UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIA Y TECNOLOGÍA

ESCUELA DE INGENIERÍA ELECTRÓNICA

IMPLEMENTACIÓN DE UN LABORATORIO VIRTUAL DE NETWORKING PARA LA FACULTAD DE CIENCIA Y TECNOLOGÍA DE LA UNIVERSIDAD DEL AZUAY

TRABAJO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO ELECTRÓNICO

AUTOR
PABLO ANDRÉS BARBECHO BAUTISTA

DIRECTOR
HUGO MARCELO TORRES SALAMEA

CUENCA - ECUADOR
2012

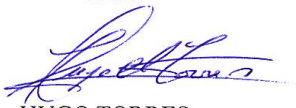
RESUMEN

Para instalar el software de distribución libre Packet Tracer y realizar un módulo de aspectos básicos del networking, se exploraron las diferentes capas de red del modelo OSI, desarrollando ejemplos prácticos y simulaciones de laboratario que facilitan, de gran manera, el estudio de las redes y equipos de comunicaciones.

Ésta implementación ayuda a los estudiantes a desarrollar configuraciones en equipos de comunicaciones y networking, tan comunes, como son routers, switchs, access points, etc. El laboratorio práctico amplía los conocimientos teóricos descritos en el módulo de aspectos básicos del networking, brindando a los estudiantes una idea clara de los equipos usados en el campo de las comunicaciones.

PABLO BARBECHO

Autor



HUGO TORRES

Director

ABSTRACT

For install the software open source Packet Tracer and make a module of basic aspects about networking, were explored the different net layers of OSI model, developing practical examples and laboratory simulations that facilitates the study of network and communication equipments.

This implementation helps the students to develop configurations in communication equipments and networking equipments, very commons, like routers, switchs, access points, etc. The practical laboratory, broad theorical knowledge described in the module about basic aspects of networking, giving to the students a clear idea of the equipments used into communication field.

PABLO BARBECHO
Autor

HUGO TORRES
Director

INDICE DE CONTENIDOS

2.1 Principios fundamentales de la capa Física

2.2 Componentes Físicos

2.2.1 Tipos de cable

2.2.2 Cable cruzado

2.3 Conexión entre conmutadores y concentradores

2.4 Configuración de una tarjeta de red usando Windows y Linux

2.5 Configuración de una tarjeta de red en Windows

2.6 Configuración de una tarjeta de red en Linux

2.7 Práctica No. 1: Configuración de tarjetas de red y manejo del software Packet Tracer.

2.8 Práctica No. 2: Uso de cable directo y cable cruzado en elementos de redes.

CAPITULO III: CONCEPTOS Y CONFIGURACIONES DE NETWORKING DE ELEMENTOS DE CAPA DOS (MODELO OSI)

3.1 Tipos de Switchs

3.1.1 Switch de Capa 2

3.1.2 Switch de Capa 3

3.2 Casos de uso de cada equipo

3.3 Conexión al puerto de consola

3.4 Práctica No. 3: Realizar configuraciones básicas en un switch capa 2

3.5 VLAN (Red Virtual de Área Local)

3.6 Beneficios de las VLAN

3.7 Tipos de VLAN

3.7.1 VLAN DE DATOS

3.7.2 VLAN PREDETERMINADA

3.7.3 VLAN NATIVA

3.7.4 VLAN DE ADMINISTRACION

3.8 Rangos de ID para las VLANs

Pablo Andrés Barbecho Bautista
Trabajo de Graduación
Hugo Marcelo Torres Salamea
Abril 2012

IMPLEMENTACIÓN DE UN LABORATORIO VIRTUAL DE NETWORKING PARA LA FACULTAD DE CIENCIA Y TECNOLOGÍA DE LA UNIVERSIDAD DEL AZUAY

INTRODUCCION

El presente trabajo monográfico, está orientado a los estudiantes de la Universidad del Azuay. En su texto se desarrollan los conceptos necesarios para formar un criterio en los estudiantes en el campo de networking, con prácticas claras y objetivas que permiten la correcta asimilación del texto monográfico.

El cuerpo del documento contempla cinco capítulos que desarrollan cada una de las capas del modelo OSI. Cada capítulo consta de dos partes, una teórica y otra práctica. La parte teórica busca explicar al estudiante los conceptos básicos de las configuraciones de los equipos networking. La parte práctica se ayuda del simulador Packet Tracer para mostrar al estudiante el entorno de los equipos de red. Este simulador es bastante amigable y contiene casi todas las funcionalidades de un equipo real.

Sin duda, el software de simulación es ideal para desarrollar en el estudiante habilidades de configuración de routers, switches, Pcs, etc. Las prácticas que se encontrarán al final de cada capítulo ponen a prueba los conceptos adquiridos, desafiando al estudiante a ir más allá del presente texto monográfico. Cada práctica se encuentra claramente especificada con pasos e imágenes que facilitan el desarrollo de las mismas. El software es de fácil manejo, con un entorno gráfico muy amigable que permite explorar casi todas las funcionalidades que ofrecen los equipos de networking de una manera muy didáctica.

CAPÍTULO I

ASPECTOS BÁSICOS DEL NETWORKING

1.1 Estructura de la red

1.1.1 Elementos de que intervienen en las comunicaciones

En el mundo, las personas se comunican de diversas formas; sin embargo existen tres elementos comunes en todos los tipos de comunicaciones, a continuación se describen estos elementos comunes que intervienen en el proceso de la comunicación:

- Origen (Emisor)
- Destino (Receptor)
- Canal (Camino)

Un concepto básico de networking es la forma en la que estos elementos convergen para realizar una comunicación. En teoría una comunicación simple como un email, video, música, etc. puede enviarse como **un stream de datos masivo**, pero si en realidad la comunicación se realizare de esta manera, el resto de elementos de la red no podría transmitir datos mientras la primera comunicación esté en curso. Esta transmisión de datos generaría retrasos en las transmisiones además de generar una pérdida total del mensaje si la comunicación se perdiese, y debería retransmitirse todo el mensaje de nuevo por completo.

Un mejor enfoque para la transferencia de datos es la **SEGMENTACION**, es decir, dividir todo el stream de datos en pequeñas partes más livianas y manejables. La segmentación del stream de datos tiene dos beneficios principales:

- Al enviar partes individuales más pequeñas del origen al destino, se pueden entrelazar otras comunicaciones en la misma red. (Multiplexación)
- La segmentación aumenta la confiabilidad en la comunicación al no ser necesario que cada parte del mensaje viaje por un mismo camino, que en su momento pudiese saturarse o fallar. Las partes del mensaje pueden atravesar diferentes caminos en la red garantizando la transmisión de los datos, y si en el peor de los casos se pierden partes de la comunicación, solo esos paquetes deberán ser retransmitidos.

La gran desventaja en este método de transmisión de datos (segmentación) es la complejidad que este método de segmentación y multiplexación agrega a la red. Cada paquete del mensaje tendría que etiquetarse con información de origen y destino, lo cual requiere mucho tiempo, trabajo y procesamiento de paquetes. Es ahí donde los equipos de networking hacen su trabajo y permiten la comunicación.

1.2 Componentes de una red

Los componentes de una red se pueden clasificar en los siguientes grupos:

1.2.1 Dispositivos Finales: Son aquellos con los que la gente interactúa. Estos dispositivos hacen de interfaz entre la red humana y la red de comunicación. A continuación se describen algunos ejemplos:

- Dispositivos móviles (Smartphone, PDA, etc)

- Computadoras (Laptops, portátiles, servidores, etc)
- Impresoras de red
- Teléfonos IP
- Cámaras IP

1.2.2 Dispositivos Intermedios: Estos dispositivos conectan los dispositivos finales o también llamados host, a la red y pueden conectar también redes individuales para formar una red interna o internetworking, como por ejemplo:

- Dispositivos de acceso a la red (hubs, switches, puntos de acceso inalámbrico)
- Dispositivos de internetworking (routers)
- Modems
- Dispositivos de seguridad (Firewalls)

Como se mención anteriormente, la comunicación por medio de la segmentación y multiplexación agrega gran cantidad de procesamiento y manejo de los paquetes en la red. Los dispositivos intermedios son los encargados de la administración y de otras funciones, que se resumen a continuación:

- Regenerar señales de la comunicación
- Retransmitir señales de la comunicación
- Guarda información sobre las rutas de la red
- Notificar a otros equipos las fallas en la comunicación de equipos pertenecientes a la red
- Re direccionar paquetes por rutas alternas cuando existen problemas en rutas vecinas
- Clasificar tráfico y paquetes al aplicar QoS en los equipos
- Aplicar reglas de seguridad permitiendo o denegando tráfico de la red.

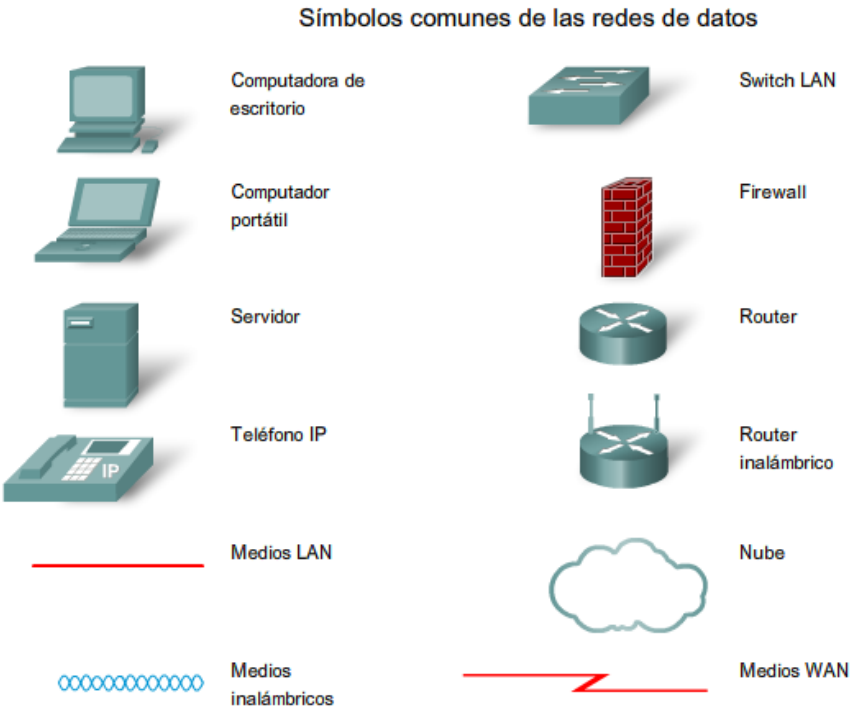


Figura 1. Símbolos de las redes de datos

1.3 Medios de la red

El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Existen tres tipos de medios de transmisión.

- Cable de cobre,
- Cable de fibra óptica,
- Transmisión Inalámbrica.

Estos medios de red tienen diferentes características, por lo cual su uso depende de ciertos aspectos:

- La distancia por la cual el medio puede transportar exitosamente una señal,

- El ambiente en el cual se instalará el medio,
- La cantidad de datos y la velocidad a la que se deben transmitir,
- El costo del medio y la facilidad de instalación.

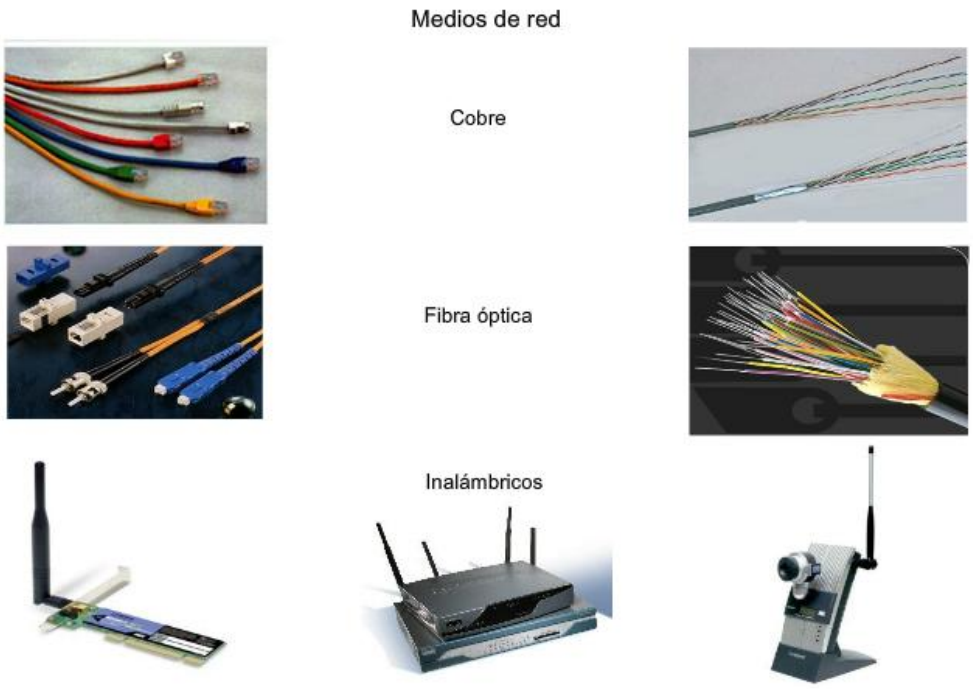


Figura 2. Medios de Red
Fuente: http://www.itecuador.com/

1.3.1 Terminología de Conexión

Es importante conocer la terminología que se usará para las prácticas de los siguientes capítulos:

Tarjeta de interfaz de red(adaptador LAN): proporciona la conexión física con la red a un host.

Puerto físico: conector de un dispositivo de red, en el cual el medio se conecta con un host o con otro dispositivo de la red.

Interfaz de red: puertos especializados de un dispositivo de internetworking que se conecta con redes individuales.

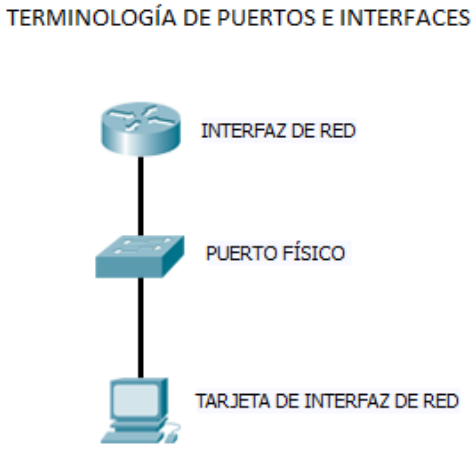


Figura 3. Terminología de puertos e interfaces

1.4 Stack de Protocolos

Otro concepto muy importante en las comunicaciones es el desarrollo e interacción de los diferentes protocolos que rigen las comunicaciones en la red. La suite de protocolos de networking describe procesos como los siguientes:

- La forma en la que se arma el mensaje (estructura del mensaje),
- Cómo los dispositivos finales comparten o distribuyen información de la topología de la red (rutas)
- Información de inicio y terminación de las sesiones de transferencia de datos.

El funcionamiento de los protocolos de red, se basa en la interconexión y comunicación de los mismos (Stack de Protocolos). A cada capa de red le corresponden ciertos protocolos, por ejemplo:

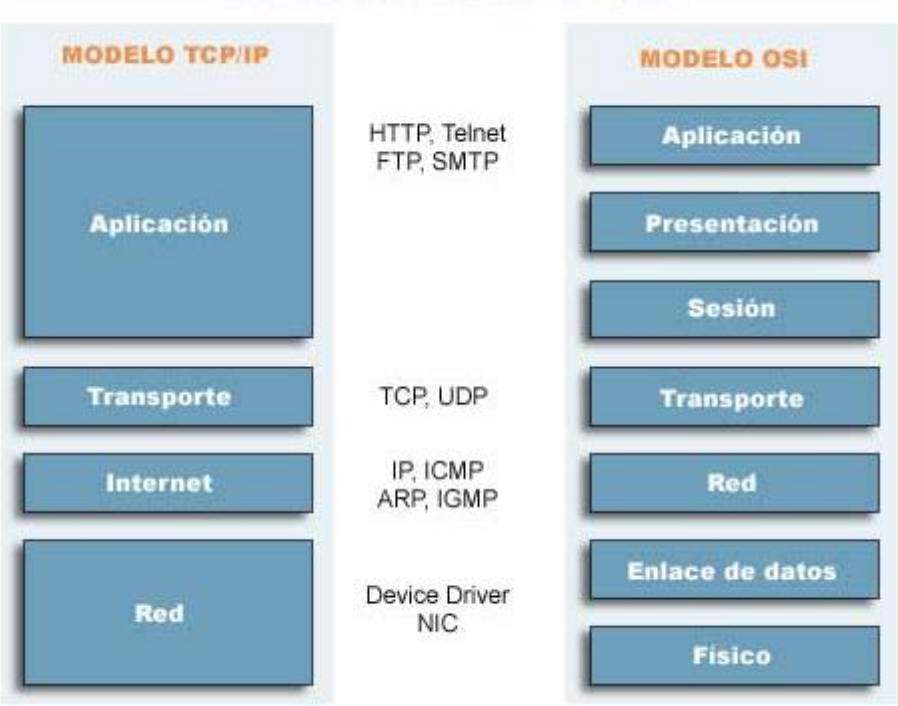


Figura 4. Capas del modelo TCP/IP y OSI

Para explicar el uso de una suite de protocolos en comunicaciones de red, se puede desarrollar la interacción entre un servidor Web y un explorador Web.

Basándonos en el modelo TCP/IP (Protocolo de Control de Transporte / Protocolo de Internet), los protocolos que intervienen en esta comunicación son los siguientes:

Protocolo de aplicación:

- HTTP, regula la comunicación entre servidor y cliente web.

Protocolo de transporte:

- TCP, como se indicó anteriormente TCP divide los mensajes HTTP en pequeñas partes, denominadas segmentos, para enviarlas al destino. Además

controla el tamaño y los intervalos a los que se intercambian los mensajes entre el servidor y el cliente.

Protocolo de internet:

- IP, es responsable de tomar los segmentos formateados del TCP, encapsularlos en paquetes, asignarles las direcciones correctas y seleccionar la mejor ruta hacia el host de destino.

Protocolos de acceso a la red: Estos protocolos describen dos funciones principales:

- Administración de enlace de datos
- Transmisión física de datos en los medios.

Los protocolos de administración de enlace de datos toman los paquetes IP y los formatean para transmitirlos por los medios. Los estándares y protocolos de los medios físicos rigen de qué manera se envían las señales por los medios y cómo las interpretan los clientes que las reciben. Los transceptores de las tarjetas de interfaz de red implementan los estándares apropiados para los medios que se utilizan.

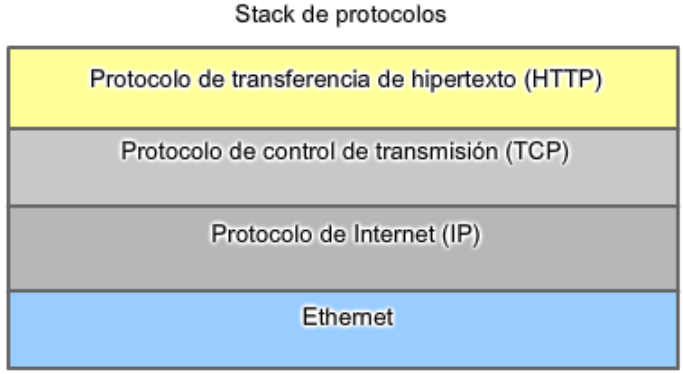


Figura 5. Stack de Protocolos

La forma en la que se adopta una sección de datos en cada capa se denomina **Unidad de Datos del Protocolo PDU**. Debido a que en cada capa, la unidad de datos del protocolo va cambiando, se definen nombres que identifican el cambio del PDU en cada capa.

Datos: el termino general para las PDUs que se utilizan en la capa de aplicación

Segmento: PDU de la capa de transporte

Paquete: PDU de la capa de internetwork

Trama: PDU de la capa de acceso a la red

Bits: una PDU que se utiliza cuando se transmiten fisicamente datos atravezde un medio.

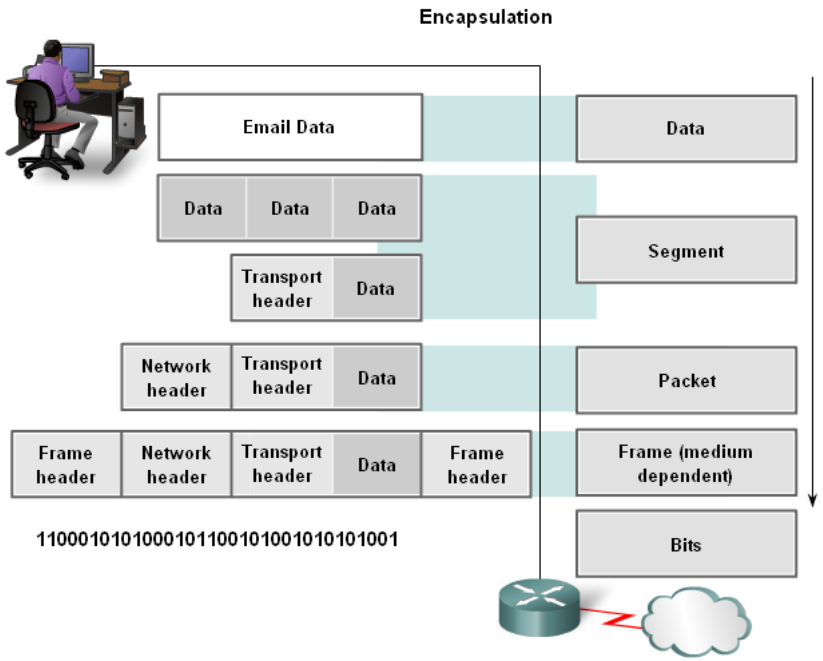


Figura 6. Paquetes de Datos

CAPÍTULO II

CONCEPTOS Y CONFIGURACIONES DE NETWORKING DE ELEMENTOS DE CAPA UNO (MODELO OSI)

El objetivo de la capa uno (capa Física) es crear la señal óptica, eléctrica o de microondas que representa a los bits en cada trama, a más de recuperar estas señales individuales desde los medios, se encarga de restaurar las señales eléctricas para sus representaciones de bits y enviar los bits hacia la capa de enlace de datos como una trama completa.

2.1 Principios fundamentales de la capa Física

Las tres funciones esenciales de la capa Física son:

- Los componentes físicos
- Codificación de datos
- Señalización

2.2 Componentes Físicos:

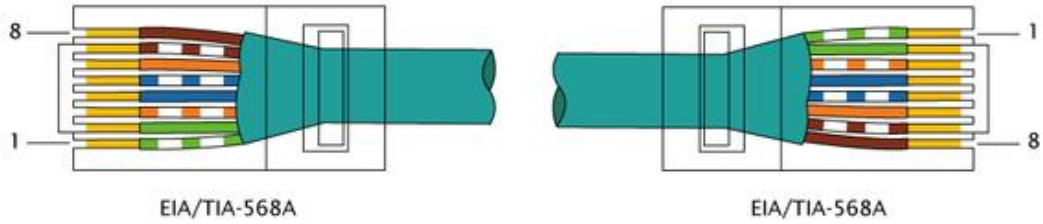
2.2.1 Tipos de cable

El cable directo de red sirve para conectar dispositivos desiguales, como un computador con un hub o switch. En este caso ambos extremos del cable deben tener la misma distribución. No existe diferencia alguna en la conectividad entre la distribución 568B y

la distribución 568A siempre y cuando en ambos extremos se use la misma, en caso contrario hablamos de un cable cruzado.

El esquema más utilizado en la práctica es tener en ambos extremos la distribución 568B.

Cable directo 568A



Cable directo 568B

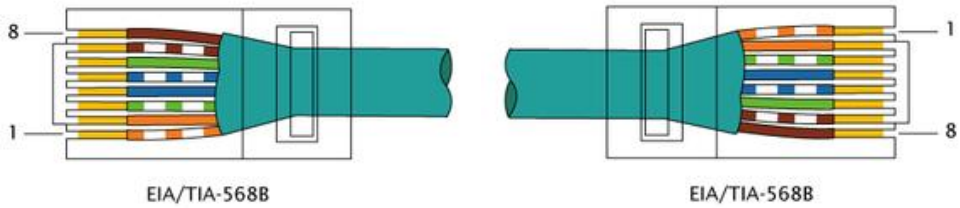


Figura 7. Cable Directo.
Fuente: http://es.wikipedia.org/wiki/RJ-45

2.2.2 Cable cruzado

Un cable cruzado es un cable que interconecta todas las señales de salida en un conector con las señales de entrada en el otro conector, y viceversa; permitiendo a dos dispositivos electrónicos conectarse entre sí con una comunicación full duplex.

El cable cruzado sirve para conectar dos dispositivos igualitarios, como 2 computadoras entre sí, para lo que se ordenan los colores de tal manera que no sea necesaria la

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

Para crear un cable cruzado que funcione, un extremo del cable debe tener la distribución 568A y el otro 568B.

Cable cruzado 568A/568B

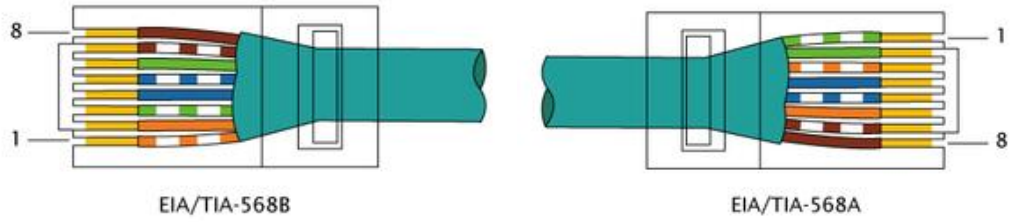


Figura 8. Cable Cruzado.

Fuente: http://es.wikipedia.org/wiki/RJ-45

Norma A

1. Blanco Verde
2. Verde
3. Blanco Naranja
4. Azul
5. Blanco Azul
6. Naranja
7. Blanco Marrón
8. Marrón

Norma B

1. Blanco Naranja
2. Naranja
3. Blanco Verde
4. Azul
5. Blanco Azul

6. Verde
7. Blanco Marrón
8. Marrón

2.3 Conexión entre conmutadores y concentradores

Dispositivos diferentes; en tal caso se pueden utilizar normas AA o BB en los extremos de los cables:

Una punta (Norma B)	**En el otro lado (Norma B)**
Blanco Naranja	Blanco Naranja
Naranja	Naranja
Blanco Verde	Blanco Verde
Azul	Azul
Blanco Azul	Blanco Azul
Verde	Verde
Blanco Marrón	Blanco Marrón
Marrón	Marrón

Conexión directa PC a PC

Una punta (Norma B)	En el otro lado (Norma A)
Blanco Naranja	Blanco Verde
Naranja	Verde
Blanco Verde	Blanco Naranja
Azul	Azul
Blanco Azul	Blanco Azul
Verde	Naranja
Blanco Marrón	Blanco Marrón
Marrón	Marrón

2.4 Configuración de una tarjeta de red usando Windows y Linux

Aunque aún no se revisa direccionamiento de red, se desarrollará estas configuraciones enfocándose en la interfaz física.

Estas configuraciones pretenden que el estudiante conozca las configuraciones más básicas de las tarjetas de red como son: configuración IP, gateways, mascaras de red, reiniciar o desactivar tarjetas de red, etc.

2.5 Configuración de una tarjeta de red en Windows

Una de las maneras para asignar una dirección IP estática ó dinámica (DHCP) en un host (equipo terminal o computador) con Windows, es la siguiente:

Figura 9. Tarjeta de Red

1. Pulsamos en Abrir centro de redes y recursos compartidos.

Figura 10. Paso 1: Configuración del Adaptador de Red

2. Cambiar configuración del adaptador

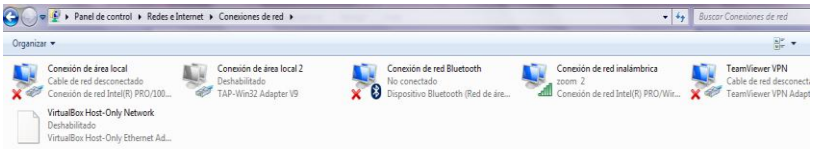


Figura 11. Paso 2: Configuración del Adaptador de Red

3. Elegimos el adaptador al cuál se le va a configurar la dirección IP

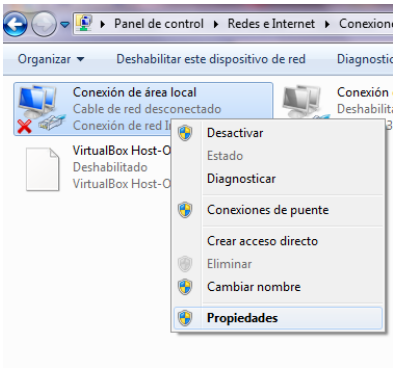


Figura 12. Paso 3: Configuración del Adaptador de Red

4. Abrimos Propiedades

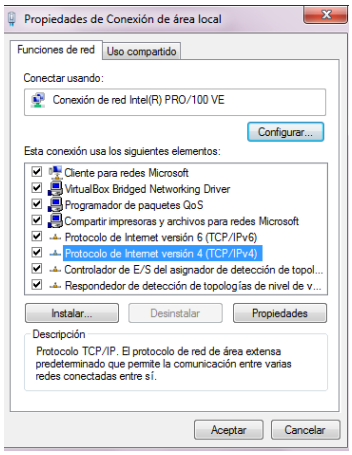


Figura 13. Paso 4: Configuración del Adaptador de Red

5. Elegimos TCP/IPv4

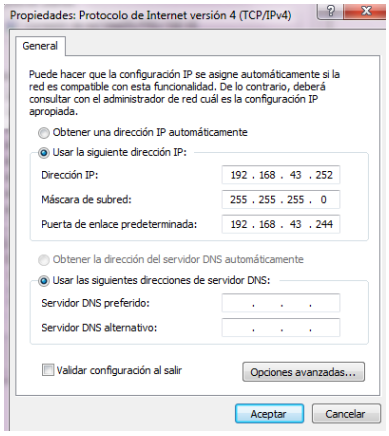


Figura 14. Paso 5: Configuración del Adaptador de Red

6. Configuramos la dirección IP estática ó dinámica, si contamos con un servidor de DHCP en nuestra intranet.

Para detección de errores en una red, tenemos las siguientes herramientas para análisis de las configuraciones realizadas:

7. Ejecutar la línea de comandos DOS.

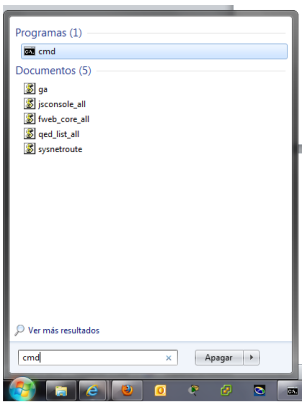


Figura 15. Paso 6: Configuración del Adaptador de Red

8. Identificar la MAC ADDRESS de nuestra tarjeta de red.

Una vez en la consola de Windows, escribimos el comando **ipconfig.**

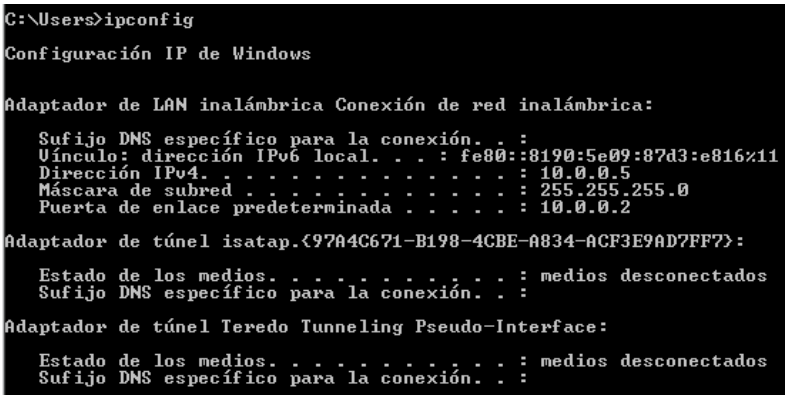


Figura 16. Paso 7: Configuración del Adaptador de Red

En esta pantalla se muestran todos los adaptadores de red que posee el computador. El comando **ipconfig** nos muestra la información relativa a los parámetros de nuestra configuración **IP** actual.

Este comando tiene una serie de modificadores para ejecutar una serie de acciones concretas. Estos modificadores son:

/all-Muestra toda la información de configuración.
/allcompartments- Muestra información para todos los compartimientos.
/release-Libera la dirección IP para el adaptador específicado (IPv4 e IPv6).
/renew- Renueva la dirección IPv4 para el adaptador específicado.
/renew6 - Renueva la dirección IPv6 para el adaptador específicado.
/flushdns- Purga la caché de resolución de DNS.
/registerdns- Actualiza todas las concesiones DHCP y vuelve a registrar los nombres DNS.
/displaydns- Muestra el contenido de la caché de resolución DNS.
/showclassid- Muestra todas los id. de clase DHCP permitidas para este adaptador.
/setclassid- Modifica el id. de clase DHCP.

Vamos a centrarnos en la información que se nos ofrece alejacutar**ipconfig /all**. Para ello escribimos en el editor de comandos **IPConfig /all** y pulsamos **enter.**

Figura 17. Comando ipconfig

Como podemos ver en la imagen, la información que nos ofrece es bastante amplia:

DHCP habilitado.- Nos indica si el servicio DHCP está habilitado o no.

Configuración automática habilitado.- Nos indica si tenemos la configuración de nuestra red en forma automática.

Vínculo: dirección IPv6 local.- Nos muestra nuestra la dirección IPv6 de nuestra máquina.

Dirección IPv4.- Nos muestra la dirección IP actual de nuestra máquina.

Máscara de subred.- Nos muestra cual es la máscara de subred de nuestra red.

Puerta de enlace predeterminada.- Nos muestra la IP de la puerta de enlace (normalmente esta es la dirección del router de la red).

Servidores DNS.- Nos muestra la IP de los servidores DNS a los que estamos conectados.

Comando Nslookup: comando que permite consultar manualmente los servidores de nombre para resolver el nombre de un host. Usado en verificación de problemas.

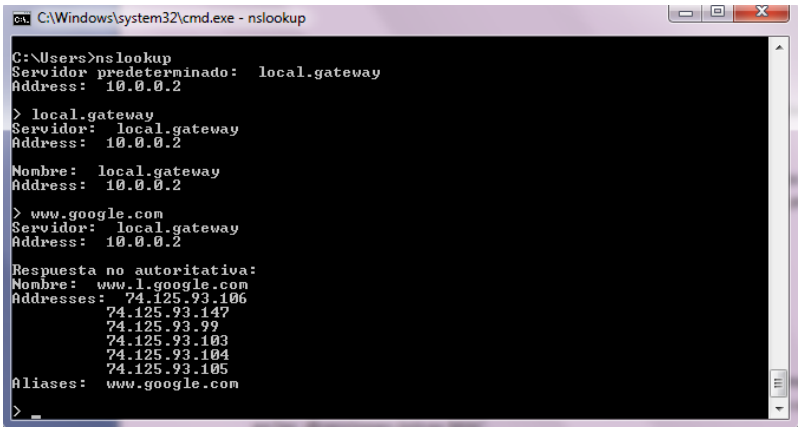


Figura 18. Comando Nslookup

2. 6 Configuración de una tarjeta de red en linux

En Linux, el comando **ifconfig** resulta lo mismo que en Windows el comando ipconfig, y nos ayuda a identificar las tarjetas de red que están activan en nuestro host.

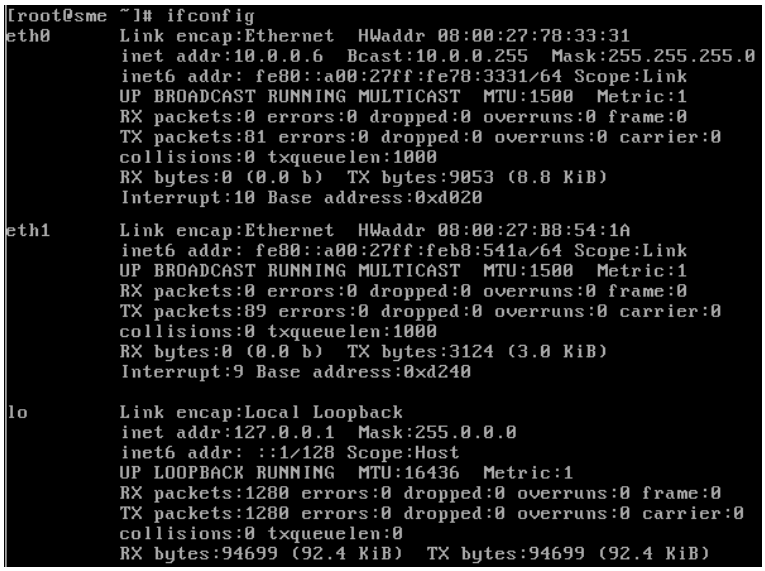


Figura 19. Comando ifconfig

- Para detener la interfaz de red eth0 se utiliza el comando ifdown eth0

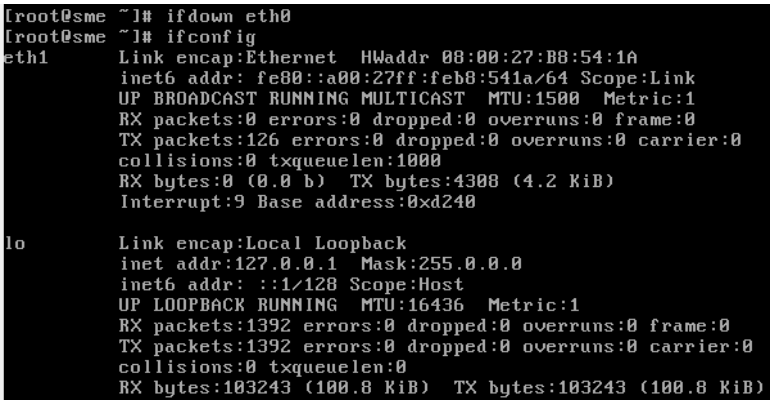


Figura 20. Interpretación del comando ifconfig

- Para iniciar la interfaz de red eth0 se utiliza el comando ifup eth0
- Para configurar una dirección IP estática:

ifconfig eth0 192.168.1.1 netmask 255.255.255.0

route add default gw 192.168.1.1

Otra forma de configurar las interfaces de red es modificando los archivos de configuración, por ejemplo:

vi /etc/sysconfig/network-scripts/ifcfg-eth2

Dependiendo de la interfaz de red el comando cambia al final eth0, eth1, etc.

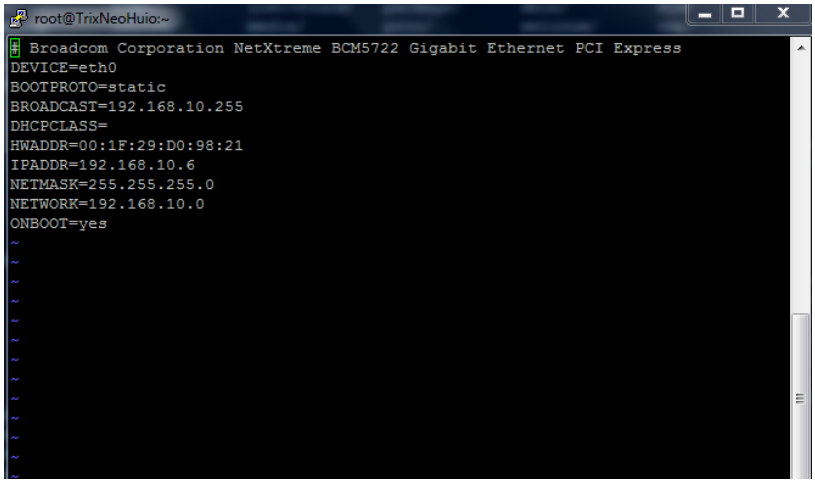


Figura 21. Interfaz de Red en Linux

En los capítulos siguientes se describirá más a fondo los diferentes parámetros de configuración, pero claramente se puede ver las configuraciones.

Nota: Para configurar el dhcp en la interfaz de red se cambia donde dice static a dhcp.

- Para reiniciar los servicios de red:

service network restart

2.7 Práctica No 1

CONFIGURACIÓN DE TARJETAS DE RED Y MANEJO DEL SOFTWARE PACKET TRACER

Basándonos en un archivo previamente configurado, se realizarán las pruebas y configuraciones de la práctica. El archivo que se usará para esta práctica será practica1.pkt.

Objetivos de la práctica:

- Configurar direcciones IP en PC0, PC1, PC2 en el simulador.
- Probar conectividad entre las máquinas con los comandos anteriormente revisados
- Determinar la funcionalidad del Gateway en las configuraciones

Resumen de la Práctica:

En la presente práctica el estudiante tendrá un primer acercamiento con el simulador Packet Tracer y realizará configuraciones de las tarjetas de red las computadoras del simulador en busca de enlazar una red pequeña de tres máquinas, dos de las cuales PC1 y PC2 se encuentran en la misma red, mientras que la PC0 se encuentra en otra red.

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED	GATEWAY
PC0	**NIC**	192.168.20.10	255.255.255.0	192.168.20.1
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC2	**NIC**	192.168.10.20	255.255.255.0	192.168.10.1
ROUTER0	**FA 0/0**	192.168.20.1	255.255.255.0	----------
	FA 0/1	192.168.10.1	255.255.255.0	----------

Tabla 1. Direccionamiento Práctica No1

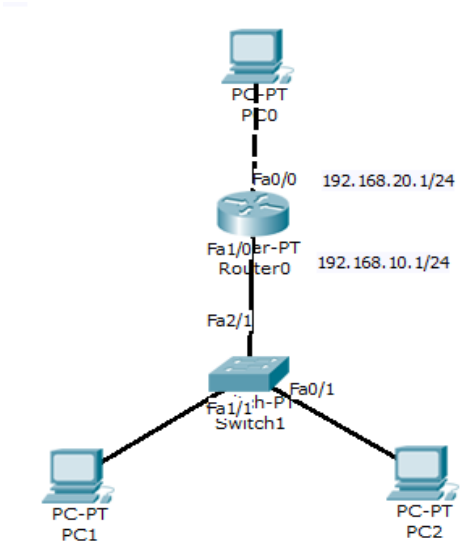


Figura 22. Topología Práctica No 1

1. Configurar las IPs de las PC0, PC1, PC2:

Dando doble clic sobre cada PC, se abre el cuadro de configuración y en la pestaña Desktop tenemos IP Configuración donde se podrá configurar los datos de la tabla 1 en las PCs.

2. Probar la configuración de la NIC de cada PC con el comando ipconfig.

En las configuraciones de la PC, en la pestaña Desktop en el icono CommandPromt, tenemos la misma funcionalidad de la línea de comandos de Windows (DoS)

Por ejemplo:

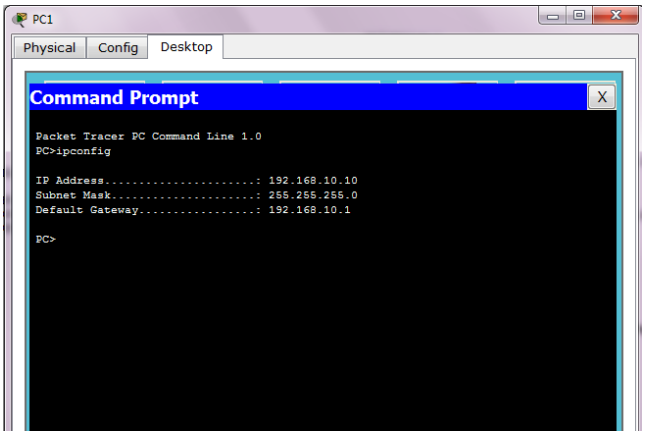


Figura 23. Comando ifconfig

Verificamos que los cambios de cada PC se hayan realizado correctamente, con las configuraciones de la IP correspondiente según se describe en la tabla 1.

Una de las principales pruebas que se pueden hacer para verificar problemas físicos de la tarjeta NIC, es hacer ping a un rango de direcciones de la red 127.0.0.0.

Por ejemplo:

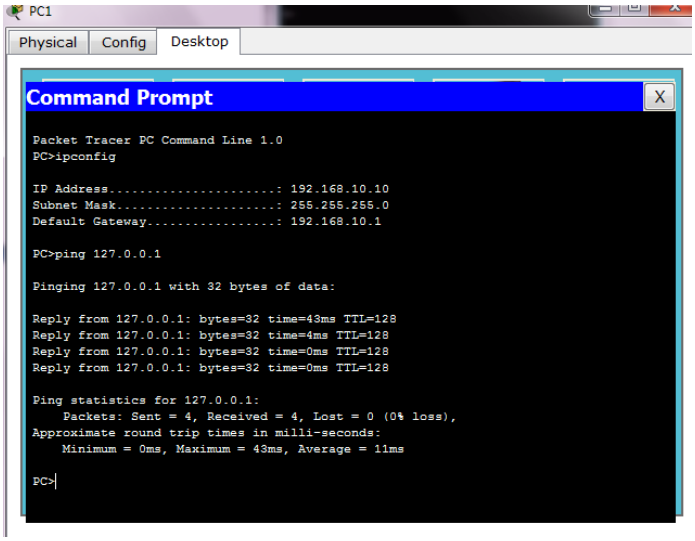


Figura 24. Comando Ping

Si el equipo responde estaremos seguros que físicamente la tarjeta de red está funcional y seguiremos con las pruebas de conectividad (Pruebas de Capa Fisca).

Otro de los problemas a nivel de capa física común es el correcto uso de los cables directo y cruzado según el dispositivo que se requiere conectar.

“Elementos de capas diferentes cable directo,
Elementos de capas iguales cable cruzado”

3. Conectar los equipos de acuerdo a la figura de la práctica, respetando las interfaces de cada equipo.

Recordar los conceptos de cables directos y cruzados.
Para realizar esta conexión:

- En el menú de la parte inferior de la ventana principal del simulador tenemos una figura en forma de rayo donde se encuentran los diferentes tipos de cables.

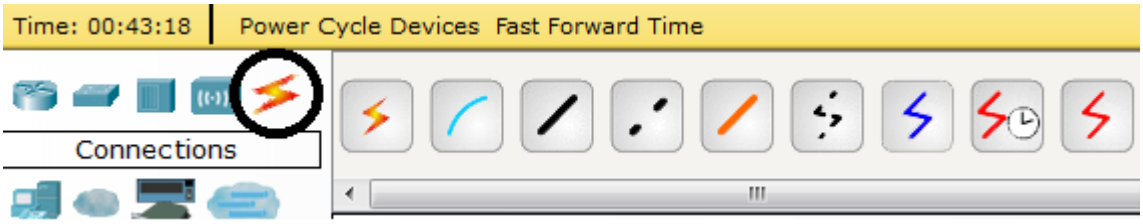


Figura 25. Menú de Cableado

Si colocamos el ratón sobre cada una de las opciones, se despliega el tipo de cable del que se trata.

4. Realizar pruebas de conectividad entre las PC de la topología.

    - Usando el comando ping realizar pruebas entra las PC0, PC1 y PC2
    - Usando el comando tracert realizar pruebas entre las PC0, PC1 y PC2
    - Tratar de identificar los saltos que realiza la traza al correr el comando tracert.
    - Eliminar las configuraciones de los Gateway de las máquinas y realizar las mismas pruebas de conectividad. Anotar los resultados y tratar de identificar porque hay ping entre las PC1 y PC2, pero no hay ping con la PC0.

5. Incluir conclusiones de la práctica determinando la funcionalidad de la dirección de Gateway en los equipos.

2.8 Práctica No 2

USO DE CABLE DIRECTO Y CABLE CRUZADO EN ELEMENTOS DE REDES

En la presente práctica se desarrolla la configuración de una red sencilla, en la cual se tendrá que seleccionar el cable correcto para las conexiones requeridas posteriormente.

Objetivos de la práctica:

- Cablear la topología propuesta
- Configurar direcciones IP en PC0, PC1, PC2 en el simulador.
- Probar conectividad entre las máquinas con los comandos anteriormente revisados

Resumen de la Práctica:

En la presente práctica el estudiante tendrá que aplicar los conocimientos adquiridos en el presenta capítulo y conectorizar los elementos propuestos con el cable correcto a mas de configurar la IPs de la computadoras como se reviso en la práctica No. 1 anterior.

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED	GATEWAY
PC0	**NIC**	192.168.20.10	255.255.255.0	192.168.20.1
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC2	**NIC**	192.168.10.20	255.255.255.0	192.168.10.1
ROUTER0	**FA 0/0**	192.168.20.1	255.255.255.0	----------
	FA 0/1	192.168.10.1	255.255.255.0	----------

Tabla 2. Direccionamiento Práctica No 2

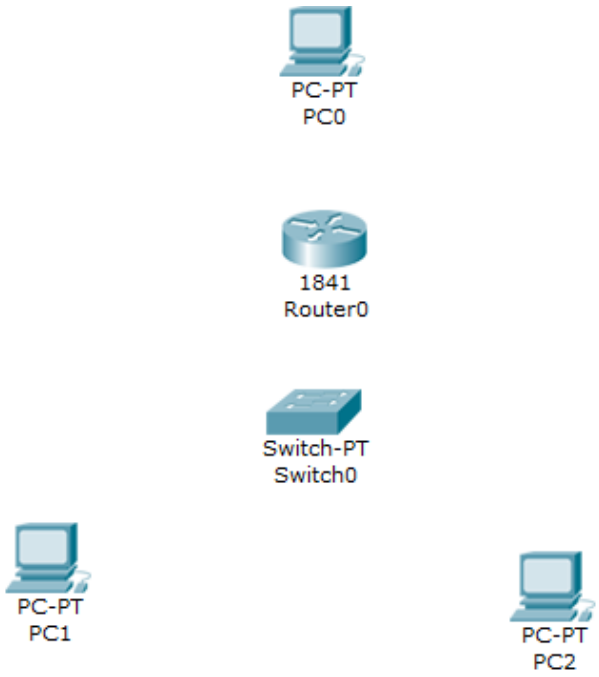


Figura 26. Topología Práctica No. 2

1. Conectorizar los elementos de la Práctica No. 2

De acuerdo a la Figura26 de la práctica cablear los equipos con cables directos o cruzados según sea el caso.

2. Configurar las IPs de las PC0, PC1, PC2:

De acuerdo a la Tabla 2 configurar las direcciones de los host de la Práctica No. 2

3. Probar la configuración de la NIC de cada PC con el comando ipconfig.

4. Realizar pruebas de conectividad entre las PC de la topología.

- Usando el comando ping realizar pruebas entra las PC0, PC1 y PC2
- Usando el comando tracert realizar pruebas entre las PC0, PC1 y PC2

Nota: Si los ping no responden, revisar nuevamente la topología y los cables usados para conectar los elementos.

5. Incluir conclusiones de la práctica determinando la funcionalidad del cable directo y cable cruzado.

CAPÍTULO III

CONCEPTOS Y CONFIGURACIONES DE NETWORKING DE ELEMENTOS DE CAPA DOS (MODELO OSI)

En este capítulo se desarrollarán conceptos sobre configuraciones básicas de elementos de capa dos como los switchs.

Antes de comenzar con las configuraciones de los equipos, se requieren tener claros conceptos básicos de tipos de tráfico en la red.

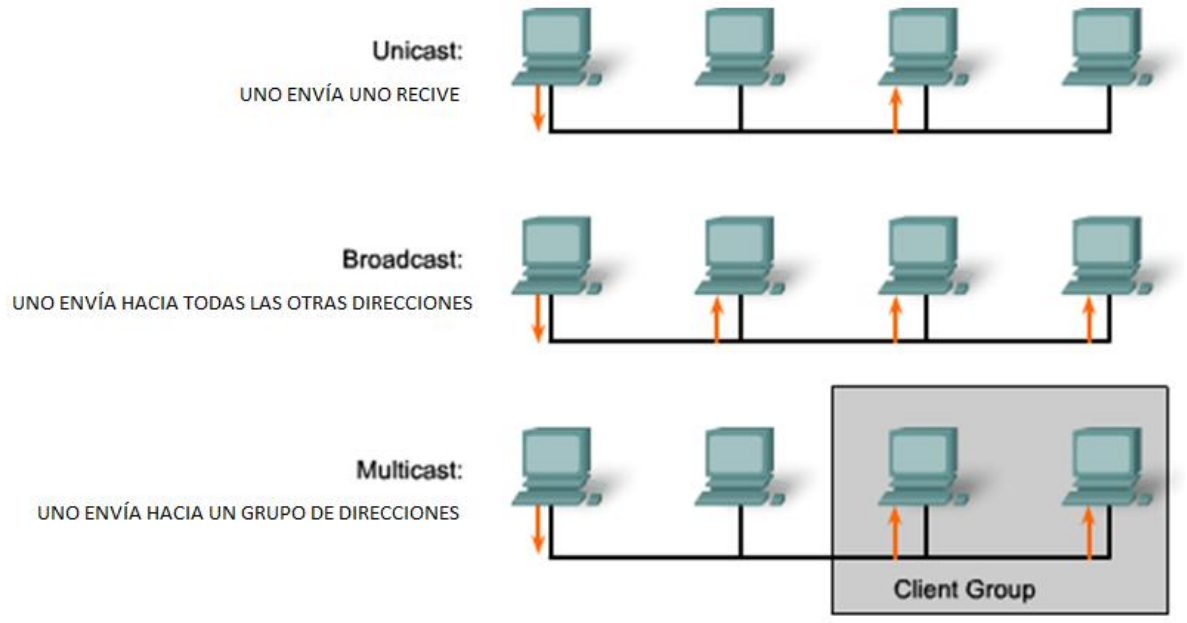


Figura 27. Tipos de Tráfico

Los switchs son dispositivos que retransmiten las tramas de broadcast. Cuando un switch recibe una trama de broadcast, la retransmite a cada uno de sus puertos con excepción del puerto en donde la recibió.

3.1 Tipos de Switchs

Existen diferentes tipos de switchs que manejan tráficos de capa 2 y capa 3. A continuación se hace una pequeña comparación entre estos tipos de equipos para entender el concepto.

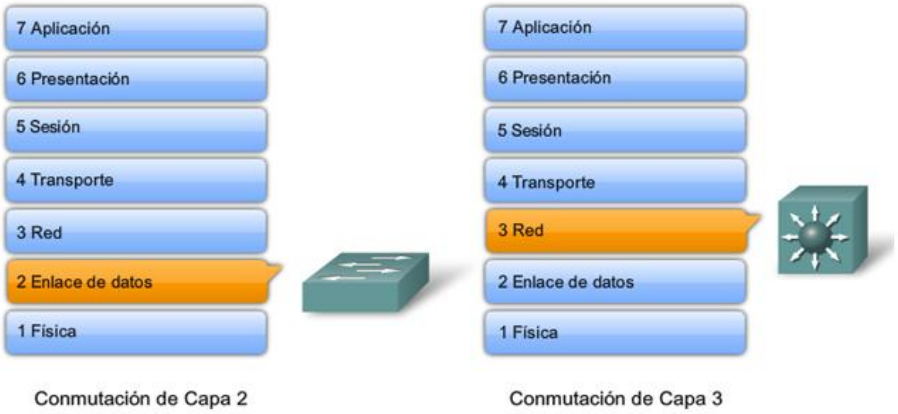


Figura 28. Capas de Trabajo del Switch Capa 2 y Capa3

3.1.1 Switch de Capa 2:

- Los switch de capa 2 realizan el proceso de conmutación basándose en la dirección física de capa 2 y en la tabla de direcciones MAC que se almacenan en el equipo.

3.1.2 Switch de Capa 3:

- Los switch de capa 3 pueden basar sus decisiones de conmutación en la dirección IP de los paquetes para reenviar por el puerto correspondiente.

Para determinar si un equipo es de capa 2 o capa 3 se puede verificar en catálogos o mediante el siguiente procedimiento:

- Simbología

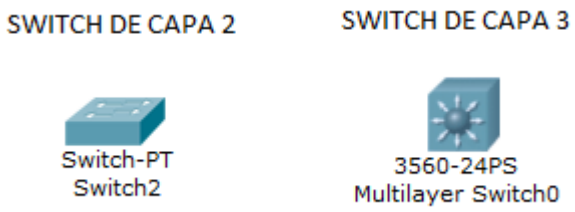


Figura 29. Switch Capa 2 y Capa 3

- Mediante configuraciones

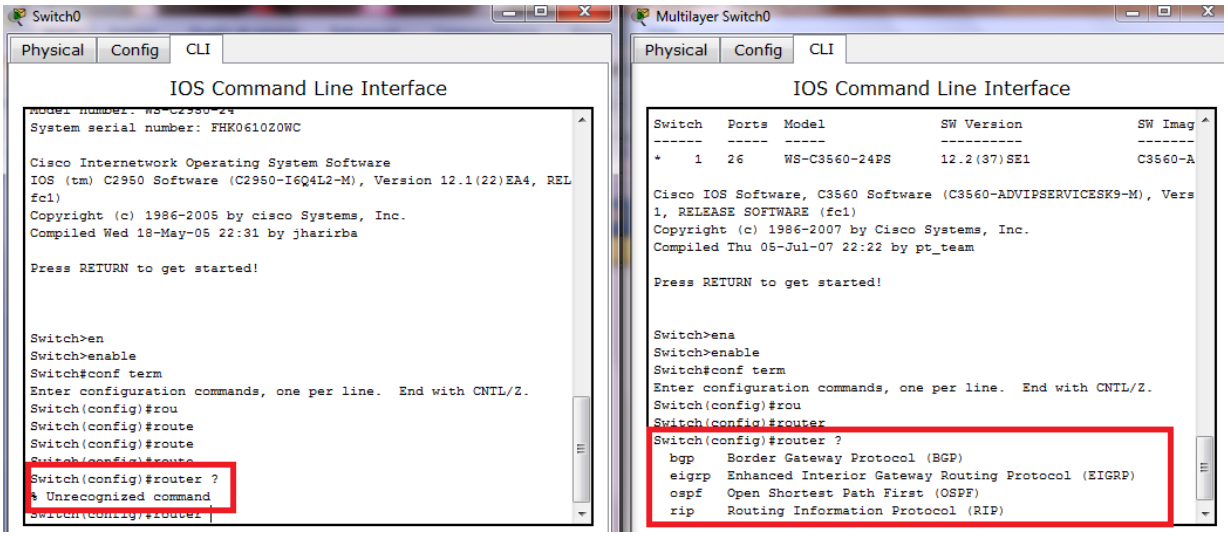


Figura 30. Menú de Ruteo en consola

En la Figura 30 se puede identificar el menú que se despliega en el switch Capa 3 al introducir el comando router para ver los protocolos de ruteo que admite el equipo (parte derecha), mientras que el switch Capa 2 no despliega ningún protocolo de enrutamiento (parte izquierda).

3.2 Casos de uso de cada equipo

- Switch Capa 2: Este equipo es usado en la capa de acceso, donde no se requiere procesamiento ni enrutamiento.
- Switch Capa 3: Este equipo es usado es usado en la capa de distribución y en la capa de núcleo, donde se requiere de mucho procesamiento y enrutamiento de capa 3.

Para realizar las configuraciones básicas de un switch, se requiere de una conexión que dependiendo de la marca y modelo del equipo puede ser vía WEB (Desde cualquier explorador de Internet) o por puerto de consola en el equipo. Para este último se usa el hyperterminal en el computador y en el switch se requiere un puerto de consola, y se procede a configurar el hyperterminal con las configuraciones que remita el fabricante y para la conexión se usa el cable que se indica en la Figura 30, el cual es propio de cada equipo.

3.3 Conexión al puerto de consola

Físicamente lo que se requiere para configurar un switch es:

- Switch con un puerto de consola
- Cable de consola del switch

- Máquina con hyperterminal instalado
- Máquina con puerto serial ó un cable conversor de serial a USB.

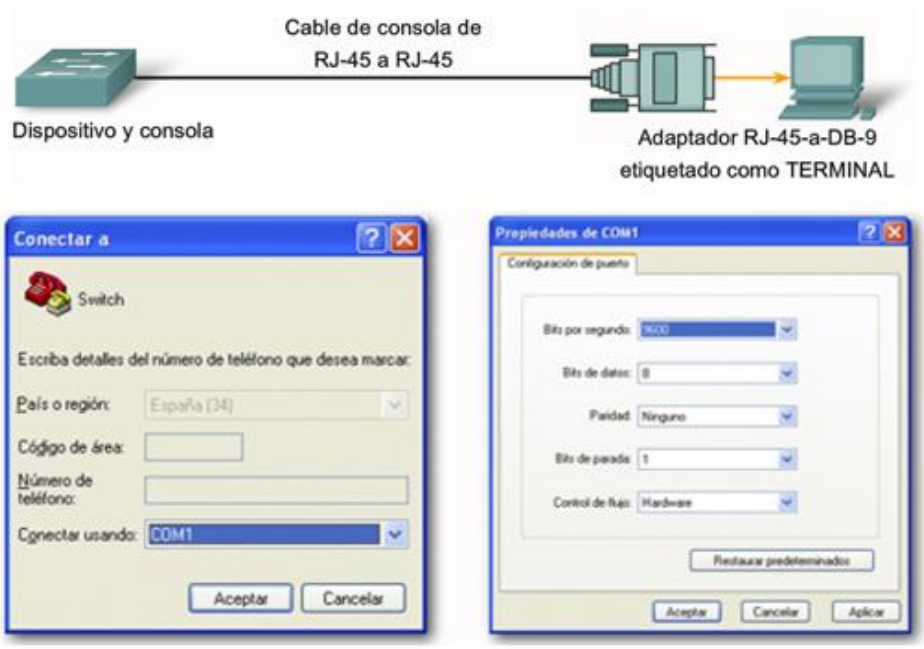


Figura 31. Cable de Consola

Una vez conectado el switch con el cable de consola a la máquina, se corre el hyperterminal y aparece la pantalla que se muestra en la Figura 31, en la cual se selecciona Conectar usando: COM1 dependiendo de puerto serial al que se conectó el cable de consola en la máquina.

Por lo general la configuración de los equipos switch cisco, tiene las siguientes configuraciones de transmisión para conexión por el puerto de consola.

Bits por segundo: 9600
Bits de Datos: 8
Paridad: Ninguno

Bits de Parada: 0

Control de flujo: Hardware

3.4 Práctica No 3

REALIZAR CONFIGURACIONES BÁSICAS EN UN SWITCH CAPA 2.

Objetivos de la práctica:

- Armar la topología propuesta.
- Realizar las configuraciones básicas de un switch, por medio del cable de consola.
- Familiarizar al estudiante con el entorno del hyperterminal y la conexión por el cable de consola.

Resumen de la Práctica:

En la presente práctica el estudiante tendrá que armar la topología propuesta ayudándose de los conocimientos adquiridos en la práctica anterior. Se realizarán configuraciones básicas del switch por medio de un cable de consola.

Figura 32. Topología Práctica No 3

1. Armar la topología propuesta.

- Elegir los elementos de la topología en el simulador en los cuadros de Switchs y End devices.
- Elegir un switch – PT genérico.
- En el cuadro de cables, seleccionar el cable de consola para realizar la conexión.
- Conectar en la PC0 el puerto RS 232 y en el switch el puerto console.

2. Realizar la conexión de la PC al switch por medio del hyperterminal.

- En la PC0 en las configuraciones en la pestaña desktop, entramos en el terminal a realizar las configuraciones del mismo para conectarnos con el switch.

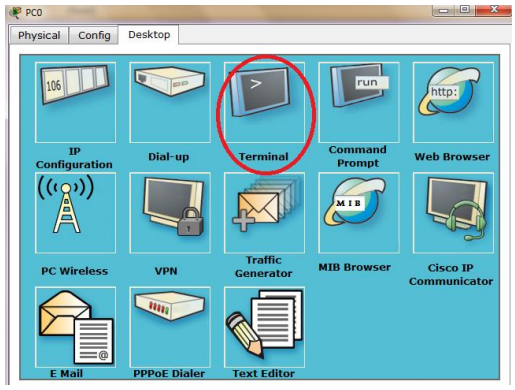


Figura 33. Pantalla del Terminal

- Realizar las configuraciones antes revisadas.

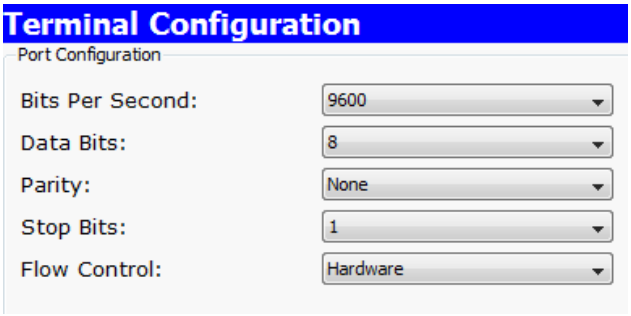


Figura 34. Configuración del Telminal

- Si aparece una pantalla como la de la figura, esta lista la conexión para comenzar con la configuración del switch.

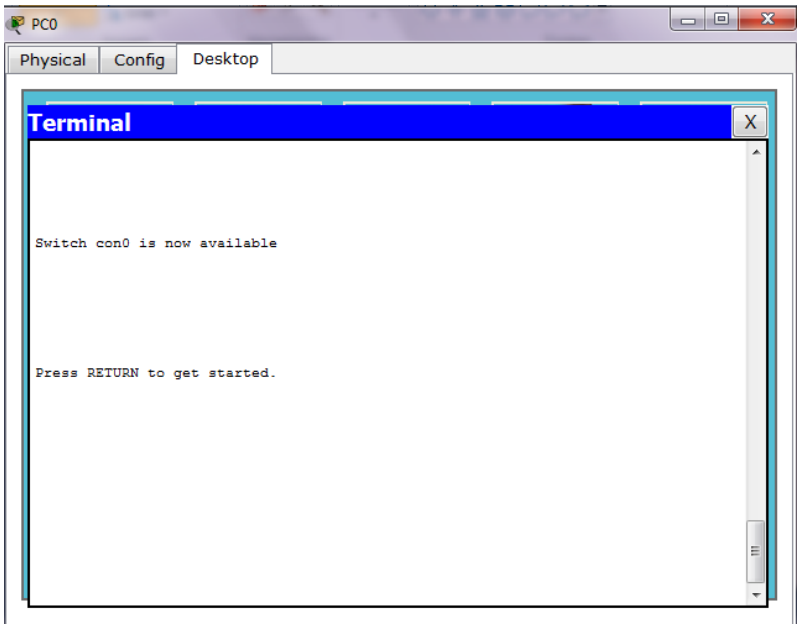


Figura 35. Pantalla del Terminal

3. Configuraciones básicas del switch:

Por razones de seguridad, el switch tiene dos niveles de acceso a los comandos para las configuraciones:

- **Modo EXEC usuario:** Las tareas típicas incluyen la verificación del estado del switch. En este modo no se permiten cambios en la configuración del switch.

- **Modo EXEC privilegiado:** Las tareas típicas incluyen cambios a la configuración del swich.

En una primera instancia presionando Enter se ingresa al modo EXEC usuario, en donde tenemos comandos de verificación del equipo. Al ingresar el símbolo "?" en este nivel, se despliegan los comando para este modo y una breve descripción de cada uno.

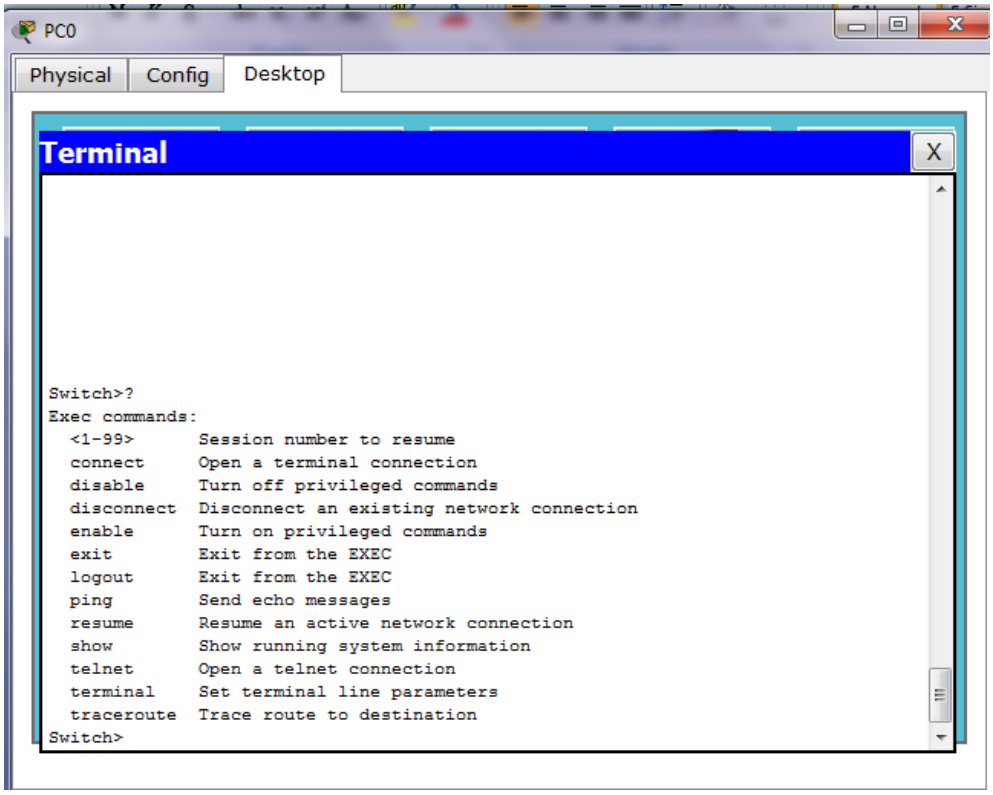


Figura 36. Configuración del Switch

En este momento podemos reconocer uno de los comando usados en la práctica anterior, el comando ping. Cada opción que se despliega, tiene submenús con más comandos que permiten verificar la operación del equipo.

Para acceder al conjunto completo de comandos para configurar el switch, se debe ingresar al modo EXEC privilegiado.

En esta práctica se van a configurar cosas básicas del switch como son las siguientes:

- Contraseñas: Línea de Consola, Línea VTY, modo EXEC privilegiado (para configurar el switch),
- Nombre del switch
- Banner de advertencia de ingreso no autorizado.

Ingresar los siguientes comandos de configuración básica de un switch:

Switch>enable	(Habilita el modo EXEC privilegiado)
Switch#configure terminal	(Entramos a configurar el terminal)

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

Switch (config) #hostname S1	(Nombre del Equipo “S1”)
S1(config)#line console 0	(Ingreso a configuraciones de la consola)
S1(config-line)#password cisco	(Password para el ingreso a la consola)
S1(config-line)#login	(Guardamos cambios realizador en la consola)
S1(config-line)#exit	(Salimos al menú anterior)
S1(config)#line vty 0 15	(Ingresamos a la línea para conexiones remotas)
S1(config-line)#password cisco	(Ponemos password a las conexiones remotas)

S1(config-line)#login (Guardamos cambios realizados en la línea de conexiones remotas)

S1(config-line)#exit (Salimos al menú anterior)

S1(config)#enablepassword clase (Ponemos password para ingresar al modo EXEC privilegiado)

S1(config)#enablesecret clase (Ponemos password secreta para ingresar al modo EXEC privilegiado)

S1(config)#banner motd #CUIDADO ACCESO SOLO PERSONAL AUTORIZADO# (Banner de seguridad)

Es importante notar el cambio del signo > a # cuando entramos en el modo EXEC privilegiado donde podremos realizar cambios en la configuración del switch.

Otro de los cambios que es importante notar es el del nombre al cambiar el hostname del equipo por S1 (Puede ingresar cualquier nombre para el equipo).

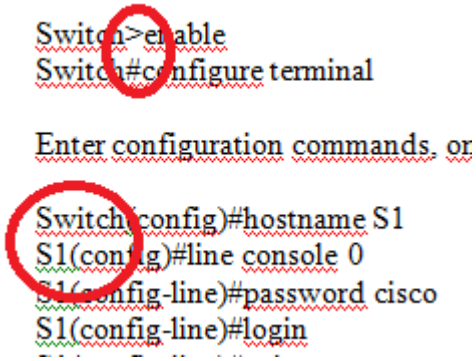


Figura 37. Modos de configuración switch y el hostname

Se procede a salir de la configuración:

S1(config)#exit

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

S1#exit

Es importante tener en cuenta el comando login antes de salir de las configuraciones de las líneas tanto de consola como vty, si no se ingresa éste comando y salimos de las líneas de consola, no se guardarán los cambios de las líneas.

Al salir del terminal, al volver a ingresar, nos pedirá las contraseñas de consola y de enable (password para ingresar al modo EXEC privilegiado)

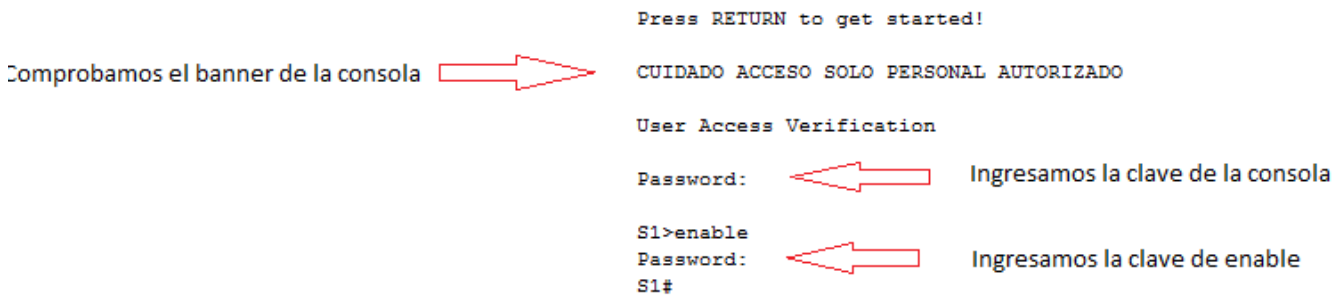


Figura 38. Banner y Contraseñas de acceso

4. Comprobar las configuraciones realizadas

Con el comando S1#show running-config en modo privilegiado, podemos ver las configuraciones que hemos realizado en el equipo y toda la información del switch.

En la figura se puede observar el resultado del comando show running-config, se puede ver el hostname "S1" del equipo, la clave la clave de ingreso al modo EXEC privilegiado (enablesecret) "5 1mERr$ZIvuLWaqZSN.IGTvVO7VE/" y la clave de ingreso al modo EXEC privilegiado (enablepassword) "cisco". Como se puede ver tenemos dos password para ingresar al modo EXEC privilegiado, la primera enablesecret es encriptada, por lo cual no se puede ver al momento de realizar un show running-config, mientras que la segunda, no es encriptada y si se puede ver en el show running-config. Al momento de ingresar a la consola y cambiar al modo privilegiado tendremos que poner la password de enablesecret, ya que como es más segura el sistema la toma como clave para el ingreso al modo privilegiado de configuración del terminal.

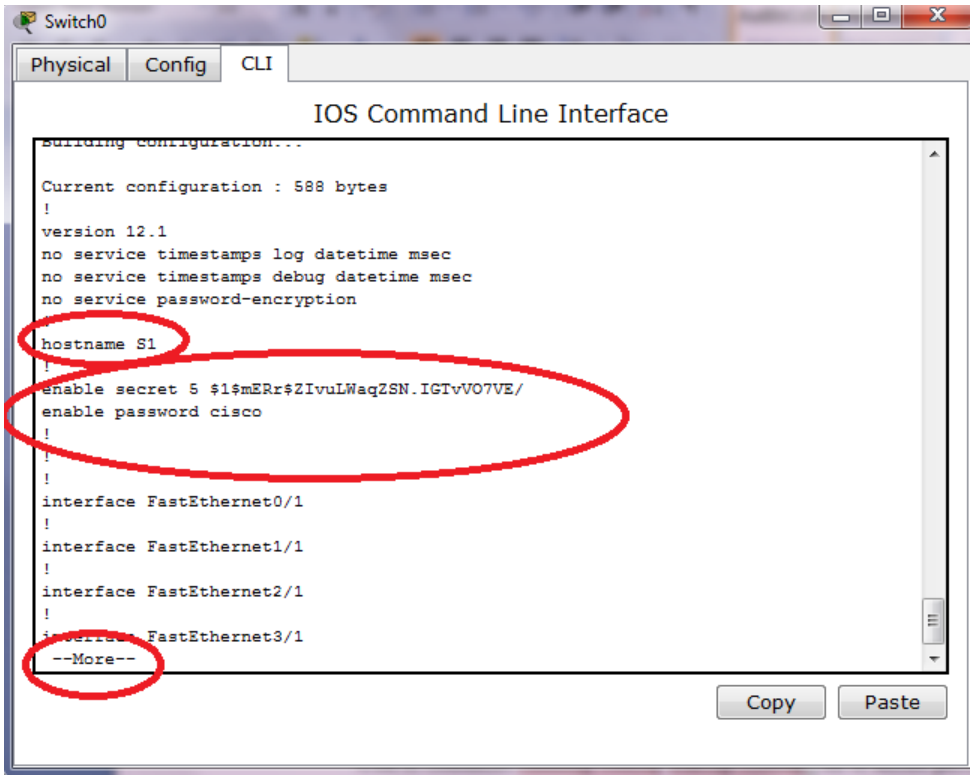


Figura 39. Comando Show Run

El --More-- indica que hay más en la pantalla para mostrar. Con la tecla enter avanzamos línea por línea y con la barra espaciadora avanzamos toda una pantalla.

En la siguiente pantalla podemos verificar el banner y las contraseñas de líneas de consola y de líneas VTY.

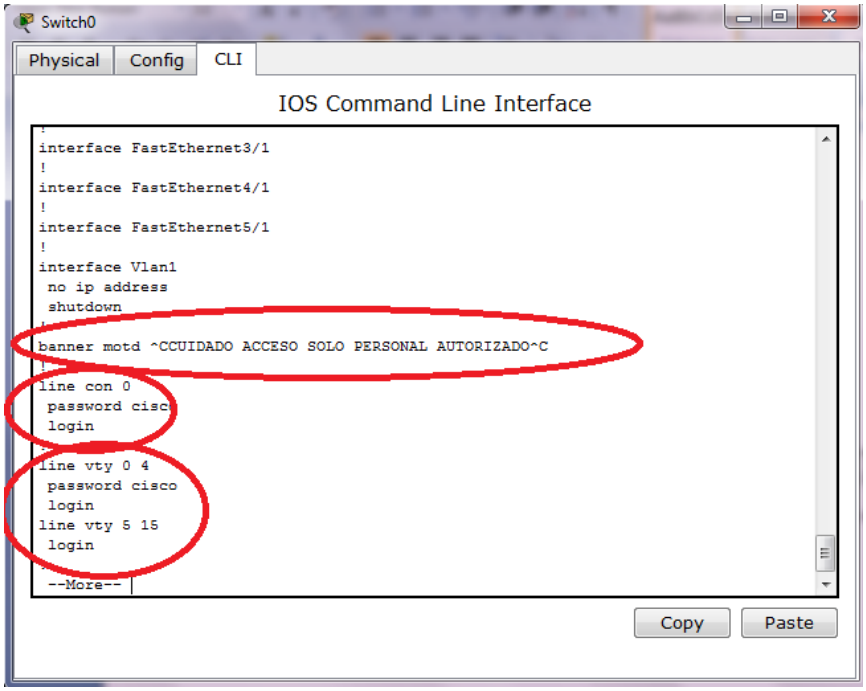


Figura 40. Comando Show Run y configuraciones iniciales

5. Guardar las configuraciones en la memoria del switch.

Con el comando running-configstartup-config , en el modo privilegiado, todos los cambios se van a guardar en la memoria del switch. Si no corremos este comando, al apagar o resetear el equipo, todas las configuraciones se perderán.

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

En este momento podemos apagar y volver a encender el equipo y todas las configuraciones estarán grabadas en la memory de arranque del switch.

Otra forma de guardar las configuraciones en la memoria del terminal es con el comando write que tiene el mismo efecto que el comando anterior:

```
S1#write
Building configuration...
[OK]
S1#
```

6. Anotar conclusiones de la presente práctica.

3.5 VLAN (Red Virtual de Área Local)

Una VLAN (acrónimo de Virtual LAN) es una subred IP separada de manera lógica, las VLAN permiten que redes IP y subredes múltiples existan en la misma red conmutada, son útiles para reducir el tamaño del broadcast y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos para una empresa, oficina, universidades, etc.) que no deberían intercambiar datos usando la red local, aumentando la seguridad del entorno.

Cada computadora de una VLAN debe tener una dirección IP y una máscara de subred correspondiente a dicha subred.

3.6 Beneficios de las VLAN:

- Mejor Rendimiento
- Mayor Seguridad
- Mitigación de tormenta de broadcast

3.7 Tipos de VLAN:

3.7.1 VLAN DE DATOS: Una VLAN de datos es una VLAN configurada para enviar solo tráfico de datos. Por un switch puede pasar tráfico de datos, de administración, etc.

3.7.2 VLAN PREDETERMINADA: por lo general los switch vienen con la VLAN 1 por defecto como predeterminada y todos los puertos están

asignados a esa VLAN 1. Esta VLAN predeterminada no se puede renombrar no borrar. Por seguridad se recomienda cambiar los puertos de la VLAN PREDETERMINADA.

3.7.3 VLAN NATIVA: Se asigna una VLAN nativa a un puerto trocal 802.1Q Los puertos troncales admiten el tráfico que llega de muchas VLANs. Éste se conoce como tráfico etiquetado.

3.7.4 VLAN DE ADMINISTRACION: Una vlan de administración es cualquier vlan que se configura para acceder a las capacidades administrativas del switch. Se asigna una dirección ip y una máscara de subred a la vlan de administración. Por defecto la VLAN de administración es la VLAN 1.

3.8 Rangos de ID para las VLANs

3.8.1 VLAN de rango normal:

- Utilizado en redes pequeñas y medianas
- Rango de 1 a 1005 (1 y 1002-1005 existen por defecto y no pueden ser eliminadas)
- Las VLAN 1002-1005 se reservan para la VLAN token ring y FDDI, en el desarrollo de la monografía no se explorara estos temas, pero se recomienda su revisión.
- Las configuraciones de VLAN se guardan en el archivo VLAN.dat almacenado en la memoria del switch.

3.8.2 VLAN extendidas:

- Utilizadas en empresas globales con mayor cantidad de clientes (1006-4094)
- Su configuración se almacena en el archivo de configuración en el archivo en ejecución. (running-config)

3.9 Aspectos importantes al momento de configurar VLANs:

- Los puertos del switch son interfaces de capa 2 y no manejan enrutamiento.
- Cuando se configura una VLAN se le deba asignar un numero ID y se le puede asignar un nombre a la VLAN.
- Una de las maneras de configurar una VLAN es asignar los puertos manualmente a determinada VLAN.

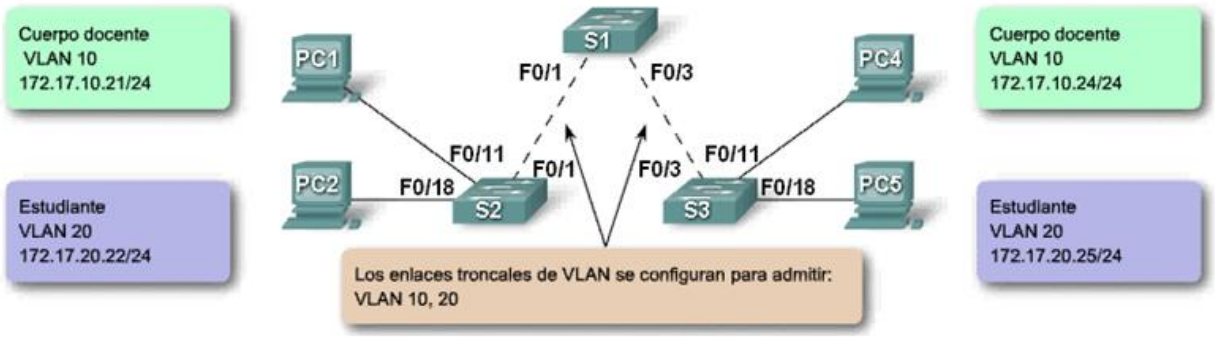


Figura 41. Topología Clásica de VLANs

3.10 Práctica No. 4

CONFIGURACIÓN BÁSICA DE VLANS

Objetivos de la práctica:

- Armar la topología de la red propuesta en la práctica
- Configurar direcciones IP en PC0, PC1, PC2, PC4 y PC5 en el simulador.
- Realizar las configuraciones básicas del switch revisadas en la práctica anterior.
- Configurar las VLANs de Administración, Estudiantes y de Servidores.
- Administrar la tabla de direcciones MAC del switch.
- Asignar direcciones MAC estáticas a los servidores.
- Examinar y verificar las configuraciones.

Resumen de la Práctica:

En la presente práctica el estudiante tendrá que configurar una red básica para una universidad la cuál contiene un área administrativa, de estudiantes y de servidores. Estas tres áreas tienen que estar lógicamente separadas para evitar tráfico innecesario en la red y por razones de seguridad los estudiantes no deben tener acceso a los servidores de notas. Para cumplir con estos requerimientos se debe separar cada red por medio de VLANs.

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED	GATEWAY
PC0	**NIC**	192.168.1.10	255.255.255.0	192.168.1.1
PC1	**NIC**	192.168.5.10	255.255.255.0	192.168.5.1
PC2	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC3	**NIC**	192.168.1.20	255.255.255.0	192.168.1.1
PC4	**NIC**	192.168.5.20	255.255.255.0	192.168.5.1
PC5	**NIC**	192.168.10.20	255.255.255.0	192.168.10.1
S1	**VLAN 10**	192.168.1.1	255.255.255.0	192.168.99.1
	VLAN 20	192.168.5.1	255.255.255.0	192.168.99.1
	VLAN 30	192.168.10.1	255.255.255.0	192.168.99.1
	VLAN 99	192.168.99.1	255.255.255.0	192.168.99.1

Tabla 3. Direccionamiento Práctica No. 4

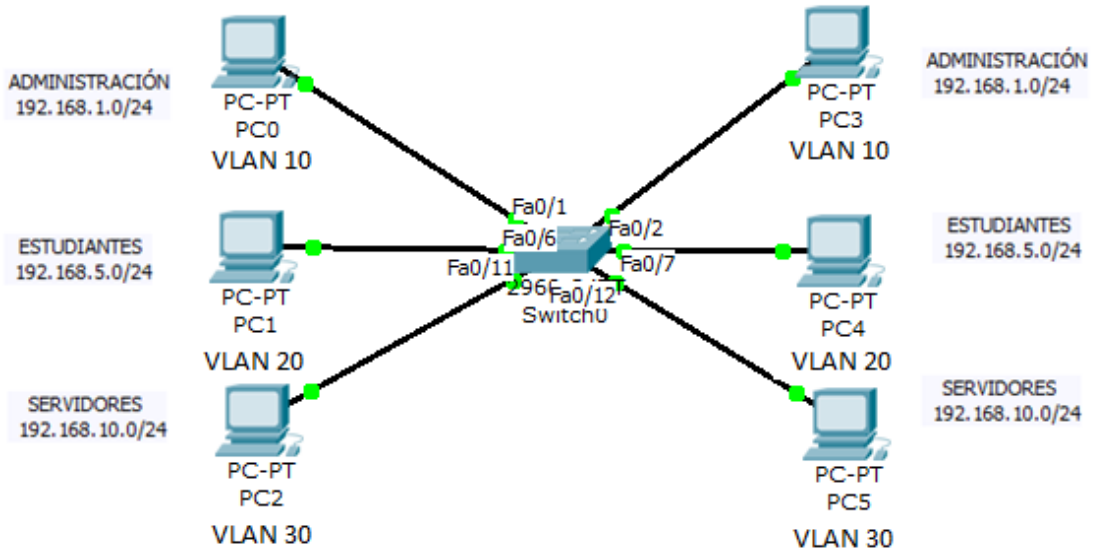


Figura 42. Topología Práctica No 4

1. Configurar las ips de las PC0, PC1, PC2, PC3, PC4 y PC5, de acuerdo a la tabla de direccionamiento.

2. Realizar las configuraciones básicas del switch revisadas en la práctica anterior.

    - Nombre del host,
    - Password de la línea de consola,
    - Password de la línea VTY,
    - Password de enable (modo privilegiado),
    - Banner de advertencia de la consola.

3. Revisar las configuraciones básicas del switch con el comando show running-config y corregir si falta alguna.

Nota: Levar un registro de las contraseñas y passwords que se configuran en el equipo.

DESCRIPCIÓN	**PASS**
Password Línea de Consola	
Password Línea VTY	
EnableSecret	

4. Configuración de las VLAN en el switch:

    - Crear las Vlan

Utilice el comando **vlan***vlan-id* en modo de configuración global (S1#configure terminal) para añadir una VLAN al switch S1. Para esta práctica se tienen 3 Vlan:

VLAN 10: Administrativa
VLAN20 Estudiantes
VLAN 30 Servidores

Después de crear las VLAN, estará en modo de configuración de vlan, donde puede asignar un nombre para la VLAN mediante el comando **name** *vlanname*

S1(config)# vlan 10
S1(config-vlan)#name Administration
S1(config-vlan)# vlan 20
S1(config-vlan)#name Estudiantes
S1(config-vlan)# vlan 30
S1(config-vlan)#name Servidores
S1(config-vlan)#end
S1#

Para verificación de las vlans creadas en el S1 tenemos los siguientes comandos. Dentro del comando show vlan tenemos:

S1#show vlan ?

brief VTP all VLAN status in brief
id VTP VLAN status by VLAN id
name VTP VLAN status by VLAN name
<cr>

Para verificar que las vlan estén correctamente creadas en el switch introducimos el comando:

S1#show vlanbrief

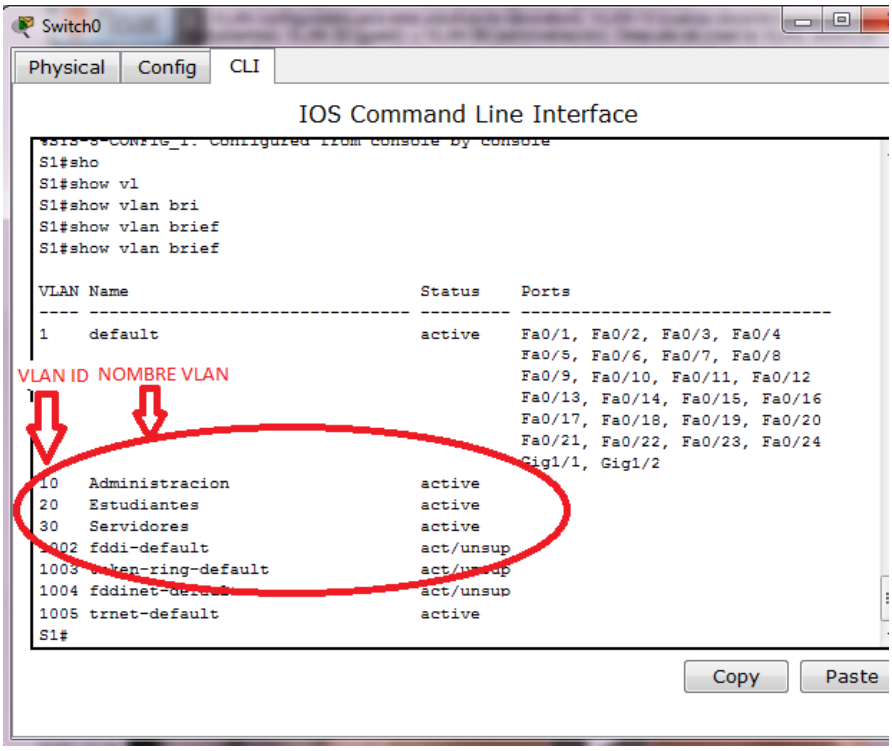


Figura 43. Comando Show VlanBrief

Asignar puertos del switch S1 a la Vlan correspondiente, según la topología de la práctica.

PUERTOS	ASIGNACIÓN	RED
Fa0/1-Fa0/5	VLAN 10: Administración	192.168.1.0/24
Fa0/6-Fa0/10	VLAN 20: Estudiantes	192.168.5.0/24
Fa0/11-Fa0/15	VLAN 30: Servidores	192.168.10.0/24

Tabla 4. Asignación de puertos a las Vlan

Consulte la Tabla 4 para la asignación de puertos. Los puertos se asignan a las VLAN en modo de configuración de interfaces, utilizando el comando **switch port access vlan** *vlan-id* . Puede asignar cada puerto en forma individual o se puede utilizar el comando

interface range para simplificar la tarea.

Por ejemplo para asignar el puerto Fast Ethernet 0/1 del switch S1 a la Vlan 10 de administración se procede de la siguiente manera:

S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface fastEthernet 0/1 (ingresamos al modo de configuración de interfaces)
S1(config-if)#switchportmodeaccess (configura el puerto en modo de acceso)
S1(config-if)#switchportaccessvlan 10 (asigna el puerto fast 0/1 a la vlan 10)
S1(config-if)#no shutdown (Prende la interfaz si estuviera apagada)

Para asignar un rango de puertos a una vlan determinada se procede de la siguiente manera:

S1(config)#interface rangefastEthernet 0/6 – 10 (ingresamos al modo de configuración de un rango de interfaces)
S1(config-if-range)#switchportmodeaccess (configura el rango de interfaces en modo de acceso)
S1(config-if-range)#switchportaccessvlan 20 (asigna los puertos del fast 0/6 al 10 a la vlan 20)
S1(config-if-range)#no shutdown (prende las interfaces si estuvieran apagadas)
S1(config-if-range)#end (sale al modo de configuración global)
%SYS-5-CONFIG_I: Configured from console by console
S1#

- Verificar la configuración de las Vlans

Con el comando S1#show vlanbrief en modo de configuración global se puede verificar que los puertos de las vlan de acuerdo a la tabla 2, queden de la siguiente manera:

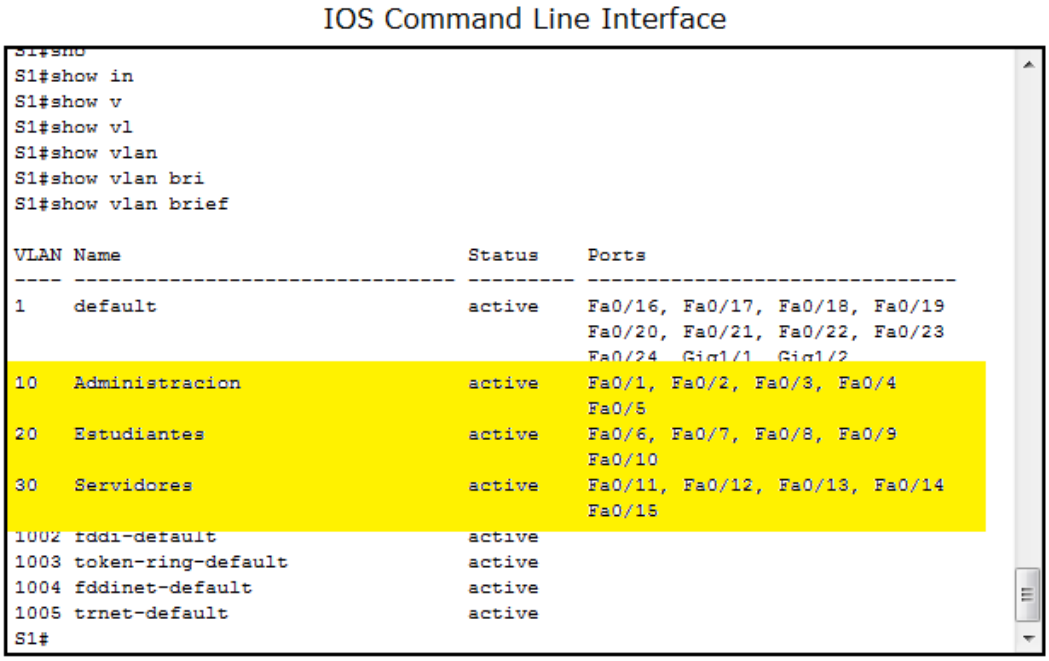


Figura 44. Revisión del Comando Show vlanbrief

En la Figura 44 claramente se puede ver que los puertos que no se agregaron a las vlans configuradas por defecto vienen agregados en la VLAN por default la VLAN 1. En esta parte de la práctica es importante apagar los puertos del switch que no se usan, para evitar futuros problemas de seguridad y consumo innecesario del switch. Para èsto se procede con el mismo concepto del rango de interfaces para evitarnos el apagar puerto por puerto.

S1(config)#interface range fastEthernet 0/16 - 24
S1(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#

Al realizar esta configuración se muestra en tiempo real la desactivación de los puertos dentro del rango seleccionado.

Si conectásemos un host a uno de estos puertos desactivados, no habría respuesta del equipo S1, ni de la NIC del host.

5. Verificación de conectividad.

Probar concetividad entra las máquinas de la misma VLAN 10, VLAN 20, VLAN 30, y entre las diferentes vlans y anotar los resultados.

6. Guardar la configuraciones del S1 con el comando:

   S1#wr

7. Incluir las conclusiones de la conectividad en las PCs.

3.11 Puertos troncales

Un enlace troncal es un enlace punto a punto entre los dispositivos de la red que llevan más de una vlan. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switchs y routers. Permite además extender las vlan a través de toda una red.

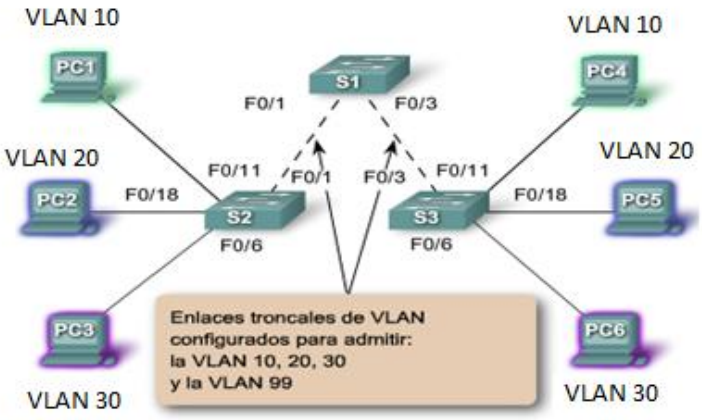


Figura 45. Puertos Troncales

Sin un puerto troncalizado, para comunicar las vlans por la red se necesitarían un cable por cada vlan.

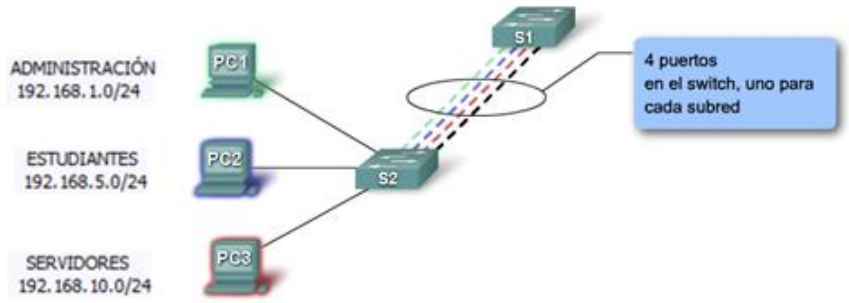


Figura 46. Puerto Troncalizado

La finalidad de un puerto troncalizado es concentrar todas las subredes, vlans, en un solo cable, ahorrando puertos del switch.

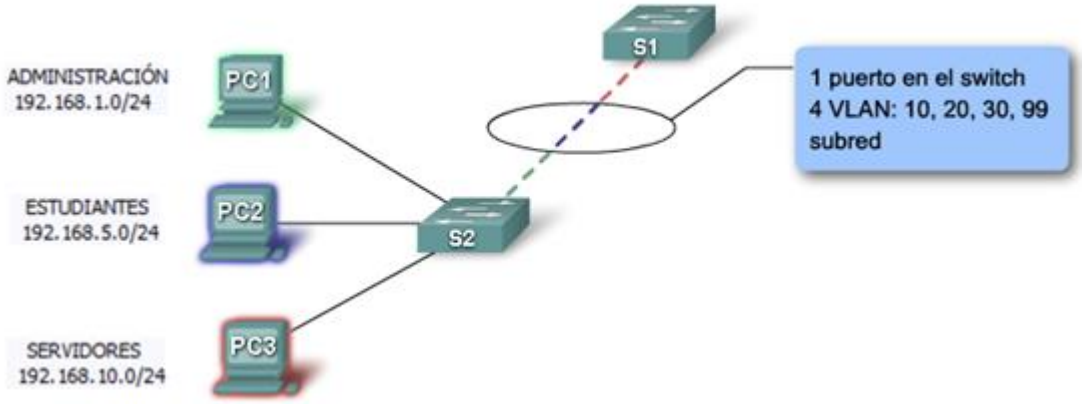


Figura 47. Puerto Troncalizado

3.11.1 Configuración de un enlace troncal 802.1Q en un Switch:

Ciscoredes# configure terminal

Ciscoredes(config)# interface interface-id

Ciscoredes(config-if)# switchport mode trunk

Ciscoredes(config-if)# switchport trunk native vlanvlan-id

Ciscoredes(config-if)# exit

Donde:

- interface .- Comando para entrar al modo de configuración de interfaz.
- Interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0
- Switchportmodetrunk .- Definir que el enlace que conecta a los switches sea un enlace troncal
- Switchport trunk native vlanvlan-id .-Especificar otra VLAN como la VLAN nativa para los enlaces troncales.

3.12 Práctica No. 5

CONFIGURACIÓN DE PUERTOS TRONCALES

Objetivos de la práctica:

- Armar la topología de la red propuesta en la práctica
- Configurar direcciones IP en PC0, PC1, PC2, PC4 y PC5 en el simulador.
- Realizar las configuraciones básicas del switch.
- Configurar las VLANs de Administración, Estudiantes, Servidores y control en S1, S2 y S3.
- Configurar los puertos trunk de los switchs.
- Examinar y verificar las configuraciones.

Resumen de la Práctica:

En la presente práctica el estudiante tendrá que configurar una red básica para una universidad la cuál contiene un área administrativa, de estudiantes y de servidores. Estas tres áreas están en edificios separados y también tiene que estar lógicamente separadas para evitar tráfico innecesario (broadcast) en la red y por razones de seguridad los estudiantes no deben tener acceso a los servidores de notas. Para cumplir con estos requerimientos se debe separar cada red por medio de VLANs y unir cada equipo de la misma LAN mediante puertos troncalizados.

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED	GATEWAY
PC0	**NIC**	192.168.1.10	255.255.255.0	192.168.1.1
PC1	**NIC**	192.168.5.10	255.255.255.0	192.168.5.1
PC2	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC3	**NIC**	192.168.1.20	255.255.255.0	192.168.1.1
PC4	**NIC**	192.168.5.20	255.255.255.0	192.168.5.1
PC5	**NIC**	192.168.10.20	255.255.255.0	192.168.10.1
PC6	**NIC**	192.168.50.2	255.255.255.0	192.168.50.1
S1	**VLAN 50**	192.168.50.10	255.255.255.0	No aplica
S2	**VLAN 50**	192.168.50.20	255.255.255.0	No aplica
S3	**VLAN 50**	192.168.50.30	255.255.255.0	No aplica

Tabla 5. Direccionamiento Práctica No. 5

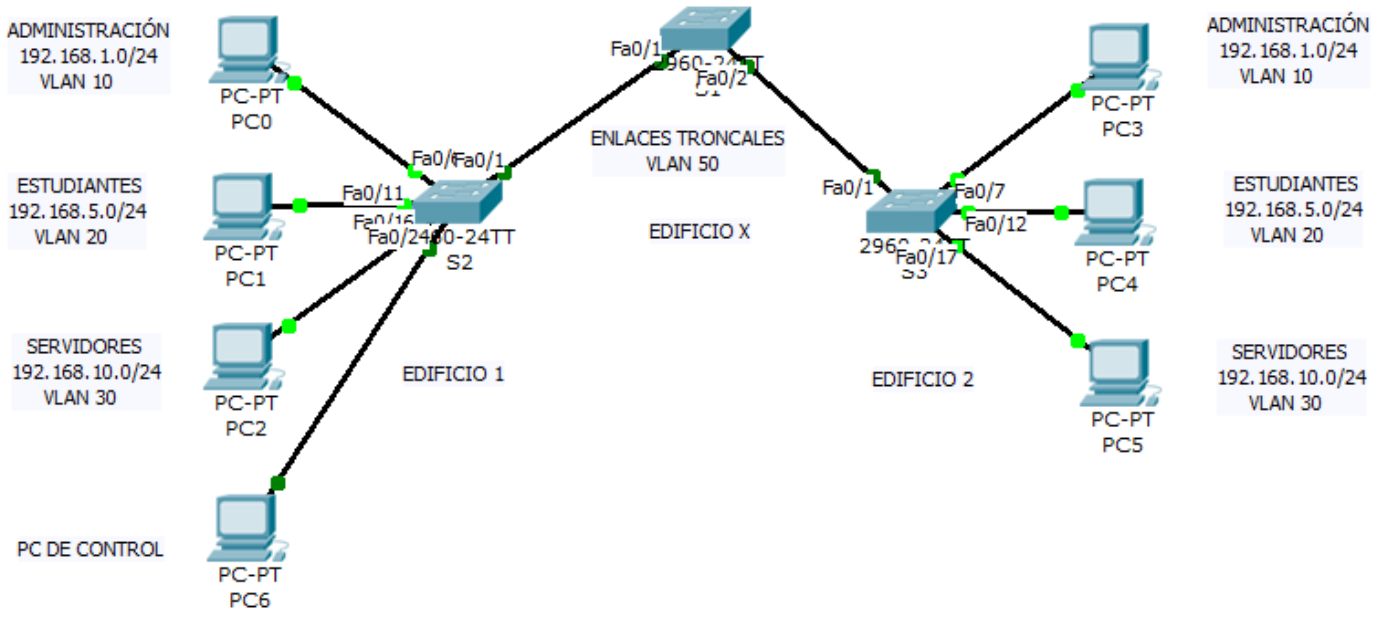


Figura 48. Topología de la Práctica No. 5

1. Configurar las ips de las PC0, PC1, PC2, PC3, PC4 y PC5, de acuerdo a la tabla de direccionamiento.

2. Realizar las configuraciones básicas de los switches S1, S2, S3.

    - Nombre del host,
    - Password de la línea de consola,
    - Password de la línea VTY,
    - Password de enable (modo privilegiado),
    - Banner de advertencia de la consola.

3. Configuración de las VLAN en los switchs:

    a. Crear las Vlan en los S1, S2, S3

        VLAN 10: Administrativa
        VLAN20 Estudiantes
        VLAN 30 Servidores
        VLAN 50 Control

    b. Asignar puertos del switch S1, S2, S3 a la Vlan correspondiente, según la topología de la práctica.

PUERTOS	ASIGNACIÓN	RED
Fa0/1-Fa0/5	Enlaces troncales	192.168.50.0/24
Fa0/6-Fa0/10	VLAN 10: Administración	192.168.1.0/24
Fa0/11-Fa0/15	VLAN 20: Estudiantes	192.168.5.0/24
Fa0/16-Fa0/20	VLAN 30: Servidores	192.168.10.0/24
Fa0/24	VLAN 50: Control	192.168.50.0/24

Tabla 6. Asignación de puertos a las vlan

c. Verificar la configuración de las Vlan de los switches S1, S2, S3.

Con el comando show vlanbrief en modo de configuración global se puede verificar que los puertos de las vlan de acuerdo a la tabla 2.

4. Configuración de los puertos troncales.

Dentro de la configuración de un rango de interfaces:

S1(config)#interface range fastEthernet 0/1-5
S1(config-if-range)#switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
S1(config-if-range)#switchport trunk native vlan 50
S1(config-if-range)#

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (50), with S2 FastEthernet0/1 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (50), with S3 FastEthernet0/1 (1).

S1(config-if-range)#no shutdown

S1(config-if-range)#end

S1#

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

5. Realizar las configuraciones del ítem anterior en los switches restantes S2 y S3.

6. Revisar las configuraciones de las interfaces troncalizadas de los switches S1, S2 y S3.

Para revisar las configuraciones de los puertos troncalizados, podemos usar el comando S2#show interfaces trunk.

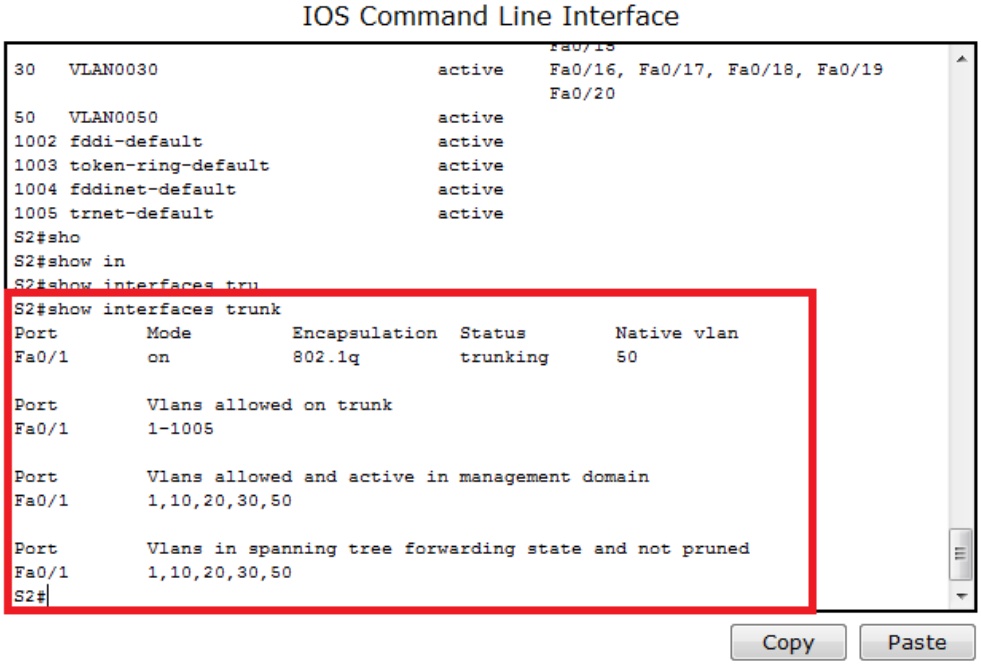


Figura 49. Comando Show interfaces trunk

En la Figura 49 podemos ver claramente los puertos que están troncalizados. En éste caso sólo nos muestra el Fa0/1, ya que es el único que está conectado.

7. Configurar la VLAN 50 para control y futuras configuraciones de los equipos.

La asignación de una dirección de control permite la comunicación IP entre los switches y permite también que cualquier host conectado a la VLAN 50 se conecte a cualquiera de los switches para configurarlos. Debido a esto cualquier puerto asignado a la VLAN 50 se considera de administración y control y debe contar con las seguridades del caso para evitar que cualquiera se pueda conectar a dicho puerto y cambiar las configuraciones de los equipos.

```
S1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface vlan 50

%LINK-5-CHANGED: Interface Vlan50, changed state to up
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up

S1(config-if)#ip address 192.168.50.10 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end

%SYS-5-CONFIG_I: Configured from console by console
S1#

S2#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
```

S2(config)#interface vlan 50

%LINK-5-CHANGED: Interface Vlan50, changed state to up
S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up

S2(config-if)#ip address 192.168.50.20 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#end

%SYS-5-CONFIG_I: Configured from console by console
S2#

S3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface vlan 50

%LINK-5-CHANGED: Interface Vlan50, changed state to up
S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up

S3(config-if)#ip address 192.168.50.30 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#end

%SYS-5-CONFIG_I: Configured from console by console
S3#

8. Probar la PC DE CONTROL (PC6)

a. Realizar un ping a todas las IP de los switch S1, S2 y S3.
b. Una vez que se haya comprobado conectividad con cada una de los switchs, se procede a conectarse mediante telnet a cualquiera de los switchs, por ejemplo, con el comando telnet 192.168.50.20 nos conectamos al switch S2.

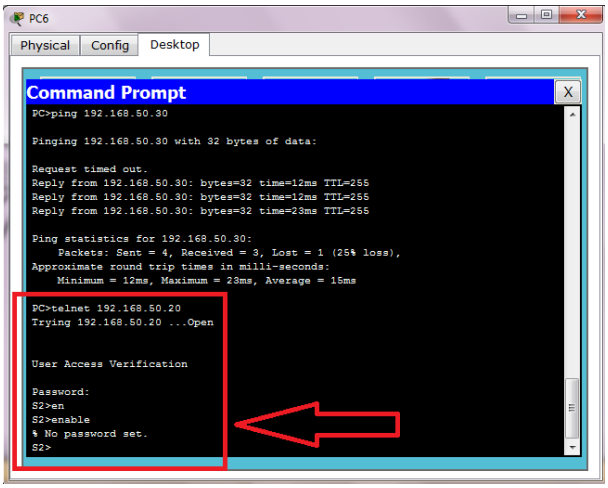


Figura 50. Comando Telnet

NOTA: Si no se han configurado correctamente las password de la línea de consola, línea VTY y la enablesecret, no podremos acceder por telnet al switch.

9. Verificación de conectividad.

Probar conectividad entra las máquinas de la misma VLAN 10, VLAN 20, VLAN 30, y entre las diferentes vlans y anotar los resultados.

10. Probar conectividad entre los switches S1, S2, y S3.

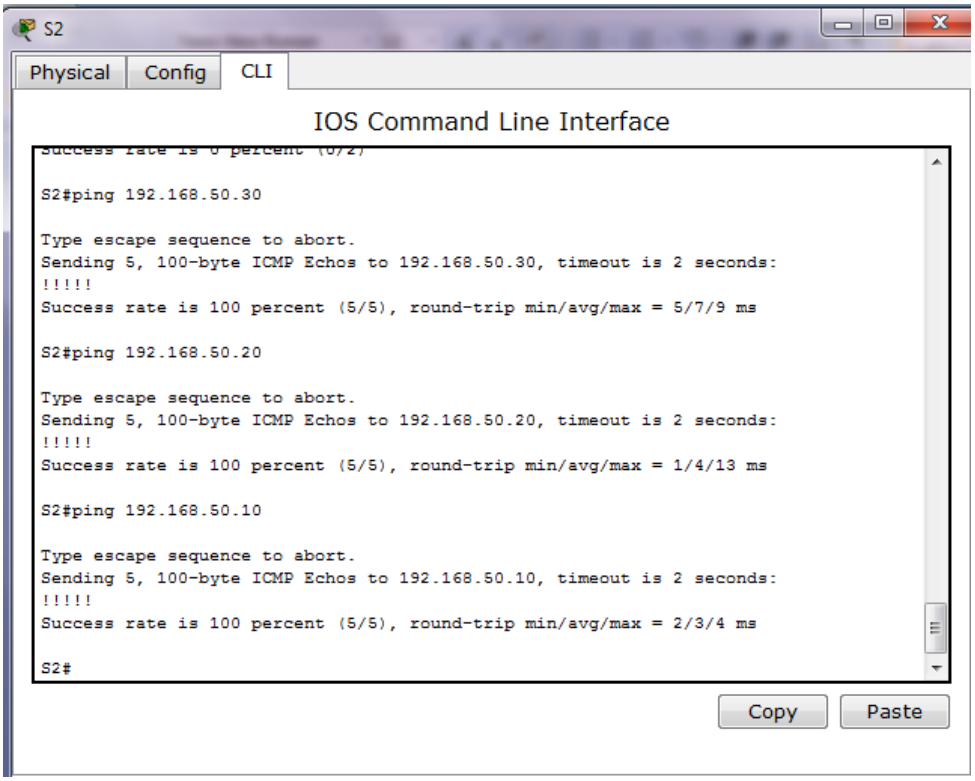


Figura 51. Comando Ping en Consola

11. Incluir las conclusiones de la conectividad en las PCs y la PC DE CONTROL.

CAPÍTULO IV

CONCEPTOS Y CONFIGURACIONES DE NETWORKING DE ELEMENTOS DE CAPA TRES (MODELO OSI)

En este capítulo se desarrollarán conceptos sobre configuraciones básicas de elementos de capa tres como son los routers. Antes de comenzar con las configuraciones de los equipos, se requieren tener claros conceptos básicos de routing.

Los routers se consideran dispositivos de capa 3 ya que su principal criterio para el reenvío de paquetes se basa en la dirección IP destino de la capa 3. La dirección IP destino del paquete es utilizada para buscar una coincidencia en la tabla de enrutamiento que poseen los equipos, al igual que los switches y su tabla de direcciones MAC, los routers poseen la tabla de enrutamiento de direcciones IP. Una vez que el router encuentra una coincidencia entre la dirección IP destino del paquete y una dirección de su tabla de enrutamiento, se dan las siguientes situaciones:

- Encapsula el paquete de capa 3 en la porción de datos de una trama de capa 2 apropiada para el tipo de interfaz.
- Los datos de la trama son codificados en las señales eléctricas.

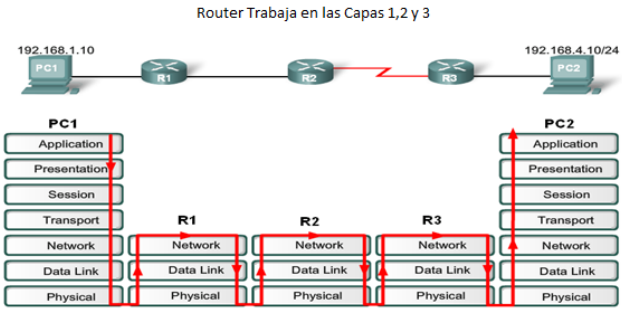


Figura 52. Capas en las que trabaja un router

4.1 Comandos básicos de configuración

COMANDOS BÁSICOS PARA CONFIGURAR UN ROUTER	
Nombre del Equipo	`Router(config)#hostname name`

Configuración de Contraseñas	`Router(config)#enable secret password`
	`Router(config)#line console 0`
	`Router(config-line)#password password`
	`Router(config-line)#login`
	`Router(config)#line vty 0 4`
	`Router(config-line)#password password`
	`Router(config-line)#login`

Mensaje de Advertencia	`Router(config)#banner motd # message #`

Configuración de la interfaz del router	`Router(config)#interface type number`
	`Router(config-if)#ip address address mask`
	`Router(config-if)#description description`
	`Router(config-if)#no shutdown`

Guardar cambios	`Router#copy running-config startup-config`

Comandos para verificación de la configuración	`Router#show running-config`
	`Router#show ip route`
	`Router#show ip interface brief`
	`Router#show interfaces`

Tabla 7. Tabla de comandos básicos para configurar un router

Show running-config: Muestra la configuración básica del router que se está ejecutando desde la RAM del equipo.

Copyrunning-configstartup-config: Copia la configuración en ejecución a la memoria no volátil NVRAM.

Show ip route: Muestra la tabla de enrutamiento actual usada por el IOS.

Show interfaces: muestra la configuración de las interfaces del router,

- Direcciones IP, máscaras de subred
- Protocolos de encapsulación
- Ancho de Banda

Show interface brief: muestra información abreviada de las interfaces. Dirección IP, mascara, status.

4.2 Tabla de enrutamiento de un router

Una tabla de enrutamiento es un archivo de datos en la RAM que se usa para almacenar la información de la ruta sobre redes remotas y conectadas directamente. Contiene una asociación entre la red de destino y la ruta de siguiente salto o interfaz de salida.

La interfaz que funciona como Gateway para una LAN, pasa a ser un host más con una dirección IP dentro de esta LAN.

- Se conoce a una red como una red directamente conectada a la interfaz del router.
- Los paquetes que tienen como destino una red directamente conectada al router no necesitan ser reenviadas a otro router.
- Las redes remotas deben ser alcanzadas reenviando el paquete a otro router que conozca su destino.
- Las redes remotas son aprendidas por el router ya sea mediante protocolos dinámicos o rutas estáticas agregadas por el administrador.

4.3 Práctica No 6

REALIZAR CONFIGURACIONES BÁSICAS EN UN ROUTER

Objetivos de la práctica:

- Realizar configuraciones básicas de un router
- Determinar las redes directamente conectadas a un router
- Determinar el uso de un router para unir redes
- Entender la tabla de enrutamiento de un router

Resumen de la Práctica

En la presente práctica el estudiante tendrá que armar la topología propuesta ayudándose de los conocimientos adquiridos en prácticas anteriores y se explorarán las configuraciones básicas de un router, a más de revisar los conceptos básicos de un router y sus funciones dentro de una red.

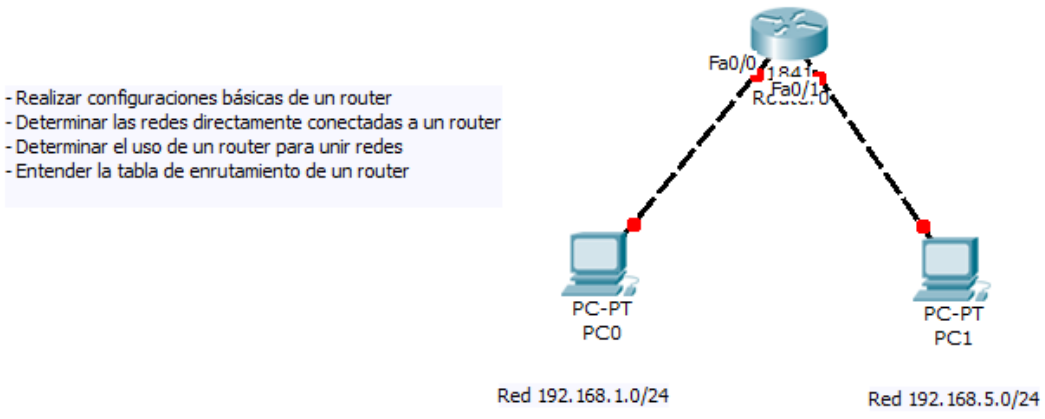


Figura 53. Topología Práctica No. 6

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED	GATEWAY
PC0	**NIC**	192.168.1.5	255.255.255.0	192.168.1.1
PC1	**NIC**	192.168.5.5	255.255.255.0	192.168.1.1
ROUTER0	**FA 0/0**	192.168.1.1	255.255.255.0	----------
	FA 0/1	192.168.5.1	255.255.255.0	----------

Tabla 8. Direccionamiento Práctica No. 6

7. Armar la topología propuesta.

    - Elegir los elementos de la topología en el simulador en los cuadros de routers y end devices. (Router 1841 y dos PCs)
    - En el cuadro de cables, seleccionar el cable de conexión cruzada, ya que son ambos elementos son de capa 3.
    - Conectar en la PC0, PC1 a las interfaces Fa0/0 y Fa0/1 respectivamente.

8. Con ayuda de los comandos anteriormente expuestos procedemos a realizar las siguientes configuraciones en el router:

    - Nombre del switch
    - Configurar Contraseñas: Línea de Consola, Línea VTY, contraseña de enable.
    - Banner de advertencia de ingreso no autorizado.

9. Analizar la tabla de enrutamiento:

Con el comando Router#showiproute se desplegará la tabla de enrutamiento que la tabla está manejando en ese momento.

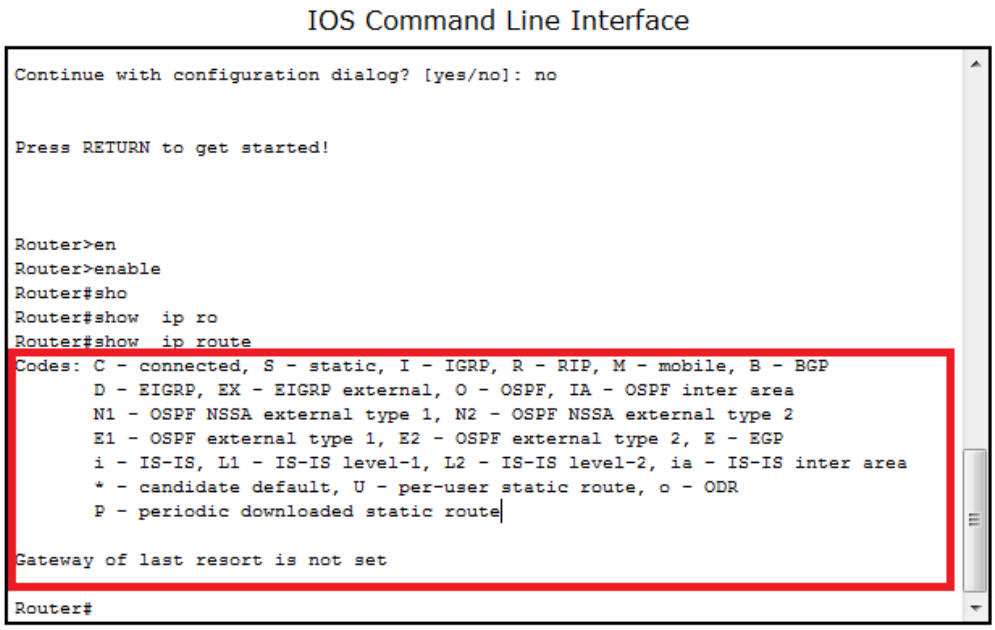


Figura 54. Comando Show ip route

Como se puede observar el comando despliega la tabla de enrutamiento actual. Como aun no se configuran las interfaces del router no aparecen las redes directamente conectadas.

Se puede observar también se despliega el código que maneja el router para las rutas de su tabla de enrutamiento:

C – Rutas directamente conectadas (redes de las interfaces)
S – Rutas estáticas configuradas
I – Rutas aprendidas automáticamente por IGRP
D – Rutas aprendidas automáticamente por EIGRP
O – Rutas aprendidas automáticamente por OSPF

10. Configurar las interfaces del router:

Para configurar las interfaces del router se procede con los siguientes comandos:

```
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

Router(config)#interface fa0/1
Router(config-if)#ip address 192.168.5.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
to up

Router(config-if)#end

%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]
Router#
```

11. Analizar nuevamente la tabla de enrutamiento:

Nuevamente con el comando show iproute.

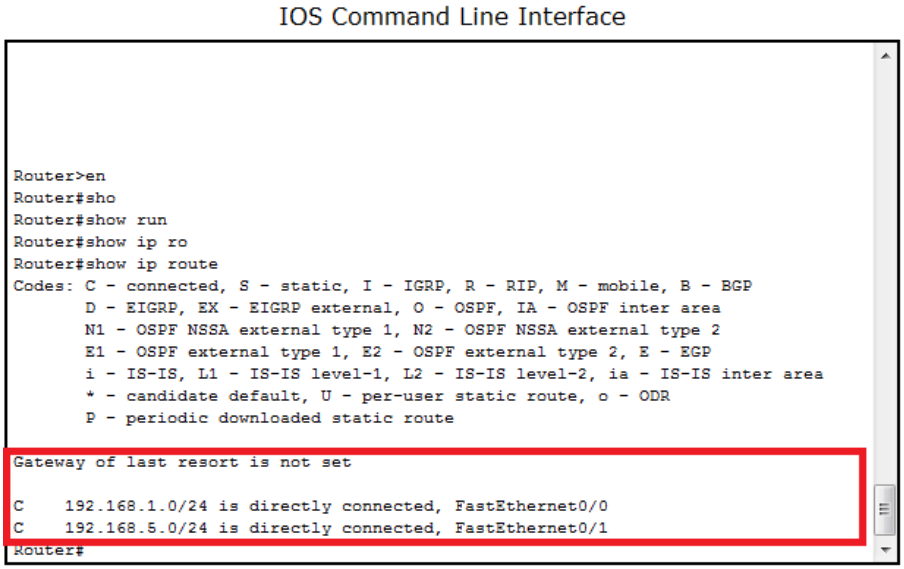


Figura 55. Comando show iproute

Podemos observar que al configurar las interfaces del router y al activarlas con el comando no shutdown, aparecen en la tabla de enrutamiento con la letra C que significa que son redes directamente conectadas.

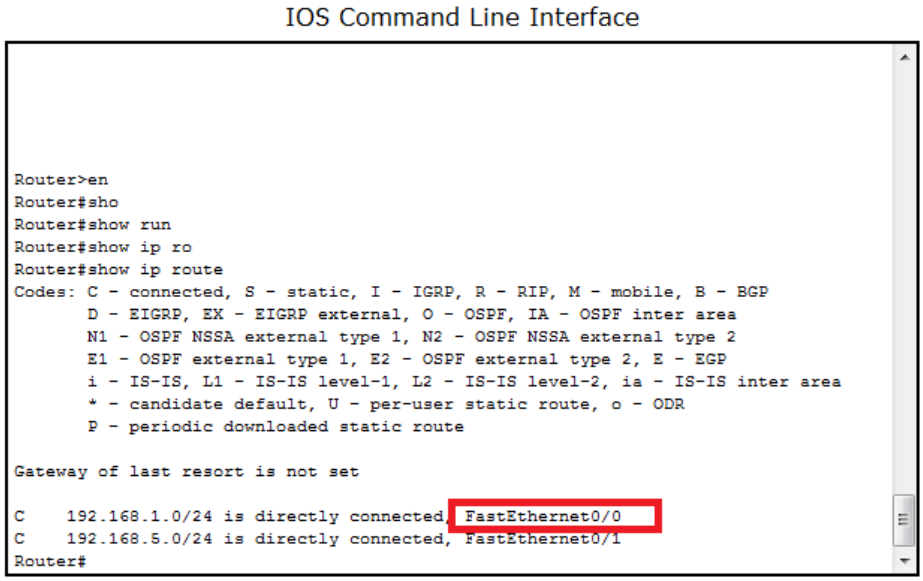


Figura 56. Comando show iproute

Cualquier requerimiento que llegue al router y en su trama tenga como IP destino una IP dentro del rango de 192.168.1.0/24, el router lo va a enviar por la interfaz Fast Ethernet 0/0. De igual manera con los paquetes que tengan como dirección IP destino una IP de la red 192.168.5.0/24

12. Configurar las PCs y realizar ping hacia las interfaces del router y entre PCs y anotar los resultados.

13. Anotar las conclusiones del punto anterior y comentar sobre las redes directamente conectadas, además de la función que desempeña un router.

4.4 Práctica No 7

ENRUTAMIENTO ESTÁTICO

Objetivos de la práctica:

- Realizar configuraciones básicas de un router
- Revisar comandos para agregar redes estáticas
- Comprender la tabla de enrutamiento de las redes estáticas y rutas directamente conectadas en un router.

Resumen de la Práctica

En la presente práctica el estudiante tendrá que armar la topología propuesta ayudándose de los conocimientos adquiridos en prácticas anteriores y se explorarán las configuraciones de rutas estáticas en un router.

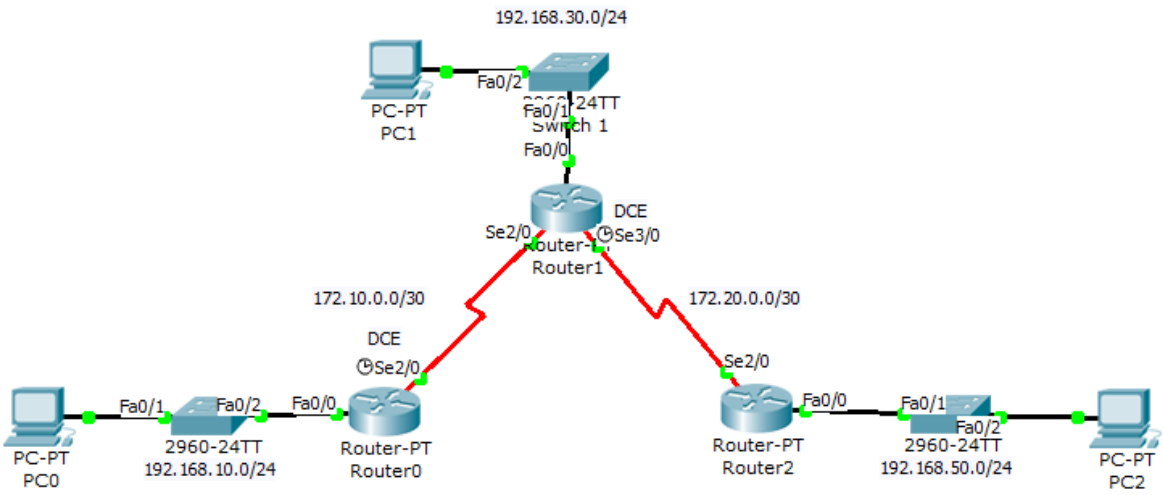


Figura 57. Topología Práctica No. 7

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARADE SUBRED	GATEWAY
PC0	**NIC**	192.168.10.5	255.255.255.0	192.168.10.1
PC1	**NIC**	192.168.30.5	255.255.255.0	192.168.30.1
PC2	**NIC**	192.168.50.5	255.255.255.0	192.168.50.1
ROUTER0	**FA 0/0**	192.168.10.1	255.255.255.0	----------
	S 0/0/0	172.10.0.1	255.255.255.248	----------
ROUTER1	**FA 0/0**	192.168.30.1	255.255.255.0	----------
	S 0/0/0	172.10.0.2	255.255.255.248	
	S 0/0/1	172.20.0.1	255.255.255.248	----------
ROUTER2	**FA 0/0**	192.168.50.1	255.255.255.0	----------
	S0/0/1	172.20.0.2	255.255.255.248	----------

Tabla 9. Direccionamiento Práctica No. 7

1. Armar la topología propuesta.

    - Elegir los elementos de la topología en el simulador en los cuadros de routers y end devices. (3 Router 1841, 3 switch 2960 y 3PCs)
    - En el cuadro de cables, seleccionar el cable de conexión serial DCE, y cablear desde donde indica la topología como DCE.
    - Conectar las PC0, PC1, PC3 a las interfaces Fa0/0 de cada uno de los routers respectivamente.

2. Con ayuda de los comandos anteriormente expuestos procedemos a realizar las siguientes configuraciones en el router:

    - Nombre del switch

- Configurar Contraseñas: Línea de Consola, Línea VTY, contraseña de enable.
- Banner de advertencia de ingreso no autorizado.

3. Analizar la tabla de enrutamiento:

   - Con el comando Router#showiproute se desplegará la tabla de enrutamiento que la tabla está manejando en ese momento.

   - Confirmamos que no existan rutas configuradas previamente.

4. Configurar PC0, PC1 y PC3

5. Configurar las interfaces del router0 “R0”:

R0(config)#interface fastEthernet 0/0
R0(config-if)#ip address 192.168.10.1 255.255.255.0
R0(config-if)#no shutdown

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

R0(config-if)#end

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

R0#conf term
Enter configuration commands, one per line. End with CNTL/Z.

R0(config)#interface serial 2/0
R0(config-if)#ip address 172.10.0.1 255.255.255.248
R0(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to down

R0(config-if)#clock rate 64000

R0(config-if)#end
R0#
%SYS-5-CONFIG_I: Configured from console by console

R0#wr
Building configuration...
[OK]
R0#

De los comandos de configuración anteriormente expuestos, se va a revisar el siguiente:

R0(config-if)#clockrate 64000: Debido a que el router 0 se conectó el lado del DCE a la interfaz S 0/0, es imprescindible configurar la velocidad en la que los bits se temporizan entre R0 y R1. Ésta configuración es solo necesaria al lado del cable serial DCE, que es el que da el clock para que las interfaces seriales de ambos routers se puedan comunicar. Para el caso de la práctica solo será necesaria la configuración del clockrate en R0 en la interfaz S0/0 y en R1 en la interfaz S1/0.

La configuración de los clocks de debe tener muy en cuenta, porque de lo contrario las interfaces seriales no se podrán comunicar.

6. Realizar las mismas configuraciones correspondientes en los routes R1 y R2.

Tener muy pendiente las configuraciones del clockrate a 64000 en los terminales DCE.

Podemos ayudarnos del comando R0#show ip interface brief para verificar que las interfaces estén levantadas y activas.

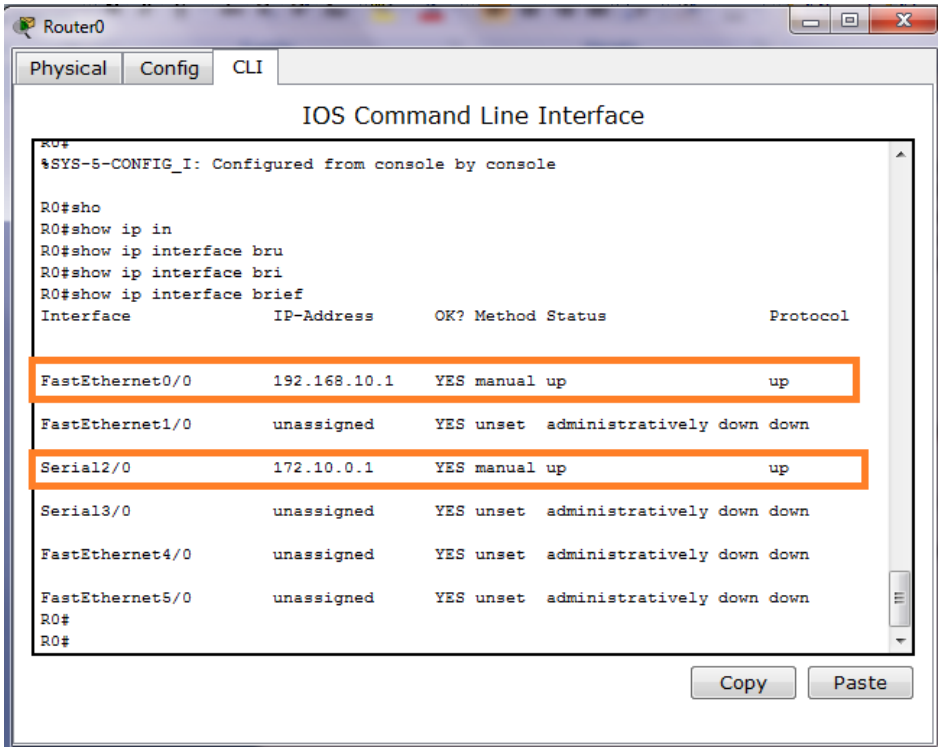


Figura 58.Comando show ip interface brief

Una de las maneras para comprobar que esté configurado el clockrate en la interfaz que corresponda es con el comando show run.

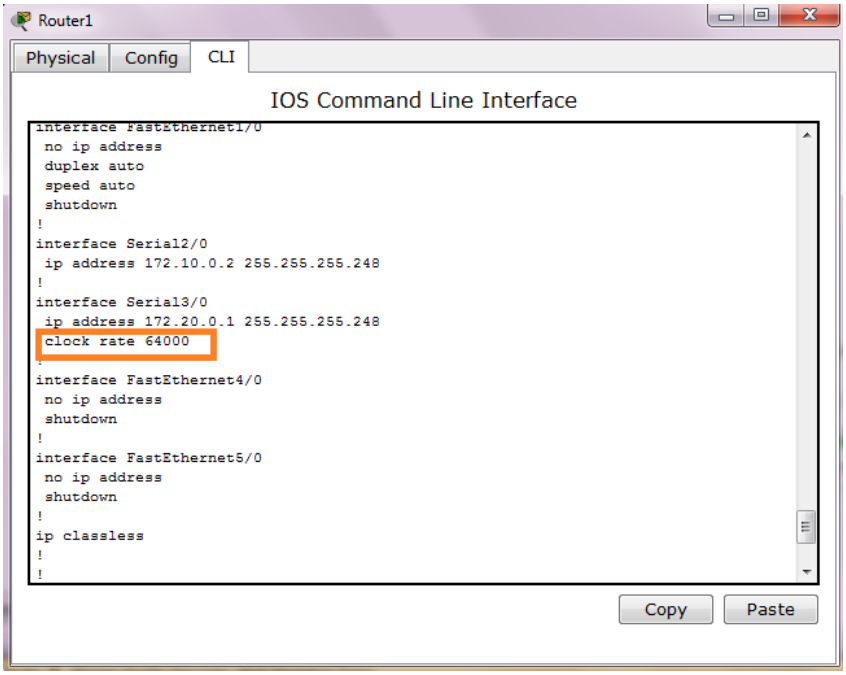


Figura 59. ClockRate

7. Analizar nuevamente la tabla de enrutamiento:

- Nuevamente con el comando show iproute.

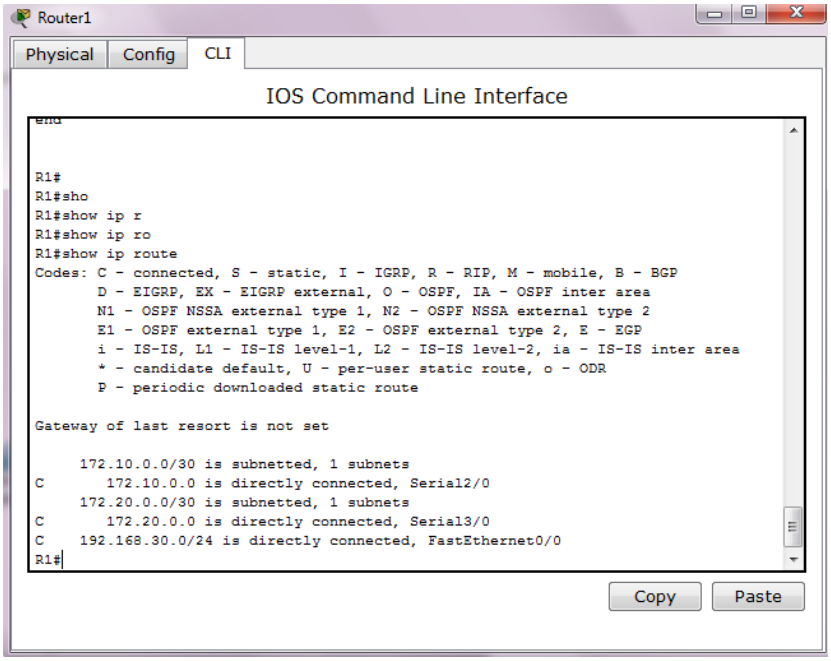


Figura 60. Comando show iproute

Como se puede observar al realizar el comando show iproute en R1 nos muestra las redes directamente conectadas “C” y en qué interfaz están conectadas cada una de ellas.

8. Realizar pruebas de conectividad entre las PC0, PC1 y PC3, además probar conectividad con las interfaces de los routers correspondientes a cada red. Anotar los resultados.

    - Utilizar el comando ping y tracert para identificar problemas.

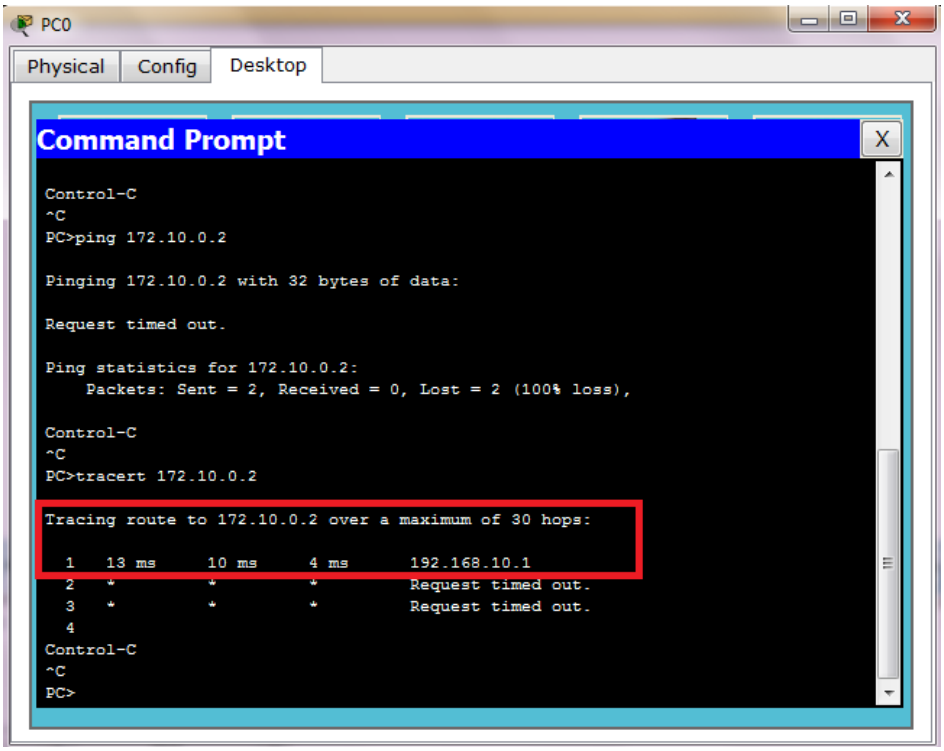


Figura 61. Comando tracert

Utilizando el comando tracert hacia la ip de la interfaz S0/0 del router R1 vemos que nos quedamos en la IP 192.168.10.1 que es el Gateway de la LAN de la PC0, lo cual nos indica que hace falta una ruta para la red 192.168.10.0/24 en R1, ya que el ping es un paquete UDP que ayudar a chequear conectividad en ambas direcciones y de equipo en equipo y al querer regresar el paquete el router R1 hacia el host de la red 192.168.10.0

no sabe por dónde, ya que él conoce únicamente las rutas para las redes directamente conectadas.

9. Configuración de rutas estáticas.

Para solucionar el problema de falta de conectividad se requieren configurar rutas estáticas para que los routers conozcan como llegar a redes que no están en su tabla de enrutamiento.

Por ejemplo se describe el router R1:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF externaltype 1, E2 - OSPF externaltype 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.10.0.0/30 is subnetted, 1 subnets
C       172.10.0.0 is directly connected, Serial2/0
     172.20.0.0/30 is subnetted, 1 subnets
C       172.20.0.0 is directly connected, Serial3/0
C    192.168.30.0/24 is directly connected, FastEthernet0/0
```

Como se puede observar en la tabla de enrutamiento de R1, no existe una ruta para la red 192.168.10.0/24 ni para la red 192.168.50.0/24 por lo cual cuando exista un requerimiento de la LAN directamente conectada 192.168.30.0/24 hacia cualquiera de las redes antes mencionadas no va a tener respuesta.

Agregamos las redes de la siguiente manera:

R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 192.168.10.0 255.255.255.0 serial 2/0
R1(config)#end

%SYS-5-CONFIG_I: Configured from console by console
R1#ping 192.168.10.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/12 ms

Como se puede observar, el comando para agregar rutas estáticas en un router es:

R1(config)#ip route 192.168.10.0 255.255.255.0 serial 2/0

Al final del comando se escribe la interfaz de R1 ó se puede escribir la ip de siguiente salto es decir la IP de la interfaz S0/0/0 del router R0.

A continuación se muestra la configuración para la red 192.168.50.0/24 con la IP de siguiente salto:

```
R1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ro
R1(config)#ip route 192.168.50.0 255.255.255.0 172.20.0.2
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#
```

10. Revisar la tabla de ruteo de R1

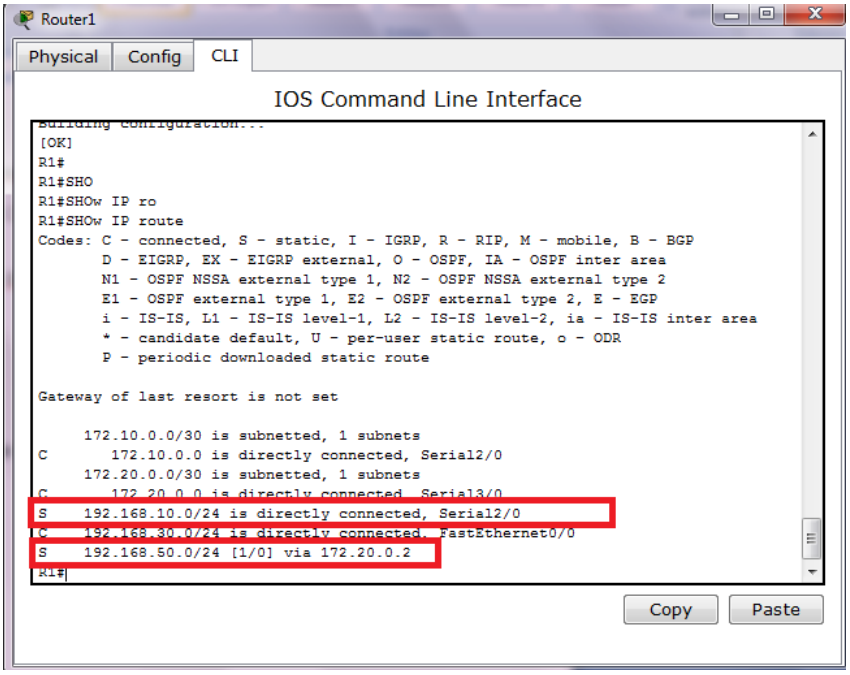


Figura 62. Comando show iproute

Se puede claramente identificar las rutas estáticas agregadas por la letra “S” que le precede a las rutas.

11. Realizar pruebas de conectividad entre las PC0, PC1 y PC2

Anotar los resultados.

12. Agregar la rutas estáticas correspondientes en R0 y R2

Para R1:

R0(config)#ip route 192.168.30.0 255.255.255.0 serial 2/0
R0(config)#ip route 192.168.50.0 255.255.255.0 serial 2/0
R2(config)#end

Para R2:

R2(config)#ip route 192.168.30.0 255.255.255.0 serial 2/0
R2(config)#ip route 192.168.10.0 255.255.255.0 serial 2/0
R2(config)#end

13. Probar conectividad entre las PCs.

Anotar resultados.

14. Revisión general.

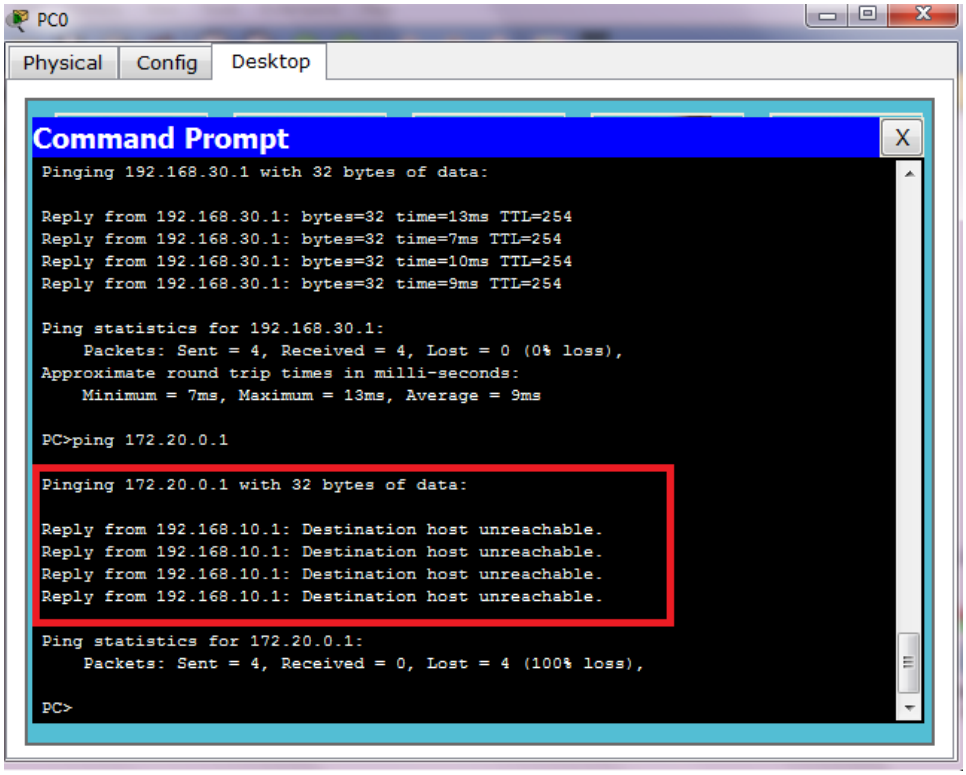


Figura 63. Comando ping para detección de fallas

En la Figura 63 se muestra un ping desde la PC0 hacia la interfaz del router R2, pero no hay respuesta, esto se debe a que hace falta una ruta para esa red en el router R0. Si se tuviera una computadora de administración de la red, el router al cuál esta máquina estuviera conectada tendría que tener en su tabla de enrutamiento cada una de las redes remotas tanto de las Lans como de las redes de conexión de los routers y equipos servidores, para administrar la red (telnet).

15. Anotar las conclusiones del punto anterior y comentar sobre las redes directamente conectadas y rutas estáticas.

4.5 Práctica No 8

ENRUTAMIENTO DINÁMICO RIP

Objetivos de la práctica:

- Realizar configuraciones básicas de un router
- Revisar comandos para configurar el enrutamiento dinámico RIP.
- Analizar las rutas aprendidas por RIP, mediante las tablas de enrutamiento.

Resumen de la Práctica

En la presente práctica el estudiante tendrá que armar la topología propuesta ayudándose de los conocimientos adquiridos en prácticas anteriores y se explorarán las configuraciones del tuteo dinámico RIP.

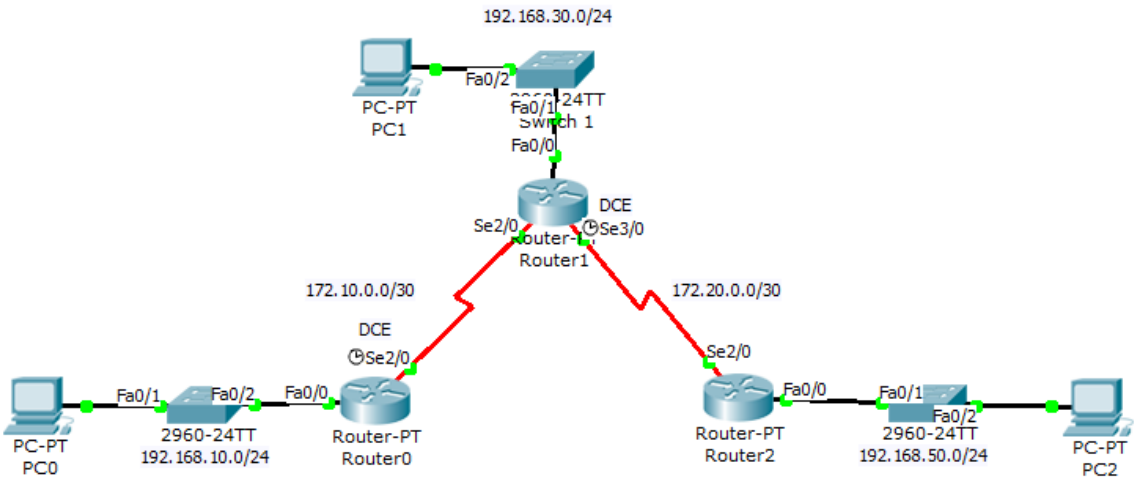


Figura 64. Topología Práctica No. 8

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED	GATEWAY
PC0	**NIC**	192.168.10.5	255.255.255.0	192.168.10.1
PC1	**NIC**	192.168.30.5	255.255.255.0	192.168.30.1
PC2	**NIC**	192.168.50.5	255.255.255.0	192.168.50.1
ROUTER0	**FA 0/0**	192.168.10.1	255.255.255.0	----------
	S 0/0/0	172.10.0.1	255.255.255.248	----------
ROUTER1	**FA 0/0**	192.168.30.1	255.255.255.0	----------
	S 0/0/0	172.10.0.2	255.255.255.248	
	S 0/0/1	172.20.0.1	255.255.255.248	----------
ROUTER2	**FA 0/0**	192.168.50.1	255.255.255.0	----------
	S0/0/1	172.20.0.2	255.255.255.248	----------

Tabla 10. Direccionamiento Práctica No. 8

1. Armar la topología propuesta.

    - Elegir los elementos de la topología en el simulador en los cuadros de routers y end devices. (3 Router 1841, 3 switch 2960 y 3 PCs)
    - En el cuadro de cables, seleccionar el cable de conexión serial DCE, y cablear desde donde indica la topología como DCE.
    - Conectar las PC0, PC1, PC3 a las interfaces Fa0/0 de cada uno de los routers respectivamente.

2. Con ayuda de los comandos anteriormente expuestos procedemos a realizar las siguientes configuraciones en el router:

    - Nombre del switch
    - Configurar Contraseñas: Línea de Consola, Línea VTY, contraseña de enable.
    - Banner de advertencia de ingreso no autorizado.

3. Analizar la tabla de enrutamiento:

Con el comando Router#showiproute se desplegará la tabla de enrutamiento que la tabla está manejando en ese momento.

Confirmamos que no existan rutas configuradas previamente.

4. Configurar las direcciones IP de las interfaces de los routers R0, R1 y R2.

Tener en cuenta las conexiones seriales y el DCE.

5. Configurar PC0, PC1 y PC3

6. Configurar las interfaces del router0 “R0”:

```
R1(config)#router  ?

bgp     Border Gateway Protocol (BGP)
eigrp   Enhanced Interior Gateway Routing Protocol (EIGRP)
ospf    Open Shortest Path First (OSPF)
rip     Routing Information Protocol (RIP)

R1(config)#router  rip
R1(config-router)#network 192.168.30.0
R1(config-router)#network 172.10.0.0
R1(config-router)#network 172.20.0.0
R1(config-router)#end
```

De los comandos de configuración anteriormente expuestos, se van a revisar los siguientes:

R1(config)#router ?

Despliega los protocolos de enrutamiento que admite el router.

R1(config)#routerrip

Habilita el protocolo de enrutamiento RIP

R1(config-router)#network X.X.X.X

El comando network habilita a RIP en todas las interfaces que pertenezcan a esta red (X.X.X.X). Ahora estas interfaces enviarán y recibirán actualizaciones RIP.

Notifica esta red en actualizaciones de enrutamiento RIP que se envían a otros routers cada 30 segundos.

7. Realizar las mismas configuraciones correspondientes en los routers R0 y R2.

Para R0:

R0(config)#router rip
R0(config-router)#network 192.168.10.0
R0(config-router)#network 172.10.0.0

R0(config-router)#end

Para R2:

R2(config)#router rip
R2(config-router)#network 192.168.50.0
R2(config-router)#network 172.20.0.0
R2(config-router)#end

8. Analizar nuevamente la tabla de enrutamiento de R0:

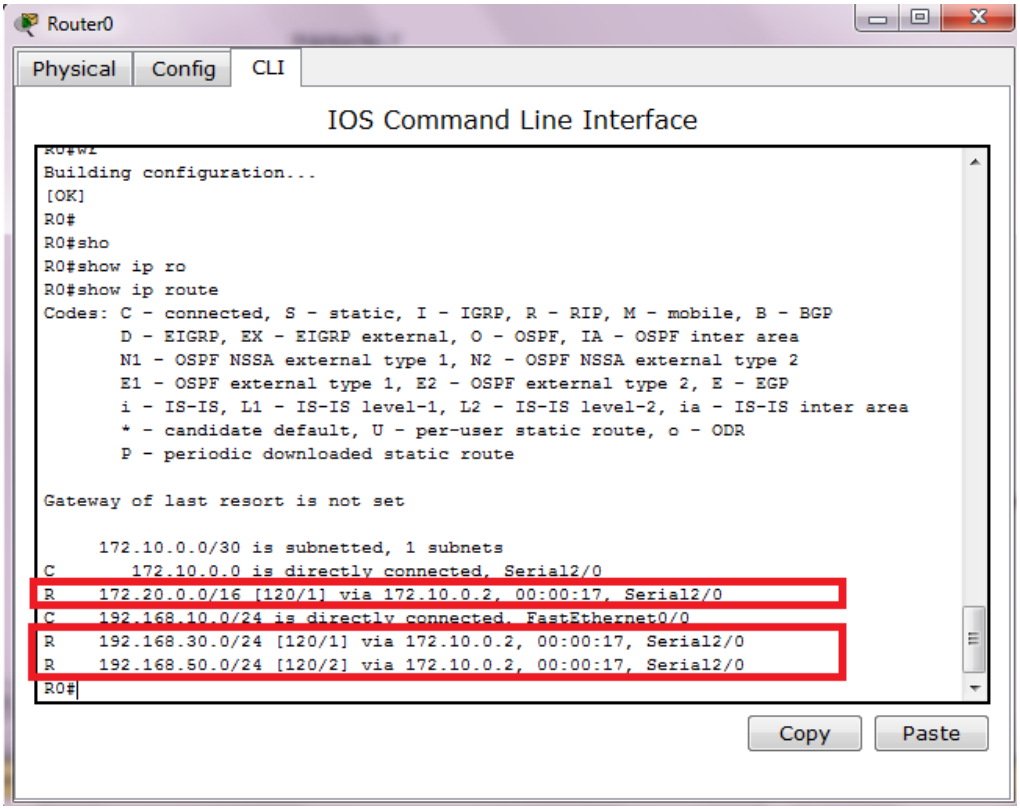


Figura 65. Comando show iproute verificando rutas

Como se puede observar al ingresar el comando show iproute en R1 nos muestra las redes directamente conectadas “C” y en qué interfaz están conectadas cada una de ellas. Una vez que se haya configurado el protocolo de enrutamiento dinámico RIP en ambos extremos de los routers (R1, R2, R3), aparecerán en las tablas de enrutamiento de cada router las rutas aprendidas por RIP. Estas redes aprendidas por RIP se especifican por la letra “R”

9. Revisar las rutas aprendidas mediante RIP en los routers R1 y R2.

Anotar los resultados.

10. Realizar pruebas de conectividad entre las PC0, PC1 y PC3, además probar conectividad con las interfaces de los routers. Anotar los resultados.

11. Anotar las conclusiones del punto anterior y comentar sobre las rutas aprendidas mediante RIP.

CAPÍTULO V

MANEJO DE SOFTWARE DE SIMULACIÓN PACKET TRACER 5.3.

5.1 Práctica No 9

DESAFIO FINAL DE CONFIGURACIONES

El presente capítulo comprende una revisión global de todas las bondades que nos brinda el simulador. Se propone resolver una práctica completa que incluye un caso de estudio y de criterio según lo revisado en los capítulos anteriores.

Objetivos de la práctica:

- Obligar al estudiante a revisar los capítulos anteriores y cimentar los conocimientos adquiridos.
- Diseñar una topología que soporte los requerimientos del diseño.
- Elegir los dispositivos necesarios para el requerimiento.
- Elegir uno o varios protocolos de enrutamiento.

Resumen de la práctica

El presente caso pretende dar una solución a una Universidad, la cual consta de tres edificaciones, cada una de ellas con un conjunto de facultades que poseen sus propios laboratorios de computación, el campus se distribuye de la siguiente manera:

EDIFICIO 1

Escuelas:

- Electrónica
- Arquitectura

EDIFICIO 2

Escuelas:

- Diseño
- Administración

EDIFICIO 3

Escuelas:

- Medicina
- Odontología

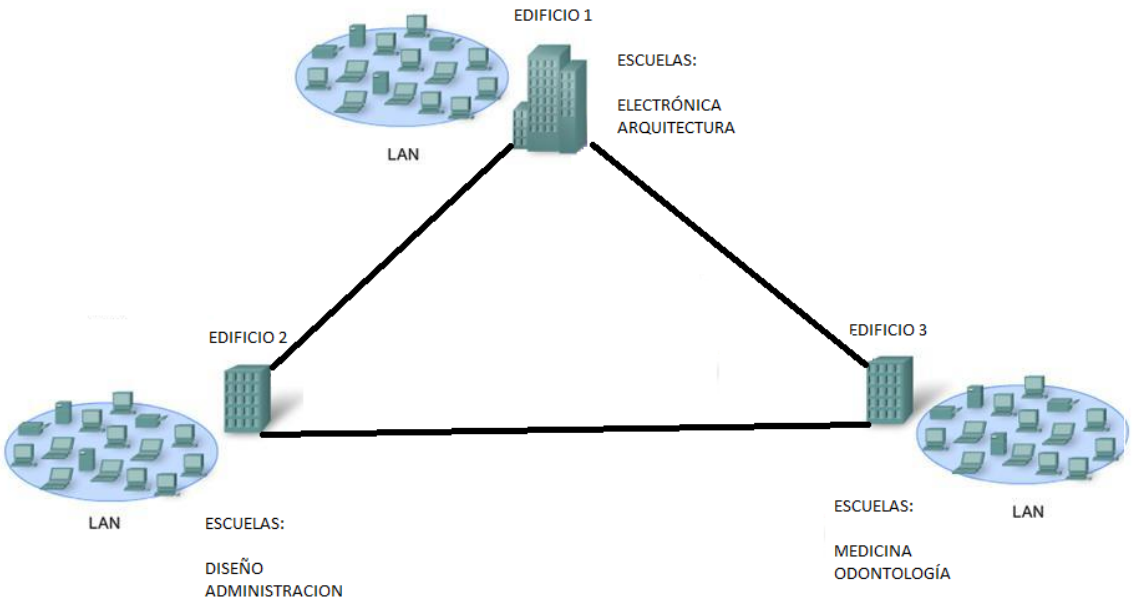


Figura 66. Topología Práctica No. 9

El campus de la Universidad por su distribución física podría albergar un switch en cada escuela, pero como requisito se necesita que cada uno de estos equipos maneje una subred diferente para cada escuela, para que no se genere tráfico innecesario entre escuelas. En el EDIFICIO 3 se encuentran los servidores de notas, a los cuales sólo máquinas de la red de profesores pueden ingresar a los mismos. A parte de esta red profesores y las de cada una de las escuelas, se debe tener en cuenta que el administrador de la red podrá ingresar de con su máquina conectándose a un puerto específico de cualquiera de los switchs de las escuelas; es decir, se deberá reservar un puerto de cada switch para administración, con una red diferente y seguridad en el puerto.

1. Armar la topología propuesta.

    - Elegir los elementos que se usarán para dar la mejor solución al caso y sin exagerar ni desperdiciar capacidades de los equipos.

EDIFICIO 1

Escuelas:

- Electrónica: Cuenta con 35 hosts y un host para administración de la red.
- Arquitectura: Cuenta con 40 hosts y un host para administración de la red.

EDIFICIO 2

Escuelas:

- Diseño: Cuenta con 20 hosts y un host para administración de la red.
- Administración: Cuenta con 35 hosts y un host para administración de la red.

EDIFICIO 3

Escuelas:

- Medicina: Cuenta con 20 hosts y un host para administración de la red.
- Odontología: Cuenta con 22 hosts y un host para administración de la red.

Para efectos de simulación se puede implementar una máquina que simule la red de cada una de las escuelas, y en el caso que se necesite más de un switch se puede implementar una máquina por equipo. Por ejemplo:

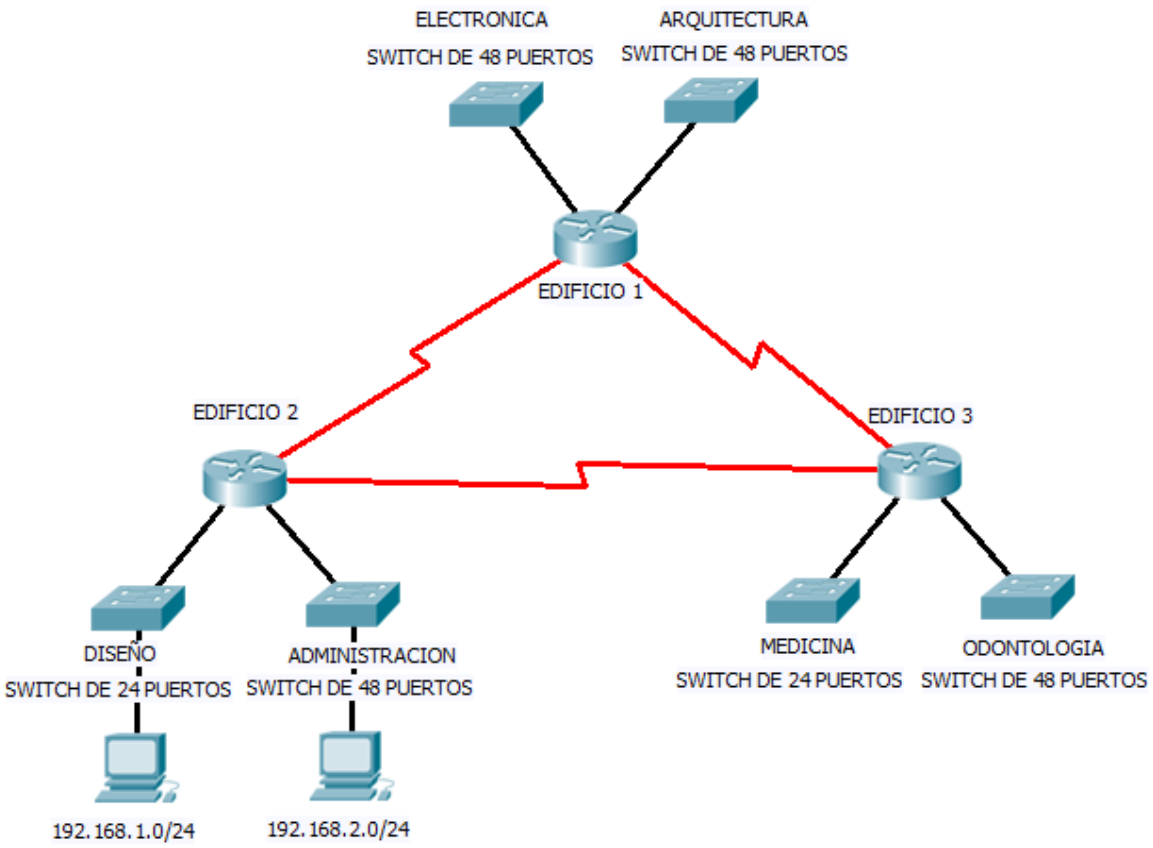


Figura 67. Topología Propuesta

2. Determinar el número de redes necesarias para cubrir el requerimiento, tener en cuenta lo siguiente:

   - Red para cada facultad
   - Red para profesores
   - Red para el administrador de la red
   - Red para la conexión de los equipos de networking

Armar la tabla de direccionamiento:

TABLA DE DIRECCIONAMIENTO						
EDIFICIO	**ESCUELA**	**DIRECCIÓN DE RED**	**MÁSCARA DE RED**	**DIRECCIÓN DE BROADCAST**	**PRIMERA DIRECCIÓN UTILIZABLE**	**ÚLTIMA DIRECCIÓN UTILIZABLE**
1	ELECTRÓNICA					
	ARQUITECTURA					
2	DISEÑO					
	ADMINISTRACIÓN					
3	MEDICINA					
	ODONTOLOGÍA					
1,2,3	RED DE PROFESORES					
1,2,3	RED PARA EQUIPOS DE COMUNICACIÓN					

Tabla 11. Direccionamiento de la Red Práctica No. 9

Llenar el cuadro de direcciones de cada interfaz:

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED	GATEWAY
PC0	**NIC**			
PC1	**NIC**			
PC2	**NIC**			
ROUTER0	**FA 0/0**			
	FA 0/1			
	S 0/0/0			
ROUTER1	**FA 0/0**			
	FA 0/1			
	S 0/0/0			
	S 0/0/1			
ROUTER2	**FA 0/0**			
	FA 0/1			
	S0/0/1			

Tabla 12. Direccionamiento Práctica No. 9

3. Realizar un respaldo de todas las configuraciones de los equipos para acostumbrarse a documentar los cambios para futuras modificaciones.

En esta parte de la práctica se pretende acostumbrar al estudiante a documentar todo el proceso de configuración para tener un respaldo en caso de daño o mala configuración de los equipos. A continuación se indicará como guardar las configuraciones de los equipos para poder cargarlas en otros equipos en caso de daño de los mismos.

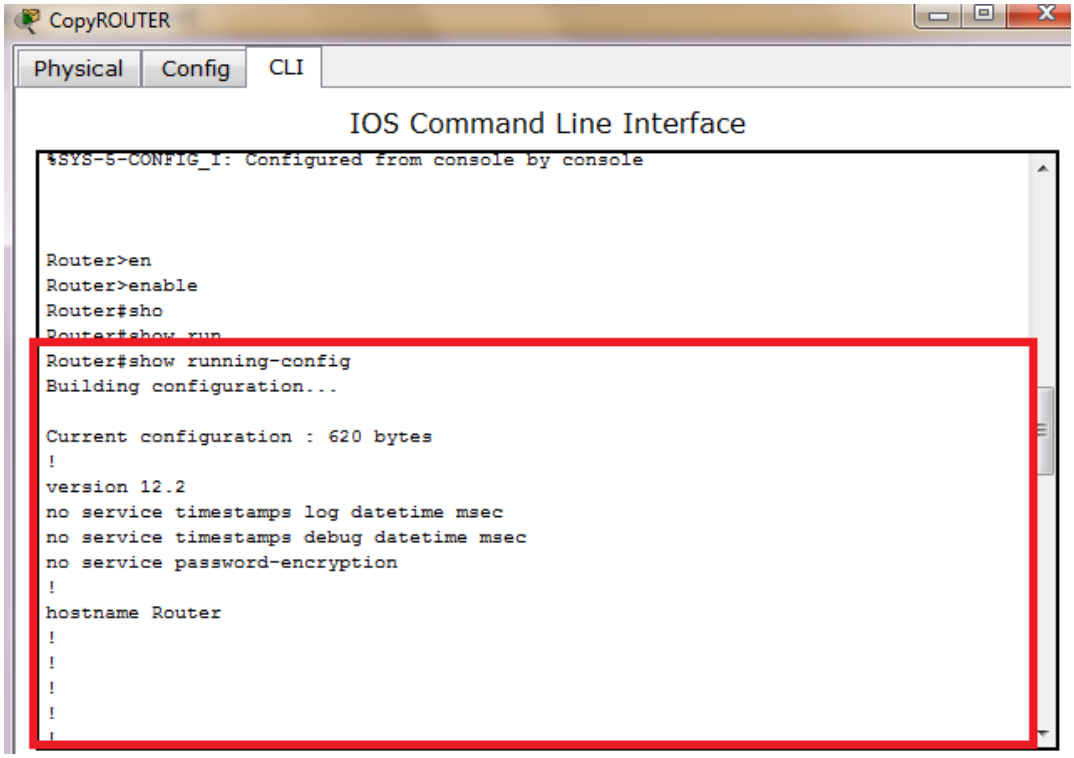


Figura 68. Comando Show running-config

Con el comando show running-config se despliega toda la configuración actual del equipo, no la que se encuentra guardada en el startup config sino la configuración en la que se ha estado trabajando antes de insertar el comando wr. Se puede guardar esta configuración en un block de notas como se indica:

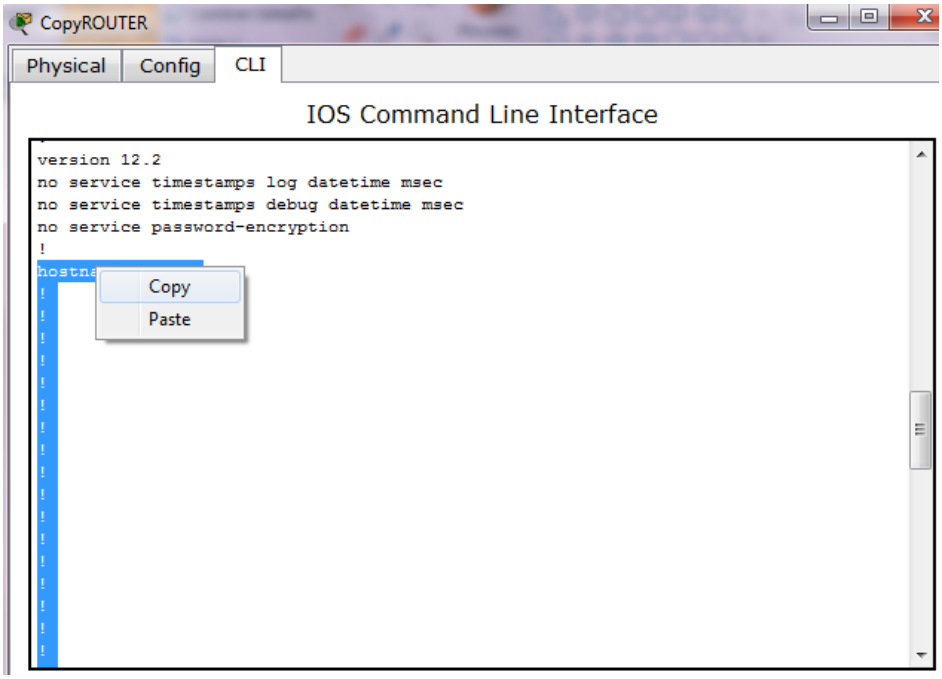


Figura 69. Respaldo del running config

Desde la configuración del hostname se marca hasta el final del running config y se guarda en un block de notas o en un archivo de texto plano como sigue:

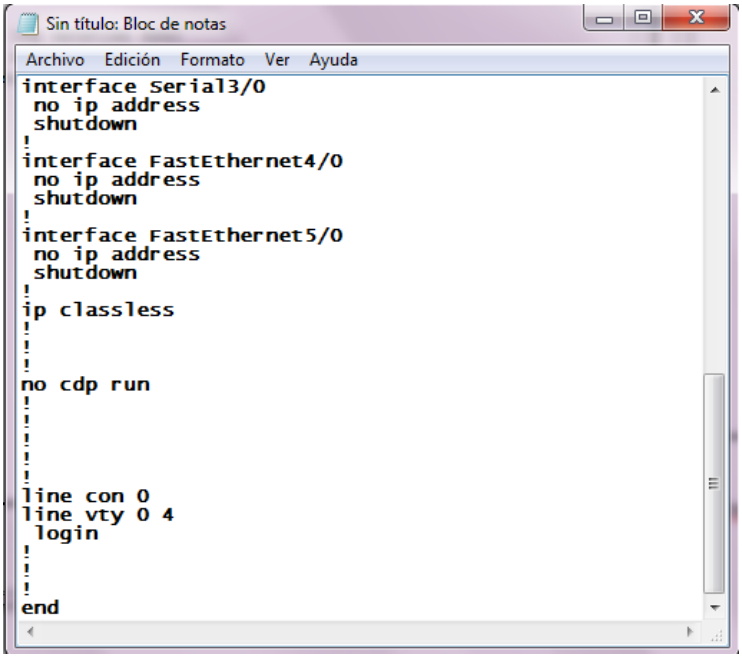


Figura 70. Configuración respaldada

Para cargar el archivo que se ha respaldado se procede de la siguiente manera:

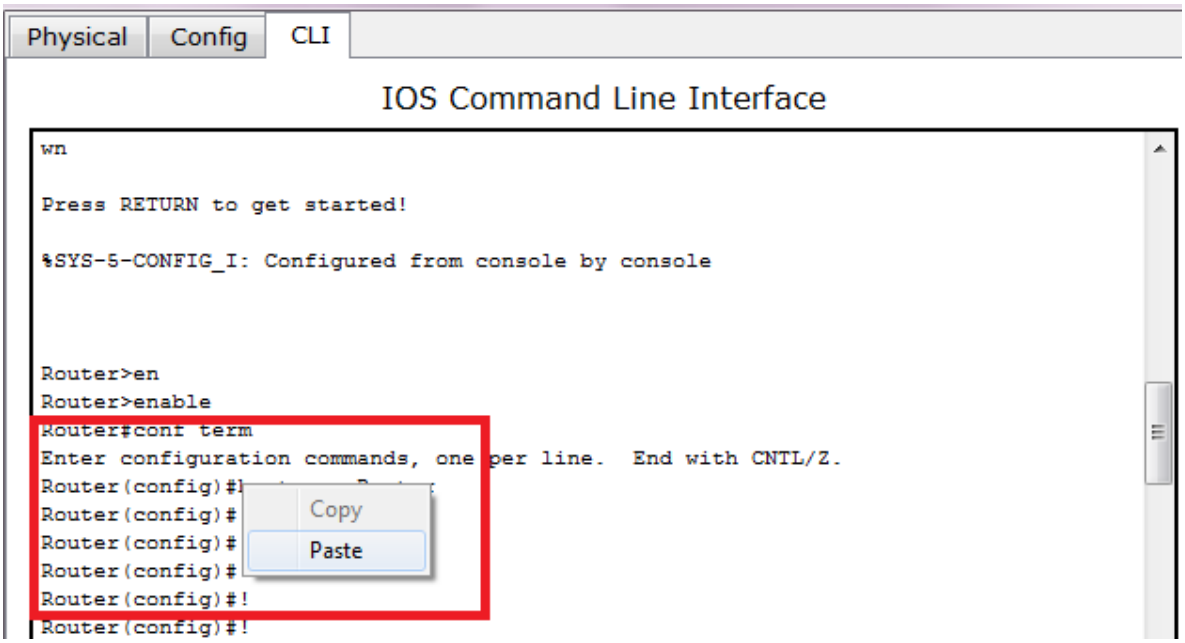


Figura 71. Comando show ip route

En el nivel de configuración del terminal se pega el archivo copiado textualmente del respaldo y el nuevo equipo cargará las nuevas configuraciones respaldadas.

4. Escoger el mejor protocolo de enrutamiento entre los revisados en las prácticas para este caso según lo revisado en los capítulos anteriores.

5. Revisar el requerimiento de seguridad para el administrador de la red.

Configurar seguridades en los puertos del switch asignados para el administrador de la red. Por medio de los comandos de port security.

6. Probar configuraciones y revisar tablas de enrutamientos para verificar los requerimientos y el funcionamiento óptimo de la red.

7. Documentar todo el proceso de pruebas para comparar resultados con sus compañeros de clase para definir el mejor protocolo de enrutamiento para este caso práctico.

8. Anotar conclusiones.

CONCLUSIONES Y RECOMENDACIONES

- En la presente monografía se desarrollaron prácticas sencillas que ayudan a los estudiantes de la Universidad del Azuay a explorar el campo de las redes de una manera totalmente práctica.

- Se desarrollaron 9 prácticas que incluyen conceptos teóricos muy necesarios para el entendimiento del funcionamiento básico de elementos y equipos de networking de capa 1, capa 2 y capa3.

- Cada práctica está compuesta de una figura explicativa de la topología y una tabla de direccionamiento de la misma, lo que ayuda al estudiante a desarrollar una a una las practicas con un guía muy ilustrativa basada en configuraciones y explicaciones gráficas.

- El uso del simulador Packet Tracer, ayuda en gran medida a desarrollar prácticas mucho más realistas. Esto le permite al estudiante irse acoplando al modo de trabajo de los equipos de networking y conocer conceptos que le permitirán manejar cualquier equipo de redes de cualquier marca o casa fabricante.

- De igual manera se concluye que el simulador Packet Tracer es muy didáctico dada su forma gráfica y variedad de opciones de equipos de redes. El simulador incluye elementos físicos de capa 1, capa 2 y capa 3. Debido a la variedad de

Equipos en el simulador, las prácticas desarrolladas en la presente monografía son muy variadas y dan una idea muy amplia al estudiante de las capacidades que posee cada uno de ellos.

- Se recomienda al estudiante seguir las prácticas en el orden que se ha especificado en el trabajo, ya que cada práctica está relacionada con la parte teórica de cada capítulo. Las prácticas se desarrollan de tal manera que desafían al estudiante a implementar su criterio basado en los conceptos aprendidos en el capítulo.

- El simulador apoya en gran medida la investigación del estudiante. Al poseer una variedad muy grande de elementos, se recomienda al estudiante investigar las configuraciones de muchos estos equipos, que al ser muy utilizados en topologías comunes, el estudiante va a necesitar de estos conocimientos para complementar trabajos tan sencillos como conectar un par de computadores, y trabajos tan complicados como conectar edificios de computadores y redes independientes.

GLOSARIO DE TÉRMINOS

ACL: Lista de control de acceso.

ADSL: Línea Digital del Suscriptor Asimétrica.

ANSI: Instituto Nacional Americano de Normalización.

ARP: Protocolo de Resolución de Direcciones.

ASCII: Código americano normalizado para el intercambio de la información.

Backbone: Columna vertebral de la red.

BGP: Protocolo de Gateway fronterizo.

Broadcast: Envío de un paquete a todos equipos de una red.

Bucle: Ciclo repetitivo de paquete que no encuentra su destino.

Cliente/servidor: Relación entre un host y un servidor en una red.

Consola : Pantalla de administración de equipos de networking.

MAC: Control de Acceso al Medio.

DNS: Sistema de denominación de dominio

Dominio: Nombre asignado a una máquina o servidor determinado.

FTP: Protocolo de Transferencia de Archivos.

HTTP: Protocolo de Transferencia de Hipertexto.

ICMP: Protocolo de mensajes de control en Internet

IEEE: Instituto de Ingeniería Eléctrica y Electrónica

IEEE802.2: Protocolo de LAN de IEEE que especifica una implementación del la subcapa LLC de la capa de enlace de datos.

IEEE 802.3: Protocolo IEEE para LAN que especifica la implementación de la capa física y de la subcapa MAC de la capa de enlace de datos.

IGRP: Protocolo de enrutamiento de Gateway interior.

IOS: Sistema Operativo de Internetworking.

NIC: Tarjeta de interfaz de red

Ping: Mensaje de eco ICMP y su respuesta.

RIP: Protocolo de información de enrutamiento

SNMP: Protocolo simple de administración de redes

TTL: Tiempo de Existencia

UDP: Protocolo de Datagrama de Usuario

UTP: Par trenzado no blindado

VLAN: LAN virtual

VoIP: Voz sobre Protocolo de Internet IP

VPN: Red Privada Virtual

BIBLIOGRAFIA

LIBROS

- BOYCE. Jim. Windows 7 bible. Inglaterra. Editorial John Wiley and Sons. 2009. Páginas 1272. 3 Edición

- STALLINGS. William. Pack comunicaciones y redes de computadores + problemas y ejercicios resueltos. España. Editorial Pearson Educación. 2005. 7 Edición

- HALSALL. Fred. Redes de computadores e Internet. España. Editorial Pearson. 2006. Páginas 826. 5 Edición

- BLUM. Richard. Linux command line and shell scripting bible. Inglaterra. Editorial John Wiley and Sons. 2008. Páginas 809.

- BLUM. Richard. Ubuntu Linux secrets. Inglaterra. Editorial John Wiley and Sons. 2009. Páginas 900.

- JANG. Michael. Mastering Red hat Linux 9. Estados Unidos. Editorial Sybex. 2006. Páginas 942.

- OPPENHEIMER. Priscilla. Troubleshooting campus networks practical analysis of Cisco and Lan protocols. Inglaterra. Editorial John Wiley and Sons. 2002. Páginas 608.

- CONLAN. Patrick. .Cisco network professional's advanced internetworking guide. Estados Unidos. Editorial Sybex. 2009. Páginas 750

- MACFARLANE. James. Network routing basics understanding IP routing in Cisco systems. Inglaterra. Editorial John Wiley and Sons. 2006. Páginas 408.

- PAYNE. Rob. CCIE Cisco Certified Internetwork Expert study guide. Editorial Sybex. 2006. Páginas 1068