



Universidad Nacional Autónoma de México
Facultad de Estudios Superiores Cuautitlán
Ingeniería en Telecomunicaciones, Sistemas y Electrónica
Departamento de Ingeniería
Sección Electrónica
Manual de prácticas de:
TRANSMISIÓN DE DATOS



Clave de la Carrera: 130

Clave de la Asignatura: 0599

Autores: Mtro. Jorge Ramírez Rodríguez
Mtro. Jorge Alberto Vázquez Maldonado
Dra. Alma Alejandra Luna Gómez.

Fecha de Revisión: diciembre de 2025

Semestre: 2026-2



ÍNDICE

CONTENIDO	3
PRÁCTICA 1. Equipos típicos en redes de computadoras (Temas de Teoría I)	7
PRÁCTICA 2. Tipos de cables utilizados en la transmisión de datos (Temas de Teoría I, II)	14
PRÁCTICA 3. Redes locales y direccionamiento con redes y subredes (Temas de Teoría III, IV)	18
PRÁCTICA 4. Configuración del Router (Temas de Teoría IV)	21
PRÁCTICA 5. Configuración del Router por comandos CLI (Temas de Teoría IV)	27
PRÁCTICA 6. Configuración del Switch por comandos CLI (Temas de Teoría III)	37
PRÁCTICA 7. Implementación de VLANS (Temas de Teoría V1)	39
PRÁCTICA 8. Servidores (Temas de Teoría VI)	44
PRÁCTICA 9. Configuración física de una red LAN (Temas de Teoría I)	49
PRÁCTICA 10. Configuración física de una red WAN (Temas de Teoría IV)	52
ANEXOS	55



CONTENIDO

INTRODUCCIÓN

Los sistemas de transmisión de datos constituyen el apoyo de los sistemas de cómputo para el transporte de la información que manejan. Sin estos sistemas, no hubiera sido posible la creación de las redes avanzadas en las que compartir información y transferir datos entre computadoras con gran difusión geográfica, sumamente rápido y en grandes volúmenes es vital para el funcionamiento eficiente de todo el engranaje económico, político y social del mundo.

Los sistemas de transmisión de datos son imprescindibles en redes cuyos enlaces exceden los 20 m. Las redes pueden ser sencillas, como una computadora enlazada a un dispositivo periférico (por ejemplo, una impresora), pasando por la conexión de punto a punto de larga distancia que se satisface con la utilización de módems, o redes ligeramente más complejas que conectan varias terminales de cómputo de edificios lejanos con la computadora principal (Host) de un centro especializado de datos, o una red de área local que se emplea en una empresa para interconectar varios dispositivos de cómputo. Las redes más complejas pueden interconectar las diferentes grandes computadoras de los principales centros financieros del mundo y suministrar a los comerciantes información del mercado de último momento a través de miles de terminales remotas. Este manual de prácticas pretende que los alumnos de la asignatura de transmisión de datos reafirmen los conocimientos teóricos adquiridos en clase mediante la realización de 10 prácticas.

En las primeras 8 prácticas trabajaremos con un simulador de aprendizaje de redes interactivo. Esta herramienta permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Se enfoca en apoyar mejor los protocolos de redes.

Este producto tiene el propósito de ser usado como educativo, brindando exposición a la interfaz de línea de comando de los dispositivos de red para practicar y aprender por descubrimiento.

En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. Luego, al hacer clic en ellos, se puede ingresar a sus consolas de configuración. Una vez completada la configuración física y lógica de la red, también se pueden hacer simulaciones de conectividad, todo ello desde las mismas consolas incluidas. Una de las grandes ventajas de utilizar este programa es que permite “ver” (opción “Simulation”) cómo deambulan los paquetes por los diferentes equipos (switches, routers, etc.). Además, se puede analizar de forma rápida el contenido de cada uno de ellos en las diferentes capas de red. (Ver anexo 1 para más información).


OBJETIVO GENERAL DE LA ASIGNATURA

El alumno conocerá y comprenderá los conceptos teóricos y prácticos de la transmisión de datos en los sistemas de comunicaciones actuales y podrá diseñar e implementar redes de información de acuerdo con las normas actuales.

OBJETIVO DEL CURSO EXPERIMENTAL

El alumno diseñará e implementará redes de Transmisión de Datos.



	UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN DEPARTAMENTO DE INGENIERÍA SECCIÓN ELECTRÓNICA
	REGLAMENTO INTERNO DE LABORATORIOS

El presente reglamento de la sección electrónica tiene por objetivo establecer los lineamientos para el uso y seguridad de laboratorios, condiciones de operación y evaluación, que deberán de conocer y aplicar, estudiantes y profesores en sus cuatro áreas: comunicaciones, control, sistemas analógicos y sistemas digitales.

1. Queda estrictamente prohibido, al interior de los laboratorios
 - a) Correr, jugar, gritar o hacer cualquier otra clase de desorden.
 - b) Dejar basura en las mesas de trabajo y/o pisos.
 - c) Fumar, consumir alimentos y/o bebidas.
 - d) Realizar o responder llamadas telefónicas y/o el envío de cualquier tipo de mensajería.
 - e) La presencia de personas ajenas en los horarios de laboratorio.
 - f) Dejar los bancos en desorden y/o sobre las mesas.
 - g) Mover equipos o quitar accesorios de una mesa de trabajo.
 - h) Usar o manipular el equipo sin la autorización del profesor.
 - i) Rayar y/o sentarse en las mesas del laboratorio.
 - j) Energizar algún circuito sin antes verificar que las conexiones sean las correctas (polaridad de las fuentes de voltaje, multímetros, etc.).
 - k) Hacer cambios en las conexiones o desconectar el equipo estando energizado.
 - l) Hacer trabajos pesados (taladrar, martillar, etc.) en las mesas de trabajo.
 - m) Instalar software y/o guardar información en los equipos de cómputo de los laboratorios.
 - n) El uso de cualquier aparato o dispositivo electrónico ajeno al propósito para la realización de la práctica.
 - o) Impartir clases teóricas, su uso es exclusivo para las sesiones de laboratorio.
2. Es responsabilidad del profesor y de los estudiantes revisar las condiciones del equipo e instalaciones del laboratorio al inicio de cada práctica (encendido, dañado, sin funcionar, maltratado, etc.). El profesor deberá generar el reporte de fallas de equipo o de cualquier anomalía y entregarlo al responsable de laboratorio o al jefe de sección.
3. Los profesores deberán de cumplir con las actividades y tiempos indicados en el “cronograma de actividades de laboratorio”.
4. Es requisito indispensable para la realización de las prácticas que el estudiante:
 - a) Descargue el manual completo y actualizado al semestre en curso, el cual podrá obtener en (<https://virtual.cuautitlan.unam.mx/ingenieriafesc/>)
 - b) Presente su circuito armado en la tableta de conexiones para poder realizar la práctica (cuando aplique), de no ser así, tendrá una evaluación de cero en la sesión correspondiente.
 - c) Realizar las actividades previas y entregarlas antes del inicio de la sesión de práctica, de no ser así, tendrá una evaluación de cero en la sesión correspondiente.



5. Estudiante que no asista a la sesión de práctica de laboratorio será evaluado con cero.
6. La evaluación de cada sesión debe realizarse con base en los criterios de evaluación incluidos en los manuales de prácticas de laboratorio y no podrán ser modificados. En caso contrario, el estudiante deberá reportarlo al jefe de sección.
7. La evaluación final del estudiante en los laboratorios será con base en lo siguiente:
 - a) **(Aprobado) Cuando el promedio total de todas las prácticas de laboratorio sea mayor o igual a 6 siempre y cuando tengan el 90% de asistencia y el 80% de prácticas acreditadas con base en los criterios de evaluación.**
 - b) **(No Aprobado) No cumplió con los requisitos mínimos establecidos en el punto anterior.**
 - c) **(No Presentó) Cuando no asistió a ninguna sesión de laboratorio o que no haya entregado actividades previas o reporte alguno.**
8. Profesores que requieran hacer uso de las instalaciones de laboratorio para realizar trabajos o proyectos, es requisito indispensable que las soliciten por escrito al jefe de sección. Siempre y cuando no interfiera con los horarios de los laboratorios.
9. Estudiantes que requieran realizar trabajos o proyectos en las instalaciones de los laboratorios, es requisito indispensable que esté presente el profesor responsable del trabajo o proyecto. En caso contrario no podrán hacer uso de las instalaciones.
10. Correo electrónico del buzón para quejas y sugerencias para cualquier asunto relacionado con los laboratorios (seccion_electronica@cuautitlan.unam.mx).
11. El incumplimiento a estas disposiciones faculta al profesor para que instruya la salida del infractor y en caso de resistencia, la suspensión de la práctica.
12. A los usuarios que, por su negligencia o descuido inexcusable, cause daños al laboratorio, materiales o equipo deberá cubrir los gastos que se generen con motivo de la reparación o reposición, indicándose en el reporte de fallas correspondiente.
13. Los usuarios de laboratorio que sean sorprendidos haciendo uso indebido de equipos, materiales, instalaciones y demás implementos, serán sancionados conforme a la legislación universitaria que le corresponda, según la gravedad de la falta cometida.
14. Los casos no previstos en el presente reglamento serán resueltos por el Jefe de Sección, de acuerdo con los lineamientos generales para el uso de los laboratorios en la Universidad Nacional Autónoma de México.

SECCIÓN ELECTRÓNICA
“POR MI RAZA HABLARÁ EL ESPÍRITU”
Cuautitlán Izcalli, Estado de Méx. a 16 de junio de 2025



INSTRUCTIVO PARA LA ELABORACIÓN DEL REPORTE

- Los reportes deberán basarse en la metodología utilizada en los manuales de prácticas de laboratorio.
- Ejemplo de portada de prácticas (obligatoria)

Universidad Nacional Autónoma de México	
Facultad de Estudios Superiores Cuautitlán	
Laboratorio de: _____	Transmisión de Datos _____ Grupo: _____
Profesor: _____	
Alumno: _____	
Nombre de Práctica: _____	No. de Práctica: _____
Fecha de realización: _____	Fecha de entrega: _____
Semestre: _____	

No. de criterio	Criterio de Evaluación para el laboratorio	Porcentaje
C1	Actividades previas indicadas en el manual de practicas	30%
C2	Desarrollo y funcionalidad de la práctica	10%
C3	Obtención de resultados correctos	10%
C4	Reporte entregado con todos los puntos indicados en el manual de practicas	50%

Evaluación de Atributos de Egreso
La evaluación del Atributo de Egreso se llevará a cabo durante la Práctica No. <u>7</u> , mediante una lista de cotejo que será aplicada en la sesión correspondiente. Esta evaluación permitirá valorar el desempeño del estudiante en relación con los atributos de egreso establecidos en el perfil del ingeniero y será de su conocimiento por el profesor y publicada en el listado único de calificaciones.

BIBLIOGRAFIA:

- William Stalling, Redes e internet de alta velocidad: rendimiento y calidad de servicio, Prentice Hall Hispanoamericana, 2ª edición, España, 2004.
- Jordi Julia Sort, Redes metropolitanas = metropolitan networks, Editorial Gustavo Gili, 1ª Edición, México, 2004.
- Natalia Olifer, Redes de computadoras, McGraw Hill Hispanoamericana, 1ª edición, México, 2009.
- William Stalling, Fundamentos de seguridad en redes; Aplicaciones estándares, Prentice Hall Hispanoamericana, 2ª edición, España, 2004.
- KUROSE, JIM y ROSS, KEITH Redes de Computadores- Un enfoque descendente basado en



-
- Internet. Segunda edición. Ed. Addison Wesley, 2003VV, AA, Redes de Computadores y Arquitecturas de Comunicaciones: Supuestos Prácticos, Pearson Education, México, 2001.
- Forouzan, Behrouz A, Transmisión de Datos y Redes de Comunicaciones, Mc.Graw Hill Interamericana, España, 2007.
 - Huidobro, Moya José Manuel, Comunicaciones en Redes WLAN, Creaciones Copyright, España, 2005.



PRÁCTICA 1: “EQUIPOS TÍPICOS EN REDES DE COMPUTADORAS”

OBJETIVO

- Conocer y entender el funcionamiento de los diferentes equipos o elementos que forman una red de computadoras.

INTRODUCCIÓN

Las computadoras, además de ser parte integral de una red, también desempeñan un papel preponderante en el mundo laboral. Las empresas utilizan sus computadoras para una gran variedad de propósitos. Utilizan los servidores para almacenar datos importantes. Emplean software de hojas de cálculo para organizar la información, procesadores de texto para llevar registros y navegadores para acceder a los distintos sitios web. Para realizar todas estas actividades, se requiere una serie de equipos o dispositivos que nos ayuden a compartir la información contenida en las diferentes computadoras y servidores.

Estos son:

1. Tarjetas de interfaz de red (NIC)
2. Hub (Concentrador).
3. Bridge (Puente).
4. Switches.
5. Routers.

ACTIVIDADES PREVIAS A LA PRÁCTICA

- Leer toda la práctica.
- Investigar los tipos de redes de datos.
- Investigar qué elementos que conforman una red de datos y su funcionamiento.

EQUIPO Y MATERIAL

- Computadora personal con el software apropiado ya instalado.

PROCEDIMIENTO EXPERIMENTAL

1.1 TARJETA DE INTERFAZ DE RED (NIC).



Figura 1

1. Encontrar la dirección MAC.

En Windows; abre una línea de comandos de DOS (o símbolo del sistema).

Una forma de hacerlo es:

Menú inicio, Ejecutar, escribir "cmd".

Escribe el comando *ipconfig /all* (Figura 2).

Identifica la sección "Adaptador de Ethernet Conexión de área local".

Identifica el valor de "Dirección física" esta es la "dirección MAC".

NOTA: Para cada computadora, este valor es diferente, si la computadora también tiene tarjeta inalámbrica, esta también tendrá una dirección física.

```
C:\Windows\system32\cmd.exe
C:\Users\Comunicaciones>ipconfig/all
Configuración IP de Windows
Nombre de host. . . . . : L-901
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : híbrido
Enrutamiento IP habilitado . . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Conexión de área local:
Estado de los medios . . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . :
Descripción . . . . . : Realtek PCIe GBE Family Controlle
Dirección física . . . . . : 74-27-EA-4A-5A-17
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí

Adaptador de LAN inalámbrica Conexión de red inalámbrica:
Sufijo DNS específico para la conexión. . . . . :
Descripción . . . . . : TP-LINK 150Mbps Wireless Lite N A
dapter
Dirección física . . . . . : C8-4A-00-28-56-E8
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí
Vínculo de dirección IPv6 local. . . . . : fe80::e0b8:b0c7:42c5:4169%10(Preferido)
Dirección IPv4. . . . . : 10.189.41.177(Preferido)
Máscara de subred . . . . . : 255.0.0.0
Conexión obtenida . . . . . : viernes, 05 de diciembre de 2014
12:32:20 p.m.
La concesión expira . . . . . : sábado, 06 de diciembre de 2014 0
1:18:44 p.m.
Puerta de enlace predeterminada . . . . . : 10.128.128.128
Servidor DHCP . . . . . : 10.128.128.128
ID DHCPv6 . . . . . : 247482880
DUID de cliente DHCPv6 . . . . . : 00-01-00-01-1B-15-0F-B3-C8-4A-00-
28-56-E8
Servidores DNS . . . . . : 10.128.128.128
NetBIOS sobre TCP/IP. . . . . : habilitado
```


Figura 2

2. Anotar las direcciones MAC encontradas.

1.2 CONCENTRADOR (HUB).



Figura 3

1. Ejecute el simulador  ver [anexo I](#).

2. Colocar un Hub.

En la sección inferior izquierda de la pantalla, seleccionar dispositivos de red y abajo seleccionar “Hubs”, a la derecha aparecen los modelos disponibles, seleccionar “**Hub-PT**”, arrastrarlo a la parte central donde armaremos la topología, y dar clic para colocar el equipo.

3. Colocar una PC.

En la sección inferior izquierda de la pantalla, seleccionar “End Devices” (Dispositivos Finales), aquí aparecen los modelos disponibles, seleccionar “**PC-PT**”, colocar el dispositivo en el escenario de tal forma que se comience a armar la topología. De esta manera colocar tres computadoras más.

4. Conectar los dispositivos.

En la sección de equipos, seleccionar “Connections” (Conexiones), esta nos dará las diferentes opciones de cables para conectar los equipos “selección cable directo”, dar clic en el Hub y mover el mouse hacia la PC0, y dar nuevamente clic y de esta manera se conectan los dispositivos, de la misma manera conectar las otras PC’s al Hub (Figura 4).

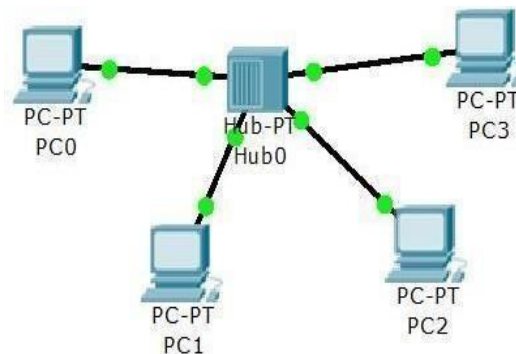


Figura 4

5. Llenar la tabla 1 con direcciones IP estáticas pertenecientes a una red privada clase B



	RED	PC0	PC1	PC2	PC3	GATEWAY
Dirección IP						
Mascara de Subred						

Tabla 1

Dando clic sobre una PC0 aparece la ventana de las propiedades del dispositivo, seleccionar la pestaña “Desktop” (Escritorio), dar clic en “IP Configuration”, en la ventana siguiente seleccionar “Static”, en el campo “IP Address” escribimos la dirección IP, cambiamos al siguiente campo y automáticamente dará la máscara de red por default para esta dirección IP, cerramos las ventanas y regresamos a la topología.

Otra forma de asignar direcciones IP es dando clic sobre otra PC, en la pestaña “Config”, seleccionar “INTERFACE”, luego “FastEthernet0” y en el campo “IP Address” escribir la dirección IP correspondiente y máscara de red por default para la clase de dirección.

- Asignar dirección IP a las otras computadoras utilizando ambos métodos y con el editor de notas “Place Note (N)” que se encuentra en la barra de herramientas o también presionando alt+n, colocar una etiqueta con las direcciones IP a los hosts.

- Colocar la imagen de la topología construida en el reporte y anotar sus comentarios.

- Verificar la configuración de cada una de las computadoras,

Dando doble clic en la PC y seleccionando la pestaña “Escritorio” y en la opción “Command Prompt” (Símbolo del Sistema), En el entorno similar al sistema operativo DOS, escribe “IPCONFIG” y presiona “Enter.

Anotar sus comentarios

- Verificar que existe comunicación entre los equipos de la red, selecciona uno de los equipos de la red y en símbolo del sistema (Command prompt) ejecutar el comando “**PING**” acompañado de la dirección IP del equipo con el cual se desea establecer comunicación. Del resultado de ello se debe observar que se enviaron y recibieron paquetes de información y el tiempo de duración.

- Anotar los resultados del comando ping de dos pruebas de diferentes equipos.

- Enviar paquetes de prueba PDU.

Estando en modo simulación, seleccionamos el icono de sobre cerrado “ADD Simple PDU (P)” (agregar PDU simple) que se encuentra del lado derecho de la ventana, y lo colocamos dando clic sobre una PC origen, que es la que envía el mensaje, a continuación, seleccionamos una PC destino que es la que recibe el mensaje y dar clic en play para ver como viaja el PDU.

Anotar sus comentarios y los protocolos involucrados.

Borrar los mensajes enviados con “Delete”.



1.3 PUENTE (BRIDGE)

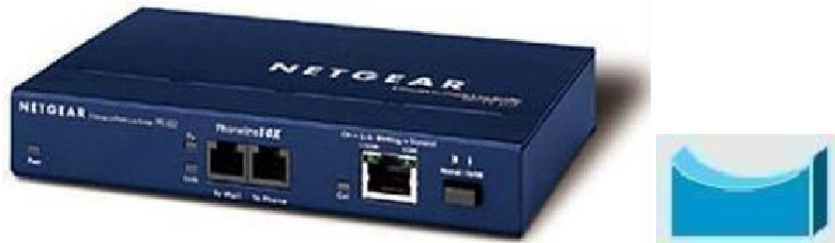


Figura 5

1. Modificar la topología utilizando las mismas PC's como se muestra en la figura 6, colocando otro Hub y un Puente. Para seleccionar el puente, ir a la sección de equipos y elegir Switches, de los modelos disponibles elegir "PT-Bridge".

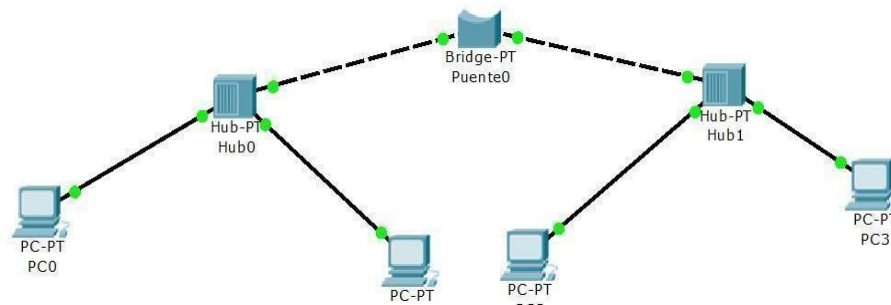


Figura 6

2. Enviar PDU's simples entre los diferentes hosts.
3. Comente lo ocurrido en cada caso, así como el funcionamiento del puente.

1.4 SWITCH



Figura 7

1. Conectar una red LAN con un switch. En la topología anterior, eliminar el puente y los dos Hub's, ir a la sección de equipos y seleccionar Switches, seleccionar el modelo **2950 - 24**, y conectarlo como se muestra en la Figura 8.
2. Esperar a que las conexiones del switch se habiliten (cuando el nodo cambie de color naranja a verde.).

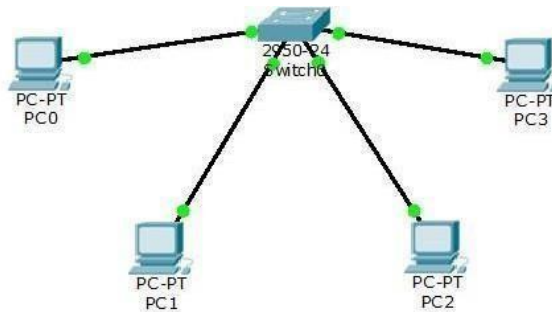


Figura 8

3. Enviar repetidamente PDU's simples entre los diferentes hosts (En modo simulación).

4. Observar el funcionamiento del Switch.

Anotar sus comentarios y los protocolos involucrados.

1.5 RUTEADOR (ROUTER)



Figura 9

1. Conectar un Ruteador a la red LAN.

En la topología anterior ir a la sección de equipos de red, ahora seleccionar Routers, esta nos dará las opciones de los modelos disponibles, seleccionar el modelo **2811**, y colocarlo como se muestra en la figura 10.

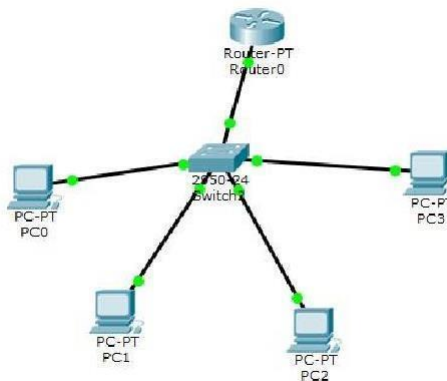


Figura 10



2. Activar el puerto del Ruteador.

Colocando el cursor en el cable que conecta el router aparecerá el puerto Fa (FastEthernet), en la pestaña “Config” seleccionar la interfaz a la que está conectado y asignar una dirección IP al puerto (Gateway), y encenderlo seleccionando ON en estatus de puerto.

3. Verificar conectividad entre los elementos de la red
Anotar sus comentarios.

CUESTIONARIO

1. ¿Cuáles son los elementos básicos de una red?, describa su función.
2. ¿Cuáles son las características de las direcciones IPV4 e IPV6?
3. ¿Qué diferencias existen entre un switch y un hub en cuanto al manejo del tráfico de red y el nivel del modelo OSI en el que operan?
4. Indique a qué capa del modelo OSI corresponde cada dispositivo visto en esta práctica.

CONCLUSIONES

BIBLIOGRAFIA

PRÁCTICA 2: “TIPOS DE CABLES UTILIZADOS EN LA TRANSMISIÓN DE DATOS”

OBJETIVO

- Fabricar un cable de red de conexión directa (Patch), un cable de red de conexión cruzada (Crossover) y un cable transpuesto (Roll Over) según los estándares T568-A o T568-B para la conexión hacia o entre los elementos de una red.

INTRODUCCIÓN

Los medios físicos de transmisión representan el soporte fundamental por donde viaja la información digital en una red. Estos se clasifican en medios guiados (cableados) y no guiados (inalámbricos). En esta práctica se trabajará con medios guiados, específicamente con el **cable de par trenzado**, el más ampliamente utilizado en redes de área local (LAN) debido a su bajo costo, facilidad de instalación y aceptable desempeño para distancias cortas.

Existen diferentes categorías de cables UTP (Unshielded Twisted Pair) y STP (Shielded Twisted Pair), que definen capacidades de transmisión de datos en función del número de vueltas por metro, el blindaje y el ancho de banda soportado.

Los estándares TIA/EIA-568 establecen las configuraciones y normas de cableado estructurado, siendo los esquemas T568-A y T568-B los más comunes en redes Ethernet. La correcta implementación de estos estándares es esencial para garantizar compatibilidad, continuidad eléctrica y funcionamiento de los equipos conectados.

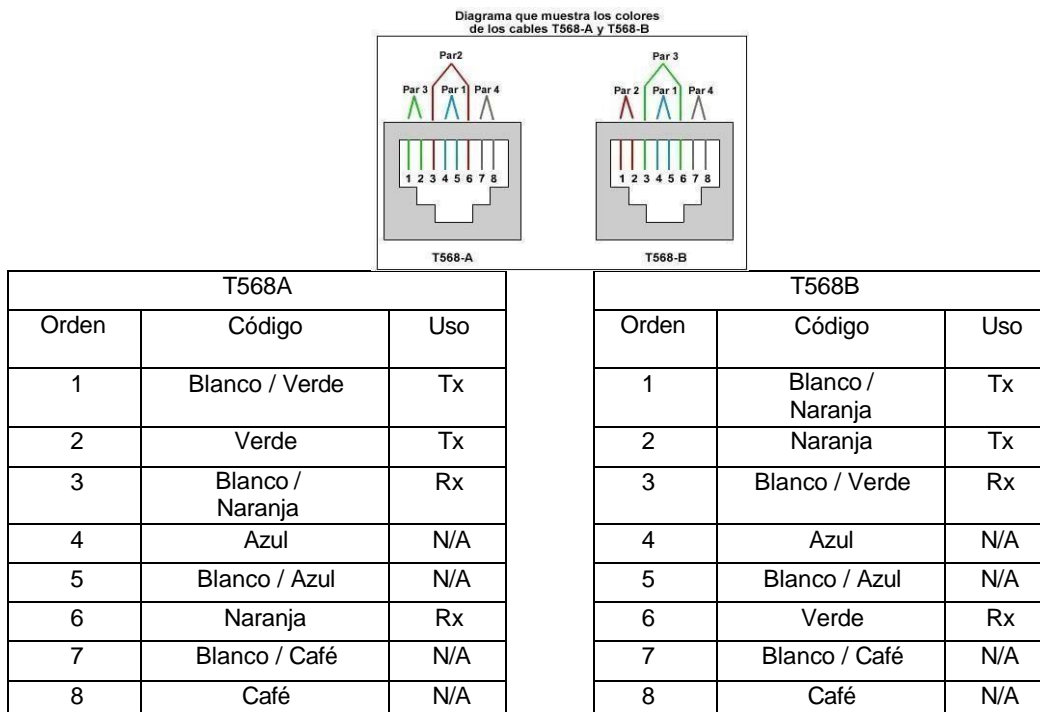


Figura 1

ACTIVIDADES PREVIAS A LA PRÁCTICA

- Leer toda la práctica.
- Investiga el significado de TIA/EIA y describe brevemente el objetivo de sus normas aplicadas al cableado estructurado.
- Consulta y enumera las categorías de cable UTP más utilizadas en redes de datos (Cat5e, Cat6, Cat6a, etc.), indicando sus características principales.

EQUIPO Y MATERIAL

- 3 tramos de Cable UTP
- 6 conectores RJ45
- Ponchadora de cables o pinza de crimpado
- Pinza de corte
- Tijeras
- Probador de continuidad para cables de LAN
- Multímetro

PROCEDIMIENTO EXPERIMENTAL

2.1 ARMAR UN CABLE DIRECTO (PATCH) CON CONECTOR RJ45 (MACHO).

1. Con la pinza para pelar cable corta aproximadamente 3 a 5 cm de la cubierta del cable UTP, teniendo cuidado de no cortar la cubierta de los conductores, retira el revestimiento de cable, (Figura 2).

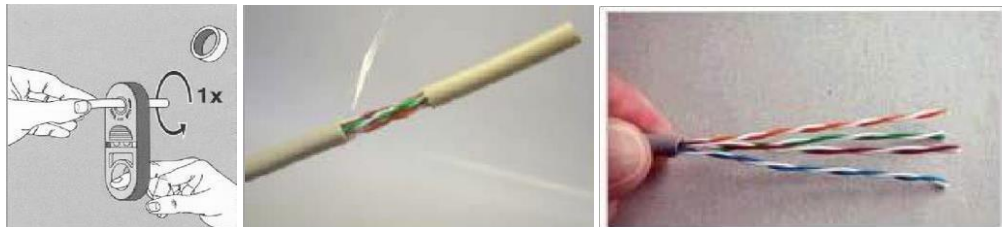


Figura 2

2. Destorcer los alambres, (Figura 3).

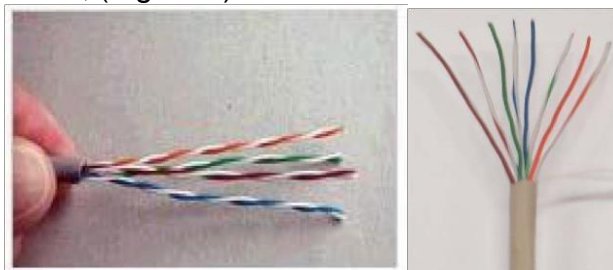


Figura 3

3. Alinear los alambres, (Figura 4).

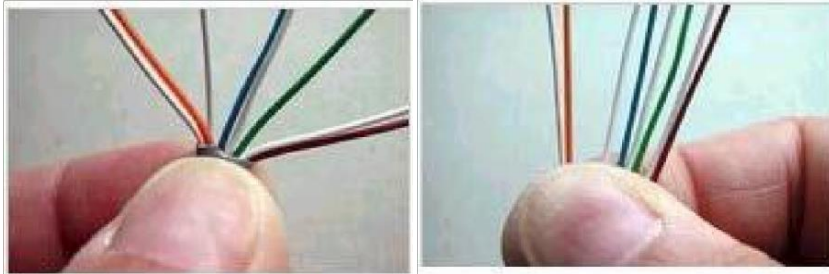


Figura 4

4. Acomodar los alambres en el orden correcto según el estándar a aplicar T568-A o T568- B, corta los alambres considerando que el revestimiento debe de quedar al tope dentro del conector aproximadamente 1.5cm, de esta manera también quedará sujeto con la cuchilla plástica (Figura 5).



Figura 5

5. Introducir los alambres dentro de las guías hasta que observes que todos los cobres se ven en la parte superior del conector, también observa el conector lateralmente para ver que los alambres llegaron hasta arriba.
6. Coloca el conector dentro de las pinzas de crimpado y ejerce presión, (Figura 6).



Figura 6

7. En el otro extremo del cable realizar el mismo procedimiento de los pasos 1 al 6, teniendo en cuenta que para un cable directo (Patch) se utiliza la misma norma en ambos extremos.

8. Prueba final del cable.

Coloca cada conector de tu cable en el probador de cable de red. (Figura 7).

Enciende el probador, observa y comenta los resultados.



Figura 7

2.2 ARMAR UN CABLE CRUZADO (CROSSOVER) CON CONECTOR RJ45 (MACHO).

1. Realizar el mismo procedimiento que se realizó con el cable directo, con la diferencia de que en cada extremo se acomodan los cables con norma diferente, es decir, si en un extremo se utilizó el estándar T568-A en el otro extremo se utiliza el estándar T568-B.

2.3 ARMAR UN CABLE DE CONSOLA (ROLLOVER) CON CONECTOR RJ45 (MACHO).

1. Realizar el mismo procedimiento 1 al 6 que se realizó con el cable directo, en un cable de consola se toman las siguientes consideraciones: el pin 1 en un extremo se conecta con el pin 8 en el otro extremo, el pin 2 se conecta al pin 7, el pin 3 se conecta al pin 6 y así sucesivamente. Por este motivo se llama también "transpuesto", porque los pines en un extremo se invierten en el otro, como si un extremo del cable se hubiera rotado o girado, sin importar el estándar utilizado (T568-A o T568-B), finalmente prueba la continuidad del cable con un multímetro y anota comentarios.

CUESTIONARIO

1. ¿Cuáles son los diferentes tipos de cables de par trenzado y sus categorías?
2. Describe las aplicaciones específicas de los cables de red: directo, cruzado y transpuesto. ¿Qué dispositivos se conectan con cada uno?
3. ¿Qué es un dominio de colisión?
4. ¿Qué es "Diafonía"?

CONCLUSIONES

BIBLIOGRAFÍA



PRÁCTICA 3: “REDES LOCALES Y DIRECCIONAMIENTO CON REDES Y SUBREDES”

OBJETIVOS:

- Conocer el direccionamiento, los tipos y clases de direcciones lógicas.
- Calcular las subredes.

INTRODUCCIÓN

Las Redes se clasifican en:

Red PAN (personal Area Network –Red de Área Personal)

Red LAN (Local Area Network - Red de Área Local)

Red MAN (Metropolitan Area Network), Red WAN (Wide Area Network– Red de Área Amplia).

Una Intranet es una Infraestructura de comunicación o red (LAN y/o WAN) privada a la cual sólo pueden acceder los miembros de la organización que la administra, una Extranet es una red privada en la infraestructura de telecomunicaciones pública, para intercambiar de manera segura, información entre clientes, proveedores y socios.

El internet es una red de alcance mundial constituida a su vez por miles de redes que conectan entre sí millones de computadoras, en la cual se puede acceder a programas e información de uso público y privado.

Una dirección IP (IPv4) es un número de 32 bits que identifica de manera única cada computadora conectada a la red.

Se representa como cuatro cifras decimales separadas por puntos como, por ejemplo: 172.16.1.31.

Cada uno de los cuatro grupos de cifras se llama "octeto" y tiene 8 bits de longitud.

Estos octetos se convierten al formato decimal para formar la dirección IP.

En cuanto a las clases de direcciones IPv4:

- Redes unicast:

- Clase A: Rango de direcciones 1.0.0.0 a 126.255.255.255.

- Clase B: Rango de direcciones 128.0.0.0 a 191.255.255.255.

- Clase C: Rango de direcciones 192.0.0.0 a 223.255.255.255.

También existen redes multicast (Clase D) y redes broadcast (Clase E).

Las subredes son una extensión de la red que mejora el direccionamiento.

Por último, la máscara de subred es una dirección de 32 bits dividida en cuatro octetos, que identifica qué parte de la dirección corresponde a la red y qué parte representa el direccionamiento del host.

ACTIVIDADES PREVIAS A LA PRÁCTICA

- Leer toda la práctica.
- Teniendo una red privada de clase “C”, Crear 16 subredes, de cada una anotar en una tabla ; la dirección de red, las 2 primeras y las 2 últimas direcciones de host y la de broadcast.

EQUIPO Y MATERIAL

Computadora personal con el software apropiado instalado.

PROCEDIMIENTO EXPERIMENTAL

3.1 DIRECCIONAMIENTO IPV4

1. Construir en el simulador una red LAN con 1 Switch y 6 Host (figura 1.)

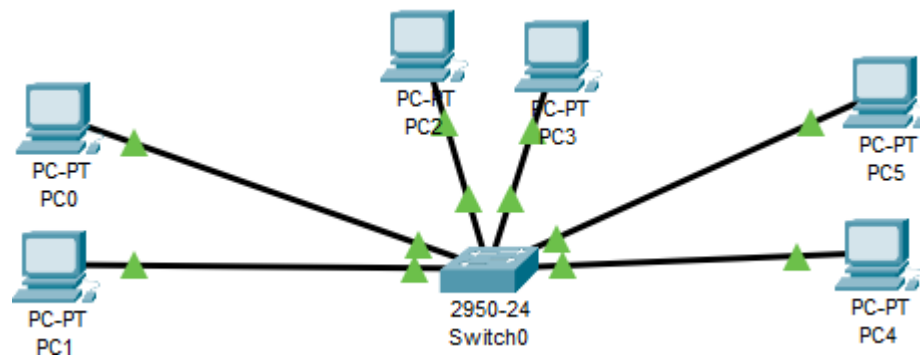


Figura 1

2. Asignar a los equipos direcciones estáticas y la máscara de red correspondiente para una dirección de red de clase “A”.
3. Enviar un ping en modo tiempo real (Realtime) entre las computadoras, observar el funcionamiento.
4. Diseñar una red con 3 subredes para la dirección anterior **y cambiar las direcciones en la topología de la figura 1**, anotar las direcciones de red, y de host. Agregar una imagen como evidencia de este paso en su reporte



5. Construir en el simulador una red basada en el diseño realizado en las actividades previas utilizando únicamente PCs y Switches.
6. Indicar en la topología las direcciones de las subredes, así como las direcciones de IP de los hosts utilizados.
7. Enviar PDU's simples entre los diferentes hosts, anotar sus comentarios

CUESTIONARIO

1. ¿A qué red pertenece un host con dirección de red 192.168 50.121 y máscara de subred 255.255.255.224?
2. ¿Cuántas direcciones de host hay disponibles para una red de clase A, B y C?
3. Con una red de clase "A" cuando se toman 6 bits de la parte de hosts ¿Cuántas subredes se crean, cuantos host por subred y cuál es su máscara de subred?
4. ¿Qué es una subred de longitud variable?

CONCLUSIONES

BIBLIOGRAFIA



PRÁCTICA 4: "CONFIGURACIÓN DE ROUTERS"

OBJETIVO

- Conocer el funcionamiento de los routers, así como la configuración de estos.

INTRODUCCIÓN

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

Un router es una computadora construida para desempeñar funciones específicas de capa tres, proporciona el hardware y software necesarios para enrutar paquetes entre redes. Se trata de dispositivos importantes de interconexión que permiten conectar subredes LAN y establecer conexiones de área amplia entre redes.

Las dos tareas principales son: la de conmutar los paquetes desde una interfaz perteneciente a una red hacia otra interfaz de una red diferente y la de enrutar, es decir, encontrar el mejor camino hacia la red destino.

Los componentes de hardware de los routers necesitan un sistema operativo, los routers Cisco funcionan con un sistema operativo llamado IOS (Sistema Operativo de Interworking).

Un router puede ser exclusivamente un dispositivo LAN o un dispositivo WAN, pero también puede estar en la frontera entre una LAN y una WAN y ser un dispositivo LAN y WAN al mismo tiempo.

Los componentes básicos de la arquitectura interna de un router son:

CPU: ejecuta las instrucciones del sistema operativo. Estas funciones incluyen inicialización del sistema, las funciones de enrutamiento y el control de la interfaz de red.

RAM: se usa para la información de tablas de enrutamiento, el cache de conmutación rápida, la configuración actual y las colas de paquetes.

MEMORIA FLASH: se utiliza para almacenar una imagen completa del software IOS.

NVRAM: se utiliza para guardar la configuración de inicio.

BUSES: la mayoría de los routers contienen un bus de sistema y un bus de CPU.

ROM: se utiliza para almacenar de forma permanente el código de diagnóstico de inicio.

FUENTE DE ALIMENTACIÓN: brinda la energía necesaria para operar los componentes internos.

Las interfaces son las conexiones de los routers con el exterior. Interfaz de red de área local (LAN). Interfaz de red de área amplia (WAN) Interfaz de consola/AUX.

Las interfaces pueden ser configuraciones fijas o modulares, las LAN pueden ser Ethernet o Token Ring, las WAN incluyen la unidad de servicio de canal (CSU) integrada, la RDSI y el serial.

Los puertos de consola son puertos seriales que se utilizan principalmente para la configuración del router.



ACTIVIDADES PREVIAS A LA PRÁCTICA

- Leer toda la práctica.
- Investigar cuales son los modos de acceso para configurar un router, y la función de cada uno de los modos.

EQUIPO Y MATERIAL

- Computadora personal con el software apropiado ya instalado.

PROCEDIMIENTO EXPERIMENTAL

4.1 CONECTAR DOS REDES CON UN ROUTER.

1. Construir la topología de la Figura 1, utilizando cuatro computadoras en dos redes independientes con su respectivo switch, colocando un router para interconectarlas.

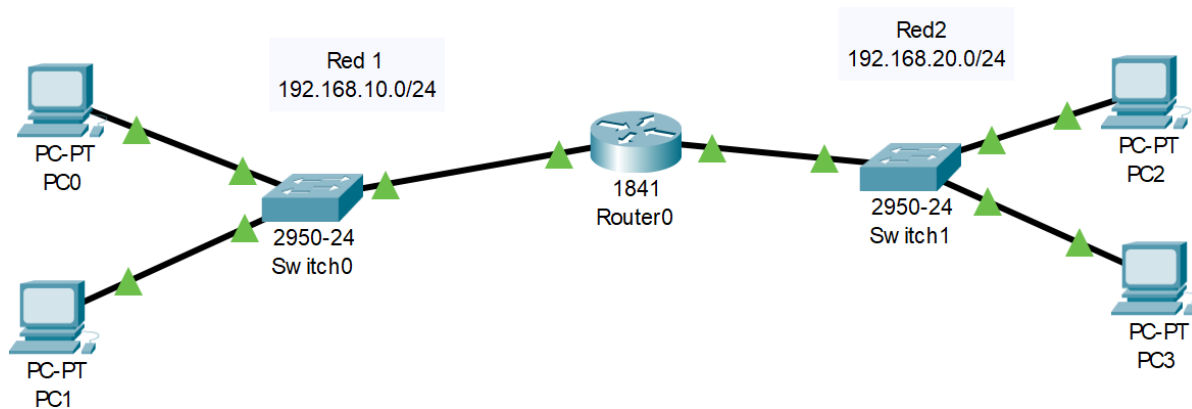


Figura 1

Nota: las direcciones indicadas son de ejemplo, Se recomienda cambiar.

2. Asignar para la Red 1 la dirección 192.168.10.0/24 y para la Red 2 la dirección 192.168.20.0/24, y asignar las direcciones IP estáticas correspondientes a las computadoras y a las interfaces del Router.

Usando el editor de notas, anotar las direcciones IP de las redes, los hosts y las interfaces en la topología.

3. En el router, ir a la pestaña de “Config”, en “GLOBAL” cambiar el nombre del dispositivo, “display name” es el nombre que se muestra en la topología, “hostname” es el nombre que se muestra en la configuración.



4. En "INTERFACE", seleccionar la interfaz que está conectada a la Red 1, encender el puerto y asignar la dirección IP correspondiente, dar tabulador y la máscara de red por default será colocada automáticamente, (para saber la interfaz en el área de trabajo seleccionar el cable del router y aparecerá la interfaz a la que está conectado).
5. Seleccionar el puerto al que está conectada la Red 2 y realizar las acciones del punto anterior con las respectivas direcciones IP, de acuerdo con la red que le corresponde.
6. Observar en la gráfica cómo los puertos del router entran en servicio.
7. Seleccionar una computadora, en la pestaña "Config" cambiar el nombre de la computadora y anotar la dirección del Gateway (puerta de enlace) que es el puerto del router al que está conectada la red.
8. Realizar los pasos del punto anterior para todas las computadoras con sus respectivas direcciones de acuerdo con la red que están conectadas.
9. En una computadora, ir a la pestaña de escritorio, y seleccionar "Command Prompt", y mandar un ping a otra PC de la red opuesta a la que se está conectado, esperar a que se carguen los datos en el router y se obtenga la respuesta, si no se obtiene la respuesta satisfactoria después de varios intentos verificar que las direcciones IP sean las correctas.

4.2 CONECTAR DOS REDES CON DOS ROUTERS

1. Modificar la topología como se muestra en la figura 2, agregando un segundo router, para separar las Red 1 de la Red 2 estas redes se unen con un cable serial, mediante una nueva red a la que llamaremos Red 4.

Nota: El router se debe configurar para tener tarjetas seriales, esto es: en la pestaña de "Físico" se debe de apagar el dispositivo, seleccionar y agregar la tarjeta adecuada, y encender el dispositivo al término de este

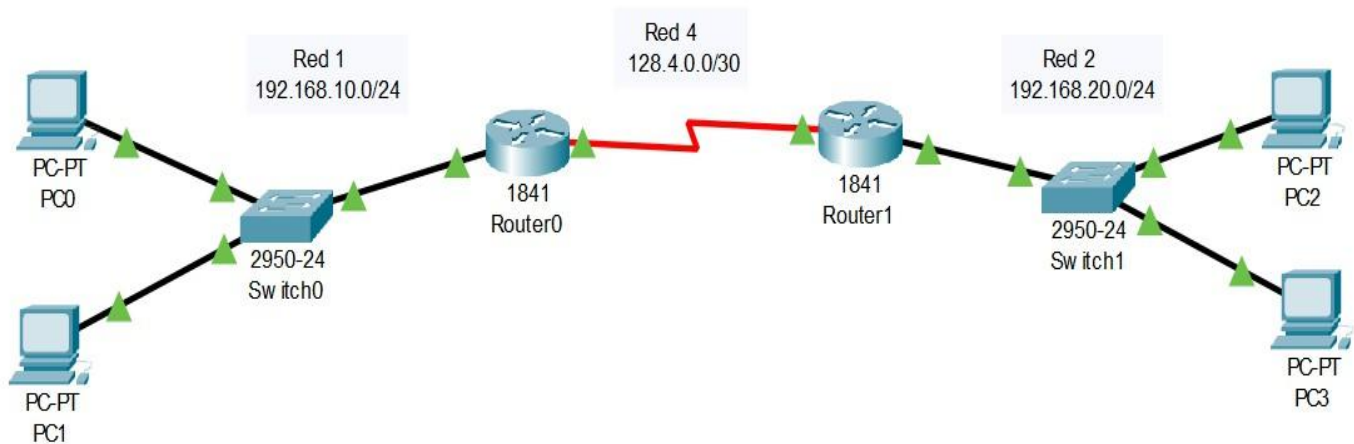


Figura 2

2. Utilizando las mismas direcciones IP del punto 4.1, configurar las direcciones de los puertos seriales de los routers para la Red 4 con dirección de red 128.4.0.0/30, (los puertos conectados entre sí deben pertenecer a la misma red).

3. ENRUTAMIENTO ESTÁTICO

La Red 1 se conecta con la Red 2 a través de la Red 4, esto se conoce como salto y debemos indicarle a los routers los saltos que deben realizar para alcanzar las redes deseadas, esto es un tipo enrutamiento.

En un router, ir a la pestaña “Config”, en enrutamiento estático, escribir la dirección de red a la que queremos llegar, la máscara de subred y en “siguiente salto” escribir la dirección de la red por la que se va a pasar, y agregar, esto se debe de hacer en ambos routers para que la comunicación sea bidireccional, después de terminar de configurar los routers debemos esperar a que reconozca los cambios.

4. Enviar el comando ping de una computadora a otra para verificar que las dos redes se interconectan, recordar que debemos dar un tiempo para que los datos se carguen en el router, si es necesario, repetir el ping hasta que sea satisfactorio. Anotar sus comentarios.

4.3 CONECTAR TRES REDES CON TRES ROUTERS EN ANILLO CON ENRUTAMIENTO ESTÁTICO

1. Agregar una tercera red con dos computadoras, un switch y un router, unir el router con cable serial en topología de anillo a los ya existentes, formando otras dos redes entre routers, Red 5 y Red 6 (Figura 3).

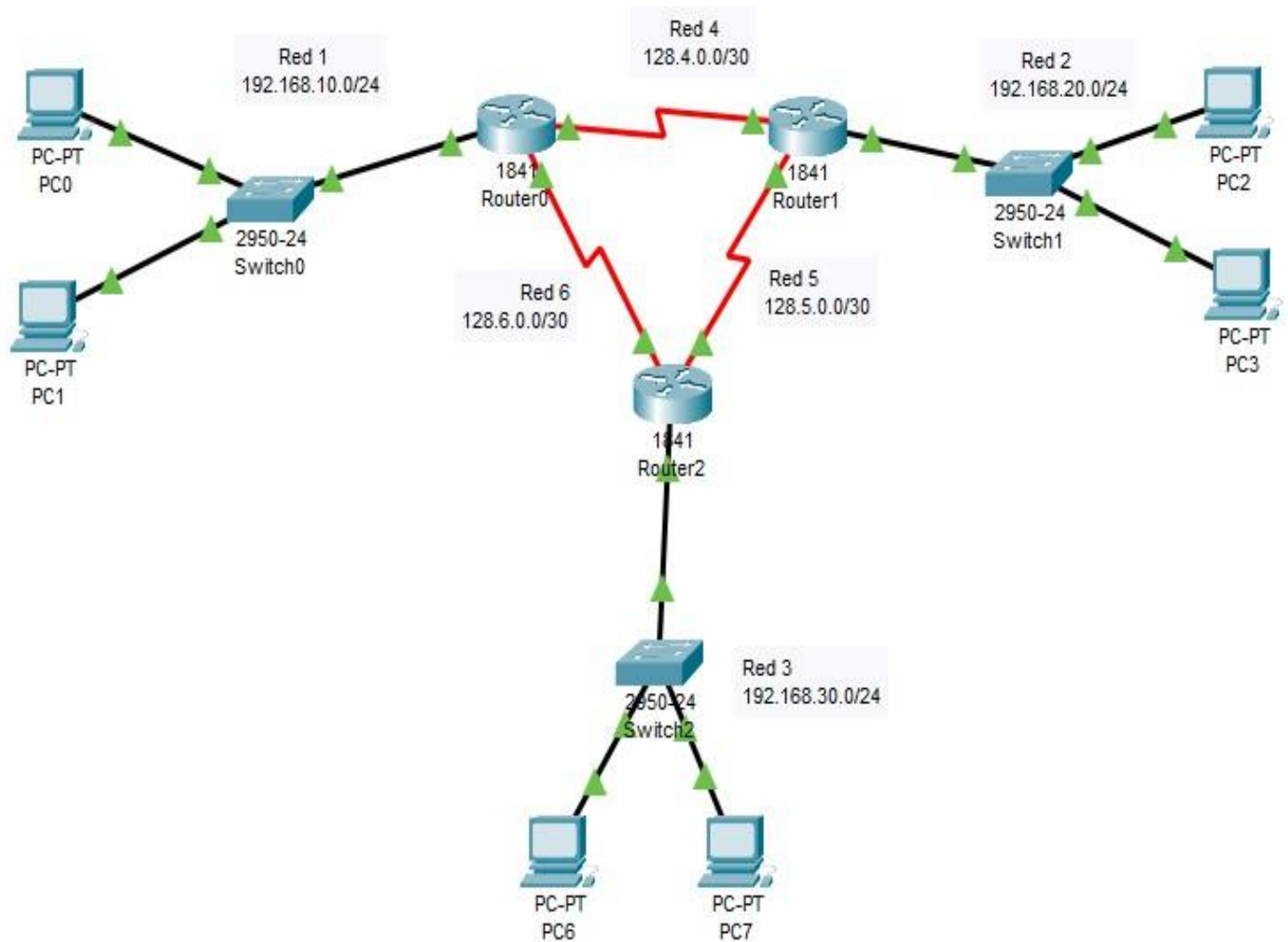


Figura 3

2. En la Red 3 con dirección 192.168.30.0/24, asignar direcciones IP a las computadoras la puerta de enlace en los puertos Fast Ethernet de los routers, para los puertos seriales utilizaremos las direcciones 128.5.0.0/30 para la Red 5 y 128.6.0.0/30 para la Red 6.

Para lograr la comunicación entre las tres redes, es necesario configurar los routers con tablas de ruteo. Siguiendo un enfoque en sentido horario:

1. La red 1 se comunicará con la red 2 y la red 3 a través la red 4.
2. La red 2 se comunicará con la red 3 y red 1 a través de la red 5
3. La red 3 se comunicará con la red 1 y la red 2 a través de la red 6



3. Para configurar el enrutamiento, indicarle a los routers las rutas a seguir para alcanzar cada una de las redes de acuerdo con el punto anterior, un enrutamiento por cada red a alcanzar. En los routers, eliminar cualquier enrutamiento estático si existe, para agregar un nuevo enrutamiento.

4. En R1 configurar enrutamiento estático: agregar la dirección de RED 2 que queremos alcanzar: 192.168.20.0, con su respectiva máscara de subred, para el siguiente salto indicamos la dirección de la red por la que se debe acceder para dirigirse al destino (RED 4), Agregar nuevo enrutamiento para alcanzar a la red 3 (192.168.30.0).

5. Para los routers 2 y 3 realizar los mismos pasos de los puntos 4 y 5 teniendo cuidado de agregar las direcciones correspondientes del siguiente salto sin olvidar el sentido de la comunicación.

6. Realizar una prueba de envío de tráfico, anotar sus comentarios.

4.4 CONECTAR TRES REDES CON ENRUTAMIENTO DINAMICO.

1. Para realizar un enrutamiento dinámico utilizar la topología construida anteriormente. En el router 1 eliminar las rutas estáticas que se encuentran en la tabla de ruteo.

2. Una vez hecho esto el router ya no tiene indicaciones de cómo realizar la comunicación, ahora, damos clic en RIP (Protocolo de Información de Ruteo). Aquí le indicamos al router todas las redes a las que está conectado directamente; una vez hecho esto cerramos la ventana y hacemos lo mismo en los otros dos routers.

3. Probar conectividad en modo simulación, observar la comunicación y los protocolos involucrados, anotar sus comentarios.

CUESTIONARIO

1. Investigar qué es DCE y DTE
2. Investigar cómo funciona el enrutamiento estático y el enrutamiento dinámico
3. . Investigar qué es la distancia administrativa

CONCLUSIONES

BIBLIOGRAFIA



PRÁCTICA 5: “CONFIGURACIÓN DE ROUTER POR COMANDOS CLI”

OBJETIVO

- Configurar un router a través de la interfaz de línea de comandos: Nombre, Dirección IP, Puerta de enlace, Seguridad y Mensaje del día.

INTRODUCCIÓN

Cuando el router se enciende realiza pruebas de inicio POST (Power On Self Test), durante este proceso se ejecutan una serie de diagnósticos para verificar la operatividad básica del CPU, la memoria y la circuitería de la interfaz.

Al iniciar por primera vez un router, no existe configuración inicial, el software pedirá un conjunto mínimo de detalles a través de un Setup, este puede mostrarse en su forma básica o extendida.

Se puede salir de este modo respondiendo que NO a la pregunta inicial (recomendado). Desde la línea de comandos el router se inicia en el **modo EXEC Usuario**.

Los routers son computadoras dedicadas al procesamiento de la interconexión de redes, que no incluyen monitor, ni teclado, por lo que debe comunicarse con ellos de una de las siguientes formas:

- Desde una terminal (PC o estación de trabajo funcionando en modo terminal) conectada a él mediante un cable llamado de consola.
- Mediante una conexión en un punto de la red.

Dado que los routers son los enlaces que mantienen unidas las redes, el diseño de medidas de seguridad dentro de ellos es muy importante; la primera medida que se debe tomar en cuenta es la asignación de una contraseña para no permitir el acceso al público en general. En los routers CISCO se utilizan las contraseñas para restringir el acceso al dispositivo, la parte privilegiada del entorno del software IOS (Internetwork Operating System) o el uso de comandos específicos del IOS.

Las contraseñas de línea se usan para controlar quién puede iniciar la sesión en un router; se define protección por contraseña en la línea terminal de consola, la línea AUX (auxiliar) y en cualquiera de las líneas de terminal virtual (vty).

El comando *enable secret* es usado para colocar una contraseña que garantice el privilegio de acceso de administración al sistema IOS, este comando es recomendable utilizarlo dado que la contraseña de consola TTY o el de sesión remota VTY puede ser usado para obtener privilegios de acceso. Esta contraseña de acceso al router se encuentra almacenado en el archivo de configuración del router, por lo que es recomendable que se utilice el comando *service password-encryption* para poder encriptarlo y no sea visto en texto claro cuando se consulta el archivo de configuración.

Todos los mecanismos de acceso interactivo usan la abstracción IOS TTY (es decir, todos invocan las sesiones en “línea”), las terminales asíncronas locales y los modems dialup



usan líneas estándares “TTYs”, las conexiones remotas de red, indiferentes del protocolo, usan TTYs virtuales, o VTYs, por lo que, el mejor camino para proteger al sistema es hacer seguros los controles que son aplicados a las líneas VTY y las líneas TTY.

Las líneas VTY permiten el acceso a un router a través de Telnet.

En forma predeterminada, los dispositivos Cisco admiten al menos cinco líneas VTY con numeración del 0 al 4.

ACTIVIDADES PREVIAS A LA PRÁCTICA

- Leer toda la practica
- Investigar qué es y que función tiene CLI.
-

MATERIAL Y EQUIPO

- Computadora personal con el software apropiado ya instalado.

PROCEDIMIENTO EXPERIMENTAL

5.1 CONFIGURACION DEL ROUTER

1. La conexión será de un router a un switch y del switch a una computadora (Figura 1). El cable que usaremos es cobre directo, la interfaz que utilizaremos es FastEthernet.

Conectar con cable de consola una laptop, del puerto RS232 al puerto de consola del router.

Nota: La conexión del router con el switch no está activa.

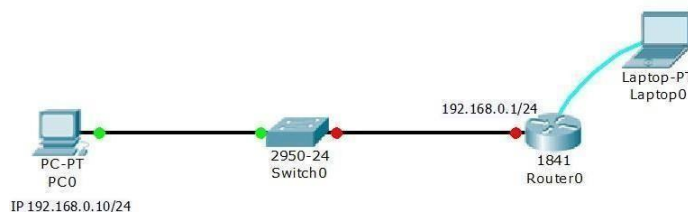


Figura 1

2. En el escritorio de la laptop, seleccionar terminal, verificar que se tengan los siguientes parámetros de comunicación: **9600 bps, 8 bits de datos, sin paridad, 1 bit de parada, sin control de flujo**, estos parámetros son para todos los dispositivos CISCO.

3. Damos ok, sin entrar al dialogo de configuración, dar enter dos veces para entrar a la línea de consola o modo de usuario.



5.2 MODOS DEL ROUTER

1. Modo EXEC Usuario.

Router>

2. Modo EXEC Privilegiado, entrar con el comando **enable**.

Router> enable (Presionar enter.)

Router#

Regresar al modo usuario, con el comando *disable*.

3. Modo de Configuración global, estando en el modo privilegiado escribir el comando **configure terminal**.

Router# configure terminal (Presionar enter.)

Router(config)#

Regresar al modo privilegiado con el comando **exit**.

4. En cada modo observe el menú de comandos disponibles, con la tecla “?”. Anotar sus comentarios.

5.3 PONERLE NOMBRE AL ROUTER Y EL MENSAJE DEL DIA

1. Cambiar nombre al router

Estando en modo de configuración global con el comando **hostname** (por ejemplo: cambiar el nombre a *Practica_5*).

Router(config)# hostname Practica_5 (Presionar enter.)

Practica_5(config)#

2. Poner el mensaje del día.

Este mensaje aparece cuando alguien ingresa al router, Estando en modo de configuración global con el comando **banner motd #mensaje#**

(por ejemplo: “!!!ACCESO AUTORIZADO!!!”)

Practica_5(config)# banner motd #!!!ACCESO AUTORIZADO!!!# (Presionar enter.)

3. Verificar mensaje del día.

Estando en modo usuario desconectarse del router con el comando *exit*, damos enter para regresar al modo EXEC Usuario, anotar sus comentarios.



5.4 CONFIGURAR CONTRASEÑAS "ENABLE PASSWORD" Y "ENABLE SECRET"

1. En modo de configuración global, establecer una contraseña (ejemplo: 456) para restringir el acceso a las configuraciones del router.

Practica_5(config)#enable password 456 (Presionar enter.)

2. Ver configuración del router.

En el modo EXEC Privilegiado ejecutar el comando show running-config y anotar las contraseñas almacenadas

Practica_5#show running-config (Presionar enter)

3. Configurar Enable Secret

En el modo de configuración global, generar una clave cifrada en el router (ejemplo: 123).

Practica_5(config)#enable secret 123 .

4. Repetir el paso 2, comparar Enable Password con Enable Secret y anotar sus comentarios.

5.5 CONFIGURAR CONTRASEÑA DE CONSOLA

1. Restringir el acceso a una sesión por consola mediante una contraseña
Estando en modo de configuración global ingresar a la línea de consola.

Practica_5(config)# line console 0 (Presionar enter.)

Practica_5(config-line)#

2. Asignar la contraseña (ejemplo: passcon).

*Practica_5(config-line)#password **passcon** (Presionar enter.)*

Practica_5(config-line)#

3. Habilitar la contraseña con el comando login para que nos permita entrar el router

Practica_5(config-line)#login (Presionar enter.)

4. Desconectarse del router e ingresar al modo EXEC Usuario.
Indicar ¿Con cuál contraseña ingreso?

5. Pasar al modo EXEC Privilegiado

Indicar ¿Con cuál contraseña ingreso?

6. Deshabilitar la contraseña cifrada con el siguiente comando:

Practica_5(config)#no enable secret



7. Desconectarse del router e ingresar al modo EXEC Privilegiado
Indicar ¿Con cuál contraseña ingreso?

8. Verificar las contraseñas del router, anotar sus comentarios.

5.6 CONFIGURAR INTERFACES FASTETHERNET

Configuración de la IP y Mascara de subred de la interfaz FastEthernet 0/0 del router al que está conectado el switch.

1. Ingresar al modo de Configuración de Interfaz.

Practica_5(config)# interface fastethernet 0/0 (Presionar enter.)

2. Asignar la dirección IP y la Máscara de subred. (ejemplo: 192.168.0.1 255.255.255.0)

Practica_5(config-if)# ip address 192.168.0.1 255.255.255.0 (Presionar enter.)

3. Activar la conexión del router al switch (encender la interfaz).

Practica_5(config-if)# no shutdown (Presionar enter.)

4. Observar comportamiento del router. Anotar sus comentarios

5. Configuración de la descripción de la interfaz.

Dar una descripción a la interfaz del router con la que podemos saber hacia dónde está conectada esta interfaz, (ejemplo: enlace_al_L-901).

Practica_5(config-if)#description enlace_al_L901 (Presionar enter.)

6. Ver la configuración del router y anotar los datos de la interface FastEthernet.

5.7 CONFIGURAR CONTRASEÑA VTY (TELNET)

Configurar la contraseña del VTY para tener acceso al router remotamente a través de la red.

1. Para conocer cuantas líneas VTY tenemos, desplegamos la configuración del router.

Practica_5#show running-config

Presionar enter hasta que aparezca en la pantalla el número de líneas de consola CON y el número de líneas virtuales VTY(en donde **n** es el número de la línea inicial y en **m** final)., anotarlas.

2. Ingresar un bloque de líneas VTY.

Practica_5(config)#line vty n m (Presionar enter.)

3. Asignar la contraseña para las líneas, (ejem. passvty).

Practica_5(config-line)#password passvty



5.8 GUARDAR LA CONFIGURACIÓN

Guardar la configuración, ya que si apagamos el router los cambios hechos se pierden. Vamos a guardar la configuración en la memoria NVRAM del router, esta memoria no es volátil como la RAM.

1. Ver configuración de inicio ejecutar el comando *show startup-config* en el modo privilegiado.

2. Copiar la configuración actual en la configuración de inicio.

```
Practica_5#copy running-config startup-config          (Presionar enter)  
Destination filename [startup-config]?                (Presionar enter nuevamente para guardar.)
```

3. Repetir el punto 1.

4. Reiniciar el router por comando haciendo una recarga de la configuración de inicio.

```
Practica_5#reload  
Proceed with reload? [confirm]      (Presionar enter para confirmar.)
```

Observar el comportamiento del router en el área de trabajo del simulador y anotar sus comentarios.

5.9 COMPROBANDO EL ACCESO POR VTY

Asignar a la PC0 la siguiente dirección IP 192.168.0.2 con su máscara de red y la puerta de enlace.

1. Verificar que se alcance la comunicación entre la PC y el router enviando un ping o un PDU.

2. Para configurar el router a través de la PC0 en red, escribir en "Símbolo del Sistema": *telnet 192.168.0.1*, que es la dirección configurada en la interfaz conectada a la red, puerta de enlace o Gateway. Entrar al modo EXEC Privilegiado del router (vía telnet).

3. Ejecutar el comando *show running-config*.

CUESTIONARIO

1. Explique que es telnet y como es su acceso.
2. ¿Qué son los modos usuario, privilegiado y configuración global?
3. Indique los protocolos que trabajan en la capa tres del modelo OSI.
4. ¿Qué son las líneas de terminal virtual y las líneas de consola?
5. ¿Qué son las líneas de control de acceso?

CONCLUSIONES

BIBLIOGRAFIA



PRÁCTICA 6: “CONFIGURACIÓN DE SWITCH POR COMANDOS CLI”

OBJETIVO

- Configurar en un switch a través de una interfaz de línea de comandos: Nombre, Dirección IP, Puerta de enlace, Seguridad y Mensaje del día.

INTRODUCCIÓN

El funcionamiento de una red consiste en conectar computadoras y periféricos mediante dos partes del equipo: switches y routers. Estos dos elementos permiten a los dispositivos conectados a la red comunicarse con los demás y con otras redes.

Los Switches se utilizan para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina. Por ejemplo, un switch puede conectar sus computadoras, impresoras y servidores, creando una red de recursos compartidos. El switch actuaría como controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí.

Mediante el uso compartido de información y la asignación de recursos, los switches permiten ahorrar dinero y aumentar la productividad.

Existen dos tipos básicos de switches: administrados y no administrados.

Los switches no administrados funcionan de forma automática y no permiten realizar cambios. Los equipos en redes domésticas suelen utilizar switches no administrados.

Los switches administrados permiten su programación. Esto proporciona una gran flexibilidad porque el switch se puede supervisar y ajustar de forma local o remota para controlar el desplazamiento del tráfico en la red y quién tiene acceso a la misma.

Un switch es un dispositivo de red que crea dominios de colisión (cada puerto de un switch es un dominio de colisión) lo cual nos ofrece microsegmentación de la LAN lo que se traduce en ancho de banda independiente en cada puerto o dominio de colisión. Un switch trabaja en la capa 2 del modelo de referencia OSI, haciéndolo más rápido que un dispositivo de capa tres (un router) pues no analiza el encabezado de capa 3, solamente crea y administra una tabla basada en direcciones MAC con la que lleva a cabo el filtrado de las tramas.

Como tal un switch puede realizar estas funciones con su configuración por default, sin embargo, para obtener provecho de funciones más avanzadas (como son seguridad básica o administración remota) es que realizamos las configuraciones pertinentes a estos dispositivos.

ACTIVIDADES PREVIAS A LA PRÁCTICA

- Leer toda la práctica.
- Investigar cuales son las capas del modelo TCP/IP y del modelo OSI.

MATERIAL Y EQUIPO

Computadora personal con el software apropiado ya instalado.

PROCEDIMIENTO EXPERIMENTAL

6.1 CONFIGURACIÓN DEL SWITCH

1. Construir la red de la figura 1. La conexión será de un router a un switch y del switch a una computadora y una Laptop.
2. Asignar a la interface del router la dirección IP 192.168.0.1/24, y encenderla. Asignar a la PC0 la dirección IP 192.168.0.10/24. Conectar una Laptop al switch con cable de consola.

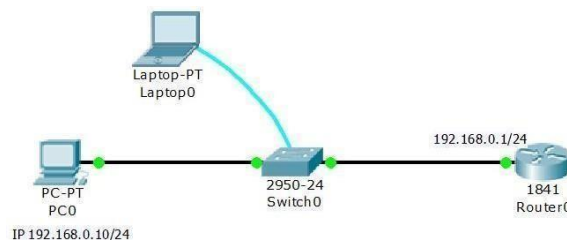


Figura 1

El switch que vamos a configurar está conectado a una laptop por el puerto de Consola desde el cual ingresaremos mediante línea de comando CLI, además está conectado a un router, el cual funciona como puerta de enlace predeterminada, que nos dará salida a internet, y la PC0 representa un host desde el cual podemos realizar configuraciones.

3. Conexión vía consola.

Verificar que los parámetros de comunicación en el modo terminal de la laptop estén configurados de la siguiente manera: **9600 bits por segundo, 8 bits de datos, Sin paridad, 1 bit de parada, Sin control de flujo.**

De esta manera ingresamos a la línea de comandos del switch.



6.2 PONERLE NOMBRE AL SWITCH

1. Configurar el switch con un nombre único en la red para identificar el dispositivo. Esto lo hacemos desde el modo de configuración global con el comando *hostname* [**nombre del dispositivo**], (ej. de nombre SW_L903).

```
Switch>enable  
Switch# configure terminal  
Switch(config)#hostname SW_L903  
SW_L903(config)#
```

6.3 CONFIGURACIÓN DE DIRECCIÓN IP DE LA VLAN

1. Configurar una dirección IP con la finalidad de administrar el switch de forma remota. Desde el modo de configuración global ingresar a modo de configuración de interface para la VLAN 1, (esta es una VLAN que viene por default en el switch y que no podemos borrar, es conocida también como la VLAN de administración y se comporta de forma similar a una interface Ethernet de un router).

```
SW_L903(config)#interface vlan1  
SW_L903(config-if)#
```

2. Una vez en el modo de configuración de interface VLAN 1, configurar la dirección IP con el comando *ip address* [**dirección IP**] [**máscara de subred**], la dirección IP será 192.168.0.3.

```
SW_L903(config-if)#ip address 192.168.0.3 255.255.255.0  
SW_L903(config-if)#
```

3. Activar la interface con el comando *no shutdown* y pasar a modo de configuración global.

```
SW_L903(config-if)#no shutdown  
SW_L903(config-if)#  
SW_L903(config-if)#exit  
SW_L903(config)#
```

4. Ver configuración del Switch. En el modo EXEC Privilegiado, ejecutar el comando *show running-config*. Anotar sus comentarios.



6.4 CONFIGURACIÓN DE LA PUERTA DE ENLACE

En el caso de que el switch necesite enviar información a una red diferente de la de administración (fuera de nuestra red), se debe configurar una puerta de enlace que es la dirección de la interface del router a la cual está conectado el switch para darnos salida a internet.

1. Configurar la puerta de enlace desde el modo de configuración global con el comando *ip default-gateway* [**dirección de la puerta de enlace**].

```
SW_L903(config)#ip default-gateway 192.168.0.1  
SW_L903(config)#
```

2. Desde la PC0, enviar un ping y un PDU simple a la dirección de administración del switch. El ping debe de ser exitoso (la primera vez puede que se pierdan algunos paquetes. Repetir el ping dos o tres veces de ser necesario). Anotar sus comentarios.
3. Repetir el punto 2 para la dirección del router.

6.5 CONFIGURACIÓN DE LAS LÍNEAS VIRTUALES (VTY) Y DE CONSOLA

Configurar la contraseña del VTY para tener acceso al switch remotamente a través de la red.

1. Para conocer cuantas líneas VTY tenemos, desplegar la configuración del switch. Anotar el número de líneas de consola CON y el número de líneas virtuales VTY.
2. Ingresar un bloque de líneas VTY.
SW_L903(config)#line vty i j (donde *i* es el número de la línea inicial y *j* el de la final).
3. Configurar una contraseña para los accesos VTY con el comando *password* [**contraseña**], (ejem.abc).

```
SW_L903 (config-line)#password abc  
SW_L903(config-line)#
```

4. Ver la configuración del Swicht. Anotar sus comentarios

6.6 PRUEBAS DE CONECTIVIDAD A TRAVÉS DE LOS PUERTOS VTY

1. Establecer una sesión con el switch vía telnet desde PC0. En la PC0, desde símbolo del Sistema:

```
PC>telnet 192.168.0.3
```

Solicitará la contraseña de acceso.



- 2 Entrar al modo EXEC Privilegiado y desplegar la configuración actual. ¿Porque no se puede acceder al modo EXEC Privilegiado?

6.7 ADMINISTRACIÓN DE LOS ACCESOS VTY

1. Acceso al modo EXEC Privilegiado.

Desde el modo EXEC Privilegiado podemos administrar el archivo de configuración y pasar a todos los niveles superiores, es por eso que es necesario restringir el acceso a este modo: para evitar que usuarios no autorizados modifiquen la configuración del dispositivo.

- 2 Configurar contraseña, estando en el modo de configuración global con el comando *enable password [contraseña]*, (ejem. redes_1)

```
SW_L903(config)#enable password redes_1
```

- 3 Ingresar al modo EXEC Privilegiado desde la PC0, y desplegar la configuración actual.

- 4 Configurar contraseña cifrada con el comando *enable secret [contraseña]*, (ejem. redes_2).

```
SW_L903(config)#enable secret redes_2
```

- 5 Acceder al modo EXEC Privilegiado del switch a través de la PC0.

En la configuración del switch ver las contraseñas *enable password* y la contraseña *enable secret* y anotar sus comentarios.

6.8 ADMINISTRACIÓN DE LOS ACCESOS DE CONSOLA

1. Restringir el acceso a una sesión por consola mediante una contraseña.

Desde el modo de configuración global pasar a modo de configuración de consola con el comando *line console 0*, y configurar la contraseña con el comando *password [contraseña]*

```
SW_L903(config)#line console 0  
SW_L903(config-line)#password consola  
SW_L903(config-line)#login  
SW_L903(config-line)#exit  
SW_L903(config)#
```

Es muy importante no olvidar escribir el comando *login*, ya que de no ponerse el switch no solicitará la contraseña al ingresar por consola y el acceso no estará restringido.



2. Ver la configuración del switch.
3. Encriptar las contraseñas que aparecen en texto plano. Desde el modo de configuración global ingresar el comando *service password-encryption*.

```
SW_L902(config)#service password-encryption
```

4. Ver las contraseñas con el comando *show running-config* y compararlas con las del punto 2. Anotar sus comentarios.

6.9 CONFIGURACIÓN DEL MENSAJE DEL DÍA

1. Desde el modo de configuración global se ingresa el comando *banner motd [carácter] mensaje [carácter]*, (El carácter puede ser % \$ # * etc. para indicar el inicio y fin del mensaje)

Ejemplo:

```
SW_L903(config)#banner motd *¡ADVERTENCIA! PROHIBIDO EL ACCESO *  
SW_L903(config)#
```

Desde la PC0, salir y reingresar a la línea de comando vía telnet al switch. Comprobar el mensaje del día.

2. Guardar la configuración con el comando *copy running-config startup-config*.

```
SW_L903#copy running-config startup-config  
Destination filename [startup-config]?  
Building configuration... [OK]  
SW_L903#
```

CUESTIONARIO

1. ¿Para qué se configura un switch?
2. ¿Para qué sirve la seguridad en el switch?
3. Indique los principales protocolos que trabajan en la capa dos del modelo OSI.

CONCLUSIONES

BIBLIOGRAFIA



PRÁCTICA 7: “IMPLANTACIÓN DE VLANS

OBJETIVO

- Conocer y configurar las redes de acceso local virtuales VLAN's.

INTRODUCCIÓN

Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física, se trata de una LAN Virtual que se puede configurar en un switch administrable con una cantidad de redes.

Con las redes virtuales (VLAN) es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos.

Las VLAN se clasifican en:

- VLAN de Datos: es la que está configurada sólo para enviar tráfico de datos generado por el usuario. A una VLAN de datos también se le denomina VLAN de usuario.
- VLAN Predeterminada: Es la VLAN a la cual todos los puertos del Switch se asignan cuando el dispositivo inicia, en algunos switches por defecto es la VLAN1.
- VLAN Nativa: una VLAN nativa está asignada a un puerto troncal, y sirve como un identificador común en extremos opuestos de un enlace troncal. Es aconsejable no utilizar la VLAN1 como la VLAN Nativa.

La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece las siguientes ventajas:

- Mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los switches.
- Aumento de la seguridad, debido a que la información se encapsula en un nivel adicional. Disminución en la transmisión de tráfico en la red.

La limitación primordial de estas es la falta de un estándar, aunque, las soluciones implementadas actualmente las realiza cada fabricante.

Administración: Un movimiento en las estaciones de trabajo hace necesario volver a configurar el puerto del switch al que está conectado el usuario.

El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.

La tecnología de las VLANs se basa en el empleo de Switches en lugar de hubs, de tal manera que permite un control más inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de aislar el tráfico incrementando la eficiencia de la red entera. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios.



ACTIVIDADES PREVIAS A LA PRÁCTICA

- Leer toda la práctica.
- Investigar los tipos de VLAN existentes.

EQUIPO Y MATERIAL

Computadora personal con el software apropiado ya instalado.

PROCEDIMIENTO EXPERIMENTAL

7.1 CONFIGURACIÓN DE VLAN'S

1. Construir la topología de la figura 1:

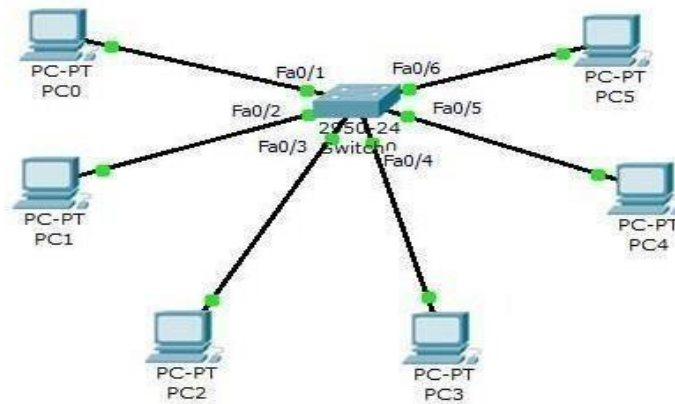


Figura 1

2. Verificar a qué Vlan corresponden los puertos del Switch. En modo EXEC Privilegiado:

```
Switch#show vlan brief
```

3. Crear tres VLAN's en el Switch.

Entrar a la base de datos de las VLAN's con el comando *vlan database*.

```
Switch#vlan database % Warning: It is recommended to configure VLAN from config mode, as VLAN database mode is being deprecated. Please consult user documentation for configuring VTP/VLAN in config mode.  
Switch(vlan)#
```



4. Poner número y nombre a la Vlan.

```
Switch(vlan)#vlan [número de vlan] name [nombre de vlan]
```

Ejemplo:

```
Switch(vlan)#vlan 100 name cien  
VLAN 100 added: Name: cien  
Switch(vlan)#
```

De la misma manera crear otras dos VLAN's.

5. Asignar VLAN en Modo Access a los puertos del switch donde están conectadas las computadoras, dos puertos por cada VLAN (Figura 2).

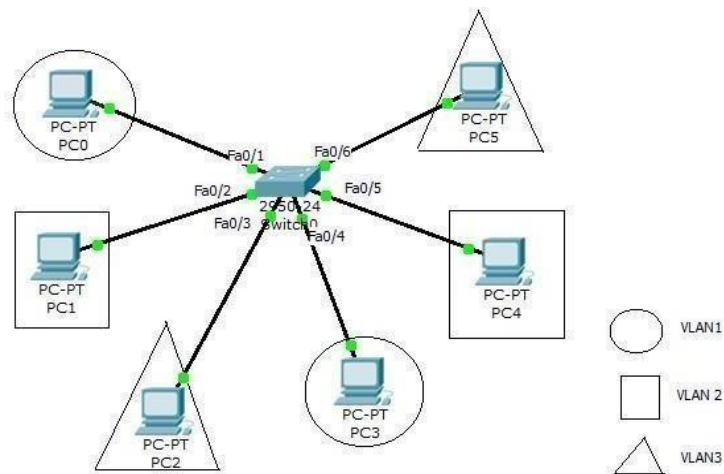


Figura 2

Acceder al puerto estando en el modo de configuración global.

```
Switch(config)#interface fastethernet [Interfaz]
```

Ejemplo:

```
Switch(config)#interface fastethernet 0/1
```

Configurar la Vlan al puerto

```
Switch(config-if)#switchport mode access  
Switch(config-if)#switchport access vlan [número de vlan]
```

6. Repetir el punto 5 para todos los puertos usados.

7. Verificar que las VLAN's estén creadas y estén en sus respectivas interfaces:

```
Switch#show vlan brief
```

8. Verificar que los puertos activos estén en modo access.

```
Switch#show running-config
```

9. Asignar IP y máscara de subred a los equipos (todos deben de ser de la misma red).

10. Realizar pruebas de conectividad entre VLAN's. Anotar sus comentarios.

7.2 CONFIGURACIÓN DE VLANS EN REDES SEPARADAS

1. Modificar la topología, colocando otro switch, y agregando tres computadoras al nuevo switch, tal como se muestra en la figura 3.

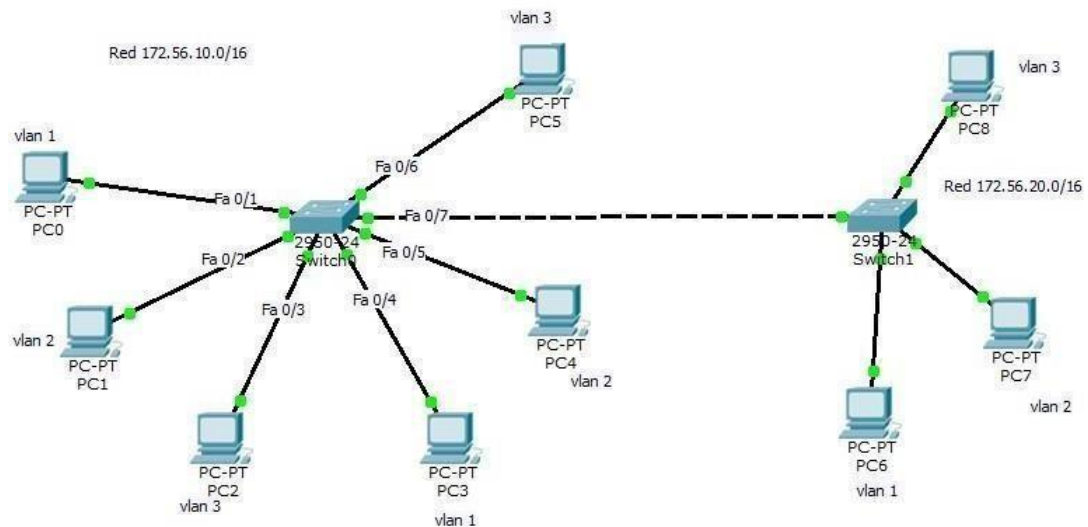


Figura 3

2. Asignar direcciones IP de la misma red que las existentes.

3. En el segundo switch crear las tres VLAN's anteriores y asignarlas a cada uno de los puertos de las computadoras.

4. Para tener conexión entre redes de cada switch, configurar el puerto que corresponde a la conexión con el otro switch en modo Trunk; hacer esto en cada uno de los switches.



```
Switch(config)#interface fastEthernet [Interfaz]  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#exit
```

5. Realizar pruebas de conectividad entre las dos redes. Anotar sus comentarios.

CUESTIONARIO

1. ¿Qué es una VLAN?
2. Menciona las ventajas de las VLAN.
3. ¿Qué tipos de puertos utilizan la VLAN?
4. ¿Cuáles son los tipos de puertos en los que se configura la VLAN?
5. ¿Cuál es el comando para borrar una VLAN?

CONCLUSIONES

BIBLIOGRAFIA



PRÁCTICA 8 “SERVIDORES”

OBJETIVO

- Configurar servidores DHCP, DNS, HTTP, WEB y Email trabajando en la capa de aplicación.

INTRODUCCIÓN

Un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes. Consta de hardware preciso y soporta tareas complejas, permite un fácil mantenimiento, ya que se pueden sustituir algunos de sus componentes dañados sin la necesidad de apagar el sistema, requiere un software para poder controlar el hardware, este está enfocado a ofrecer uno o varios servicios, estos servicios pueden estar diseñados para ofrecer funcionalidades de red o en muchos casos ofrecer funcionalidades para los usuarios de la red.

Algunos tipos de servidor son:

- Servidores FTP (FTP Servers): File Transfer Protocol es uno de los servicios más antiguos de Internet, File Transfer Protocol. Su función es permitir el intercambio de datos entre diferentes servidores/computadoras.
- Servidores WEB (Web Servers): Básicamente, un servidor web es un programa diseñado para alojar y transferir páginas web. Estos servidores se mantienen a la espera de peticiones que le hará un cliente o un usuario en internet.
- Servidor de Base de Datos (Database Server): Provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.
- Servidor de correo: Almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con email para los clientes de la red. Estos mueven y almacenan el correo electrónico a través de las redes corporativas (vía LANs y WANs) y a través de Internet.
- Servidor de telefonía: Realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o el Internet, por ejemplo, la entrada excesiva de voz sobre IP (VoIP), etc.
- Servidores Telnet (Telnet Servers): Un servidor telnet permite a los usuarios entrar en un ordenador huésped y realizar tareas como si estuviera trabajando directamente en ese ordenador.

ACTIVIDADES PREVIAS A LA PRÁCTICA

- Leer toda la practica
- Investigar que es un servidor y los tipos de servidores.

EQUIPO Y MATERIAL

Computadora personal con el software apropiado ya instalado.

PROCEDIMIENTO EXPERIMENTAL

8.1 CONSTRUCCIÓN DE LA RED

1. Inicie el simulador y arme la topología de la figura 1.

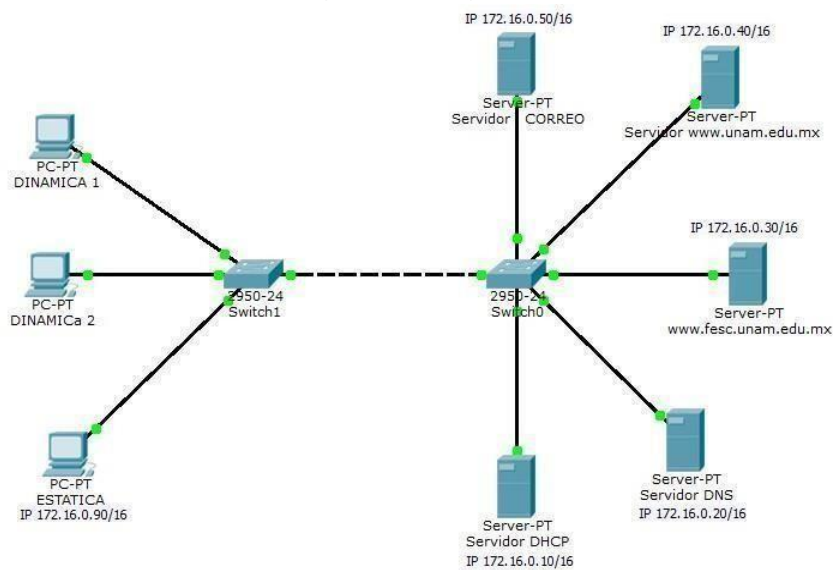


Figura 1

8.2 CONFIGURAR EL SERVIDOR DHCP

1. Seleccionar un servidor (server). En la Configuración Global:
 - Cambie el Nombre a “Servidor DHCP”.
 - Establezca el Gateway a 172.16.0.1.
2. Asignar dirección IP al servidor DHCP.
 - En la INTERFACE FastEthernet: Establezca la Dirección IP a 172.16.0.10/16.



3. Asignar dirección IP de la Puerta de Enlace. Seleccione Servicios DHCP:
 - Establezca el Gateway por defecto a 172.16.0.1.
 - Establezca la dirección IP del Servidor DNS a 172.16.0.20.
4. Configurar bloque de direcciones IP a asignar.
 - Establezca el Inicio de las Direcciones IP (por ejemplo 172.16.0.100) y el número máximo de usuarios.
 - Salve la configuración.
 - Seleccione DNS y verifique que este servicio este apagado.

8.3 CONFIGURAR EL SERVIDOR DNS

1. Seleccionar otro servidor.
 - Cambie el Nombre a “Servidor DNS”.
 - Establezca el Gateway a 172.16.0.1.
2. Asignar dirección IP al servidor DNS.
 - En INTERFACE FastEthernet: Establezca la Dirección IP a 172.16.0.20/16.
 - Seleccione DHCP y verifique que éste servicio este apagado.
 - Seleccione DNS y encienda el servicio.
 - Agregar el nombre de dominio www.fesc.unam.edu.mx y la dirección IP 172.16.0.30.
 - Agregue el nombre de dominio www.unam.edu.mx y la dirección IP 172.16.0.40.

8.4 CONFIGURAR EL SERVIDOR WEB www.fesc.unam.edu.mx.

1. Seleccionar el otro servidor.
 - Cambie el Nombre a “Servidor Web www.fesc.unam.edu.mx”.
 - Establezca el Gateway a 172.16.0.1.
2. Asignar dirección IP al servidor WEB.
 - En INTERFACE FastEthernet: Establezca la Dirección IP a 172.16.0.30/16.
 - Verifique que los servicios DHCP y DNS estén apagados para este servidor.

8.5 CONFIGURAR EL SERVIDOR WEB www.unam.edu.mx

1. Seleccionar un servidor (server).
 - Cambié el Nombre a “Servidor Web www.unam.edu.mx”.



- Establezca el Gateway a 172.16.0.1.
2. Asignar dirección IP al servidor WEB.
 - En INTERFACE FastEthernet: Establezca la Dirección IP a 172.16.0.40/16.
 - Verifique que los servicios DHCP y DNS estén apagados para este servidor.

8.6 CONFIGURAR EL SERVIDOR DE CORREO

1. Seleccionar un servidor (server).
 - Cambie el Nombre a “*Servidor CORREO*”.
 - Establezca el Gateway a 172.16.0.1.
 - En INTERFACE FastEthernet: Establezca la Dirección IP a 172.16.0.50/16.
 - Seleccione Servicios EMAIL.
 - Asignar domino de correo y usuarios: Establezca el Domain Name como itse.com.mx y de clic en set.
 - Crear los usuarios y sus contraseñas Dando clic en +.
 - Verifique que los servicios DHCP y DNS estén apagados para este servidor.

8.7 CONFIGURAR TRES COMPUTADORAS COMO CLIENTES

1. Configurar dos de las computadoras usando DHCP como clientes.
 - Cambie el nombre de las computadoras por: “Dinámica 1” y “Dinámica 2”, respectivamente.
 - En INTERFACE FastEthernet seleccione DHCP y anote la dirección que fue asignada a cada computadora.

Nota: En caso de que que no se asigne la dirección, verificar que el servicio en el servidor se encuentre encendido.

2. Configurar una computadora cliente usando Direccionamiento IP estático.
 - Cambie el Nombre a “*Estática*”.
 - Establezca el Gateway/DNS a Estático. Establezca el Gateway a 172.16.0.1.
 - Establezca la dirección IP del Servidor DNS. En INTERFACE FastEthernet, asigne la dirección IP estática 172.16.0.90/16
3. Configurar el correo en las 3 computadoras.
 - En la pestaña Escritorio, E Mail escriba el nombre del usuario, la dirección de correo (usuario@dominio, el usuario previamente dado de alta en el servidor de correo). En Server Information poner la dirección IP del servidor de correo en entrada y en salida. En logon information poner nombre de usuario y contraseña dada de alta por el administrador de correo.



8.8 VERIFICAR LA CONECTIVIDAD

1. Ping (ICMP).

En una de las computadoras pruebe hacer ping con los servidores.

2. Renovación de dirección IP dinámica.

En una de las computadoras dinámicas, desde la línea de comandos, solicitar una nueva dirección IP al servidor DHCP, ingresando el comando: *C> ipconfig /renew*. Anotar sus comentarios.

3. E-mail.

Hacer una prueba enviando correos electrónicos entre usuarios. En una computadora abrir el correo y en *Compose* enviar. En la computadora destino dar click en Recibir.

4. Web Browser (HTTP)

En una de las computadoras use el Navegador Web e ingrese la dirección del Servidor WEB www.unam.edu.mx para ver la página WEB contenida.

-Editar página WEB.

En la configuración de servicios HTTP del servidor, editar index.html. Cambie el tamaño y color de la letra, así como el mensaje:

```
<html>
```

```
<center><font size='+2' color='blue'>Cisco Packet Tracer</font></center>
```

```
<hr>Welcome to Cisco Packet Tracer. Opening doors to new opportunities.  
Mind Wide Open.
```

Refrescar la página WEB en la computadora y observar los cambios realizados.

5. Protocolos.

Estando en modo simulación editar los filtros y seleccionar únicamente los siguientes protocolos: **DHCP, ICMP, HTTP, DNS, POP3, SMNP y Web Browser (HTTP)**.

Repetir el punto 2 para el servidor web www.fesc.unam.edu.mx

Enviar los paquetes automáticamente con **Auto Capture/Play** o parcialmente con **Capture Forward**. Anotar sus comentarios.

CUESTIONARIO

1. ¿Qué es y cómo funciona un servidor DNS?
2. ¿Qué es y que hace un servidor DHCP?
3. ¿Qué es y que hace un servidor HTTP?

CONCLUSIONES

BIBLIOGRAFIA



PRÁCTICA 9: “CONFIGURACION FISICA DE UNA RED LAN”

OBJETIVOS

- Acceder a un Switch Cisco a través del puerto de consola.
- Realizar una configuración básica en S1.

INTRODUCCIÓN

Se utilizan una variedad de modelos de switches y routers en redes de todo tipo. Estos dispositivos se administran mediante una conexión de consola local o una conexión remota. Casi todos los dispositivos tienen un puerto serie de consola al que el usuario puede conectarse.

En esta práctica de laboratorio, aprenderá cómo acceder a un dispositivo a través de una conexión local directa al puerto de consola mediante un programa de emulación de terminal, llamado Tera Term. También aprenderá a configurar los parámetros del puerto serie para la conexión de consola de Tera Term. Después de establecer una conexión de la consola con el dispositivo, puede ver o modificar la configuración del dispositivo.

Después de haber realizado las conexiones, primero se efectuarán las configuraciones básicas del switch. A continuación, implementará conectividad básica mediante la configuración de la asignación de direcciones IP en switches. Cuando haya finalizado la configuración de la asignación de direcciones IP, utilizará diversos comandos *show* para verificar las configuraciones y utilizará el comando *ping* para verificar la conectividad básica entre los dispositivos.

ACTIVIDADES PREVIAS A LA PRÁCTICA

- Leer toda la práctica.
- Descargar el siguiente archivo y realizar la actividad de Packet Tracer, enviando una copia a su profesor <https://drive.google.com/file/d/1E-44F24JtkMXSGmUazwPG8NKnTB76Vxe/view?usp=sharing>

EQUIPO Y MATERIAL

- Cable de consola (DB-9 a RJ-45).
- Patch cords necesarios para la conexión de los equipos.
- 1 Switch Catalyst 2960 plus series.
- 2 computadoras con el software apropiado ya instalado.

PROCEDIMIENTO EXPERIMENTAL

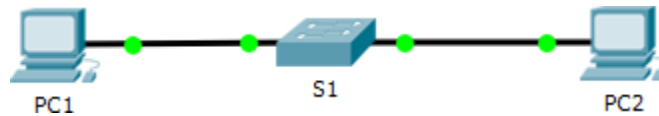


Figura 1

Dispositivo	Interfaz	Dirección IP	Mascara de subred
S1	VLAN 1	192.168.10.254	255.255.255.0
S2	VLAN 1	192.168.20.254	255.255.255.0

Tabla 1

*Esta práctica se realizará por equipos, de acuerdo con la mesa de trabajo en la que se encuentren, la mesa 01 utilizará el Switch 1 y la mesa 02 el Switch 2.

9.1 REALIZAR LA CONFIGURACIÓN BÁSICA DEL SWITCH POR CONSOLA ([ver anexo 2](#)).

***NOTA: NO REALIZAR NINGUN TIPO DE CONFIGURACION ADICIONAL AL INDICADO EN LA PRACTICA.**

1. Configurar un nombre de host en el Switch.

- Entre al modo de configuración global en S1.
- Introduzca el comando correcto para configurar el nombre de host **S1**

2. Configurar un aviso de MOTD.

Utilice un texto de aviso adecuado para advertir sobre el acceso no autorizado. El siguiente texto es un ejemplo:

“Acceso autorizado únicamente. Los infractores se procesarán en la medida en que lo permita la ley.”

9.2 CONFIGURACIÓN DE LA INTERFAZ ADMINISTRACIÓN DEL SWITCH.

1. Configurar el S1 con una dirección IP.

Use los siguientes comandos para configurar el S1 con una dirección IP.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.253 255.255.255.0
S1(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# exit
S1#
```



9.3 VERIFIQUE LA CONFIGURACIÓN DE DIRECCIONES IP EN EL SWITCH

Use el comando *show ip interface brief* para ver la dirección IP y el estado de todos los puertos y las interfaces del Switch. También puede utilizar el comando *show running-config*.

Agregar capturas de pantalla donde señale el resultado obtenido.

9.4 DIRECCIONES IP DE LAS PC

Las direcciones IP de las PCs ya se encuentran configuradas de manera estática, ingrese al CMD de cada pc y con el comando *ipconfig/all* obtenga la dirección IP de cada PC. ¿Cuáles son las direcciones IP de las PC utilizadas?

9.5 VERIFIQUE LA CONECTIVIDAD DE LA RED.

Puede verificarse la conectividad de la red mediante el comando *ping*. Es muy importante que haya conectividad en toda la red. Se deben tomar medidas correctivas si se produce una falla. Desde la PC1 y la PC2, haga ping al Switch.

1. En las PC abra una ventana de símbolo de sistema o CMD (puede hacerlo con la combinación de teclas **Windows + R**).
2. Desde PC1 envíe un ping a la dirección IP de la PC2.
3. Desde PC1 envíe un ping a la dirección IP del S1.

Nota: También puede usar el comando ping en la CLI del Switch y en la PC2.

Todos los pings deben tener éxito. Si el resultado del primer ping es 80%, inténtelo otra vez, ahora debería ser 100 %. Si los pings no resultan exitosos a ninguno de los dispositivos, vuelva a revisar la configuración para detectar errores y corríjalos.

CUESTIONARIO

1. Además del puerto de consola, ¿de qué otra forma se puede acceder a un equipo de red para configurarlo?
2. Mencione qué otro tipo de Switch existe, además de los utilizados en la práctica.
3. ¿Cuál sería la diferencia en cuanto al uso de la interfaz de Packet Tracer y la CLI del equipo físico?

CONCLUSIONES

BIBLIOGRAFIA



PRÁCTICA 10: “CONFIGURACIÓN FÍSICA DE UNA RED WAN

OBJETIVOS

- Realizar la correcta configuración de los equipos incluidos en la topología.
- Implementar ruteo estático para que la conectividad sea exitosa.

INTRODUCCIÓN

El enrutamiento estático proporciona un método que otorga a los ingenieros de redes control absoluto sobre las rutas por las que se transmiten los datos en una red. Para adquirir este control, en lugar de configurar protocolos de enrutamiento dinámico para que creen las tablas de enrutamiento, se crean manualmente. Es importante entender las ventajas y desventajas de la implementación de rutas estáticas, ya que se utilizan extensamente en redes pequeñas y para establecer la conectividad con proveedores de servicios. Es posible que se crea 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).

ACTIVIDADES PREVIAS A LA PRACTICA.

- Leer toda la práctica.
- Investigar las características del Router Cisco 2900 series.

EQUIPO Y MATERIAL

- Cable de consola (DB-9 a RJ-45).
- Patch cords necesarios para la conexión de los equipos.
- 2 Switch Catalyst 2960 plus series.
- 1 Router 2900 series.
- 3 computadoras con el software apropiado ya instalado.



PROCEDIMIENTO EXPERIMENTAL

10.1 CONEXIÓN DE LOS EQUIPOS.

Realice la conexión de los equipos de acuerdo con la Figura 1.

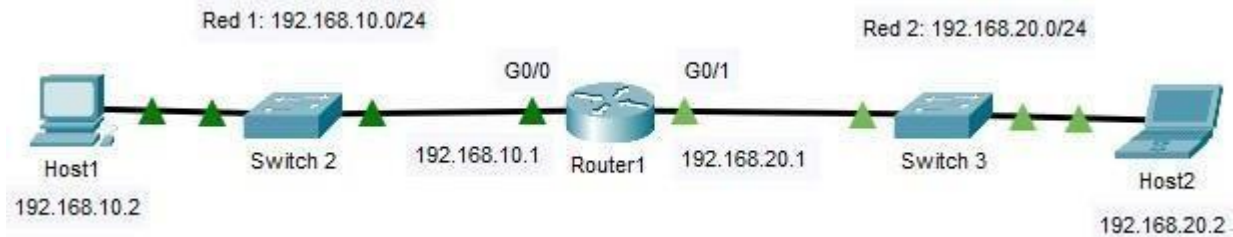


Figura 1

Dispositivo	Interfaz	Dirección IP	Mascara de red	Gateway
PC1	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.2	255.255.255.0	192.168.20.1
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.20.1	255.255.255.0	N/A

Tabla 1

***Nota: Las direcciones IP de las PC ya se encuentran configuradas de forma estática.**

10.2 DIRECCIONES IP DE LAS PC

- Las direcciones IP de las PC se encuentran asignadas en un segmento de red distinto de acuerdo con la red en la cual se encuentra la PC:

Red 1: 192.168.10.0/24

Red 2 :192.168.20.0/24

Indicar para cada red una dirección IP que se le puede asignar a otra PC y su dirección de Broadcast

Red1

PC: _____ Broadcast: _____

Red2

PC: _____ Broadcast: _____



10.3 CONFIGURACIÓN DE LOS EQUIPOS

1. Para realizar la configuración de los equipos de red, conéctese mediante el puerto de consola (consulte el [anexo 2](#)).

***NOTA: NO REALIZAR NINGUN TIPO DE CONFIGURACION ADICIONAL AL INDICADO EN LA PRACTICA.**

10.4 CONFIGURACIÓN DE LOS SWITCHES

1. Indicar el procedimiento para realizar las siguientes configuraciones:
 - a. Cambiar el nombre del equipo.
 - b. Configurar un banner MOTD.
 - c. Asignar una dirección IP a la interfaz de administración.

10.5 CONFIGURACIÓN DEL ROUTER

1. Realizar los siguientes cambios en la configuración del router.
 - a. Realice la configuración de las direcciones IP correspondientes a las interfaces G0/0 y G0/1 de acuerdo con la tabla 1.
2. Indicar los resultados obtenidos y anotar sus observaciones.

10.6 VERIFICACIÓN DE LA CONECTIVIDAD EN LA RED

1. Realizar las pruebas pertinentes para comprobar que se tenga conectividad entre ambas PC y agregar una captura de pantalla del resultado obtenido.

CUESTIONARIO

1. ¿En qué situaciones resulta más conveniente utilizar direccionamiento estático en lugar de dinámico?
2. ¿Qué modificaciones sería necesario hacer en la configuración de los equipos para agregar más computadoras?

CONCLUSIONES

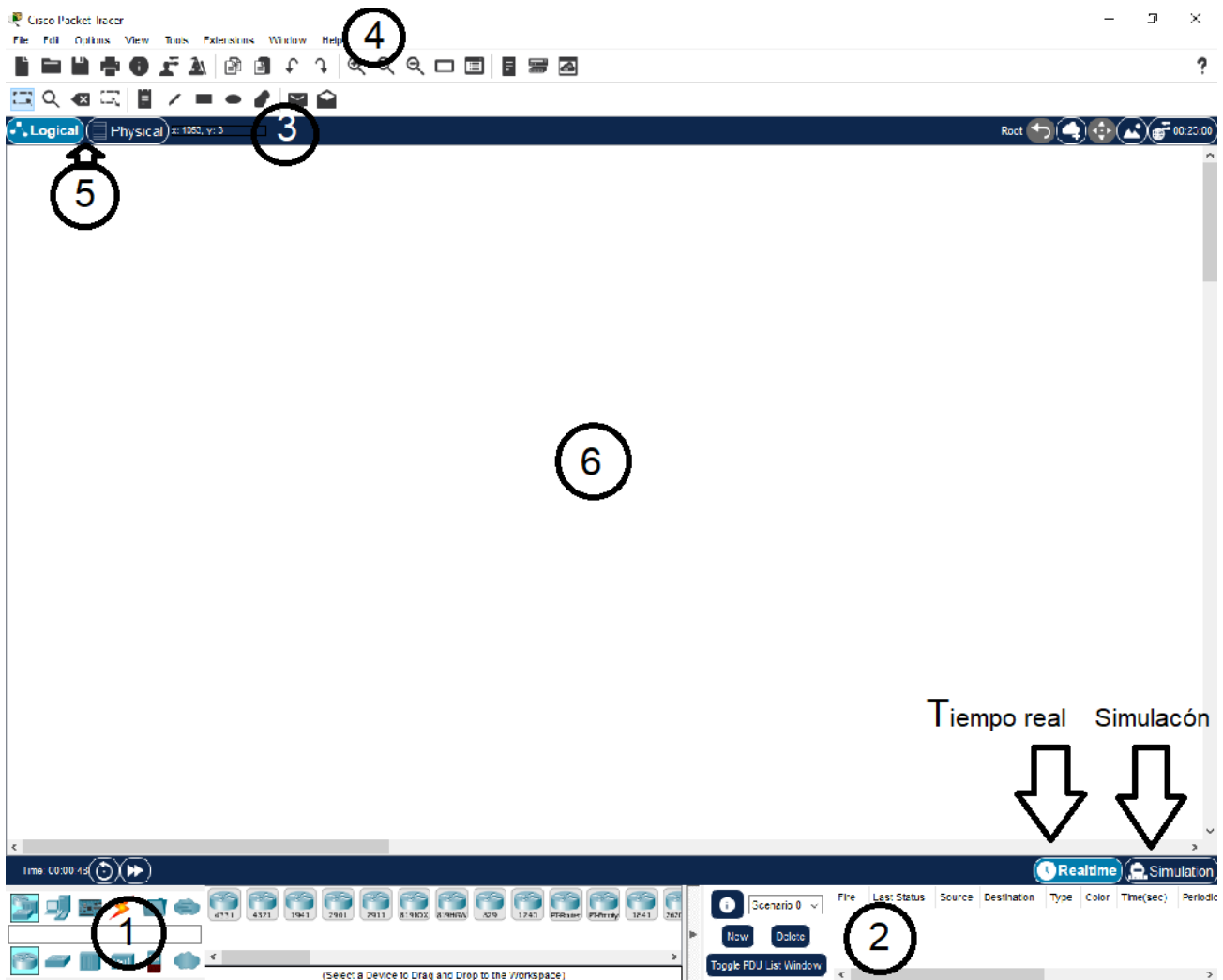
BIBLIOGRAFIA



ANEXO I

1. El simulador que vamos a utilizar lo encontramos en la página: <https://www.netacad.com/>
2. Aquí nos registramos gratuitamente con una cuenta de correo, una vez que hayamos validado nuestra cuenta vamos a *Recursos de Packet Tracer* y descargamos la versión que corresponda con nuestro equipo de cómputo.
3. Una vez descargado e instalado podemos utilizar el programa.

4. Al ejecutar el simulador  veremos la siguiente ventana:





Parte 1

En esta parte tenemos los equipos de red (routers, switches, hubs, PC, etc.) y también encontramos los conectores (icono del rayo), es decir, los cables para que los equipos se puedan conectar (cable derecho, cruzado, serial, etc.). Para agregar un equipo, hacemos un clic en la categoría que necesitamos, seleccionamos el equipo y, por último, le damos clic en el fondo blanco (parte 6).

Parte 2

Aquí encontramos los escenarios donde nos muestra información de los PDU enviados. Donde dice "Tiempo real" y "Simulación", podemos hacer el seguimiento de los PDU. En tiempo real, cuando enviamos un PDU, no vamos a poder ver en detalle lo que pasa. En cambio, en simulación (nos abre un menú), podemos verlo y además podemos seleccionar los protocolos que queremos ver. Si queremos ver solo el protocolo ICMP (ping), vamos a editar filtros y marcamos solo ICMP.

Parte 3

En esta sección encontramos herramientas para modificar la topología. Rectángulo punteado seleccionado con una flecha que sirve para arrastrar equipos, cambiar la interfaz a la cual se conectan los cables y muchas cosas más. También contamos con el icono de mano que nos sirve para mover toda la topología. Además, está el icono Con forma de nota que sirve para poner anotaciones. Por ejemplo, si tenemos una topología extensa, podemos agregar información útil para no perdernos entre tantos equipos y direcciones IP.

El icono de cruz roja sirve para eliminar equipos y cables.

Por último, tenemos dos sobres, el primer sobre (icono de sobre cerrado) sirve para mandar un PDU simple, y el otro cumple la misma función, pero en este último podemos configurar el TTL, TOS y algunas otras opciones.

Mi recomendación es que cuando quieran mandar un PDU, usen el simple (icono de sobre cerrado).

Parte 4

Barra de menú, podemos hacer lo que hacemos con cualquier programa, guardar, salir, abrir, etc.

Parte 5

Como vemos en la imagen hay 2 espacios de trabajo, uno lógico y otro físico. El espacio lógico es donde nosotros armamos la topología, ya sea grande, chica o mediana y tenemos todo ahí. En cambio, en el espacio físico, como es un programa que simula redes, podemos armar conexiones entre distintas zonas y lo que muestra es como sería en la vida real la red que estamos armando. Generalmente se trabaja en el espacio lógico.

Parte 6

En esta parte está el escenario, es donde vamos a armar nuestra topología. Realtime y Simulation, en esta parte seleccionamos el modo, ya sea tiempo real o simulación.

ANEXO II

Conexión de una PC a un equipo por medio del puerto de Consola.



Figura 1

Esta conexión le permitirá acceder a la interfaz de línea de comandos.

1. Conecte un switch y una PC mediante un cable de consola.

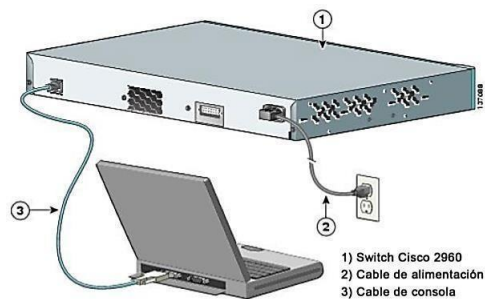


Figura 2

a. Conecte el cable de consola al puerto serie COM de la PC.

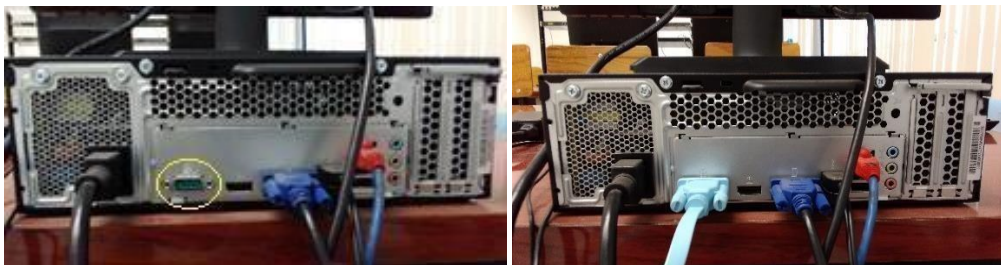


Figura 3

b. Conecte el otro extremo del cable de consola Al puerto del switch con el mismo nombre.

c. Encienda el switch

2. Configure Tera Term para establecer una sesión de consola con el switch.

Tera Term es un programa de emulación de terminal. Este programa le permite acceder a la CLI del switch, en donde es posible configurar el switch.

- a. Inicie Tera Term haciendo clic en el botón Inicio de Windows, situado en la barra de tareas. Localice Tera Term en Todos los programas.
- b. En el cuadro de diálogo Conexión nueva, haga clic en el botón de opción Serial. Verifique que esté seleccionado el puerto COM correcto y haga clic en Aceptar para continuar.

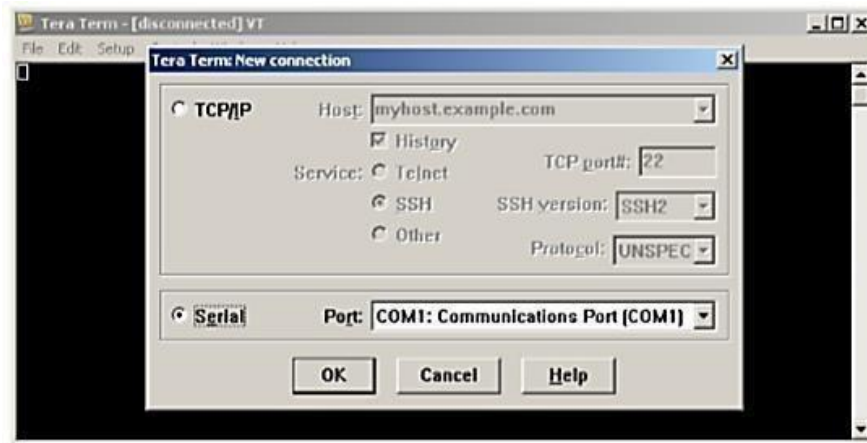


Figura 4

- c. En el menú Configuración de Tera Term, seleccione Puerto serie... para verificar los parámetros de serie. Los parámetros predeterminados para el puerto de consola son **9600 baudios, 8 bits de datos, ninguna paridad, 1 bit de parada y ningún control del flujo**. Los parámetros predeterminados de Tera Term coinciden con los parámetros del puerto de consola para las comunicaciones SSH con el switch de Cisco IOS. Damos Ok para continuar.

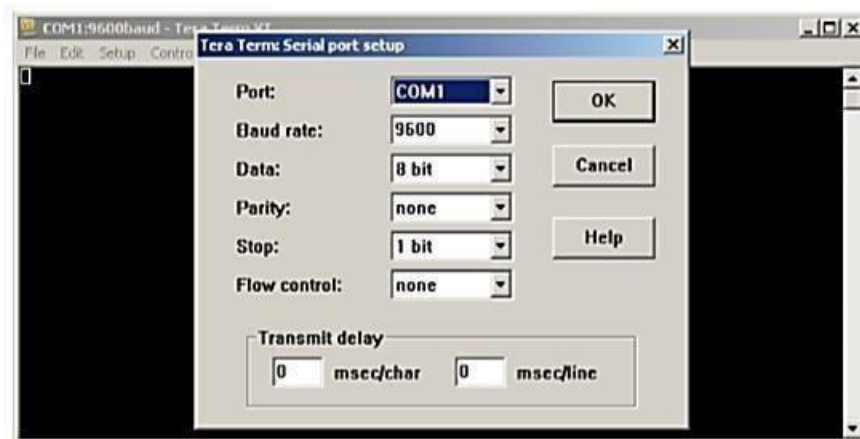


Figura 5

- d. Cuando pueda ver el resultado de terminal, estará listo para configurar un switch. El siguiente ejemplo de la consola muestra el resultado para el terminal del switch durante la carga.

```
COM1:9600baud - Tera Term VT
File Edit Setup Control Window Help
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEA
SE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_teamInitializing flashfs...
Using driver version 3 for media type 1
mifs[4]: 0 files, 1 directories
mifs[4]: Total bytes      : 3870720
mifs[4]: Bytes used      : 1024
mifs[4]: Bytes available : 3869696
mifs[4]: mifs fsck took 1 seconds.
mifs[4]: Initialization complete.
```

Figura 6

- e. Una vez que el switch completa el proceso de inicio, se muestra el siguiente mensaje.

Introduzca: **n** para continuar.

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

Nota: Si no ve el mensaje que se muestra arriba, consulte con el profesor para restablecer el switch a la configuración inicial.

Existen más emuladores de terminal que se pueden usar, por ejemplo: Hyperterminal y Putty, donde la configuración es la misma que la vista para Tera Term.