-line)# login (habilita la contraseña)  
RouterA(config-line)# exit  
RouterA(config)#{}
```

•CONFIGURAR CONTRASEÑA VTY (TELNET) RouterA> enable

```
RouterA# config terminal  
RouterA(config)# line vty 0 4 (crea las 5 líneas VTY, pero podría  
ser una sola. Ej: line vty 0)  
RouterA(config-line)# password contraseña (contraseña para las 5  
líneas en este caso)
```

```
RouterA(config-line)# login (habilita la contraseña)  
RouterA(config-line)# exit
```

```
RouterA(config)#{}
```

•CONFIGURAR INTERFACES ETHERNET 6 FAST ETHERNET RouterA> enable

```
RouterA# config terminal
```

```
RouterA(config)# interface fastethernet 0/0 * (ingresa al Submodo de
```

Configuración de Interfaz)

```
RouterA(config-if)# ip address 192.168.0.1 255.255.255.0 (configura la IP en la interfaz)
```

```
RouterA(config-if)# no shutdown (levanta la interfaz).
```

```
RouterA(config-if)# description lan (asigna un nombre a la interfaz)
```

```
RouterA(config-if)# exit
```

```
RouterA(config)#
```

* Tener en cuenta que la interfaz puede ser Ethernet o Fast Ethernet y que el número de interfaz puede ser 0, 1, 0/0, 0/1, etc. Esto varía según el router.

- **CONFIGURAR INTERFACES SERIAL COMO DTE**
RouterA> enable

```
RouterA# config terminal
```

```
RouterA(config)# interface serial 0/0 * (ingresa al Submodo de Configuración de Interfaz)
```

```
RouterA(config-if)# ip address 10.0.0.1 255.0.0.0 (configura la IP en la interfaz)
```

```
RouterA(config-if)# no shutdown (levanta la interfaz)  
RouterA(config-if)# description red (asigna un nombre a la interfaz)  
RouterA(config-if)# exit
```

```
RouterA(config)#
```

* Tener en cuenta que el número de interfaz puede ser 0, 1, 0/0, 0/1, etc. Esto varía según el router.

- **CONFIGURAR INTERFACES SERIAL COMO DCE**
RouterB> enable

```
RouterB# config terminal
```

```
RouterB(config)# interface serial 0/1 * (ingresa al Submodo de Configuración de Interfaz)
```

```
RouterB(config-if)# ip address 10.0.0.2 255.0.0.0 (configura la IP en la interfaz)
```

```
RouterB(config-if)# clock rate 56000 (configura la sincronización entre los enlaces)
```

```
RouterB(config-if)# no shutdown (levanta la interfaz)  
RouterB(config-if)# description red (asigna un nombre a la interfaz)  
RouterB(config-if)# exit
```

```
RouterB(config)#
```

* Tener en cuenta que el número de interfaz puede ser 0, 1, 0/0, 0/1, etc. Esto varía según el router.

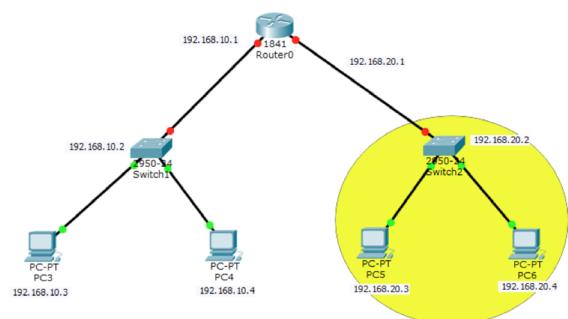
Por último, una vez configurada la interfaz lan (fastethernet), se conectará un switch al router y los pcs de la clase se conectarán al switch y podrán comunicarse entre si.

PRÁCTICAS DE LABORATORIO

Fecha:		Practica #	6
Tema o Descripción:	Configuración de una red con un Router Cisco, dos switch y 4 computadores.		
Nombre del alumno:			
Ciclo:			

INTRODUCCIÓN:

Configurar una red con un router, dos switch y 4 pc distribuidas en dos redes, al principio parece una tarea complicada. Con el paso del tiempo, aprendiendo los comandos, sus funciones y configurando, nos vamos a dar cuenta que no lo es para nada, todo lo contrario, termina siendo un proceso simple, mecánico.



DESARROLLO DE LA PRÁCTICA

Para la resolución de este ejercicio, se utilizará el software de simulación Cisco Packet Tracer 6.3.

Materiales y equipos a utilizar

- Router
- 2 Switch
- 4 Pcs

Todos estos equipos se encuentran distribuidos en dos redes, tal como se puede visualizar en el grafico anterior, los rangos de IP utilizados son los siguientes:

RED 1

Puerto 0/0 de router	192.168.10.1	255.255.255.0
Switch	192.168.10.2	255.255.255.0
Pc1	192.168.10.3	255.255.255.0
Pc2	192.168.10.4	255.255.255.0

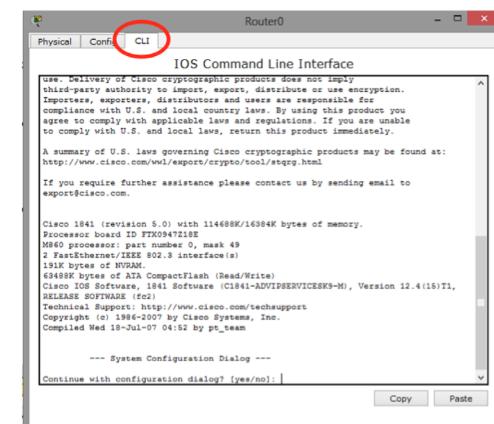
RED 2

Puerto 0/1 de router	192.168.20.1	255.255.255.0
Switch	192.168.20.2	255.255.255.0
Pc3	192.168.20.3	255.255.255.0
Pc4	192.168.20.4	255.255.255.0

Asignamos direcciones IP a las PCs según la tabla indicada y en el parámetro Gateway ponemos la dirección del router (la dirección del segmento de router que pertenece a esa red).

CONFIGURACIÓN INICIAL DEL ROUTER.

- Ingresamos al router y seleccionamos la opción CLI, que me permite trabajar con línea de comandos.



- En la pantalla que nos aparece iniciamos la palabra **NO** y enter
- Una vez ahí realizamos la siguiente configuración:

PRIMER PUERTO DEL ROUTER

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname prueba

prueba(config)#interface GigabitEthernet 0/0

prueba(config-if)#ip address 192.168.10.1 255.255.255.0

prueba(config-if)#no shutdown

prueba(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
exit

prueba(config)#exit

prueba#

%SYS-5-CONFIG_I: Configured from console by console

exit

SEGUNDO PUERTO DEL ROUTER

Router>enable

Router#configure terminal

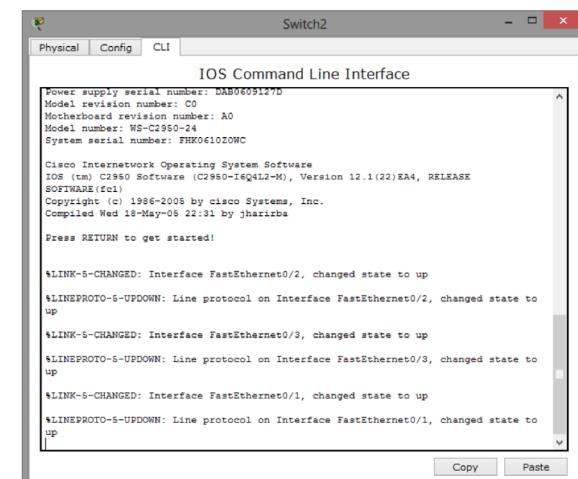
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname prueba

prueba(config)#interface GigabitEthernet 0/1

```
prueba(config-if)#ip address 192.168.20.1 255.255.255.0
prueba(config-if)#no shutdown
prueba(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
exit
prueba(config)#exit
prueba#
%SYS-5-CONFIG_I: Configured from console by console
Exit
```

Hasta el momento se ha configurado el router, el siguiente paso es la configuración de los Switchs de cada segmento de red, para esto seguimos el mismo procedimiento, en primer lugar, seleccionamos el switch del lado del puerto 0/0 y hacemos clic sobre el para luego seleccionarlo y escoger la opción de consola en la pantalla en la opción CLI.



Iniciamos la configuración del Switch:

PRIMER SWITCH

Switch>enable

Switch#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#**hostname prueba**

prueba(config)#**interface vlan1**

prueba(config-if)#**ip address 192.168.10.2 255.255.255.0**

prueba(config-if)#**no shutdown**

prueba(config-if)#{

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

exit

prueba(config)#**ip default-gateway 192.168.10.1**

prueba(config)#**do write**

Building configuration...

[OK]

prueba(config)#{

SEGUNDO SWITCH

Switch>**enable**

Switch#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#**hostname prueba**

prueba(config)#**interface vlan1**

prueba(config-if)#**ip address 192.168.20.2 255.255.255.0**

prueba(config-if)#**no shutdown**

prueba(config-if)#{

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

exit

prueba(config)#**ip default-gateway 192.168.20.1**

prueba(config)#**do write**

Building configuration...

[OK]

prueba(config)#{

GLOSARIO

- AAA: Abreviatura de Autenticación (Authentication), Autorización (Authorization) y Contabilidad (Accounting), sistema en redes IP para qué recursos informáticos tiene acceso el usuario y rastrear la actividad del usuario en la red.
- ACCOUNTING: Es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede así como los datos transferidos durante la sesión.
- AD HOC: Una WLAN bajo topología “Ad Hoc” consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso.
- AES: También conocido como “Rijndael”, algoritmo de encriptación simétrica de 128 bits desarrollado por los belgas Joan Daemen y Vincent Rijmen.
- ALGORITMO DE ENCRYPTACIÓN: Codificadores de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma/producto modular y transformaciones lineales.
- ATAQUES A PASSWORDS: Es un intento de obtener o descifrar una contraseña legítima de usuario.
- ATAQUE DE DICCCIONARIO: Método empleado para romper la seguridad de los sistemas basados en contraseñas en la que el atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles o recogidas en un diccionario idiomático.
- ATAQUE DE FUERZA BRUTA: Método empleado para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras (distinto del ataque de diccionario que prueba palabras aisladas).

- AUDITORÍA: Análisis de las condiciones de una instalación informática por un auditor externo e independiente que realiza un dictamen sobre diferentes aspectos.
- AUTENTICACIÓN: Es el proceso de identificación de un individuo, normalmente mediante un nombre de usuario y contraseña.
- AUTORIZACIÓN: Es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito.
- BRIDGE: Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar.
- CHAP (Challenge Handshake Authentication Protocol): Protocolo de autenticación para servidores PPP donde la contraseña no sólo se exige al empezar la conexión sino también durante la conexión, lo cual lo hace un protocolo mucho más seguro que el PAP.
- CIFRADO: Proceso para transformar la información escrita en texto simple a texto codificado.
- CIFRADO ASIMÉTRICO: Cifrado que permite que la clave utilizada para cifrar sea diferente a la utilizada para descifrar.
- CIFRADO DE ARCHIVOS: Transformación de los contenidos texto simple de un archivo a un formato ininteligible mediante algún sistema de cifrado.
- CLIENTE INALÁMBRICO: Todo dispositivo susceptible de integrarse en una red inalámbrica como PDAs, portátiles, cámaras inalámbricas, impresoras.
- CLAVE DE CIFRADO: Serie de números utilizados por un algoritmo de cifrado para transformar texto sin cifrar que se puede leer directamente en datos cifrados y viceversa.
- CONFIDENCIALIDAD: Garantizar que la información sea asequible sólo a aquellas personas autorizadas a tener acceso a ella.

- CONTROL DE ACCESOS: Se utiliza para restringir el acceso a determinadas áreas del computador, de la red, etc.
- EAP - Protocolo de Autenticación Extensible (Extensible Authentication Protocol): Extensión del Protocolo Punto a Punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación.
- ESTÁNDAR: Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos.
- FAST (Flexible Authentication Secure Tunneling): Protocolo de seguridad WLAN del tipo EAP. Impide los denominados ataques de diccionario por fuerza bruta enviando una autenticación de contraseña entre el cliente WLAN y el punto de acceso inalámbrico a través de un túnel cifrado seguro. Elimina la necesidad de instalar servidores separados para tratar los certificados digitales empleados en otro sistema de seguridad WLAN (como el PEAP).
- HOT SPOT: Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles) que proporciona servicios de red inalámbrica de banda ancha a visitantes móviles.
- IEEE: Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización entre otras actividades, su trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales.
- INFRAESTRUCTURA: Topología de una red inalámbrica que consta de dos elementos básicos: estaciones clientes inalámbricos y puntos de acceso.
- ISP: Proveedor de Servicios de Internet.
- LEAP (Lightweight Extensible Authentication Protocol): Protocolo del tipo EAP patentado por Cisco basado en nombre de usuario y contraseña que se envía sin protección.

- MAC - Dirección de Control de Acceso al Medio (Media Access Control Address): Dirección hardware de 6 bytes (48 bits) única que identifica cada tarjeta de una red y se representa en notación hexadecimal.
- MD5: Algoritmo de cifrado de 128-bits del tipo EAP empleado para crear firmas digitales.
- 802.11: Familia de estándares desarrollados por la IEEE para tecnologías de red inalámbricas.
- 802.11a: Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de 5 GHz.
- 802.11b: Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 11 Mbps en una banda de 2.4 GHz. Utiliza la tecnología DSSS (Direct Sequencing Spread). La mayoría de los equipos utilizados en la actualidad son de esta tecnología. No es compatible con el 802.11a pues funciona en otra banda de frecuencia.
- 802.11e: Estándar destinado a mejorar la calidad de servicio en Wi-Fi. Es de suma importancia para la transmisión de voz y video.
- 802.11g: Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de frecuencia de 2.4 GHz. Una de sus ventajas es la compatibilidad con el estándar 802.11b.
- 802.11i: Estándar de seguridad para redes Wi-Fi aprobado a mediados de 2004. En él se define al protocolo de encriptación WPA2 basado en el algoritmo AES.
- 802.11n: Estándar para conseguir mayores velocidades de transmisión para Wi-Fi. Estas serán superiores a 100 Mbps.
- 802.16: Estándar de transmisión inalámbrica conocido como WIMAX. Es compatible con Wi-Fi. La tecnología permite alcanzar velocidades de transmisión de hasta 70 MBit/s en una banda de frecuencias entre 10 GHz y 66 GHz.

- 802.16d: Estándar de transmisión inalámbrica WIMAX que suministra una velocidad de entre 300 Kbps y 2 Mbps en una banda de frecuencia de 2GHz a 11GHz. Se utiliza para el cubrimiento de la “primer milla”.
- 802.1x: Estándar de seguridad para redes inalámbricas y cableadas. Se apoya en el protocolo EAP y establece la necesidad de autenticar y autorizar a cada usuario que se conecte a una red.
- PAP - Protocolo de Autenticación de Contraseñas (Password Authentication Protocol): El método más básico de autenticación, en el cual el nombre de usuario y la contraseña se transmiten a través de una red y se compara con una tabla de parejas nombre-clave, la no coincidencia provocará la desconexión.
- PEAP (Protected Extensible Authentication Protocol): Protocolo del tipo EAP para la transmisión de datos autenticados, incluso claves, sobre redes inalámbricas 802.11. Autentica clientes de red Wi-Fi empleando sólo certificados del lado servidor creando un túnel SSL/TLS cifrado entre el cliente y el servidor de autenticación.
- PKI - Infraestructura de Clave Pública: Sistema de certificados digitales, Autoridades Certificadores y otras entidades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción vía Internet.
- PUNTO DE ACCESO (AP): Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles tanto para centralización como para enrutamiento.
- RADIUS (Remote Authentication Dial-In User Service): Sistema de autenticación y contabilidad empleado por la mayoría de proveedores de servicios de Internet (ISPs).
- RAS - Servidor de Acceso Remoto: Servidor dedicado a la gestión de usuarios que no están en una red pero necesitan acceder remotamente a ésta.
- ROUTER: Es un conmutador de paquetes que opera en el nivel de red del modelo OSI, proporciona un control del tráfico

- y funciones de filtrado; está conectado al menos a dos redes, generalmente dos LANs o WANs o una LAN y la red de un ISP.
- ROAMING: En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad.
 - SERVIDOR DE AUTENTICACIÓN (AS): Servidor que gestiona las bases de datos de todos los usuarios de una red y sus respectivas contraseñas para acceder a determinados recursos.
 - SISTEMA DE CIFRADO: Colección completa de algoritmos que tienen su propia denominación en función de las claves que utilizan para cifrar.
 - SNIFFERS: Programa y/o dispositivo que monitorea la circulación de datos a través de una red. Los sniffers pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información.
 - SSID: Identificador de red inalámbrica, similar al nombre de la red pero a nivel Wi-Fi.
 - TKIP - Protocolo de Integridad de Clave Temporal: Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.
 - VLAN - Red de Área Local Virtual: Tipo de red que aparentemente parece ser una pequeña red de área local (LAN) cuando en realidad es una construcción lógica que permite la conectividad con diferentes paquetes de software. Sus usuarios pueden ser locales o estar distribuidos en diversos lugares.
 - WAN – Red de Área Amplia: Tipo de red compuesta por dos o más redes de área local (LANs).
 - WARCHALKING: Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico.

- WARDRIVING: Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar puntos de acceso inalámbrico.
- WARSPAMMING: Acceso no autorizado a una red inalámbrica y uso ilegítimo de la misma para enviar correo masivo (spam) o realizar otro tipo de acciones que comprometan el correcto uso de un sistema.
- WEP – Privacidad Equivalente a Cableado: Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes inalámbricas que permite cifrar la información que se transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del Vector de inicialización IV), de 128 bits (104 bits más 24 bits del vector de inicialización IV).
- Wi-Fi (Wireless Fidelity): Es el nombre comercial con el cual se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica.
- WIMAX - Interoperabilidad Mundial para Acceso por Microondas: Es un estándar de transmisión inalámbrica de datos (802.16 MAN) proporcionando accesos concurrentes en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa entre el punto transmisor y el receptor.
- WPA - Acceso Protegido Wi-Fi: Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado).
- WPA2 – Protocolo de Aplicación Inalámbrica: Protocolo de seguridad para redes Wi-Fi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Puntos de Acceso de última generación.

REFERENCIA BIBLIOGRÁFICAS

CITADA:

- [1] TANENBAUM Andrew. Redes de Computadores. Pearson Education. México.
- [2] VILLAROEL Carlos, RODRÍGUEZ Angie, VALLE Julio. Diseño de una red de área local inalámbrica. Universidad de Tarapacá Departamento de Electrónica. Arica, Chile 2012.
- [3] STALLINGS William. Wireless Communications and Networks. Prentice - Hall. Estados Unidos 2016.
- [4] BARBERO, Lucas. Tutorial Ethereal. Universidad Tecnológica Nacional 2012.
- [5] YUTACA, Hayacawa. Sistemas de medida wireless LAN y software específico. Revista Española de Electrónica. Barcelona.
- [6] Marcelo Najnudel. “ESTUDO DE PROPAGAÇÃO EM AMBIENTES FECHADOS PARA O PLANEJAMENTO DE WLANS”. Río de Janeiro, Febrero de 2004.
- [7] ANSI/IEEE Std 802.11g. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band. Estados Unidos: Institute of Electrical and Electronics Engineers, 2003. ISBN 0-7381-3701-4 SS95134.
- [8] ATHEROS COMMUNICATIONS INC. 802.11 Wireless LAN Performance. Doc. 991-00002-006. Sunnyvale, CA. 2012.
- [9] CHEUNG, David y PRETTIE Cliff. A Path Loss Comparison Between the 5 GHz UNII Band (802.11a) and the 2.4 GHz ISM Band (802.11b), Inter Labs, Intel Corporation, Enero 2012.
- [10] DE LUQUE Luis, DÍAZ Irina, VASQUEZ Sandra. Predicción del nivel de intensidad de señal recibid RSSI en una red inalámbrica 802.11b mediante un modelo neuronal. Proyecto de Grado. E3T UIS. Bucaramanga 2015.
- [11] ETHEREAL Network Analyzer. Disponible en Internet, URL <<http://www.ethereal.com>>, Enero 2014.

[12] JANGEUN, Jun y MIHAIL, Sichitiu. "The Nominal Capacity of Gíreles Mesh Networks", IEEE Wireless Communications Magazine, Oct. 2003.

[13] LIN Yu-Ju, LATCHMAN Haniph y NEWMAN Richard. "A Comparative Performance Study of Wireless and Power Line Networks", IEEE Communications Magazine, abril 2013.

[14] ARANGO, Jhon, "El Atacante Informàtico", 2016.

[15] GOMEZ, Alvaro, "Encliclopedia de Seguridad Informatica", 2015.

[17] REBOLLEDO, Miguel, Manual de Packet tracer 5.0

CONSULTADA

• TANENBAUM Andrew. Redes de Computadores. Pearson Education. México.

• VILLAROEL Carlos, RODRÍGUEZ Angie, VALLE Julio. Diseño de una red de área local inalámbrica. Universidad de Tarapacá Departamento de Electrónica. Arica, Chile 2012.

• STALLINGS William. Wireless Communications and Networks. Prentice - Hall. Estados Unidos 2016.

• BARBERO, Lucas. Tutorial Ethereal. Universidad Tecnológica Nacional 2012.

• YUTACA, Hayacawa. Sistemas de medida wireless LAN y software específico. Revista Española de Electrónica. Barcelona.

• Marcelo Najnudel. "ESTUDO DE PROPAGAÇÃO EM AMBIENTES FECHADOS PARA O PLANEJAMENTO DE WLANS". Rio de Janeiro, febrero de 2004.

• ANSI/IEEE Std 802.11g. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band. Estados Unidos: Institute of Electrical and Electronics Engineers, 2003. ISBN 0-7381-3701-4 SS95134.

•ATHEROS COMMUNICATIONS INC. 802.11 Wireless LAN Performance. Doc. 991-00002-006. Sunnyvale, CA. 2012.

• CHEUNG, David y PRETTIE Cliff. A Path Loss Comparison Between the 5 GHz UNII Band (802.11a) and the 2.4 GHz ISM Band (802.11b), Inter Labs, Intel Corporation, Enero 2012.

• DE LUQUE Luis, DÍAZ Irina, VASQUEZ Sandra. Predicción del nivel de intensidad de señal recibid RSSI en una red inalámbrica 802.11b mediante un modelo neuronal. Proyecto de Grado. E3T UIS. Bucaramanga 2015.

• ETHEREAL Network Analyzer. Disponible en Internet, URL <<http://www.ethereal.com>>, Enero 2014.

• JANGEUN, Jun y MIHAIL, Sichitiu. "The Nominal Capacity of Gíreles Mesh Networks", IEEE Wireless Communications Magazine, Oct. 2003.

• LIN Yu-Ju, LATCHMAN Haniph y NEWMAN Richard. "A Comparative Performance Study of Wireless and Power Line Networks", IEEE Communications Magazine, abril 2013.

• ARANGO, Jhon, "El Atacante Informàtico", 2016.

• GOMEZ, Alvaro, "Encliclopedia de Seguridad Informatica", 2015.

• REBOLLEDO, Miguel, Manual de Packet tracer 5.0

Direcciones web de referencia.

• <http://www.amp.co/networking/warranty.html>

• <http://www.cintel.org.com.co>

• <http://www.linksys.com>

• <http://www.cisco.com>

• <http://www.trendware.com>

• <http://www.wi-fi.org>

• <http://www.wi-fiplanet.com/tutorials/article.php/1116311>. 2003

• <http://www.3com.com>

• <http://www.upv>.



Universidad
Técnica de
Cotopaxi

ISBN: 978-9978-395-41-7

A standard linear barcode is positioned in the center of a white rectangular box. The box also contains the ISBN number: 9 789978 395417.

9 789978 395417