TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE HERMOSILLO

CONMUTACION Y ENRUTAMIENTO EN REDES DE DATOS

(SCD-1004)

Manual de Prácticas

SEP
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DE HERMOSILLO

CONMUTACION Y ENRUTAMIENTO

EN REDES DE DATOS

(SCD-1004)

Manual de Prácticas

ING. JESÚS EMILIO BARAJAS MARISCAL
Departamento de Sistemas y Computación

Agosto, 2018

TABLA DE CONTENIDOS

PRACTICAS

Departamento de Sistemas y Computación

Ingeniería en Sistemas Computacionales

Instituto Tecnológico de Hermosillo

INTRODUCCION

El presente manual de prácticas constituye una herramienta de apoyo para la comprensión de los conceptos de Conmutación y Enrutamiento en las Redes de Datos. Los cuales son abordados dentro del programa de estudios de la asignatura *Conmutación y Enrutamiento en Redes de Datos (SCD-1004)* correspondiente a la retícula de la carrera Ingeniería en Sistemas Computacionales.

Siguiendo un orden conceptual progresivo en los contenidos de la materia, en la primera sección de este manual de prácticas se aborda el concepto de direccionamiento IP, lo cual es de suma importancia en aplicaciones de tecnología WAN, ya que son las bases del diseño lógico en redes de datos. Además de conocer sus versiones, se introduce el concepto de dominios y subredes mediante lo cual es posible crear estrategias se solución y diseño de redes WAN como el VLSM con el que se aplica la segmentación de dominios. También en este primer tema se comienza a trabajar con el enrutamiento estático y el enrutamiento dinámico entre redes contiguas y no contiguas.

En la segunda sección llamada Tecnologías WAN, de manera más práctica se aborda el tema de administración y monitoreo de los dispositivos WAN. Se describen este tipo de dispositivos, se trata el desarrollo de configuración y la implementación de dispositivos WAN en redes amplias de datos.

Como tercera sección se presenta la parte de diseño e implementación de las Redes Inalámbricas, describiendo la clasificación de las mismas, los dispositivos que la conforman y la configuración básica de sus elementos. Se aborda el tema de seguridad y de algunos servicios especiales que les dan a estas redes inalámbricas, el potencial tecnológico de servicio, flexible y confiable, a los usuarios que cada vez más se suman a esta solución de intercomunicación móvil.

1. DIRECCIONAMIENTO Y ENRUTAMIENTO IP

Objetivo: Conocer la evolución del direccionamiento IP así como las versiones que se han dado a conocer como estándares en el ambiente de la redes de computadoras.

Temas relacionados de la Asignatura: 1.1, 1.1.1, 1.1.2, 1.1.3, 1.4.1, 1.4.2

Sugerencias didácticas: Fomentar actividades grupales que propicien la comunicación, el intercambio argumentado de ideas, la reflexión, la integración y la colaboración entre los estudiantes. Relacionar los contenidos de esta asignatura con las demás del plan de estudios para desarrollar una visión interdisciplinaria en el estudiante. Facilitar el contacto directo con materiales e instrumentos, al llevar a cabo las actividades prácticas, para contribuir a la formación de las competencias definidas.

1.1. DIRECCIONAMIENTO IP Y SUS VERSIONES.

Que es el direccionamiento IP?

El direccionamiento es una función clave de los protocolos de capa de Red que permite la transmisión de datos entre hosts de la misma red o en redes diferentes.

El Protocolo de Internet, llamado comúnmente IP, provee información sobre la red y el host (terminal de datos o dispositivo) ofreciendo direccionamiento jerárquico para paquetes que transportan datos.

Características del direccionamiento IP:

- Las direcciones IP se denominan direcciones lógicas.
- Tienen un direccionamiento Jerárquico.

- Representan una conexión de la máquina a la red y no la máquina misma.
- Utiliza una dirección de 32 bits, agrupados en 4 octetos separados por puntos y representados en forma decimal.
- Cada bit en el octeto tiene un peso binario. El valor mínimo de un octeto, en formato decimal, es de 0 y el máximo de 255.

Existen dos tipos de direcciones especiales:

- *Dirección de red*: permite el enrutamiento entre router. Posee 0 binarios en todos los bits de la parte del Host. Por ejemplo: 172.16.0.0
- *Dirección de broadcast*: permite enviar datos a todos los dispositivos de una red. Posee 1 binarios en todos los bits de la parte del Host.
  Por ejemplo: 172.16.255.255

Versiones del Direccionamiento IP

Actualmente existen dos versiones de IP las cuales se aplican en la red de redes, el Internet: las direcciones del ***IPv4*** (Protocolo de Internet Versión 4) definida en el RFC 791 y las direcciones del ***IPv6*** (Protocolo de Internet versión 6), definida en el RFC 2460.

La diferencia básica entre una y otra es la cantidad de bits que la conforman siendo la IPv4 de 32 bits, mientras que en la IPv6 se utilizan 128 bits.

Clases de Redes según su Direccionamiento (IPv4)

- **CLASE A** del 0 . 0 . 0 .0 al 127. 255. 255. 255
- **CLASE B** del 128 . 0 . 0 .0 al 191. 255. 255. 255
- **CLASE C** del 192 . 0 . 0 .0 al 223. 255. 255. 255
- **CLASE D** del 224 . 0 . 0 .0 al 239. 255. 255. 255

.

Clase A - Esta clase es para las redes muy grandes, tales como las de una gran compañía internacional. Del IP con un primer octeto a partir de 1 al 126 son parte de esta clase. Los otros tres octetos son usados para identificar cada host. Esto significa que hay 126 redes de la clase A con 16,777,214 posibles hosts para un total de 2,147,483,648 direcciones únicas. Las redes de la clase A contemplan la mitad de las direcciones disponibles totales del direccionamiento IP.

Clase B - La clase B se utiliza para las redes de tamaño mediano. Un buen ejemplo es un campus universitario o una nave industrial. Las direcciones del IP con un primer octeto a partir del 128 al 191 son parte de esta clase. Las direcciones de la clase B también incluyen el segundo octeto como parte del identificador neto. Utilizan a los otros dos octetos para identificar cada host.

Clase C - Las direcciones de la clase C se utilizan comúnmente para los negocios pequeños a medianos tamaños. Las direcciones del IP con un primer octeto a partir del 192 al 223 son parte de esta clase. Las direcciones de la clase C también incluyen a segundos y terceros octetos como parte del identificador neto. Utilizan al último octeto para identificar cada host.

Clase D - Utilizado para los multicast, la clase D es levemente diferente de las primeras tres clases. Tiene un primer bit con valor de 1, segundo bit con valor de 1, tercer bit con valor de 1 y cuarto bit con valor de 0. Los otros 28 bits se utilizan para identificar el grupo de computadoras al que el mensaje del multicast está dirigido. Esta clase de redes se utiliza de manera muy particular.

* P R A C T I C A *

Programa SCD-1004:	Práctica Numero:	Nombre de la Práctica:
1.1 Direccionamiento IP y sus Versiones	**1**	**Direccionamiento IP y sus Versiones**

OBJETIVO ESPECIFICO: Conocerá el direccionamiento IP, que es y cómo se aplica. Identificará las distintas versiones y características básicas que permitan al alumno utilizarlas en la configuración de redes de computadoras.

INFORMACION PREVIA: El Protocolo de Internet (IP) es un protocolo de capa de red (Capa 3) diseñado en 1981 para usarse en sistemas interconectados de redes de comunicación computacional de conmutación de paquetes. El Protocolo de Internet y el Protocolo de Control de Transmisión (TCP) son la base de los protocolos de Internet.

El IP tiene dos funciones principales:

- Entrega de datagramas a través de la Internet bajo el mejor esfuerzo.
- Fragmentación y re ensamblado de datagramas.

Se considera al IP un protocolo de “mejor esfuerzo”, ya que no garantiza que un paquete transmitido realmente llegue al destino ni que los datagramas transmitidos sean recibidos en el orden en que fueron enviados. La función principal de IP es llevar paquetes de datos de un nodo fuente a un nodo destino. Este proceso se logra identificando cada paquete enviado con una dirección numérica llamada dirección IP.

Existen dos versiones de direccionamiento IP: la versión 4 (IPv4) y la versión 6 (IPv6). Actualmente la mayoría del tráfico IP es realizado con direccionamiento IPv4, y aunque se pretende que IPv6 reemplace a IPv4 en un futuro, ambos protocolos coexistirán durante algún tiempo.

PROCEDIMIENTO: El alumno elaborará una tabla de referencia del direccionamiento IP analizando la información proveniente de diversas fuentes donde indique, las clases de redes, rangos de direcciones, numero de redes, numero de hosts por subred con su máscara default. Anotando al final, ejemplos de aplicaciones prácticas.

DESARROLLO:

a) Realizar labor de investigación de los conceptos IPv4 e IPv6.
b) Analizar la información para construir una tabla comparativa.
c) Elaborar una tabla que muestre las clases de redes y rangos de direcciones para ambas versiones de IP.
d) Anotar el número de redes, número de hosts por subred con su máscara default.
e) Agregar ejemplos de aplicaciones prácticas de cada una de ellas.

Anota ejemplos prácticos de aplicación de redes clase A, clase B y clase C:

_____

_____

_____

_____

_____

Elabora una tabla comparativa de las versiones del direccionamiento IP

La tabla debe contener las clases de redes, rangos de direcciones, número de redes, número de hosts por subred y su máscara correspondiente.

1.2 El direccionamiento IP y el concepto de Dominio.

Direccionamiento IP.

Las direcciones IP son números que entran en un formato específico el cual contempla cuatro números, separados por puntos e inferiores a 256. Dichos números se encuentran en notación decimal, sin embargo corresponden a la conversión de los números binarios de ocho dígitos. Ejemplo: 192.255.248.0, es decir, 11000000.11111111.11110000.00000000 Cada computadora conectada a Internet tiene al menos una dirección IP.

Las direcciones IP son las que utilizan las computadoras, pero los humanos preferimos utilizar los nombres de dominio, que utilizan letras y están por tanto más próximos a nuestro lenguaje y los podemos recordar más fácilmente.

Dominios de red.

Un dominio de Internet es una red de identificación asociada a un grupo de dispositivos o equipos conectados a la red.
El propósito principal de los nombres de dominio en Internet y del sistema de nombres de dominio (DNS), es traducir las direcciones IP de cada nodo activo en la red (dirección en formato numérico), a términos memorizables y fáciles de encontrar (dirección en termino nemónico, nombre). Esta abstracción hace posible que cualquier servicio de red pueda moverse de un lugar geográfico a otro en la red, aun cuando el cambio implique que tendrá una dirección IP diferente.
Sin la ayuda del sistema de nombres de dominio, los usuarios de Internet tendrían que acceder a cada servicio web utilizando la dirección IP del nodo, es decir, utilizando la dirección numérica. Por ejemplo, sería necesario utilizar http://192.168.32.10 en vez de http://www.empleo.com lo cual se vuelve más difícil en el momento de intentar recordar un buen número de sitios en la red.

Si bien el concepto de dominio de red se puede definir como el grupo de dispositivos en red que pertenecen al mismo proveedor del direccionamiento que se le asignó; También puede referirse al grupo de dispositivos que pertenecen al mismo segmento que el direccionamiento lógico ha creado. Entonces los dos enfoques, uno desde la parte funcional hacia el usuario como dominio de nombres o nombres de dominio y el otro desde la parte operativa de segmentación por direccionamiento lógico utilizando las clases de red y sus máscaras como elementos que definen cada uno de los dominios de red.

Para que las computadoras queden configuradas con sus respectivas direcciones IP, se prevé la necesidad de que una autoridad se encargue de distribuir y mantener esta información de direccionamiento de forma que no se produzcan duplicados o direcciones repetidas en la misma red, evitando conflictos de "identidad" y con ello colisiones de paquetes que se traduce en problemas o fallas en la calidad de respuesta de la red. Esta autoridad es, a escala mundial, el InterNIC, encargándose, diferentes gestores regionales, de asignar las direcciones IP en los diferentes dominios internacionales. Esta autoridad, controla el registro asignado a cada dominio de red y mantiene el buen funcionamiento de la red.
El nombre de dominio se apega a un formato o estructura estándar, el cual se compone de palabras separadas por puntos, como por ejemplo www.rectoria.uson.edu.mx. En este caso "uson" sería un sub-subdominio que a su vez está comprendido en otro subdominio de alcance mayor "edu" y así hasta la última palabra que corresponde al dominio principal o de primer nivel. En el ejemplo, "mx" corresponde al dominio principal.

Hay muchos nombres de dominio más largos, pero siempre siguen la misma estructura. La primera palabra del nombre de dominio corresponde siempre al nombre del servidor o equipo que ofrece algún recurso y/o servicio y es un indicativo de su función. El resto del nombre se apega a la estructura de dominios y subdominios arriba mencionados cada uno de ellos registrada en InterNIC.

Dominios principales			*Subdominios*	
México	.mx		.com	Empresa comercial
Japón	.jp		.edu	Educación
Francia	.fr		.gov	Entidad de gobierno
Argentina	.ar		.mil	Militar
Italia	.it		.org	Otras organizaciones
España	.es		.net	Sitios en la red

Tabla que muestra algunos ejemplos de dominios principales y subdominios.

Los nombres de los sub-subdominios son generalmente arbitrarios y dependen de los administradores de las redes locales. Los dominios principales y también algunos subdominios amplios, responden sin embargo a unas reglas establecidas. Los dominios principales constan de dos letras que indican el país al que pertenece.

Dado que existen también los nombres de dominio que pueden considerarse mucho más significativos desde el punto de vista del lenguaje humano lo único que será necesario es que haya un mecanismo para traducir de uno a otro, de forma que la red pueda funcionar con las direcciones IP independientemente de que sea ese el dato que hayamos introducido para designar a una computadora o bien hayamos utilizado su nombre de dominio. Este servicio se presta mediante una base de datos denominada DNS (Domain Name System o Sistema de Nombres de Dominio) que se encuentra distribuida de forma jerárquica por toda la red y que es consultada para realizar la traducción numérica a nemónica.

* P R A C T I C A *

	**TECNOLOGICO NACIONAL DE MEXICO** **Instituto Tecnológico de Hermosillo**	
PRACTICA DE LABORATORIO 2. Tema 1.2		**Pág. 1 de 3**

Programa SCD-1004:	Práctica Numero:	Nombre de la Práctica:
1.1.1 Direccionamiento IP y el concepto de Dominio	**2**	**Direccionamiento IP y el concepto de Dominio**

OBJETIVO ESPECIFICO: El alumno conocerá e identificará los diferentes elementos de configuración de una terminal para que ésta se conecte a la red. Establecerá su dirección IP y mascara de subred, para que pertenezca a un dominio de red.

INFORMACION PREVIA.

Todas las computadoras, necesitan tener una dirección tanto en la red local como en Internet. La mayoría de los sistemas operativos vienen con un servicio que asigna automáticamente estas direcciones. Pero a veces es probable que quieras especificar la dirección de una computadora en especial o solucionar los problemas de una conexión. Los Dispositivos a interconectarse pueden ser: PC´s, servidores de cualquier tipo, impresoras, cámaras web, dispositivos móviles como celulares, lap-tops, etcétera y cada uno requiere de su debido direccionamiento.

PROCEDIMIENTO: EL Alumno asignará la dirección IP y la máscara de subred a una terminal, configurándola para que se logre conectar a la red. Identificará la dirección del DNS y realizará las pruebas de verificación de conectividad.

Sugerencias didácticas: Con el fin de propiciar la colaboración, integración y trabajo en equipo, se recomienda que esta práctica se elabore por grupos de no más de tres alumnos.
Desarrolle los pasos que a continuación se describen, para la realización completa de esta práctica. Al final deberá describir el proceso realizado y resumir sus conclusiones.

DESARROLLO:

PASO 1. Abre la configuración de tu red.

- En tu computadora local abre el panel de control.
- Ubica el icono de “centro de redes y recursos compartidos” (el nombre varía dependiendo del sistema operativo). Haz clic en el icono.

PASO 2. Encuentra la conexión de red que represente a tu conexión a Internet Usualmente se llama "Conexión de área local". Selecciona "Propiedades".

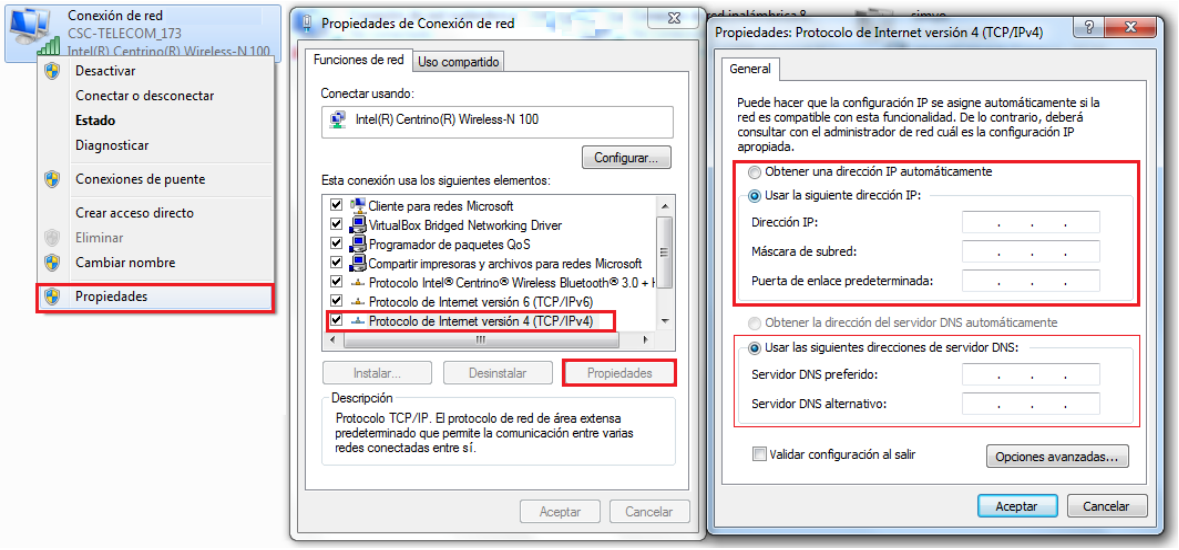
- Haz doble clic en “Protocolo de Internet versión 4 (TCP/IPv4)”.
- Ahora selecciona la opción que dice “Usar la siguiente dirección IP”.

PASO 3. Introduce una dirección IP válida para tu computadora.

- Configúrala para que tu terminal se integre a la red. Si no sabes qué dirección usar, averigua la dirección de la red y ajusta tu PC local en un host de esa red. No olvides tomar la dirección de la puerta de enlace predeterminada. Debe ser la misma para todas las terminales de la red.
- Usualmente funcionan las siguientes direcciones: 192.168.1.2, o 192.168.10.1

PASO 4. Verificar la máscara de red.

Después de introducir la dirección IP, revisa que la casilla de "máscara de subred" esté activada. Esto le permite a nuestra terminal pertenecer a un segmento del dominio jerárquico del direccionamiento IP. Ya que identifica tanto al host (PC) como la parte que identifica a la red (dominio al que pertenece).



PASO 5. Ahora necesitas escoger la información del servidor DNS, o puedes dejar que se obtenga automáticamente, lo cual es más recomendable.

Para mejorar el desempeño de tu computadora, intenta configurarla a un servicio de "DNS abierto" el cual ofrece servidores más rápidos, para acelerar el proceso de URL a IP; lo cual, en teoría, hace que navegar la red sea más rápido. Introduce “208.67.222.222” en el campo de “Servidor DNS preferido” y “208.67.220.220” en el campo de “Servidor DNS alternativo”.

PASO 6. Dale tiempo a tu PC para que aplique los cambios y revisa que estés conectado a Internet y que puedas navegar la red sin problemas. NOTA: el último dígito que escribas en la dirección IP, es el identificador único. Si usaste 192.168.1.1 (por ejemplo), entonces ".1" es único y no puede volver a usarse siempre que esté en esa PC. Para la siguiente PC, usa 192.168.1.2 (por ejemplo) y así sucesivamente para que cada una tenga un ID único. Ten cuidado de que no entren en conflicto con cada uno de ellos o con el enrutador (u otro dispositivo) o se presentarán errores.

Anota el procedimiento realizado y comentarios al respecto:

Elaborar un esquema mental de la estructura de direccionamiento y dominios.

Debes de interpretar gráficamente la forma en que se representa la estructura jerárquica, tanto del direccionamiento IP como del sistema de nombres de dominio.

1.3 Creación de subredes en dominios de direcciones.

La configuración de red de nuestro equipo exige aportar la dirección IP, la máscara de subred y la puerta de enlace predeterminado. Ya hemos configurado o simplemente consultado estos tres datos que son fundamentales en cualquier dispositivo conectado a la red. Está claro que la dirección IP identifica al equipo dentro de una LAN o Internet. Sin embargo, ¿para qué sirve la máscara de subred? Qué pasaría si no asigno una máscara en la configuración de mi PC?

Podríamos decir la máscara de subred nos indica qué parte de la dirección IP pertenece a la subred a la que se encuentra conectado el equipo. Pero esto no sirve de nada si no entramos en detalle de cómo se componen las direcciones IP.
Una dirección IP está compuesta por 32 bits que están agrupados en octetos, hasta alcanzar un total de 4. Es decir, 4 grupos de 1 byte. Como ejemplo de dirección IP tomemos una dirección del tipo 192.168.1.xx, que nos puede servir sin ningún problema para explicar todos los aspectos restantes. Para ser más exactos, esta pertenece a la clase C, pero no vamos a entrar en detalles de las diferentes clases existentes a nivel de direcciones IP, eso ya fue mencionado.
Partiendo de la dirección 192.168.1.*24*. Si tenemos una máscara de subred 255.255.255.0, quiere decir que todas las direcciones tendrán como parte fija 192.168.1.__ y el último octeto será que el presentará la variación. Esto es: desde la 192.168.1.0 a 192.168.1.255. De este rango, la primera dirección se reserva para identificar la red, mientras que la última queda reservada como dirección de broadcast, por lo cual no deben asignarse a ningún dispositivo.
Ahora bien, si cambiamos la máscara a 255.255.255.128 el dominio inicial quedará dividido en dos subredes, las cuales tendrán un rango como sigue:
1ra subred: 192.168.1.0 al 192.168.1.127
2da subred: 192.168.1.128 al 192.168.1.255
Donde el inicio y final de cada subred, serán direcciones reservadas y no deberán utilizarse para la configuración de ningún dispositivo.

Mascaras de red.

Una máscara de red ayuda a saber qué parte de la dirección identifica la red y qué parte de la dirección identifica el nodo. Las redes de la clase A, B, y C tienen máscaras predeterminadas, también conocidas como máscaras default, como se muestra aquí:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

Una dirección IP de una red de la Clase A que no se haya convertido en subred tendrá un par dirección/máscara similar a: 8.20.15.1 255.0.0.0. Para ver cómo la máscara le ayuda a identificar a las partes de la red y del nodo el direccionamiento, convierta el direccionamiento y la máscara a los números binarios.

8.20.15.1 = 00001000.00010100.00001111.00000001 (dirección IP de una PC)
255.0.0.0 = 11111111.00000000.00000000.00000000 (mascara default, clase A)

Una vez que usted hace el direccionamiento y la máscara representar en el binario, después la identificación de la red y del ID del host es más fácil. Cualquier bit de dirección que tenga el bit de máscara correspondiente establecido en 1 representa la identificación de red. Cualquier bit de dirección que tenga el bit de máscara correspondiente establecido en 0 representa la identificación de nodo.

8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000
---
net id | host id

netid = 00001000 = 8
hostid = 00010100.00001111.00000001 = 20.15.1

Tabla de máscaras de red

Binario	Decimal	CIDR	Nº hosts	Clase
11111111.11111111.11111111.11111111	255.255.255.255	/32	No Aplica	
11111111.11111111.11111111.11111110	255.255.255.254	/31	No Aplica	
11111111.11111111.11111111.11111100	255.255.255.252	/30	2	
11111111.11111111.11111111.11111000	255.255.255.248	/29	6	
11111111.11111111.11111111.11110000	255.255.255.240	/28	14	
11111111.11111111.11111111.11100000	255.255.255.224	/27	30	
11111111.11111111.11111111.11000000	255.255.255.192	/26	62	
11111111.11111111.11111111.10000000	255.255.255.128	/25	126	
11111111.11111111.11111111.00000000	255.255.255.0	/24	254	C
11111111.11111111.11111110.00000000	255.255.254.0	/23	510	
11111111.11111111.11111100.00000000	255.255.252.0	/22	1022	
11111111.11111111.11111000.00000000	255.255.248.0	/21	2046	
11111111.11111111.11110000.00000000	255.255.240.0	/20	4094	
11111111.11111111.11100000.00000000	255.255.224.0	/19	8190	
11111111.11111111.11000000.00000000	255.255.192.0	/18	16382	
11111111.11111111.10000000.00000000	255.255.128.0	/17	32766	
11111111.11111111.00000000.00000000	255.255.0.0	/16	65534	B
11111111.11111110.00000000.00000000	255.254.0.0	/15	131070	
11111111.11111100.00000000.00000000	255.252.0.0	/14	262142	

11111111.11111000.00000000.00000000	255.248.0.0	/13	524286	
11111111.11110000.00000000.00000000	255.240.0.0	/12	1048574	
11111111.11100000.00000000.00000000	255.224.0.0	/11	2097150	
11111111.11000000.00000000.00000000	255.192.0.0	/10	4194302	
11111111.10000000.00000000.00000000	255.128.0.0	/9	8388606	
11111111.00000000.00000000.00000000	255.0.0.0	/8	16777214	A
11111110.00000000.00000000.00000000	254.0.0.0	/7	33554430	
11111100.00000000.00000000.00000000	252.0.0.0	/6	67108862	
11111000.00000000.00000000.00000000	248.0.0.0	/5	134217726	
11110000.00000000.00000000.00000000	240.0.0.0	/4	268435454	
11100000.00000000.00000000.00000000	224.0.0.0	/3	536870910	
11000000.00000000.00000000.00000000	192.0.0.0	/2	1073741822	
10000000.00000000.00000000.00000000	128.0.0.0	/1	2147483646	
00000000.00000000.00000000.00000000	0.	/0	4294967294	

El número de hosts se determina como el número de IP's posibles menos dos, en cada subred hay una IP con todos los bits a ceros en la parte del host reservada para nombrar la subred y otra con todos los bits a uno reservada para la dirección de broadcast.

* P R A C T I C A *

Programa SCD-1004:	Práctica Numero:	Nombre de la Práctica:
1.1.2 Creación de subredes en dominios de direcciones	**3**	**Creación de subredes en dominios de direcciones**

OBJETIVO ESPECIFICO: El alumno utilizará las diferentes técnicas de segmentación de dominios creando subredes que permitan la agrupación de dispositivos de red mediante la asignación de la dirección de mascara de red.

INFORMACION PREVIA: La máscara de subred debe configurarse por igual a todas las terminales que pertenezcan al dominio, de tal manera que la segmentación lograda en las subredes obtenidas, sea homogénea a lo largo del dominio segmentado. También se hace la aclaración, que siendo una creación de subredes a partir de un direccionamiento lógico, cada elemento perteneciente a cada subred creada no podrá tener conectividad directa con los demás elementos pertenecientes a las otras subredes (aunque pertenezcan al mismo dominio). Para poder llevar a cabo la conectividad entre los dispositivos de diferente subred, debe utilizarse un router, el cual le dará seguimiento a las peticiones de direccionamiento entre redes y con ello se dispondrá del uso integral del dominio segmentado.

Las máscaras de redes se utilizan como validación de direcciones realizando una operación AND lógica entre la dirección IP y la máscara para validar al equipo, lo cual permite realizar una verificación de la dirección de la Red y con un XOR y la máscara negada se obtiene la dirección del broadcasting.

PROCEDIMIENTO: EL Alumno desarrollará los cálculos necesarios para segmentar un dominio de red en dos subredes. Configurar las terminales con direcciones de diferentes subredes y comprobar su conectividad. Realizar los cambios requeridos para que pertenezcan a la misma subred y verificar su conectividad. Anotar sus observaciones y conclusiones particulares.

Sugerencias didácticas: Con el fin de propiciar la colaboración, integración y trabajo en equipo, se recomienda que esta práctica se elabore por grupos de no más de tres alumnos. Utilizar al menos dos terminales y modificar su configuración ajustándose a los cálculos realizados anteriormente. Utilice la herramienta de software ping para verificar la conectividad entre las terminales.

DESARROLLO:

a) Tomar un dominio de red y realizar los cálculos de segmentación.
b) Con los rangos de las dos subredes calculadas configure las terminales.
c) Asignar una dirección de un rango a una terminal y otra a la segunda PC.
d) Verificar la conectividad mediante el uso del comando Ping.
e) Cambie la dirección IP de una terminal al rango de la otra PC configurada.
f) Verifique nuevamente la conectividad entre terminales.
g) Elaborar el reporte final integrado por el desarrollo de la práctica y conclusiones de la misma.

Anota tus conclusiones y observaciones:

Elabora un diagrama de flujo de los pasos realizados en esta práctica.

El diagrama de flujo deberá describir el procedimiento de prueba y error en la asignación y verificación de conectividad de las terminales.

1.4 VLSM como estrategia de segmentación de dominios

Cuando una red se vuelve muy grande, conviene dividirla en subredes lógicas. Esto sirve para establecer una estructura jerárquica cómoda y poder administrar la red de manera más amigable.

Ahora bien, el segmentar un dominio nos crea las subredes con las que podemos trabajar para asignarlas a nuestros grupos de trabajo (los hosts), sin embargo, existen ocasiones en que la cantidad de direcciones de una subred superan en una gran cantidad a los requerimientos prácticos de nuestro diseño de red. Por lo que se "desperdician" muchas direcciones que podrían utilizarse en otras subredes. vlsm ofrece solución a estas situaciones cada vez más comunes en la actualidad.

VLSM (Variable Lenght Subnet Mask) o máscara de subred de longitud variable, es una técnica que se diseñó con el fin de optimizar el direccionamiento IP, ya que con la técnica de la creación de subredes y sub-subredes (el llamado subnetting) se desperdiciaban muchas direcciones. Recuerden que en subnetting todas las direcciones tienen la misma máscara, por tanto una red de pocos hosts, tiene la máscara de una red con una cantidad de hosts igual a la de las demás. Si una subred requiere muchas direcciones y la otra subred requiere unas cuantes direcciones, al aplicar subnetting todas las subredes creadas tendrán el mismo número de hosts validos de tal forma, que funcionará excelentemente para la subred de muchos hosts, pero para la subred de unos cuantos hosts, dejará muchas direcciones validas sin uso.

En VLSM la máscara de subred se adapta al requerimiento de los hosts, por lo tanto VLSM es una técnica más eficiente.

Es importante mencionar que el direccionamiento basado en clases (Clase A, B, C, etc.) ya pasó a la historia. En los años 90s IETF (Internet Engineering Task Force) introdujo CIDR (Classless Inter-Domain Routing), o enrutamiento sin Clases. CIDR elimina los límites de clases y agrega flexibilidad a la hora de realizar un direccionamiento, permite VLSM y la sumarización de rutas. Esto quiere decir que una dirección, como por ejemplo: 192.168.0.0 puede tener una máscara /16 (255.255.0.0) ó /8 (255.0.0.0) Como las clases no existen la máscara más pequeña que puede tener una red es /8 lo cual en decimal es:

255.0.0.0 VLSM se enfoca en la cantidad de hosts que se encuentran en una subred, para en base a este requerimiento aplicar una máscara, diferente a subnetting, cuyo enfoque se encuentra en el número de redes requeridas.

* P R A C T I C A *

	TECNOLOGICO NACIONAL DE MEXICO **Instituto Tecnológico de Hermosillo**	
PRACTICA DE LABORATORIO 4.	**Tema 1.4**	**Pág. 1 de 3**

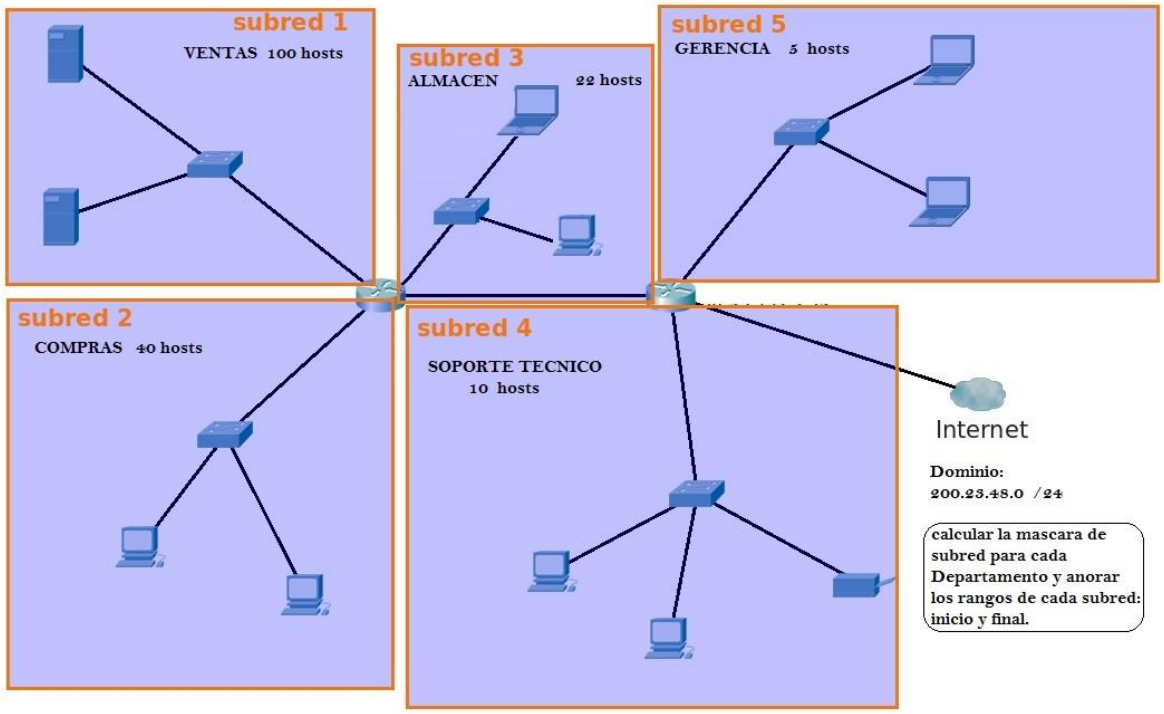
Programa SCD-1004:	**Práctica Numero:**	**Nombre de la Práctica:**
1.1.3 VLSM como estrategia de segmentación de dominios	**4**	**VLSM como estrategia de segmentación de dominios**

OBJETIVO ESPECIFICO: El alumno conocerá la técnica de VLSM para la segmentación de dominios. Realizará los cálculos necesarios para proponer una solución válida a la situación propuesta en la parte de información previa.

INFORMACION PREVIA: Las redes de computadoras son más fáciles de administrar cuando se segmentan en subredes o grupos de dispositivos más pequeños, o en algunos casos cuando se diseñan con la finalidad de ajustarse al número de hosts que se requieren por departamento o sección. Es en este momento cuando aplicamos la técnica del VLSM al dominio en cuestión y logramos calcular los rangos de direcciones que asignaremos a cada subred de nuestro dominio o lo que es igual, al departamento de nuestra empresa.

Para la realización de esta práctica, utilizaremos el dominio: 200.23.48.0 /24 el cual utilizaremos en nuestra empresa ficticia y se requiere la creación de cinco subredes, una para cada departamento, con las siguientes cantidades de hosts:

Ventas 100 hosts, Compras 40 hosts, Almacén 22, Soporte Técnico 10 hosts, hosts y Gerencia 5 hosts.



PROCEDIMIENTO: EL Alumno realizará para cada segmento de red el cálculo del número de hosts válidos y obtendrá la dirección de mascara que se debe aplicar para dicho segmento. A continuación se realiza el cálculo para el primer segmento, la subred para el departamento de Ventas con 100 hosts:

Red de Ventas: 100 hosts

128 64 32 16 8 4 2 1
1 1 1 1 1 1 1 1 <--- Este es el cuarto octeto. El VLSM al igual que
1 0 0 0 0 0 0 0 el subnetting se hace tomando bits prestados de la porción de hosts. Con una máscara /24 sólo tendremos 8 bits disponibles para realizar el direccionamiento.

2^7=128 hosts - 2= **126 direcciones** de hosts disponibles en esta red. Recuerde que -2 es porque en cada subred se pierden 2 direcciones, una de red y la otra de broadcast. Como solo requerimos 100 Hosts, podemos utilizar esta mascara y quedarían solo 6 hosts como reserva para ampliaciones futuras en el departamento.

La máscara de subred es 255.255.255.128 ó /25. Recordar que en vlsm para realizar el direccionamiento se hace de derecha izquierda, apagando los bits de acuerdo a la cantidad de hosts que haya en la red.
De la misma manera se deben realizar los cálculos para los cuatro departamentos más del presente ejercicio.

DESARROLLO:

a) Realizar los cálculos para obtener las máscaras de cada subred.
b) sujetándose a la información previa de los 5 departamentos.
c) Anotar los inicios y finales de cada segmento de red.
d) Asignar las direcciones de subred calculadas a cada host de cada subred
e) Explique brevemente como aplicar vlsm y las ventajas que esto ofrece.
f) Elaborar una tabla donde se muestren los nombres de los departamentos, las direcciones de inicio y final de cada rango y su número de hosts.

Explique con sus palabras como aplicar vlsm y las ventajas que ofrece:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Elabora una tabla con los resultados obtenidos.

Elaborar una tabla donde se muestren los nombres de los departamentos, las direcciones de inicio y final de cada rango y su número de hosts.

1.5 Enrutamiento estático.

El enrutamiento estático proporciona un método que otorga a los administradores de redes control absoluto sobre las rutas por las que se transmiten los datos en una conexión de red de redes, o sea de inter-redes, también con un término en inglés: conexión de *internetwork*. Para adquirir este control, en lugar de configurar protocolos de enrutamiento dinámico para que creen las tablas de enrutamiento de manera "automática", estas se crean manualmente.
La comprensión del enrutamiento estático es fundamental porque se usa tanto en internetworks más pequeñas como en internetworks grandes, como estrategia de enrutamiento de respaldo. El uso de rutas estáticas permite que los administradores creen tablas de enrutamiento de forma manual, en lugar de dejar esta tarea a los protocolos de enrutamiento dinámico.

Es importante entender las ventajas y desventajas de la implementación de rutas estáticas, porque se utilizan extensamente en internetworks pequeñas y solo para establecer la conectividad con proveedores de servicios. Es posible suponer que el enrutamiento estático es sólo un método antiguo de enrutamiento y que el enrutamiento dinámico es el único método usado en la actualidad. Esto no es así, además, se destaca que escribir una ruta estática en un router no es más que especificar una ruta y un destino en la tabla de enrutamiento y que los protocolos de enrutamiento hacen lo mismo, sólo que de manera automática. Sólo hay dos maneras de completar una tabla de enrutamiento: manualmente (el administrador agrega rutas estáticas) y automáticamente (por medio de protocolos de enrutamiento dinámico).
En algunos casos, un router sólo está conectado a otro router. Este tipo de routers se denomina router de conexión única y el enlace con el cual se establece la comunicación se denomina red de conexión única. Una ruta estática por defecto proporciona un método por el cual los paquetes cuyo destino son redes externas a la red de conexión única, pueden salir de dicha red.

Función del *Router*

El router es una computadora diseñada para fines especiales que desempeña un rol clave en el funcionamiento de cualquier red de datos. Los routers son responsables principalmente de la interconexión de redes por medio de:

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

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

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

Tabla de enrutamiento.

La tabla de enrutamiento es la recopilación de toda la información que puede obtener un router por medio de la configuración de sus interfaces y por el intercambio de información de un router con otros routers vecinos de la misma red. La información de las rutas o destinos en la red se almacena en la memoria interna del router y mediante algoritmos especiales procesa la información calculando la mejor vía o camino para realizar la entrega o seguimiento de un paquete de datos. Esta información de rutas en una red, establece la topología integral de enlace interworking por lo que es de especial ayuda lograr mantener actualizada dicha tabla de enrutamiento.
Las rutas con las cuales se elabora la tabla de enrutamiento, pueden ser creadas mediante protocolos de ruteo. Dichas rutas son llamadas rutas dinámicas ya que

se ajustan a los cambios de la topología de la red. Las otras rutas llamadas estáticas, son creadas manualmente por el administrador de la red, por lo cual siempre se conservan igual mientras no sean modificadas de la misma manera, manualmente.

* P R A C T I C A *

	TECNOLOGICO NACIONAL DE MEXICO **Instituto Tecnológico de Hermosillo**	
PRACTICA DE LABORATORIO 5.	**Tema 1.5**	**Pág. 1 de 3**

Programa SCD-1004:	Práctica Numero:	Nombre de la Práctica:
1.4.1 Enrutamiento Estático.	**5**	**Enrutamiento Estático.**

OBJETIVO ESPECIFICO: El alumno realizará la configuración de una ruta estática. Conocerá la sintaxis del comando utilizado y verificará mediante la tabla de ruteo, la creación de la misma. Deberá poder eliminar las rutas estáticas.

INFORMACION PREVIA: Existen routers que permiten la configuración especifica de tablas de ruteo mediante la creación de rutas estáticas. Hay otros que no disponen de esa opción ya que su capacidad no lo requiere. En nuestro caso, se deberá utilizar un router de mediano calado que permita el acceso a la configuración por la interface de línea de comando, de tal manera que mediante los comandos debidos se pueda dar de alta rutas estáticas y también se puedan verificarlas mostrando el contenido de la tabla de ruteo.

El comando para crear una ruta estática es el *ip route* y la sintaxis es esta:

ip route 10.0.1.0 255.255.255.0 serial 1/1/0

"ip route" seguido de la dirección IP de la red (ejemplo: 10.0.1.0) seguido de la máscara de subred (ejemplo: "255.255.255.0") seguido por la interfaz por la que saldrá el paquete para llegar a la red solicitada (ejemplo: "serial 1/1/0")

Para verificar el estado de la tabla de ruteo, utilizamos el comando *show ip route*

show ip route

El resultado de este comando nos mostrará la conformación de las rutas establecidas las cuales pueden ser "conectadas directamente" estas se registran al configurar las interfaces seriales y locales con las que cuenta nuestro router y las rutas dinámicas y estáticas que se crean por medio de protocolos de ruteo para las dinámicas o en nuestro caso, se crean manualmente (las rutas estáticas).

Para eliminar una ruta estática existente, solo debes anteponer la palabra "no" a la línea de comando. Ejemplo:

no ip route 10.0.1.0 255.255.255.0 serial 1/1/0

Puedes crear tantas rutas estáticas como creas convenientes y si se requiere las puedes eliminar fácilmente.

PROCEDIMIENTO: EL Alumno creará las rutas estáticas que le permitan al router acceder a redes no adyacentes en una topología de red WAN. Verificará su creación mostrando la tabla de ruteo y posteriormente las eliminará para dejar el router como inicialmente se encontraba.

DESARROLLO:

a) Encender el router y acceder al modo de administrador.
b) Acceder al modo de operación de configuración global.
c) Realizar los comandos respetando la sintaxis para crear rutas estáticas.
d) Comprobar que dichas rutas han sido creadas con el comando *show*.
e) Eliminar las rutas estáticas y después de verificar que hayan sido borradas.

Anota tus observaciones y conclusiones personales:

_____

_____

_____

_____

_____

_____

_____

1.6 Enrutamiento Dinámico.

El router realiza la función de darle seguimiento a los paquetes de datos con la intención de hacerlos llegar a su destino final, siempre buscando la mejor ruta o vía para hacer la entrega. Gracias al enrutamiento estático y al enrutamiento dinámico el router puede aprender rutas que le extiendan su alcance o dicho de otro modo, que se amplíe su topología de comunicación. El enrutamiento dinámico se propicia mediante los protocolos de ruteo de tipo vector distancia y/o estado de enlace, los cuales realizan su labor "descubriendo" rutas que permitan alcanzar los destinos no adyacentes a nuestro router de área local. Ejemplos de estos protocolos, *RIP, IGRP, EIGRP, OSPF, IS-IS y BGP*, por mencionar algunos.

Cuando hablamos de compartir información y de realizar la comunicación entre distintos sistemas, el enrutamiento dinámico es uno delos más socorridos. Bajo este proceso una serie de máquinas que se encuentren dentro de una misma red tendrán capacidad para llevar a cabo una comunicación entre ellas de forma permanente. Su comunicación se ocupará de que las tablas de enrutamiento estén siempre en una actualización adecuada, se controlará el estado vinculado a los enlaces y además se podrán comprobar cuáles son las rutas más convenientes en base al estado del análisis de la red.

Otros de los objetivos de este tipo de enrutamiento incluyen que los routers puedan llevar a cabo procesos para compartir información dinámicamente, realizar el descubrimiento de redes remotas y optimizar el rendimiento para utilizar siempre la mejor ruta. El enrutamiento dinámico se identifica bajo dos tipos de protocolos los "*vector distancia*" y los de "*estado de enlace*".

Protocolo de ruteo dinámico tipo vector distancia.

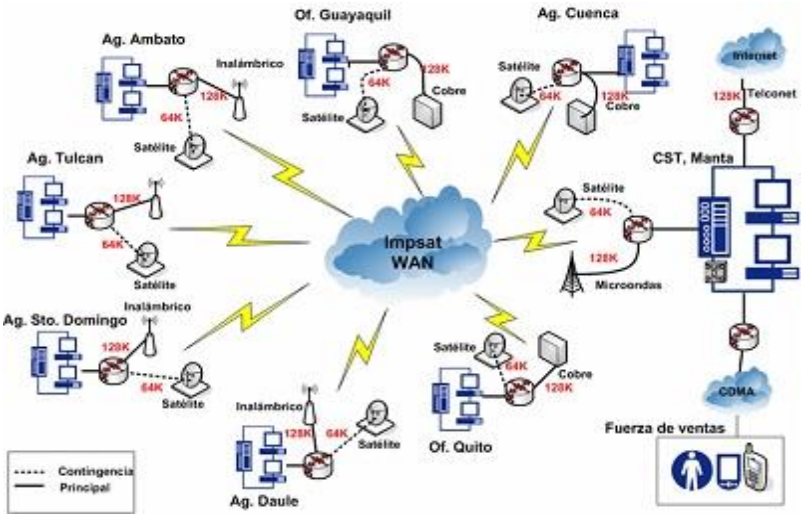
Este protocolo se beneficia del uso de vectores para poder saber cuál es la distancia que hay en una ruta. Implica un proceso pausado que dependerá del tamaño de la red y del sistema. No requiere grandes conocimientos para realizar su configuración, siendo uno de los protocolos más utilizados debido a la sencillez

que implica su optimización. Cuando ya está funcionando el protocolo se dedica al envío de la tabla del enrutamiento, ocupándose de ello a través de sistemas multicast o broadcast dependiendo del caso. RIP e IGRP son ejemplos de ellos.

Protocolo de ruteo dinámico tipo estado de enlace.

Este es otro de los protocolos principales de los que tenemos que hablar y saber cuándo nos referimos al enrutamiento dinámico. Incluye los correspondientes a OSPF e IS-IS, destacando por ser más rápidos y por mantenerse actualizados de una manera distinta, mucho más dinámica y funcional. Son protocolos más eficientes y aprovechan la red con una mayor capacidad, pero esto también significa que es más complicado trabajar con ellos. Debemos tener una formación adecuada a la hora de conseguir configurarlos y exprimir sus posibilidades.

Entre sus rasgos más destacados hay que mencionar que utilizan el protocolo hello, con el cual tienen capacidad para saber si los routers cercanos se encuentran activos. Esto se consigue gracias a que todos los routers que disponen de este mismo protocolo están conectados en una simbiosis por la cual funcionan de forma más conveniente. Se utiliza en redes muy amplias, mundialmente hablando y se requiere un hardware del router bastante robusto para trabajar.



*** P R A C T I C A ***

Programa SCD-1004:	Práctica Numero:	Nombre de la Práctica:
1.4.2 Enrutamiento Dinámico.	**6**	**Enrutamiento Dinámico.**

OBJETIVO ESPECIFICO: El alumno realizará la configuración de un protocolo dinámico del tipo vector distancia llamado RIP. Certificará su operación visualizando las tablas de ruteo.

INFORMACION PREVIA: El protocolo de enrutamiento RIP,(Routing Information Protocol) pertenece a la familia de protocolos IGP, (Interior Gateway Protocol) Es de los más sencillos en su operación y configuración, crea rutas dinámicas y presenta las siguientes características:

1. Pertenece a la familia de protocolos de vector distancia los cuales buscan el camino más corto determinando la dirección y la distancia a cualquier enlace. Estos algoritmos de enrutamiento basados en vectores, pasan copias periódicas de una tabla de enrutamiento de un router a otro.
2. La métrica empleada es el número de saltos que hay entre el router origen y destino. Una red directamente conectada tendrá un coste igual a 1.
3. Para el intercambio de información emplean datagramas UDP.
4. El Puerto reservado para este protocolo es el 520.
5. Emplea el algoritmo de Bellman-Ford distribuido.
6. Las rutas tienen un tiempo de vida de 180 segundos. Si pasado este tiempo, no se han recibido mensajes que confirmen que esa ruta está activa, se borra. Estos 180 segundos, corresponden a 6 intercambios de información.

7. RIP no es capaz de detectar rutas circulares (bucles), por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como infinito o inalcanzable y el destino es eliminado de la tabla de ruteo.

Las rutas establecidas por el RIP, pueden verificarse mostrando la tabla de ruteo y también pueden corroborarse realizando un PING.

El ping permite enviar paquetes de datos de prueba hacia la dirección que se indica, en este caso a través de la ruta dinámica creada mediante el RIP, el resultado de este comando nos permite comprobar la correcta o fallida conectividad con la terminal a la que se hace referencia en la línea de comando.

PROCEDIMIENTO: EL Alumno utilizará los comandos de configuración del router (CLI, command Line Interface), para dar de alta el servicio de ruteo dinámico. Aplicar los parámetros que permitan su correcta instalación y verificar que esté operando monitoreando las tablas de ruteo. Realizará una recopilación de información acerca de este protocolo dinámico indicando sus ventajas y desventajas.

DESARROLLO:

a) Encender el router y acceder al modo de administrador.
b) Acceder al modo de operación de configuración global.
c) Realizar los comandos respetando la sintaxis para crear rutas dinámicas. Aplicar el protocolo RIP usando sus parámetros.
d) Comprobar que dichas rutas han sido creadas con el comando *show*.
e) Elaborar un trabajo de investigación describiendo el protocolo RIP indicando sus ventajas y desventajas.

Anota el procedimiento realizado y tus observaciones particulares:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

2. TECNOLOGIAS WAN.

Objetivo: El Alumno identificara distintos dispositivos de tecnologías WAN desarrollando habilidades para configurarlos y administrarlos en las diferentes plataformas y entornos de trabajo.

Temas relacionados de la Asignatura: 2.5.1, 2.5.2, 2.5.3, 2.5.4

Sugerencias didácticas: Fomentar actividades grupales que propicien la comunicación, el intercambio argumentado de ideas, la reflexión, la integración y la colaboración entre los estudiantes. Relacionar los contenidos de esta asignatura con las demás del plan de estudios para desarrollar una visión interdisciplinaria en el estudiante. Facilitar el contacto directo con materiales e instrumentos, al llevar a cabo las actividades prácticas, para contribuir a la formación de las competencias definidas.

2.1. Administración y monitoreo de tecnologías WAN.

Una *WAN* (Wide Area Network o Red de Cobertura Amplia) es una red de comunicación de datos que opera más allá del alcance geográfico de una LAN. En realidad una WAN se conforma de numerosas redes tipo LAN organizadas topológicamente en una estructura jerárquica y entrelazadas por distintos medios de comunicación de largo alcance como lo son las estaciones de antenas microondas, enlaces satelitales o la fibra óptica.

Los protocolos de capa física WAN describen cómo proporcionar conexiones eléctricas, mecánicas, operacionales y funcionales para los servicios de una red de área amplia. Estos servicios se obtienen en la mayoría de los casos de proveedores de servicio WAN tales como las compañías telefónicas, portadoras alternas, y agencias de Correo, Teléfono, y Telégrafo (PTT: Post, Telephone and Telegraph). Los protocolos de enlace de datos WAN describen cómo los marcos

se llevan entre los sistemas en un único enlace de datos. Incluyen los protocolos diseñados para operar sobre recursos punto a punto dedicados, recursos multipunto basados en recursos dedicados y los servicios conmutados multiacceso tales como Frame Relay. Los estándares WAN son definidos y clasificados con sus referencias técnicas, por un grupo de autoridades reconocidas en el área, de las cuales se pueden mencionar las siguientes:

- **ITU-T**, International Telecommunication Union - Telecommunication (Anteriormente llamada: CCITT, Consultative Committee for International Telegraph and Telephone).
- **ISO**, International Organization for Standardization.
- **IETF**, Internet Engineering Task Force.
- **ETA**, Electronic Industries Association.

Capa Física: WAN

La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de conexión de los datos (DCE). Típicamente, el DCE es el proveedor de servicio, y el DTE es el dispositivo asociado. En este modelo, los servicios ofrecidos al DTE se hacen disponibles a través de un módem o unidad de servicio del canal/unidad de servicios de datos (CSU / DSU).

Algunos estándares de la capa física que especifican esta interfaz son:

- *EIA/TIA-232*: Esta norma fue definida como una interfaz estándar para conectar un DTE a un DCE.
- *EIA/TIA-449*: Junto a la 422 y 423 forman la norma para transmisión en serie que extienden las distancias y velocidades de transmisión más allá de la norma 232.
- *V.35*: Según su definición original, serviría para conectar un DTE a un DCE síncrono de banda ancha (analógico) que operara en el intervalo de 48 a 168 kbps.
- *X.21*: Estándar CCITT para redes de conmutación de circuitos. Conecta un DTE al DCE de una red de datos pública.
- *High-Speed Serial Interface (HSSI):* Estándar de red para las conexiones seriales de alta velocidad (hasta 52 Mbps) sobre conexiones WAN.

Enlaces conmutados.

Los enlaces conmutados se dividen en dos tipos:

- *Analógicos:* llegan hasta velocidades de 53 kbps para el downlink y hasta de 48 kbps para el uplink.
- *Digitales:* transmiten a 64 kbps o 128 kbps. Estos últimos son conocidos como enlaces RDSI (Red Digital de Servicios Integrados).

Enlaces dedicados.

Fueron la primera tecnología WAN que se adoptó usando la infraestructura de voz de los distintos operadores de telefonía. Sistema analógico de comunicaciones.

Se necesitaban conexiones físicas reales necesitando de un proveedor en cada sitio resultando en una solo línea de comunicación entre dos partes.

- Son enlaces donde solo interviene la red de transporte del proveedor de servicios.
- En el mercado corporativo comúnmente van desde los 64 a los 2048 kbps.
- Elevada eficiencia en las transmisiones.
- Tarifas planas, sin influencia del tráfico cruzado, en función del ancho de banda contratado.

Tecnologías WAN más aplicadas: PPP, XDSL, Frame Relay, ATM

- *Tecnología PPP:* Point-to-point Protocol (en español Protocolo punto a punto),

Comúnmente usado para establecer una conexión directa entre dos nodos de red. Puede proveer autentificación de conexión, cifrado de transmisión (usando ECP, RFC 1968), y compresión. PPP es usado en varios tipos de redes físicas incluyendo, cable serial, línea telefónica, line troncal, telefonía celular, especializado en enlace de radio y enlace de fibra óptica como SONET.

- *Tecnología XDSL*: Línea Suscriptora Digital (DSL), la “x” define variantes.

XDSL está formado por un conjunto de tecnologías que proveen un gran ancho de banda sobre circuitos locales de cable de cobre, sin amplificadores ni repetidores de señal a lo largo de la ruta del cableado, entre la conexión del cliente y el primer nodo de la red. Son unas tecnologías de acceso punto a punto a través de la red

pública, que permiten un flujo de información tanto simétrica como asimétrica y de alta velocidad.

Las tecnologías XDSL convierten las líneas analógicas convencionales en digitales de alta velocidad, con las que es posible ofrecer servicios de banda ancha en el domicilio de los clientes, similares a los de las redes de cable o las inalámbricas, aprovechando los pares de cobre existentes, siempre que estos reúnan un mínimo de requisitos en cuanto a la calidad del circuito y distancia.

- *Tecnología Frame Relay*: (Frame-mode Bearer Service), conmutación de tramas.

Es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos ("frames") para datos, perfecto para la transmisión de grandes cantidades de datos.

La técnica Frame Relay se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor.

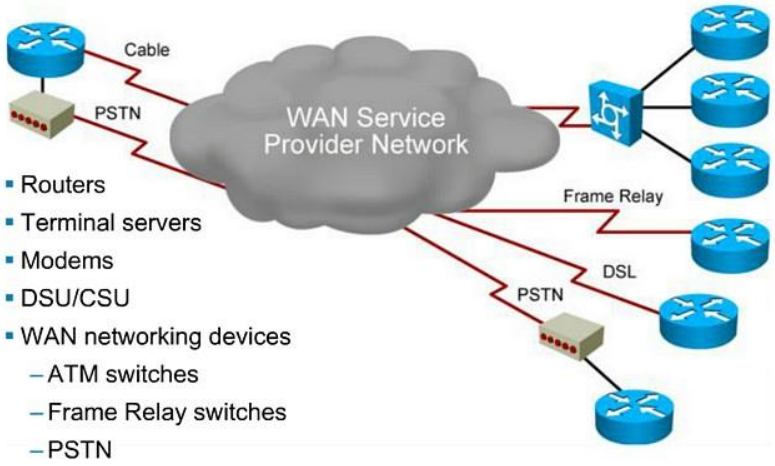
- *Tecnología ATM:* Asynchronous Transfer Mode, (Modo Transferencia Asíncrona).

Es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Con esta tecnología, a fin de aprovechar al máximo la capacidad de los sistemas de transmisión, sean estos de cable o radioeléctricos, la información no es transmitida y conmutada a través de canales asignados en permanencia, sino en forma de cortos paquetes (celdas ATM) de longitud constante y que pueden ser en rutadas individualmente mediante el uso de los denominados canales virtuales y trayectos virtuales. Son estructuras de datos de 53 bytes compuestas por dos campos principales:

1. *Header*, sus 5 bytes tienen tres funciones principales: identificación del canal, información para la detección de errores y si la célula es o no utilizada. Eventualmente puede contener también corrección de errores y un número de secuencia.

2. *Payload*, tiene 48 bytes fundamentalmente con datos del usuario y protocolos de control que también son considerados como datos del usuario.



* P R A C T I C A *

	TECNOLOGICO NACIONAL DE MEXICO **Instituto Tecnológico de Hermosillo**	
PRACTICA DE LABORATORIO 7.	**Tema 2.1**	**Pág. 1 de 3**

Programa SCD-1004:	Práctica Numero:	Nombre de la Práctica:
2.5.1 Administración de dispositivos WAN	**7**	**Administración de dispositivos WAN.**

OBJETIVO ESPECIFICO: El alumno realizará la visita a una red de computadoras real y operativa donde bajo la supervisión del administrador de la red, podrá observar algunas de las técnicas de administración y monitoreo de la red mediante comandos y entornos de trabajo disponibles.

INFORMACION PREVIA: Existen dos tipo de modelos de interconexión de redes. Uno es predecesor del otro y facilita la manera en que el desarrollo tecnológico ha podido expandirse logrando una real interconexión de dispositivos independientemente de su plataforma de hardware o software. Al conocer la historia y evolución de cada estrategia de desarrollo, se logra comprender como en la actualidad es posible tener una red de computadoras de dimensiones mundiales, tan funcional y practica como lo es el INTERNET.
En cada nodo o punto de conexión a internet existen redes que permiten a grupos de usuarios tener el acceso a las aplicaciones disponibles en ellas. Es de suma importancia que se pueda lograr un control o supervisión en las diferentes actividades en la red. Este control se puede lograr gracias a plataformas de administración de redes y estrategias de políticas de seguridad que favorecen a un ambiente de trabajo armonioso y amigable para el desempeño integral de la red, lo cual se traduce a su vez, en una red humana y productiva.

El Administrador de red, es el cargo que adquiere una persona la cual tiene la responsabilidad del buen desempeño de la red en general. Realiza instalaciones, cambios en actualizaciones tanto de hardware como de software, supervisa las actividades de entrada y salida de la red, impone orden haciendo cumplir las reglas y normativas que rigen al usuario de la red.

PROCEDIMIENTO: Realizar una visita a la red operativa y consultar con el responsable de la red las características generales de la red, que dispositivos existen para la conexión con el proveedor de servicio de internet. Indagar acerca de los procedimientos de administración y monitoreo de la red y anotar los puntos más relevantes.

DESARROLLO:

a) Realizar una visita a una red de computadoras real operativa.
b) Entrevistar al administrador de la red acerca de procedimientos aplicados para el monitoreo de la red.
c) Enlistar las normas o reglas que se imponen para el uso de la red.
d) Analizar la información acerca de la administración y control de la red.
e) Elaborar un reporte final anotando sus propias observaciones.

Anota tus conclusiones y observaciones personales:

_____

_____

_____

_____

_____

_____

_____

Elabora un reporte final. Enriquécelo con fotos de la visita.

Elabora un reporte final con la información recopilada en la entrevista, la observación del sitio visitado y la investigación por medio de consultas bibliográficas y digitales.

2.2 Dispositivos WAN.

Las tecnologías WAN se conmutan por circuitos o por paquetes. El tipo de dispositivo usado depende de la tecnología WAN implementada. Existen muchos tipos de dispositivos que son específicos de los entornos WAN, algunos de ellos son los siguientes:

- *Módem dial-up:* considerado una tecnología WAN antigua, un módem de banda de voz convierte (es decir, modula) las señales digitales producidas por una computadora en frecuencias de voz que se pueden transmitir a través de las líneas analógicas de la red de telefonía pública. En el otro lado de la conexión, otro módem convierte nuevamente los sonidos en una señal digital (es decir, los demodula) como entrada para una computadora o una conexión de red.

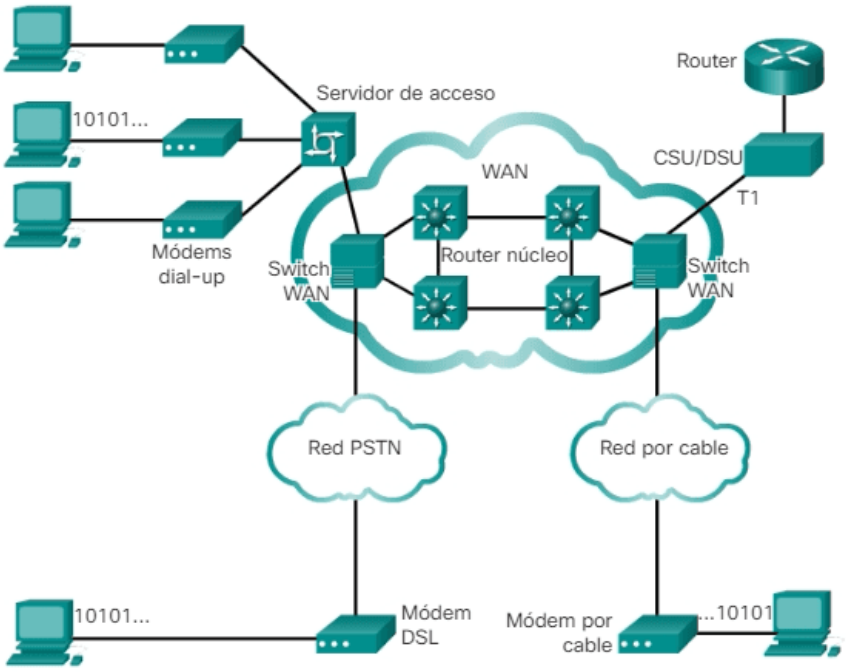
- *Servidor de acceso:* concentra las comunicaciones de entrada y de salida del módem dial-up de los usuarios. Considerado una tecnología antigua; un servidor de acceso puede tener una combinación de interfaces analógicas y digitales y admitir cientos de usuarios simultáneos.

- *Módem de banda ancha*: un tipo de módem digital que se utiliza con servicio de Internet por DSL o por cable de alta velocidad. Ambos funcionan de manera similar al módem de banda de voz, pero usan mayores velocidades de transmisión y frecuencias de banda ancha.

- *CSU/DSU*: las líneas arrendadas digitales requieren una CSU y una DSU. Una CSU/DSU puede ser un dispositivo separado, como un módem, o puede ser una interfaz en un router. La CSU proporciona terminación de la señal digital y asegura la integridad de la conexión mediante la corrección de errores y el monitoreo de la línea. La DSU convierte las tramas de línea en tramas que la LAN puede interpretar y viceversa.

- *Switch WAN:* un dispositivo de internetworking de varios puertos utilizado en las redes de los proveedores de servicios. Por lo general, estos dispositivos conmutan el tráfico, como Frame Relay o ATM, y operan en la capa 2.

- *Router:* proporciona internetworking y puertos de interfaz de acceso WAN que se usan para conectarse a la red del proveedor de servicios. Estas interfaces pueden ser conexiones seriales, Ethernet u otras interfaces WAN. Con algunos tipos de interfaces WAN, se requiere un dispositivo externo, como una DSU/CSU o un módem (analógico, por cable o DSL) para conectar el router al proveedor de servicios local.



Dispositivos WAN comunes

*** P R A C T I C A ***

Programa SCD-1004:	Práctica Numero:	Nombre de la Práctica:
2.5.2 Dispositivos WAN	**8**	**Dispositivos WAN**

OBJETIVO ESPECIFICO: El alumno identificara los diferentes dispositivos de tecnología WAN en una red de computadoras real. Identificará sus interfaces de conexión y los tipos de enlaces del proveedor de servicio de internet.

INFORMACION PREVIA: Conmutación de circuitos contra conmutación de paquetes: Las redes de conmutación de circuitos son aquellas que establecen un circuito (o canal) dedicado entre los nodos y las terminales antes de que los usuarios se puedan comunicar. Específicamente, la conmutación de circuitos establece una conexión virtual dedicada para voz o datos entre un emisor y un receptor en forma dinámica. Antes de que la comunicación pueda comenzar, es necesario establecer la conexión a través de la red del proveedor de servicios.

Como ejemplo, cuando un suscriptor realiza una llamada telefónica, el número marcado se usa para establecer los switches en los intercambios a lo largo de la ruta de la llamada, de modo que haya un circuito continuo desde el origen hasta el destinatario de la llamada. Debido a la operación de conmutación utilizada para establecer el circuito, el sistema telefónico se denomina "*red de conmutación de circuitos*". Si los teléfonos se reemplazan por módems, el circuito de conmutación puede transportar datos informáticos.

Los dos tipos más comunes de tecnologías WAN de conmutación de circuitos son la red pública de telefonía de conmutación (PSTN) y la red digital de servicios integrados (ISDN).

Conmutación de paquetes: A diferencia de la conmutación de circuitos, la conmutación de paquetes divide los datos en tráfico en paquetes que se enrutan a través de una red compartida. Las redes con conmutación de paquetes no requieren que se establezca un circuito y permiten que muchos pares de nodos se comuniquen a través del mismo canal.

En una red de conmutación de paquetes (PSN), los switches determinan los enlaces a través de los que se deben enviar los paquetes según la información de direccionamiento en cada paquete. Los siguientes son dos enfoques de esta determinación de enlaces:

- Sistemas sin conexión: se debe transportar toda la información de direccionamiento en cada paquete. Cada switch debe evaluar la dirección para determinar adónde enviar el paquete. Un ejemplo de sistema sin conexión es Internet.
- Sistemas orientados a la conexión: la red predetermina la ruta para un paquete, y cada paquete solo tiene que transportar un identificador. El switch determina la ruta siguiente al buscar el identificador en las tablas almacenadas en la memoria. El conjunto de entradas en las tablas identifica una ruta o un circuito particular a través del sistema.

Si el circuito se establece en forma temporal mientras un paquete viaja a través de él y luego se divide nuevamente, se lo denomina “circuito virtual” (VC). Un ejemplo de un sistema orientado a la conexión es Frame Relay. En el caso de Frame Relay, los identificadores utilizados se denominan “identificadores de conexión de enlace de datos” (DLCI).

PROCEDIMIENTO: EL Alumno realizara una visita a una red de computadoras en operación e identificará los dispositivos WAN con los que cuenta. Realizará una investigación acerca de las características técnicas de cada dispositivo, así como de los enlaces con los que cuenta.

DESARROLLO:

f) Realizar una visita guiada a una red real en operación.
g) Identificar los dispositivos WAN que existan en la red.
h) Investigar la información técnica de cada dispositivo.
i) Realizar una descripción completa de los tipos de enlaces utilizados.
j) Hacer un diagrama de la red identificando los dispositivos WAN y sus enlaces así como las áreas de operación de las terminales de trabajo.

Anota tus observaciones y conclusiones particulares:

_____

_____

_____

_____

_____

_____

_____

Elabora un diagrama básico de la red visitada.

Hacer un diagrama de la red identificando los dispositivos WAN, sus interfaces y sus enlaces así como las áreas de operación de las terminales de trabajo.

2.3 Configuración de dispositivos WAN.

Establecer la configuración básica de un router no es más que activar las distintas interfaces del router y configurar los parámetros de software para los protocolos enrutados y de enrutamiento. Existen distintas formas de llevar a cabo la configuración del router, pero para establecer la configuración básica de un router des configurado, se aconseja utilizar siempre el puerto de la consola.

Puerto Consola del router. El router puede configurarse directamente desde un PC conectado al puerto de la consola del router por medio del cable especial llamado rollover que incorpora el router. Antes de iniciar el router, verifique la alimentación, el cableado y la conexión de la consola, de forma que al arrancar el router, si se produjese algún error aparecería en la consola. Utilizar el comando de modo de activación *config terminal*.

La Terminal virtual. Se puede conectar con el router vía Telnet por medio de una terminal virtual. Utilizar el comando de modo de activación *config terminal.*

Servidor TFTP. Se puede cargar una configuración de router desde un servidor TFTP incluido en la red.

Modos de trabajo de administración de un router.

- *Modo Usuario.* Proporciona un acceso limitado al router, mediante el cual se puede examinar la configuración del router, sin permitir cambiar su configuración. Es el modo que se activa por defecto al volver a arrancar el router, apreciándose al aparecer como indicador el nombre del router seguido del signo > (mayor que).
- *Modo Privilegiado.* Conocido también como modo de Activación (Enabled). Para acceder al modo privilegiado, desde el modo usuario ejecutaremos el comando enable, tras lo cual se nos preguntará por la contraseña de dicho modo. Una vez finalizado el trabajo en el modo privilegiado, debe volver al modo usuario para no dejar la configuración del router al descubierto, para

lo cual ejecutaremos el comando disable. El modo privilegiado ofrece una cantidad de comandos mucho más amplio que el modo usuario.

- *Modo Configuración.* Permite determinar todos los parámetros relacionados con el hardware y el software del router (interfaces, protocolos ruteados y de enrutamiento, contraseñas, etc). Al modo configuración se accede desde el modo privilegiado mediante el comando *config terminal*, o bien ejecutando directamente el comando config t (en su modo reducido). Con ello podrá entrar en modo de configuración global.

Configuraciones básicas:

Hostname (Nuevo Nombre), Se utiliza para cambiar el nombre del router.

Enable secret, Se utiliza para especificar la contraseña del modo Privilegiado.

El comando show

Uno de los comandos más útiles es el comando *show* o su abreviatura **sh,** que permite visualizar el estado de todas las interfaces incluidas en el router, así como las estadísticas para cada elemento, como la memoria Flash, la memoria RAM y los protocolos de red que están siendo ruteados. A continuación se muestran varios comandos show del modo usuario:

- El comando **show running-config,** muestra la configuración que actualmente se está ejecutando en el router, es decir almacenado en la RAM, y que proporciona información acerca de las interfaces que están actualmente configuradas, protocolos de enrutamiento que han sido activados, la contraseña establecida para el router (esta aparecerá cifrada en pantalla), entre otras.
- El comando **show startup-config,** muestra la configuración de arranque del router, es decir, almacenado en la NVRAM, por lo que se presenta similar al comando anterior. Este viene siendo el respaldo del anterior.

Al margen del modo en el que nos encontremos, el IOS siempre puede mostrarnos un listado completo de los comandos disponibles ejecutando el comando **?**. Así, también podemos obtener ayuda sobre un comando específico introduciendo el nombre de dicho comando seguido de **?**, como por ejemplo ***show ?***

Configurar fecha y hora:

Para configurar la fecha y hora, debemos entrar en modo privilegiado (enable), y ejecutar el comando clock set seguido de la hora y la fecha. Como ejemplo un formato válido sería: **clock set 21:43:05 13 june 2021.**

* P R A C T I C A *

	TECNOLOGICO NACIONAL DE MEXICO **Instituto Tecnológico de Hermosillo**	
PRACTICA DE LABORATORIO 9.	**Tema 2.3**	**Pág. 1 de 2**

Programa SCD-1004:	Práctica Numero:	Nombre de la Práctica:
2.5.3 Configuración de dispositivos WAN	**9**	**Configuración de dispositivos WAN**

OBJETIVO ESPECIFICO: El alumno realizará la configuración básica de un router asignándole un nombre y una contraseña de entrada como medida de seguridad, ajustando la fecha y hora del router y configurará una interface Ethernet y una interface serial poniéndolas en operación.

INFORMACION PREVIA: Una de las primeras tareas de configuración es asignar un nombre exclusivo al router. Esto se realiza en el modo de configuración global, mediante el siguiente comando:

router(config)#hostname <nombre_router>

Por ejemplo, sí que desea asignar al router el nombre Tokio, habrá que ejecutar:

router(config)#hostname Tokio

Tokyo(config)#

Al presionar la tecla Enter, el prompt de entrada ya no mostrará el nombre de host por defecto ('router'), sino el nombre de host que se acaba de configurar, 'Tokio' en el ejemplo anterior.

- **Asignar una contraseña:**

Aunque es opcional, se recomienda configurar una contraseña para acceder a la línea de comando. Para fijar dicha contraseña se utilizan los siguientes comandos:

router(config)#**line console 0**
router(config-line)#**password <contraseña>**
router(config-line)#**login**
router(config-line)#**exit**

- **Para establecer contraseñas en las líneas de terminales virtuales:**

router(config)# **line vty 0 4**
router(config-line)# **password <contraseña>**
router(config-line)# **login**
router(config-line)# **exit**

Para realizar el cifrado de la contraseña se utiliza el siguiente comando:

router(config)#**service password-encryption**

- **Configuración de una interface Ethernet.**

La configuración de las interfaces de un router se realiza desde el submodo de configuración de interfaces. Para entrar en este submodo de configuración, hay que teclear el comando interface estando en el modo de configuración global. El

prompt de entrada cambiará pasando a ser: (config-if)#

router(config)# **interface <tipo> <puerto>**
router(config)# **interface <tipo> <slot/puerto>**
router(config-if)#

A cada interfaz ethernet se le debe asignar una dirección IP y la correspondiente máscara de red o subred. El estado predeterminado de una interfaz es inactivo. Por tanto, habrá que usar el comando *no shutdown* para activar la interfaz.

La secuencia de comandos de configuración de una interfaz ethernet será:
router(config)# **interface ethernet|fastethernet <slot/puerto>**
router(config-if)# **ip address <dirección_IP> <máscara>**
router(config-if)# **no shutdown**
router(config-if)# **exit**
router(config)# **exit**

- **Configuración de una interface Serial.**

Las interfaces serial del router se utilizan para interconectar routers entre si y para conectar un router a la red WAN.

La secuencia de comandos para la configuración de una interfaz de un router como DCE será la siguiente partiendo del modo de configuración global:
router(config)# **interface serial <slot/puerto>**
router(config-if)# i**p address <dirección_IP> <máscara>**
router(config-if)# **clock rate <ratio>**
router(config-if)# **no shutdown**
router(config-if)# **exit**
router(config)# **exit**

PROCEDIMIENTO: EL Alumno realizara la configuración de un router con sus parámetros básicos como nombre fecha y contraseña. Configurará dos interfaces, una Ethernet y otro serial con los comandos y sintaxis correspondientes.

DESARROLLO:

a) Encender el router conectado a la terminal por medio de consola.
b) Entrar al modo privilegiado para cambiar nombre, fecha y hora.
c) Desde le modo privilegiado asignar una contraseña que sea cifrada.
d) Entrar al modo de configuración global y dar de alta la interface Ethernet.
e) Estando en el modo de config terminal, dar de alta la interface serial.
f) Verificar las acciones realizadas mediante el comando show.

Anota tus comentarios y observaciones particulares:

_____

_____

_____

_____

_____

_____

2.4 Implementación de dispositivos WAN.

Las WAN se diferencian de las LAN en varios aspectos. Mientras que una LAN conecta computadoras, dispositivos periféricos y otros dispositivos de un solo edificio u de otra área geográfica pequeña, una WAN permite la transmisión de datos a través de distancias geográficas mayores. Además, la empresa debe suscribirse a un proveedor de servicios WAN para poder utilizar los servicios de red de portadora de WAN.
Las LAN normalmente son propiedad de la empresa o de la organización que las utiliza.

Las WAN utilizan instalaciones suministradas por un proveedor de servicios, o portadora, como una empresa proveedora de servicios de telefonía o una empresa proveedora de servicios de cable, para conectar los sitios de una organización entre sí con sitios de otras organizaciones, con servicios externos y con usuarios remotos.
En general, las WAN transportan varios tipos de tráfico, tales como voz, datos y video.

Las tres características principales de las WAN son las siguientes:

- Las WAN generalmente conectan dispositivos que están separados por un área geográfica más extensa que la que puede cubrir una LAN.
- Las WAN utilizan los servicios de operadoras, como empresas proveedoras de servicios de telefonía, empresas proveedoras de servicios de cable, sistemas satelitales y proveedores de servicios de red.
- Las WAN usan conexiones seriales de diversos tipos para brindar acceso al ancho de banda a través de áreas geográficas extensas.

Requisitos para llevar a cabo un diseño de red WAN.

A continuación se describen varias áreas que se deben analizar cuidadosamente al planificar una implementación WAN. Los pasos que se

describen aquí pueden llevar a mejorar el costo y desempeño de la WAN. Las empresas pueden mejorar constantemente sus WAN incorporando estos puntos al proceso de planificación.

Disponibilidad de aplicaciones: Las redes transportan información de aplicaciones entre computadores. Si las aplicaciones no están disponibles para los usuarios de la red, la red no está cumpliendo su función.

Costo total de propiedad: El presupuesto de los departamentos de Sistemas de Información a menudo alcanzan los millones de dólares. A medida que las empresas aumentan el uso de los datos electrónicos para administrar las actividades empresariales, los costos asociados con los recursos informáticos seguirán creciendo. Una WAN bien diseñada puede ayudar a equilibrar estos objetivos. Cuando se implementa correctamente, la infraestructura de la WAN puede optimizar la disponibilidad de las aplicaciones y permitir el uso económico de los recursos de red existentes.

En general, las necesidades de diseño de la WAN deben tener en cuenta tres factores generales:

Variables de entorno: Las variables de entorno incluyen la ubicación de hosts, servidores, terminales y otros nodos finales, el tráfico proyectado para en el entorno y los costos proyectados de la entrega de diferentes niveles de servicio.

Límites de desempeño: Los límites de desempeño consisten en la confiabilidad de la red, el rendimiento de tráfico, y las velocidades de computación host/cliente (por ejemplo, tarjetas de interfaz de red y velocidades de acceso del disco duro).

Variables de networking: Las variables de networking incluyen la topología de la red, capacidades de línea y tráfico de paquetes.

* P R A C T I C A *

Programa SCD-1004:	Práctica Numero:	Nombre de la Práctica:
2.5.4 Implementación de dispositivos WAN	**10**	**Implementación de dispositivos WAN**

OBJETIVO ESPECIFICO: El alumno deberá describir los requisitos que permiten realizar conexiones a grandes distancias a través de dispositivos WAN. Realizará una investigación acerca de los proveedores de servicio de la localidad y comparará servicios y costes para plantear el cotos-beneficio de implementación de una red WAN en nuestra localidad.

INFORMACION PREVIA:

OTROS REQUISITOS DEL DISEÑO WAN

La velocidad de transmisión de datos en una WAN (ancho de banda) es mucho menos a 100 Mbps, que es común en una LAN. Las conexiones entre los routers y la red del proveedor del servicio son seriales. Los costos de provisión de enlace son el elemento más caro de las WAN y el diseño debe buscar proveer un máximo de ancho de banda a un costo aceptable. Las tecnologías WAN funcionan en las tres capas inferiores del modelo de referencia OSI.

Los routers determinan el destino de los datos a partir de los encabezados de capa de red y transfieren los paquetes a la conexión de enlace de datos indicada para su envío en la conexión física.

La caracterización del tráfico de red es fundamental para la planificación exitosa de las WAN, pero pocos planificadores ejecutan correctamente esta tarea clave, si es que lo hacen en absoluto.

El objetivo general del diseño WAN es minimizar el costo basándose en estos elementos, proporcionando servicios que no comprometan los requisitos de disponibilidad establecidos.

El primer paso en el proceso de diseño es comprender los requisitos de la empresa; este tema se analiza en las secciones siguientes. Los requisitos de la WAN deben reflejar los objetivos, características, procesos empresariales y políticas de la empresa en la que opera.

.

PROCEDIMIENTO: El Alumno realizará la planificación de una red WAN con la información recabada sobre ISPs de la localidad. Realizará un diseño viable de implementación describiendo los dispositivos, enlaces y servicios con que contará.

DESARROLLO:

a) Investigar sobre proveedores de servicio de internet en nuestra localidad.
b) Recopilar información acerca de costos y servicios que se ofrecen.
c) Analizar la información y desarrollar la planificación de una red WAN.
d) Desarrollar un reporte final que contemple la viabilidad del proyecto.
e) Elaborar un plano de diseño de red WAN.

Registra la información que se vaya recabando para utilizarla en el proyecto:

_____

_____

_____

_____

_____

_____

_____

ELABORA UN ESQUEMA BASICO DE UNA CONEXIÓN EXTREMO-EXTREMO

Elaborar un plano de diseño de red la WAN conteniendo los puntos de llegada de servicios, tipos de enlaces, dispositivos que se conectan.

3. TECNOLOGIAS INALAMBRICAS

Objetivo: El alumno analizará y aplicará los diferentes mecanismos para integrar alto rendimiento y conectividad segura en redes inalámbricas. Identificará y clasificará los diferentes dispositivos que se utilizan para la implementación de redes inalámbricas. Conocerá los alcances y proyecciones en los entornos inalámbricos así como las velocidades de recepción y transmisión y protocolos de seguridad tales como WEP, WAP, PSK, WEP2, WPA-PSK.

.

Temas relacionados de la Asignatura: 3.1, 3.3.1, 3.3.2

Sugerencias didácticas: Se propone la formalización de los conceptos a partir de experiencias específicas; se busca que el alumno tenga el primer contacto con el concepto en forma concreta y sea a través de la observación, la reflexión y la discusión de manera práctica, que se dé la formalización. Se sugiere que se diseñen problemas con datos reales o simulados de manera que el alumno se ejercite en la identificación de información relevante y elaboración de soluciones viables.

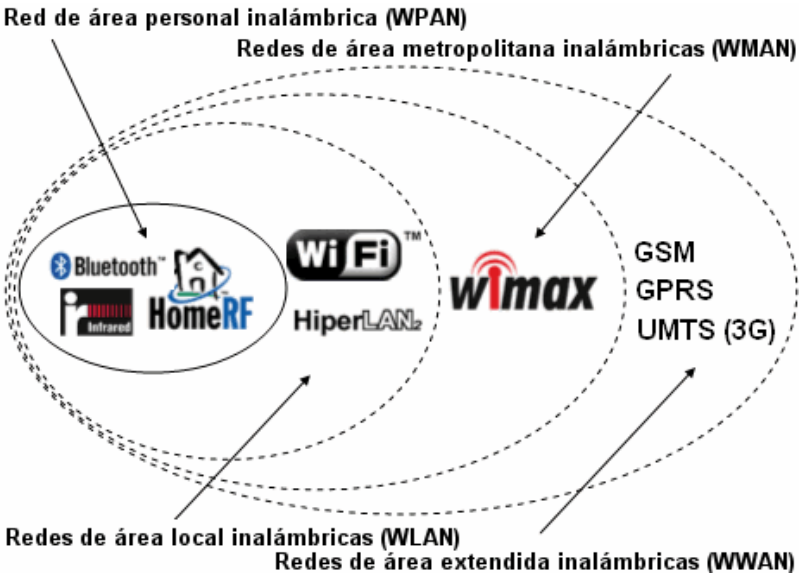
3.1 Clasificación de redes inalámbricas.

Cuando se logra la conexión de red entre dos o más terminales sin la necesidad de utilizar algún tipo de cableado, se establece una red de computadoras del tipo inalámbrico. En su término en inglés es llamada: Wireless Network.

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas de radio o en especiales ocasiones luz infrarroja, en lugar de cableado estándar. Existen diversas tecnologías que se caracterizan por la banda de frecuencia de transmisión en la que operan y la velocidad de transmisión. Gracias a las redes inalámbricas, un usuario puede mantenerse conectado con otros dispositivos presentes en la red, aun cuando se desplaza o moviliza siempre y cuando se

mantenga dentro de una determinada área geográfica, lo cual se determina como área de cobertura de la red.

Por el otro lado, existen algunas cuestiones relacionadas con la regulación legal del espectro electromagnético. Las ondas electromagnéticas se transmiten a través de muchos dispositivos de uso militar, científico e inclusive, de aficionados, pero son propensos a las interferencias. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y la potencia de transmisión que se permite a cada categoría de uso. Además, las ondas hertzianas no se confinan fácilmente a una superficie geográfica restringida. Por este motivo, un intruso puede, con facilidad, escuchar una red si los datos que se transmiten no están codificados. Por lo tanto, se deben tomar medidas para garantizar la privacidad de los datos que se transmiten a través de redes inalámbricas.



Por lo general, las redes inalámbricas se clasifican en varias categorías, de acuerdo al área geográfica desde la que el usuario se conecta a la red:

- WPAN, redes de área personal.
- WLAN, redes de áreas locales inalámbricas.

- WMAN, redes de áreas metropolitanas inalámbricas.
- WWAN, redes de áreas extendidas inalámbricas.

El tipo de red inalámbrica mayormente utilizada es la WLAN, ya que en la mayoría de los servicios residenciales se presta como servicio de conexión a internet por los diversos proveedores (ISP, Internet Service Provider). Esta clase de red requiere especialmente de dispositivos intermedios con interfaces inalámbricas, la cual generalmente es una antena, mediante la cual permite la conectividad con los dispositivos móviles.

La tecnología inalámbrica llamada WiFi, que en inglés significa Wireless Fidelity brinda solución a las WLAN´s de manera estándar por lo que existe una compatibilidad de interconexión entre dispositivos y entre redes; Lo cual lo hace una de las tecnologías móviles mayormente utilizada en la actualidad. WiFi es una solución informática que comprende un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11, lo cual asegura la conectividad e interoperabilidad en los equipos certificados bajo esta denominación.

Para su funcionamiento, el WiFi necesita de un router o Access point conectado a internet y dotado de una antena, para que a su vez redistribuya esta señal de manera inalámbrica dentro de un radio determinado de alcance. Los equipos receptores que se encuentren dentro del área de cobertura, al mismo tiempo, deben estar dotados con elementos compatibles con la tecnología WiFi para que puedan tener acceso a internet. Mientras más cerca se encuentren los equipos de la fuente de la señal, mejor será la conexión en cuanto a calidad y velocidad se refiere.

* P R A C T I C A *

	TECNOLOGICO NACIONAL DE MEXICO **Instituto Tecnológico de Hermosillo**	
PRACTICA DE LABORATORIO 11.	**Tema 3.1**	**Pág. 1 de 3**

Programa SCD-1004:	Práctica Numero:	Nombre de la Práctica:
3.1 Clasificación de redes inalámbricas	**11**	**Clasificación de redes inalámbricas**

OBJETIVO ESPECIFICO: El alumno identificara y clasificará una red inalámbrica operativa con la cual realizará la toma de información relevante, sus características principales y definirá los alcances de proyección al monitorear su señal en el área de cobertura de la red.

INFORMACION PREVIA: Básicamente la diferencia entre las diferentes clases de redes inalámbricas consiste en la frecuencia de transmisión y la velocidad de transferencia de datos cosa que difícilmente podría apreciarse a simple vista. Es necesario tomar información de los dispositivos de interconexión de la red inalámbrica, como el router o el Access Point, para investigar sus características particulares. Dicho de otra manera, se debe conocer las marcas y modelos de estos dispositivos para consultar su ficha técnica y lograr recopilar la información deseada. Los estándares más utilizados en redes inalámbricas son:

Estándar	Banda de frecuencia	Velocidad de transmisión
802.11a	5 Ghz	54 Mbits/s
802.11b	2.4 Ghz	11 Mbits/s
802.11g	2.4 Ghz	22 Mbits/s
802.11.n	2.4 Ghz y 5 Ghz	Hasta 600 Mbits/s

Sus áreas de coberturas son generalmente las mismas, 300 pies contemplando una calidad y velocidad de transferencia integra, esto es 100 metros a la redonda del punto de transmisión. Se debe tomar en cuenta que los materiales u obstáculos que se encuentren entre el transmisor y el receptor, impedirán el perfecto viaje de las señales de radiofrecuencia por lo que esto afecta directamente en la calidad y velocidad de los datos. Los distintos tipos de estándares, utilizan diferentes métodos de modulación de frecuencia con el fin de minimizar este problema. Algunos métodos de señalización utilizados en redes inalámbricas son: DSSS, Espectro ensanchado por secuencia directa y OFDM multiplexación por división de frecuencia ortogonal.

PROCEDIMIENTO: EL alumno realizara una visita guiada a una red inalámbrica y mediante el uso de un dispositivo móvil como laptop, Tablet o Smartphone, identificará la presencia de señal de red WiFi. Utilizar la aplicación WiFi-Analyzer. Debe anotar el SSID (Service Set Identifier) y poder consultar sus características, banda de frecuencias,canal que utiliza, tipo de seguridad configurada y definir el alcance de la red.

DESARROLLO:

a) Visita guiada por un asesor a una red inalámbrica.
b) Utilizar dispositivo móvil en modo de conexión inalámbrica con la aplicación WiFi- Analizar previamente instalada.
c) Identificar la señal de presencia de la red (SSID).
d) Desplazarse en un entorno considerado para definir el área de cobertura de la red. Tomar lectura de la intensidad de señal.
e) Elaborar un reporte a cerca de la información recabada.
f) Realizar un plano geográfico de cobertura de señal.

Describe la forma en que identificas la presencia de una red inalámbrica:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Realiza un croquis del sitio, contemplando el área de cobertura de la red.

Debes de dibujar un croquis del lugar tomando como centro el punto de distribución de la red. Tomar lecturas de la señal alrededor de la red inalámbrica.

3.2 Dispositivos y configuración en redes inalámbricas.

Cada vez más dispositivos soportan conexión a la red de redes. Desde nuestro teléfono hasta nuestro televisor y aunque parezca raro, también nuestros electrodomésticos como refrigerador, lavadora, cafetera entre otros ya se conectan a Internet. Un usuario común cuenta al menos con una laptop, un Smartphone, una Tablet, el smartTV… todos estos dispositivos, que potencian sus recursos al contar con una conexión a Internet, son fáciles de adquirir y existen de distintas capacidades. Se puede decir, que en los tiempos en que vivimos hoy en día, es indispensable una conexión a internet en el hogar en la oficina o incluso en los lugares de esparcimiento ya que esto ha cambiado nuestra forma de estudiar, de trabajar, de divertirnos en una palabra: de convivir.

Independientemente de los dispositivos finales que se utilizan en estas redes móviles, es indispensable los puntos de acceso a la red inalámbrica los cuales proveen la conexión entre nuestro punto de servicio de internet (ISP) y los dispositivos móviles.

El Router.

Generalmente el router viene siendo nuestro principal punto de acceso a la red inalámbrica ya que es quien gestiona la comunicación favoreciendo la conectividad entre dispositivos finales y la salida al internet. Esta característica es la que convierte a nuestro router en un pequeño cuello de botella. También es quien otorga las identidades con las que dispondrán de acceso los dispositivos móviles mediante una batería de direcciones IP llamada DHCP, la cual asigna IP´s a medida que se conectan a la red y cuando un dispositivo deja la red, libera o vuelve disponible esa dirección para otro nuevo solicitante.

Los routers doble banda, son capaces de transmitir a través de las frecuencias 2.4GHz y 5GHz simultaneamente. Esta segunda banda cuenta con la ventaja de estar mucho menos congestionada ya que muy pocos dispositivos la utilizan.

También existe la tecnología MIMO (“Múltiples receptores y múltiples emisores”). Esta se vale de varias antenas para lograr una cobertura multifrecuencia. Envía y recibe a través de varias antenas, por lo que aun cuando una de estas conexiones se interrumpe, no se reflejará ese problema en la ejecución de nuestra aplicación. El router se conecta mediante cableado al ISP, pero permite conectividad con los clientes gracias a las transmisiones de radiofrecuencia que aportan las antenas.

Las Antenas.

Existen muchos tipos de antenas, una para cada aplicación; Sin embargo, esto puede simplificarse en dos tipos: la ganancia y la direccionalidad. La ganancia es la cantidad de energía que la antena añade a la señal de radio frecuencia en el lóbulo principal y la direccionalidad tiene que ver con la apertura del espectro de radio que estas ofrecen.

Las antenas tipo dipolo, por ejemplo, son las más utilizadas y ofrecen cobertura *omnidireccional* es decir, que radia por igual en todas direcciones (hacia arriba y hacia abajo no). Los fabricantes dicen que tienen un alcance de cientos de metros, pero eso debe ser en condiciones muy excepcionales. En uso interior, y dependiendo del tipo de paredes puede alcanzar 10 o 20 metros. La atenuación, que es la disminución de la potencia de la señal en el espacio, no es uniforme y se ve afectada por múltiples efectos como las reflexiones, el tipo de paredes, las fuentes de ruido, entre otras.

Las antenas con mayor ganancia son las unidireccionales, pudiendo una parabólica comunicar dos bridges, un tipo especial de punto de acceso especializado en comunicar redes separadas, distanciados a 40 km.

* P R A C T I C A *

	TECNOLOGICO NACIONAL DE MEXICO **Instituto Tecnológico de Hermosillo**	
PRACTICA DE LABORATORIO 12.	**Tema 3.2**	**Pág. 1 de 3**

Programa SCD-1004:	**Práctica Numero:**	**Nombre de la Práctica:**
3.3.1 Dispositivos y configuración en redes inalámbricas	**12**	**Dispositivos y configuración en redes inalámbricas**

OBJETIVO ESPECIFICO: El Alumno construirá una red inalámbrica mediante los dispositivos elementales de punto de acceso y dispositivos finales. Realizará la configuración de estos para después confirmar su conectividad. Utilizar alguna herramienta de software para la realización de las pruebas finales.

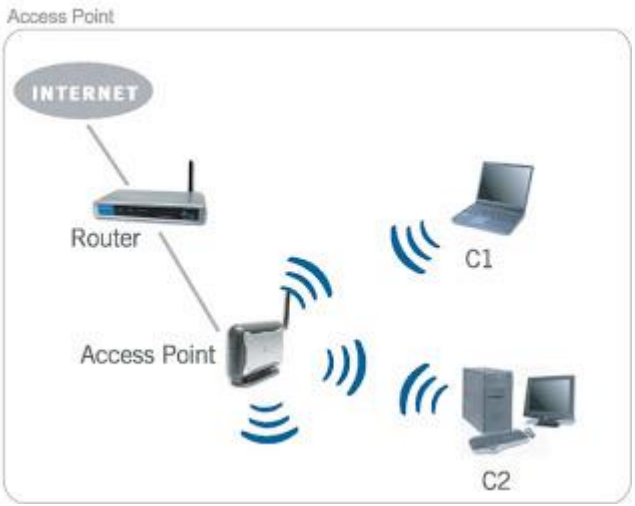
INFORMACION PREVIA:

Para crear una red inalámbrica se requiere de lo siguiente:

Conexión a Internet de banda ancha y módem. Una conexión a Internet de banda ancha es una conexión a Internet a alta velocidad. ADSL (línea de suscriptor digital) y cable son dos de las conexiones de banda ancha más comunes. Normalmente, los ISP que ofrecen ADSL son compañías telefónicas y los ISP que ofrecen cable son compañías de TV por cable. Con frecuencia, los ISP ofrecen módems de banda ancha. Algunos ISP también ofrecen una combinación de módem y router inalámbrico en un mismo dispositivo.

Enrutador o router inalámbrico. Un router envía información entre la red e Internet. Con un router inalámbrico, puedes conectar equipos a la red mediante señales de radio en lugar de cables. Hay varios tipos de tecnologías de red inalámbrica, entre las que se incluyen 802.11a, 802.11b, 802.11g, 802.11n y 802.11ac. Este equipo lo entrega el ISP a manera de comodato al abonado.

Un **adaptador de red inalámbrica** (tarjeta o interface de red inalámbrica) es un dispositivo que conecta el equipo a una red inalámbrica. Para conectar el equipo portátil o de escritorio a tu red inalámbrica, el equipo debe tener un adaptador de red inalámbrica. La mayoría de los portátiles y tabletas (y algunos equipos de escritorio), se distribuyen con un adaptador de red inalámbrica ya instalado. En caso de no tenerla, se deberá adquirirse e instalarse para lograr conexión Wireless.



PROCEDIMIENTO: Considerando que se cuenta con al menos dos dispositivos finales y un router inalámbrico, se procederá a la configuración inicial de los mismos. Sigue los pasos indicados en el desarrollo. Sabedores de que esta práctica requiere habilidades manuales, se recomienda apoyar en todo momento a quienes por alguna razón no les favorezca su condición física.

DESARROLLO: Las computadoras y el router deben estar en la misma área de cobertura, deben estar encendidos y operables en su modo estándar. El router por default inicializa al encenderlo tomando el SSID como el modelo y marca o el número de serie del mismo. Generalmente así viene de fábrica. No hay necesidad de configurar nada. Mientras que las terminales se configuran dependiendo del sistema operativo correspondiente. Sin embargo a continuación se muestran los pasos utilizando Windows 7. En otras plataformas la secuencia y etiquetas de cada elemento cambian un poco pero es fácil ubicarlos.

PASO 1. Barra de tareas.

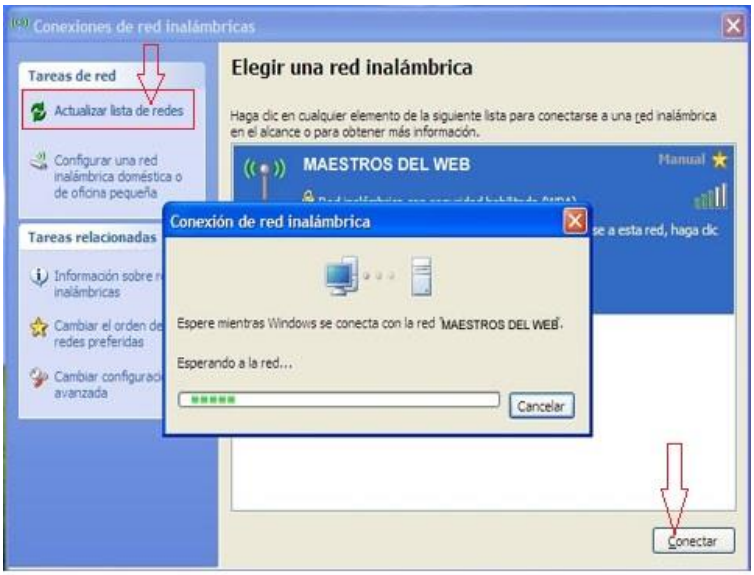
Iniciaremos buscando el icono de redes, que se encuentra en la barra de tareas, allí podremos saber si la máquina tiene la red desconectada y si podremos habilitarla.

PASO 2. Búsqueda de la red.

Al encontrar el icono, damos clic derecho sobre él y a continuación nos saldrá un menú textual, con varias opciones, de las cuales debemos seleccionar "*ver redes inalámbricas disponibles*".

PASO 3. Elegir una red.

En la ventana de conexiones de redes inalámbricas, debemos seleccionar la opción "*elegir una red inalámbrica*". Luego, seleccionamos la opción "actualizar lista de redes" con esto podremos ver las redes inalámbricas a las cuales tenemos alcance. Selecciona la red y luego presiona el botón "*conectar*" al final de la página.

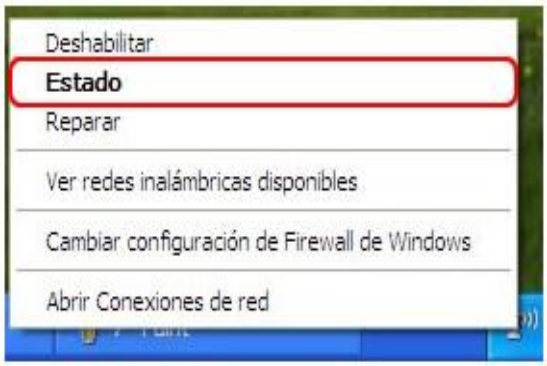


PASO 4. Al intentar conectarnos a esta red inalámbrica, nos solicita la clave de red para acceder a ella. Esta clave viene en la etiqueta del router, junto al número de serie.

Introducimos la clave y luego seleccionamos nuevamente el botón "*conectar*".

PASO 5. La terminal ha sido conectada exitosamente a la red inalámbrica. Ahora nos aparecerán los detalles de la conexión. Verifica esta conexión siguiendo los pasos seis en adelante. Para conectar las demás terminales se deberán realizar los cinco pasos anteriores con cada terminal.

PASO 6. Para verificar las características particulares de esta conexión, debemos regresar a la barra de tareas como en el paso 1 y seleccionar el icono de redes, como ya logramos establecer una conexión, al dar click derecho se despliega un menú de opciones donde seleccionaremos "*estado*".



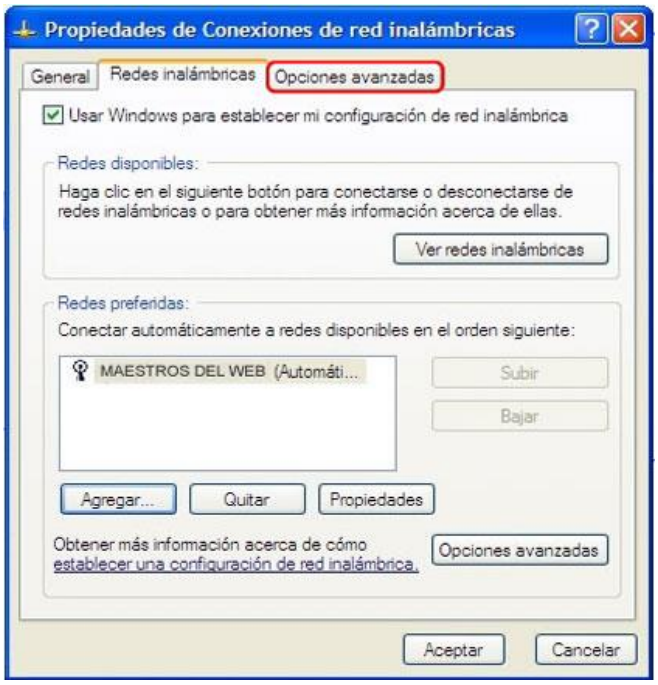
PASO 7. En la ventana de Estado de conexiones de las redes inalámbricas, nos muestra las características de la conexión: estado, red, duración, velocidad, intensidad de señal, paquetes recibidos y enviados.

Seleccione el botón de "*propiedades*".

PASO 8. Al seleccionar el botón de "propiedades", nos aparecerá en la misma ventana el adaptador de red que se está utilizando, mostrando la marca y modelo así como la opción de configurarla. También están los elementos que esta conexión de red utiliza se pueden instalar o desinstalar algunos otros, inclusive entrar a "propiedades" de uno de estos elementos. Seleccione el botón "*redes inalámbricas*"

PASO 9. En la pestaña “Redes inalámbricas” podemos definir, si esta conexión que creamos se conectará automáticamente. También, podemos agregar nuevas conexiones, quitar, o ver las propiedades de alguna de ellas.

Entrar a “*opciones avanzadas*”



PASO 10. En la pestaña Opciones Avanzadas se pueden definir las configuraciones de los cortafuegos o Firewall. Esto significa, poder proteger el equipo limitando o impidiendo el acceso de otros, desde fuera de mi red inalámbrica.

También puedo definir si la conexión será compartida.

Finalmente le damos “*Aceptar*” para terminar con la configuración.

Anota tus observaciones y conclusiones:

_____

_____

_____

_____

Realiza un diagrama de flujo indicando el proceso de configuración.

Mediante la simbología para realizar diagramas de flujo, realizar un esquema que describa el proceso de configuración de una terminal a una red inalámbrica.

3.3 Seguridad y servicios especiales en redes inalámbricas.

Las redes inalámbricas solucionan de una manera rápida y eficaz la necesidad de interconexión de los diferentes dispositivos móviles en nuestro entorno. Son imprescindibles para edificios donde por diferentes razones (valor protegido del inmueble, dificultad de acceso, entre otros) no podemos instalar estructuras definitivas como cableado, canaletas, plafones, regletas, etc. En soluciones especiales como para conectar edificios separados por algún obstáculo que hiciera muy caro o imposible llegar por cable; El cruzar un área específica o una calle, por ejemplo. También en operativos itinerantes donde la instalación de la red debe ser móvil debido a los breves periodos en los que se prestará servicio en el sitio. Tal es el caso de puntos de revisión, campañas de salud, trabajos de monitoreo y consultas de la región, etcétera.

Sin embargo, no debe dejarse de lado el aspecto de seguridad ya que al permitir conectividad inalámbrica, básicamente en todo el espacio aéreo de cobertura se dispondrá de la señal de la red. Esto podría ser aprovechado por personas ajenas a nuestro propósito de red y contraer situaciones poco agradables. En redes cableadas el recinto donde se realizan los enlaces o conexiones a la red se protege físicamente prohibiendo el acceso y vigilando este punto vulnerable de la red. En redes inalámbricas, la señal captada inclusive por fuera de nuestro edificio empresarial o de nuestro hogar por una persona malintencionada puede causarnos fuertes dolores de cabeza.

Algunas técnicas de seguridad en redes inalámbricas son las siguientes:

- WEP. Significa Wired Equivalet Privacy, y fue introducido para intentar asegurar la autenticación, protección de las tramas y confidencialidad en la comunicación entre los dispositivos inalámbricos. Puede ser WEP64 (40 bits reales) WEP128 (104 bits reales) y algunas marcas están introduciendo el WEP256. Es INSEGURO debido a su arquitectura, por lo que el aumentar los tamaños de las claves de encriptación sólo aumenta el tiempo necesario para romperlo.

- El cifrado TKIP que significa “Protocolo de integridad de clave temporal.” Fue un protocolo de encriptación provisional introducida con WPA para reemplazar el cifrado WEP, este cifrado es bastante débil y es vulnerado con facilidad. TKIP es en realidad muy similar a la encriptación WEP. Este cifrado ya no se considera seguro, y ahora está en desuso.
- AES se traduce como “Advanced Encryption Standard.” Este fue un protocolo de cifrado más seguro introducida con WPA2, que sustituyó al estándar WPA. AES es un fuerte estándar de cifrado usado en todo el mundo, incluso ha sido adoptado por el gobierno de Estados Unidos. AES se considera generalmente bastante seguro, y las principales debilidades sería ataques de fuerza bruta (evitadas por el uso de una contraseña fuerte) y las debilidades de seguridad en otros aspectos de WPA2.
- WPA2 usa AES para una seguridad óptima, también tiene la opción de utilizar TKIP para la compatibilidad con dispositivos asociados. En tal caso, los dispositivos compatibles con WPA2 se conectarán con WPA2 y dispositivos compatibles con WPA se conectará con WPA. Así que “WPA2” no siempre significa WPA2-AES. Sin embargo, en los dispositivos sin un “TKIP” visible o la opción “AES”, WPA2 es generalmente sinónimo de WPA2-AES.
- ACL. Significa Access Control List, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas. Esta técnica de seguridad viene a ser un servicio especial que eleva el nivel de confianza en los permisos de acceso a nuestra Wireless Network. Generalmente estas listas se elaboran manualmente.
- Otra técnica de seguridad o servicio especial viene siendo el cambiar el SSID y modificar su intervalo de difusión. Cada casa comercial reconfigura el suyo en sus dispositivos, por ello es muy fácil descubrirlo. Debemos cambiarlo por uno lo suficientemente difícil como para que lo adivinen. Así mismo debemos modificar la frecuencia de visualización del SSID, deteniendo su difusión de ser posible.

Métodos de cifrado más comunes que se encuentran en un router inalámbrico
➢ Abiertas (riesgo): Las redes abiertas Wi-Fi no tienen contraseña.
➢ WEP de 64 (riesgoso): El viejo estándar de encriptación WEP es vulnerable y no se debe utilizar.
➢ WEP 128 (riesgoso): WEP con un cifrado de clave de mayor tamaño, no significa que es mucho mejor.
➢ WPA-PSK (TKIP): Este es básicamente el estándar de cifrado WPA o WPA1. Se ha superado y no es seguro.
➢ WPA-PSK (AES): Esto selecciona el protocolo de cifrado inalámbrico WPA con el cifrado AES. Los dispositivos que soportan AES casi siempre soportarán WPA2, mientras que los dispositivos que requieren WPA1 casi nunca podrán usar el cifrado AES.
➢ WPA2-PSK (TKIP): Utiliza el estándar WPA2 con cifrado TKIP más moderno. Esto no es seguro, y es sólo una buena idea si tienes los dispositivos más antiguos que no pueden conectarse a una red WPA2-PSK (AES).
➢ WPA2-PSK (AES): Esta es la ***opción más segura***. Utiliza WPA2, el último estándar de encriptación Wi-Fi, y el más reciente protocolo de encriptación AES.
➢ WPAWPA2-PSK (TKIP / AES) (recomendado): Esto cifrado permite tanto WPA y WPA2 con TKIP y AES. Esto proporciona la máxima compatibilidad con todos los dispositivos antiguos que pueda tener, sino que también garantiza que un atacante no pueda acceder a la red tan fácilmente

.:

*** P R A C T I C A ***

Programa IFD-1020:	Practica Numero:	Nombre de la Practica:
3.3.2 Seguridad y servicios especiales en redes inalámbricas	**13**	**Seguridad y servicios especiales en redes inalámbricas**

OBJETIVO ESPECIFICO: EL Alumno analizará la seguridad implementada en una red inalámbrica, determinando sus vulnerabilidades. Realizará cambios en la configuración de la red, modificando el SSID ocultándolo, desactivando el DHCP y creando filtrado de direcciones MAC (ACL, access control list). Comprobará cada actividad realizada mediante pruebas de acceso o conexión a la red inalámbrica.

INFORMACION PREVIA: Acrylic WiFi es un programa que nos va a permitir monitorear redes inalámbricas y comprobar su seguridad, además de poder capturar y mostrar la información de las redes inalámbricas que se encuentran a nuestro alcance.

Con Acrylic WiFi vamos a poder:

- Capturar el tráfico de una red.
- Obtener información sobre las redes disponibles.
- Obtener información sobre los clientes conectados a las redes.
- Permite ejecutar scripts, con lo cual se pueden romper claves de acceso.

Esta herramienta de software puede descargarse de internet a modo prueba por un periodo de tiempo, lo cual es suficiente para la realización de nuestra práctica.

Para modificar los parámetros de configuración de nuestra red inalámbrica, es necesario tener libre acceso a nuestro punto de acceso o router por lo cual es indispensable conseguir inicialmente dicha clave o presionar el botón de “reset” en

el router con la intención de que se reestablezcan los parámetros a los establecidos de fábrica. La clave de acceso de fábrica viene impresa en la etiqueta de características y número de serie del dispositivo.
La forma de configurar el router cambia según la marca y modelo, sin embargo prácticamente todos muestran en su menú de opciones los apartados de SSID (nombre de la red), configuración del DHCP (batería de direcciones IP) donde se puede activar o desactivar y la creación de listas de acceso basados en direcciones MAC (ACL).

Riesgos relacionados con las redes inalámbricas:

- Access Point Spoofing: Este es un ataque que consiste en hacerse pasar por un AP verdadero. El cliente cree que se está conectado a una red verdadera y toda la información será capturada.
- MAC spoofing: Ocurre cuando alguien roba una dirección MAC de una red haciéndose pasar por un cliente autorizado. En general, las tarjetas de redes permiten el cambio de la MAC por otro, lo que posibilita este tipo de ataque.

- Denial of service (Negativa de Servicio): También conocido por *D.O.S.* Consiste en negar algún tipo de recurso o servicio. Puede ser utilizado para "inundar" la red con pedidos de disociación, imposibilitando así el acceso de los usuarios, pues los componentes de la red se asocian y desasocian una y otra vez.
- Sniffing: Este tipo de ataque consiste en interceptar el tráfico de una red. Para ello, tanto atacante con víctima, deben estar en la misma red, con lo que suele ser un ataque típico en redes no seguras, como redes abiertas o las proporcionadas en lugares públicos (hoteles, cafeterías, entre otras.

PROCEDIMIENTO: EL Alumno implementará las configuraciones requeridas para poder ocultar el SSID de nuestra red Wireless, desactivar el DHCP para evitar accesos dinámicos o de dispositivos no registrados y elaborará una lista de acceso por direcciones MAC de los dispositivos a los cuales dará acceso.

DESARROLLO:

a) Establecer acceso en nuestra terminal a la red inalámbrica.
b) Entrar al modo de configuración del router.
c) Desactivar la publicación del SSID para que quede oculto.
d) Entrar al modo configuración del DHCP y deshabilitarlo.
e) En el apartado de ACL, registrar la MAC de nuestra terminal.
f) Analizar los cambios realizados y lograr conectar dos terminales.
g) Certificar que la configuración de seguridad realizada, funcione de la manera correcta, intentando acceso desde una nueva terminal.

Anota tus observaciones y conclusiones del procedimiento realizado:

_____

_____

_____

_____

_____

Enlista paso a paso el procedimiento realizado para establecer seguridad.

Con tus propias palabras describe el desarrollo de la configuración realizada, menciona el grado de seguridad que se logra y sus ventajas y desventajas.

REFERENCIAS DE CONSULTA

- B. Sanz, Brio Martín, "Direccionamiento IP". (2da Edición). México, 2002.
- S. Tanenbaum, "Redes de Computadoras". 4º Edición. Pearson Education, Mexico, 2003.
- Iván Bernal, Tesis Doctoral "Visión general de Tecnologías Inalámbricas". Escuela Politécnica Nacional de Ecuador, 2007
- Luis Fernando Valle Islas, Tesis Doctoral "Coexistencia de Redes WLAN & WPAN". Universidad de las Américas Puebla, 2005.
- J. S. Beasley, "Networking". 2º Edición. Pearson Education, Michigan, 2008.
- "Academia de Networking de Cisco Systems: Guía del segundo año CCNA 3 y 4". 3º Edición. Cisco Press, Madrid, 2008.
- Stig Erik Arnesen y Kjell Age Haland, Tesis Doctoral "Modelling of coverage in WLAN". Agder University College, 2001.

REFERENCIAS ELECTRONICAS:

El ABC de IPv4 (parte 1)
[1] http://www.eveliux.com/mx/El-ABC-de-IPv4-parte-1.html

El ABC de IPv4 (parte 2)
[2] http://www.eveliux.com/mx/El-ABC-de-IPv4-parte-2.html

[3] http://grouper.ieee.org/groups/802/15/index.html

[4] http://www.ieee802.org/11/

[5] http://grouper.ieee.org/groups/802/16/index.html

[6] http://www.ieee802.org/22/

[7] http://es.kioskea.net/contents/wireless/

[8] http://wikipedia.org/