Pontificia Universidad Católica del Ecuador

Facultad De Ingeniería

Escuela de Sistemas

TEMA:

DISEÑO DE RED PARA EMPRESAS APLICANDO QOS PARA EL TRÁFICO DE RED Y VLANS

AUTOR:

Josue Andrés Estrella Onofa

TRABAJO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

QUITO, 2022

DEDICATORIA

Esta tesis va dedicada a mi familia por ser ese pilar para mí, por ser mi apoyo incondicional en los tiempos difíciles, ayudarme a siempre salir adelante y siempre inspirarme a dar lo mejor de mí.

También dedico esta tesis, a uno de mis mejores amigos y una de las mejores personas que conocí en mi vida, mi gran amigo Miguel Andrade, que por problemas de salud no pudo continuar con sus estudios.

AGRADECIMIENTO

Quiero agradecer a mis padres Wilson y Roció, por siempre ayudarme a salir adelante y ser ese pilar en mi vida, de igual manera a mis hermanas Johanna y Dayana, por ser un gran ejemplo para seguir para mí, por siempre ayudarme y estar junto a mí en todo momento no solo académico, sino que también personal.

Agradecer también a mis amigos de carrera, Miguel, Mateo, Ronny, Christopher, Zabdiel, Juan Carlos, Adrián por los momentos de risas, y las experiencias compartidas a lo largo de todo este tiempo en la universidad, sobre todo agradecer a Javier Murillo por siempre ayudar a mis compañeros y a mí en lo académico, de igual forma a Marco Altamirano y Stalin Cabezas por siempre estar dispuestos a brindar su ayuda y sus conocimientos para así poder llegar a donde estoy.

RESUMEN

Este tema surge como una respuesta a los problemas relacionados con la estabilidad de red que pueden llegar a presentarse en las empresas, por lo que en este trabajo se busca optimizar los recursos de la red como el ancho de banda para protocolos de red críticos mediante la implementación de calidad de servicios, así como implementar VLANS para segmentar la red de la empresa por departamentos con el fin de ayudar a mejorar el tráfico de red. Se busca implementar un tipo de encolamiento para la calidad de servicios que se adecue a las prioridades de tráfico de red que se tenga en una empresa con el objetivo de optimizar sus recursos de red.

ÍNDICE

ÍNDICE DE FIGURAS, GRÁFICOS Y TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I: MARCO DE REFERENCIA

1.1. Justificación

Actualmente la gran mayoría de empresas realiza su trabajo mediante el uso de internet, ya sea para subir documentos, descargar archivos o para realizar reuniones mediante herramientas de videochat como lo son Zoom o Microsoft Teams, por lo cual, un buen diseño de red debería priorizar el tipo de tráfico de red que requiera cada departamento de la empresa, por ejemplo, en medio de una reunión virtual de gerencia sería un gran problema si se llegase a perder estabilidad en la conexión o se llegue a perder la conexión en su totalidad.

Este problema se solucionaría si se aplica la Calidad de Servicios que garantiza que el tráfico de red para las reuniones virtuales siempre se mantenga estable, evitando posibles pérdidas económicas o de otro tipo que puedan perjudicar a una empresa. De igual forma se puede identificar este tipo de problemas en las distintas áreas de una empresa, por lo que, priorizando el tráfico de red, además de segmentar la red mediante el uso de VLANS para facilitar la administración de red para cada área de una empresa, se busca que las tareas que realice cada departamento no se vean afectadas por los problemas de conectividad a la red.

1.2. Planteamiento del problema

El problema que se busca solventar en este trabajo de disertación es, evitar los problemas de conexión de red que se pueden llegar a dar en una empresa, por lo que se busca en primer lugar, identificar el tráfico de red que sea más importante para cada departamento de la empresa, seguido de esto se busca realizar un diseño de red utilizando VLANS para ayudar a segmentar la red de la empresa creando una VLAN para cada departamento, esto con el fin de poder realizar la

configuración de la calidad de servicios para el tráfico de red para cada departamento y así poder garantizar el buen funcionamiento de la red.

Para poder realizar el diseño con la configuración de la red se utilizará la herramienta Packet Tracer, donde se puede realizar las respectivas configuraciones de las redes VLANS y configurar el tráfico de red identificado para cada departamento.

1.3. Objetivo General

- Diseñar una red local para empresas aplicando calidad de servicios (QoS) y redes VLANS para cada departamento.

1.4. Objetivos Específicos

- Identificar las prioridades de tráfico de red para cada departamento de una empresa.
- Analizar el mejor tipo de encolamiento para aplicar la calidad de servicios.
- Desarrollar un prototipo del diseño de red mediante el uso de la herramienta Packet Tracer.

1.5. Antecedentes

La aplicación de la calidad de servicios en las soluciones de red es algo relativamente nuevo, que en ciertos casos de estudio que se los analiza son hechos para centros educativos donde se busca mantener una conexión estable para que los estudiantes puedan cumplir con sus tareas apoyados con el uso de la red. De igual forma en una empresa también se ha visto la necesidad de poder garantizar que exista una conectividad estable a la red, ya que sin importar el ancho de banda, no se puede garantizar una conexión estable si no existe un buen diseño y configuración de red que asegure la misma.

En el día a día del trabajo en cualquier empresa una perdida en la conexión de red puede llegar a generar pérdidas de bajo o alto costo, o también puede llegar a pasar que se pierda una comunicación importante mediante alguna reunión virtual que se realice, es por esto que el garantizar una estabilidad en la conectividad de red mediante una buena configuración y priorización del tráfico de red, además de la segmentación de la red para ayudar a administrarla mejor resulta muy beneficiosa para las empresas.

1.6. Alcance

Este trabajo de titulación busca generar un prototipo de diseño de red mediante el uso de la herramienta Packet Tracer, la cual permite realizar simulaciones de entornos de red, en donde se buscará determinar la topología de red necesaria, además de la respectiva configuración en los dispositivos que se utilicen para que se garantice el tráfico de red prioritario para cada departamento de una empresa.

Para poder identificar que la solución cumple con lo que se está proponiendo se realizaran pruebas enviando distintos tipos de paquetes mediante esta herramienta de simulación, donde se podrá verificar si la configuración de los dispositivos se encuentra correctamente realizada.

1.7. Metodología

Para desarrollar un prototipo de red donde se pueda comprobar las distintas configuraciones con respecto a calidad de servicios y la conectividad mediante el uso de redes VLAN, se va a utilizar la herramienta Packet Tracer de Cisco, donde se va a aplicar las siguientes fases:

Definición de topología: En esta fase se debe buscar la topología que sea más recomendable para la finalidad que va a tener esta red.

Fase de elaboración del diseño: En esta fase se empezará a construir la red con los equipos adecuados y las configuraciones necesarias, basados en la topología definida en la fase anterior.

Fase de pruebas: Aquí se pondrá a prueba las configuraciones que se haya realizado en la fase anterior para verificar que la red cumple con lo establecido para su funcionamiento.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1. Modelo OSI

Rivera (2018) define al modelo OSI como un modelo conceptual que caracteriza y estandariza la comunicación de las redes de datos y telecomunicaciones para lograr interoperabilidad, la arquitectura del modelo se dividió en capas de comunicación de extremo a extremo para dividir de manera diferenciada y definida las funciones con el objetivo de normalizar la comunicación entre capas, dar manejabilidad y minimizar el flujo entre capas.

En el modelo OSI cada capa realiza diferentes funciones con el fin de resolver los diferentes problemas que se presenten, además de que cada capa superior debe sustentar a la capa inferior y está debe proporcionar los servicios a la capa superior, también hay que considerar que los cambios que se realicen en una capa no deben implicar cambios en las demás capas.

En este modelo se definen siete capas de protocolos en donde la capa 1 es la inferior y la capa 7 la superior:

2.1.1. Capa 7 – Aplicación

Esta es la única capa en donde se puede interactuar de forma directa con los datos del usuario, esta capa es esencial para que las aplicaciones como clientes de correo electrónico o páginas web puedan iniciar sus comunicaciones ya que aquí se establece la conexión para los otros niveles y prepara las funciones para las aplicaciones, en esta capa se utilizan protocolos que funcionan en la capa de aplicación como lo son HTTP, HTTPS, SMTP.

2.1.2. Capa 6 – Presentación

La principal función de esta capa es preparar los datos para que puedan ser utilizados en la capa de aplicación, aquí se realiza la compresión, el cifrado y la traducción de los datos. En términos de cifrado esta capa se debe asegurar de añadir el cifrado de extremo a extremo, así como, encargarse de decodificar el cifrado para que los datos puedan ser entendibles en la capa de aplicación. Otro punto importante a tomar en cuenta en la capa 6 es la compresión de los datos que se reciben de la capa de aplicación para ser enviados a la capa de sesión, esto se lo hace con el fin de mejorar la eficiencia y la velocidad de la comunicación.

2.1.3. Capa 5 – Sesión

En esta capa es conocida como capa de sesión debido a que así se denomina al tiempo que existe entre la apertura de la comunicación y el cierre de esta, en el tiempo que la sesión permanece abierta debe ser el suficiente para que todos los datos sean transferidos de modo que, no se desperdicien recursos si se deja abierta por mucho tiempo, además, se utilizan puntos de control para la transferencia de datos para asegurar que no existan pérdidas en el transporte.

2.1.4. Capa 4 – Transporte

Esta capa funciona como una mediadora entre las capas de aplicaciones y las capas enfocadas al transporte y es la responsable de que exista comunicaciones de un extremo a otro extremo entre dos dispositivos, funciona tomando los datos de la 4 y los fragmenta en segmentos para ser enviados a un dispositivo receptor donde este será el encargado de volver a unir los segmentos para que puedan ser utilizados en las capas superiores.

2.1.5. Capa 3 – Red

En esta capa se produce el direccionamiento lógico de los paquetes de datos, es también responsable de realizar transferencias de datos entre dos redes diferentes ya que en esta capa se

da la salida a internet. En esta capa los datos de la capa 3 o de transporte se desfragmentan en componentes más pequeños llamados paquetes en el dispositivo emisor para ser rearmados una vez lleguen al dispositivo receptor.

2.1.6. Capa 2 – Enlace de datos

La capa de enlace de datos es la encargada de tomar los datos netos y transformarlos en datos libre de errores de transmisión para la siguiente capa, codifica las tramas que se reciben en la capa de red para ser transmitidas por medio de la capa física. Las tramas contienen información que va desde las direcciones de origen y destino por medio de las direcciones MAC, información de control y un registro de los datos que se envían.

2.1.7. Capa 1 – Física

En esta capa física es donde se efectúa la transformación de los bits de un paquete de datos en una señal que pueda ser transmitida por algún medio físico como puede ser fibra de vidrio, aire o cobre, en esta capa se utilizan normas o protocolos como lo son el DSL, bluetooth, ISDN, o ethernet.

2.2. Protocolos de comunicación

Como menciona Dordoigne (2015), La materialización de las capas del modelo teórico OSI toma la forma de protocolos que constituye un conjunto de reglas de comunicación.

Lo que se puede entender como un estándar de comunicaciones donde se establecen las reglas necesarias, así como la información correcta para que se pueda establecer una comunicación entre equipos, estos protocolos se encuentran en distintas capas del modelo OSI.

2.2.1. Protocolos de capa 1

- Frame Relay.
- Ethernet physical layer.
- DSL

2.2.2. Protocolos de capa 2

- PPP: Protocolo de punto a punto.
- STP: Protocolo de árbol esparcido.
- MPLS: Multiprotocolo de etiqueta

2.2.3. Protocolos de capa 3

- ARP: Protocolo de resolución de direcciones.
- ICMP: Protocolo de mensaje de control de internet.
- IPv4: Protocolo de internet versión 4.
- IPv6: Protocolo de internet versión 6.
- OSPF: Protocolo para abrir la trayectoria más corta en primer lugar.

2.2.4. Protocolos de capa 4

- TCP: Protocolo de control de transmisión.
- UDP: Protocolo de datagramas de usuario.
- DCCP: Protocolo de control de congestión de datagramas.

2.2.5. Protocolos de capa 5

- SMB: Protocolo de bloque del mensaje del servidor.
- SMPP: Protocolo de mensaje de corto punto a punto.

2.2.6. Protocolos de capa 6

- SSL: Protocolo de capa de conexión segura.
- TLS: Protocolo de seguridad en la capa de transporte.

2.2.7. Protocolos de capa 7

- DHCP: Protocolo de configuración dinámica de host.
- DNS: Protocolo de nombre de sistema de dominio.
- HTTP: Protocolo de transferencia de hipertexto.
- HTTPS: Protocolo de transferencia de hipertexto seguro.
- SMTP: Protocolo de transferencia simple de correo.
- POP3: Protocolo de oficina de correo.

2.3. VLAN

Una red VLAN o también conocida por sus siglas en ingles Virtual Local Area Network o red de área local virtual, se la puede considerar como una tecnología que tiene como característica principal el poder crear redes lógicas que puedan funcionar de forma independiente dentro de una misma red, lo cual tiene como principal beneficio el facilitar la segmentación de una red, además de brindar seguridad, flexibilidad y sobre todo el permitir optimizar la red en general.

Castillo (2019), Menciona que la VLAN funciona como agrupaciones definidas por software de estaciones LAN, las cuales se comunican entre sí como si estuviesen conectadas al mismo cable, sin importar que no se encuentren dentro de un mismo segmento de red o en un lugar físico distinto.

2.3.1. Segmentación de red

Una de las principales ventajas que se puede considerar como importante que ofrece las VLANS es el poder segmentar los distintos equipos en redes diferentes, para cada subred se le va a asignar una VLAN distinta, es decir, en el caso de una empresa se pueden crear redes VLAN distintas para cada departamento, ya sea marketing, contabilidad, talento humano, sistemas, otra para administrarla, incluso una subred diferente para invitados, de modo que quienes se conecten a la subred de invitados no puedan tener comunicación con los dispositivos de las otras subredes, garantizando la seguridad de la información por medio de las VLANS.

2.3.2. Flexibilidad

La flexibilidad de red al usar VLANS se da principalmente por el hecho de administrar la red de forma rápida y fácil, ya que se puede crear políticas de comunicación individuales para cada subred que se cree, donde se puede determinar el tipo de tráfico de red que se vaya a tener o incluso se puede denegar el tráfico de cierto tipo como el tráfico de streaming de video.

2.3.3. Optimización de red.

Cuando se habla de optimización de red, se tiene en cuenta principalmente la reducción de transmisión de mensajes de broadcast, esto se debe a que dentro de una red sin la implementación de VLANS, los mensajes de broadcast que se transmiten van a ser dirigidos a todos los dispositivos conectados a esa red, es decir, los dispositivos para los cuales la difusión de algún mensaje no sea dirigida para estos, de igual manera va a recibir el mensaje. Al crear VLANS se crearan dominios de broadcast más pequeños optimizando el tráfico de red y previniendo que la red pueda llegar a saturarse o colapsarse por el continuo envío de mensajes de broadcast que tienen como destino destinatarios innecesarios, por lo tanto, al usar subredes el tráfico de red se va a ver beneficiado principalmente por la reducción en la difusión al agrupar

los destinatarios que si deben tener comunicación dentro de una sub red, optimizando el tráfico de red y manteniendo una red más estable.

2.3.4. Administración

Otra ventaja de crear subredes es que nos ofrece crear redes lógicas que funcionen de forma independiente, es decir cada subred funciona de forma aislada con otra, evitando que exista el tráfico entre VLANS, obligando a que se use dispositivos como Routers o Switches multicapa para que exista comunicación entre las subredes. Al tener subredes y no existir comunicación entre estas se puede asegurar que la información se encuentre fuera del alcance de personas que no estén dentro de la misma subred.

A pesar de que el uso de las VLAN nos ofrece muchos beneficios para administrar y configurar una red, también es importante analizar los puntos negativos de su implementación.

2.3.5. Latencia

Como se mencionó anteriormente, si se usa las VLANS, la optimización de red es notoria, sin embargo, no tiene el mismo nivel de eficacia si lo compara con una WAN (Wide Area Network) donde si va a existir una clara diferencia al segmentar las redes mediante las VLANS, a comparación de una LAN (Local Area Network), que al ser una red relativamente pequeña no tendría mucha diferencia en la latencia de red.

2.3.6. Seguridad en las VLANS

La seguridad dentro de las VLANS depende de forma fundamental de la forma en que se la administre, además de las prestaciones de los equipos que se utilicen para formar las VLANS (Castillo, 2019).

De igual forma se puede decir que la administración va de la mano con la seguridad, esto debido a que mientras más seguridad se busque implementar en una red, esta deberá tener contar con un mayor control a los accesos a los recursos de la red, así como también, controlar las acciones que los miembros de dicha red puedan realizar, lo que significa que la red debe ser administrada de forma rigurosa. Es necesario recalcar que, si no existe una buena asignación de usuarios para que pertenezcan a una VLAN, al contrario, estos se empiezan a trasladar entre VLANS, ponen en un alto riesgo la seguridad del recurso más preciado para una empresa que es la información que exista en dichas VLANS.

En el ámbito empresarial el uso de las VLANS resulta ser de mucho provecho, ya que, permite crear grupos de trabajo, es decir, agrupar miembros de un mismo departamento para que se puedan conectar a una misma LAN, lo que les permite acceder únicamente a los recursos exclusivos de ese departamento. Además, a estos grupos de trabajo se los puede establecer la configuración dedicando el 80% al tráfico de información dentro de la VLAN y el 20 % restante en el tráfico entre VLANS reduciendo de forma considerable el tráfico entre redes virtuales y el uso de enrutadores, esta configuración también es conocida como el criterio 80/20.

Si se habla de reducción de enrutadores es debido a que en una VLAN un switch sabe que puertos son los que pertenecen a cada dominio de broadcast por lo que envía únicamente la información a dichos puertos sin necesidad de tener un enrutador como seria en el caso de que se use una red LAN (Local Area Network o Red de Área Local) normal donde los dominios de broadcast son determinados por los enrutadores.

Mediante el uso de las VLAN principalmente se puede controlar el uso y delimitar el ancho de banda de la red, esto se logra mediante las restricciones a los dominios de broadcast hacia los dominios lógicos donde hayan sido generados, esta restricción se pueden configurar al momento

de crear una VLAN, además dependiendo del tipo de switch que se use, se puede hacer un filtrado de paquetes mediante métodos de identificación los cuales determinan la prioridad que tiene cada paquete para llegar a su destino.

Existen distintos tipos de VLANS las cuales se definen por niveles y son las siguientes:

2.3.7. VLAN por puerto

Es también conocida como VLAN de nivel 1, la cual se define como una red virtual según los puertos a los que se encuentren conectados los equipos con el conmutador, este tipo de VLAN permite que el tráfico de broadcast que produce una VLAN no afecte el rendimiento de otras VLANS que se encuentren creadas ya que el tráfico se mantiene únicamente dentro de la VLAN que produce el tráfico. Sin embargo, al realizar un cambio físico de un dispositivo que pertenezca a esta red, se debe realizar el respectivo cambio de puerto en el conmutador, para evitar realizar este tipo de cambios seguido, es recomendable utilizar mecanismos de asignación dinámica de VLAN para los equipos como puede ser la dirección MAC.

2.3.8. VLAN por dirección MAC

También conocida como VLAN de nivel 2, permite definir una red virtual mediante las direcciones MAC que poseen los equipos, lo que evita realizar cambios de puertos en el conmutador cada vez que un dispositivo asignado a una VLAN se cambie de lugar físicamente, sin embargo, mantiene un complejo nivel de administración y configuración debido a que se debe asignar manualmente las direcciones MAC de cada equipo, por ejemplo, en una empresa grande se tiene una gran cantidad de equipos, por lo que, asignar manualmente las direcciones MAC de cada dispositivo para que pueda ser asignado a una VLAN es muy complejo, pero a la larga ahorra una gran cantidad de tiempo en la administración de los dispositivos cuando estos a se encuentren asignados. Por otra parte, si bien es cierto que este tipo de VLAN permite que un

dispositivo pueda pertenecer a varias VLANS, da como resultado que, el tráfico de paquetes de broadcast sea difundido por todas las VLANS a las que pertenece influyendo directamente en el ancho de banda de la red.

2.3.9. VLAN por filtros

Esta VLAN también conocida como de nivel 3 se basa en asignar dispositivos a una VLAN mediante protocolos como IPv4, IPv6 o por los tipos de encapsulación, los filtros se aplican a las tramas para determinar a qué VLAN pertenece, por ejemplo, todo el tráfico que sea por protocolo IPv6 será asignado a la VLAN3 y el tráfico por protocolo IPv4 será asignado a la VLAN4, por otra parte para implementar este tipo de VLAN es necesario que no existan protocolos dinámicos como lo es el protocolo DHCP siempre y cuando no se encuentre configurado la dirección IP en los dispositivos, ya que el conmutador no podrá clasificar cada equipo a su respectiva VLAN, otro punto a mencionar es el rendimiento en general de conmutador ya que se verá afectado al realizar búsquedas en las tablas de pertenencia asociadas a los protocolos que se vaya a usar, lo que puede producir retardos en la transmisión

2.4. Calidad de servicios (QoS)

Ortega (2019) define a la calidad de servicios como un conjunto de requisitos de asistencia que la red debe realizar para asegurar un nivel que se considere como adecuado para la transmisión de los datos los cuales están basados en estándares de funcionalidad que permiten que los programas en tiempo real puedan optimizar el uso del ancho de banda de la res, asegurando de cierta manera que se pueda utilizar los recursos de la red de forma adecuada.

Una de las principales razones que existen para utilizar QoS es debido a que las redes inalámbricas suelen presentar intermitencias las cuales provocan que los paquetes enviados se pierdan o simplemente no lleguen a su destino, lo cual afecta directamente a la comunicación por

servicios de voz o video a través de aplicaciones por internet que se puede considerar como un gran problema, por esta razón el uso de QoS es importante cuando se utilice este tipo de servicios.

La Calidad de Servicio es el rendimiento de extremo a extremo de los servicios electrónicos tal como lo percibe el usuario final. Los principales parámetros que una red con calidad de servicio debe vigilar que no lleguen a degradar la comunicación son el jitter, el retardo y la pérdida de paquetes a fin de garantizar cierto nivel de calidad según Chauca (2016).

2.4.1. Jitter o variación de retardo

Es una medida de variación para el retraso que existe en el envío de paquetes, mediante las variaciones de un ping en un periodo de tiempo entre el dispositivo que recibe el paquete, así como el que lo envía y viceversa, por lo que lo ideal en una red es que el jitter sea lo menor posible, lo que significa que la red es estable y nos garantiza que el envío de paquetes llegue a su destino sin ningún inconveniente mayor que afecte a la calidad del servicio.

2.4.2. Retardo o Delay

El retardo o Delay o también conocido como la latencia hace referencia al tiempo que se demora un paquete en su trayecto desde el emisor hacia el receptor, por lo que, si se demora en llegar el paquete da la impresión de que la red es lenta. Hoy en día gracias al uso de la fibra óptica para la conectividad por internet, la latencia es muy buena, siempre y cuando se esté conectado por un cable de red, por otra parte, al estar conectado por Wi-Fi las conexiones pueden llegar a ser inestables.

2.4.3. Pérdida de paquetes

En algún momento puede llegar a pasar que un conjunto paquetes que viajan a través de una red no llegue completo, por lo que algunos paquetes pueden llegar a perderse en este medio, puede ser producida por errores en los equipos que estén encargados de brindar conectividad a la red o por excederse en la capacidad que soporte algún buffer.

Existen distintas técnicas para trabajar y solucionar la congestión de una red, las cuales son utilizadas para administrar y priorizar el tráfico de red, en donde pueden existir aplicaciones que soliciten un ancho de banda superior al que la red no les pueda proporcionar, para solucionar estos inconvenientes se prioriza un determinado tipo de tráfico con el único fin de que los usuarios de la red puedan usar las aplicaciones o servicios sin tener problemas como los mencionados anteriormente.

Existen modelos de servicio los cuales se los puede describir como un conjunto de capacidades de calidad de servicio o QoS de extremo a extremo, que es la habilidad que tiene la red para proporcionar un nivel específico de servicio que pueda garantizar el tráfico de red de cada extremo, dentro de este conjunto se tiene tres niveles de servicio que son:

Modelo de mejor esfuerzo de servicio, que se encarga que la red realice todo lo que esté a su alcance para poder entregar el paquete, sin embargo, para lograr esto no garantiza que el paquete siempre use la misma trayectoria.

Modelo de servicio integrado, este modelo permite garantizar un determinado servicio a través de negociación de parámetros de red que van de un extremo a otro extremo para las aplicaciones, además, estas negociaciones tienen el poder de solicitar un nivel de servicio que se considere como adecuado con el fin de que su funcionamiento no se vea afectado o interrumpido,

para esto, es importante mencionar que la aplicación no va a enviar ningún tipo de tráfico hasta que reciba una señal de la red la cual le garantice que la red esta apta para manejar la carga y entregar los paquetes a su destino.

Por último, existe al modelo de servicios diferenciado, que incluye un conjunto de herramientas para la clasificación y para la gestión de colas para su correcto funcionamiento junto con la prestación de ciertos protocolos, los servicios diferenciados funcionan en base a sus Routers que se encuentren en cada extremo, con el único fin de ejecutar la clasificación de los distintos paquetes que sean usados por la red.

2.5. Tipos de encolamiento o queueing.

El encolamiento es la herramienta que permite controlar la congestión del tráfico de una red, la cual permite priorizar y reordenar paquetes antes de que estos sean transmitidos a su dirección de destino.

2.5.1. FIFO

Llamado así por sus siglas en ingles First-in, First-out, el primero en llegar es el primero en salir, es conocido como el método de encolamiento más sencillo, ya que, no supone una prioridad de entrega de paquetes debido a que los paquetes son colocados en una única cola y estos son entregados a medida que van llegando, una de las principales desventajas que presenta este encolamiento es que, si se llegase a llenar la cola, los paquetes que quisieran entrar se van a perder y no van a llegar a su dirección de destino.

2.5.2. WFQ

Conocido también como encolamiento controlado basado en pesos, este tipo de encolamiento se caracteriza por asignar y priorizar un ancho de banda para el distinto tipo de tráfico de la red,

gracias a esta asignación se puede decidir el orden en el que los paquetes van a ser entregados, se crea una cola para las colas, las cuales van a pasar a través de un servidor “todos contra todos” en un orden secuencial circular, debido a que cada flujo posee una cola asignada, si se llegase a presentar demasiadas tramas de datos, el único afectado va a ser la cola con la clase específica para dicha trama de datos.

2.5.3. CBWFQ

Es el encolamiento basado en pesos que a su vez se basa en clases, se caracteriza por utilizar el campo DSCP, o campo de calidad de servicio, del datagrama IP, utiliza también listas de acceso o las propias interfaces de entrada para configurar el encolamiento que van a tener los paquetes, este encolamiento funciona con una cola que va a reservar para cada clase, y el tráfico correspondiente va automáticamente a la cola que haya sido asignada. Al usar este encolamiento es importante especificar el límite que tendrá la cola con la clase, esto incluye el ancho de banda de la red, la cantidad de paquetes máxima que se admitirán, así como, el ancho de banda que se tendrá en el caso de que la red se llegue a congestionar.

2.5.4. LLQ

Conocido como encolamiento de baja latencia, está basado en el uso de colas de prioridad personalizadas, estas colas se basan en clases de tráfico que hayan sido configuradas previamente por un administrador de red, en este encolamiento las colas que se hayan determinado como más importantes son las que tendrán preferencia.

CAPÍTULO III: DISEÑO Y CONFIGURACIÓN DE RED

3. Diseño de red en Cisco Packet Tracer

En este capítulo se llevará a cabo el diseño y la configuración de la red, para lo cual se hará uso del simulador de Cisco llamado Packet Tracer, el cual nos permite realizar simulaciones de un entorno de red, ya que cuenta con un número considerable de dispositivos de red los cuales se pueden configurar para las diferentes necesidades o problemas que se busque encontrar una solución.

En este trabajo se utilizó la versión 8.2 de Packet Tracer, que está disponible para distintas plataformas como Windows, Linux y Mac.

3.1. Diseño y configuración de red

Para empezar la configuración se procede a poner el caso hipotético que existen seis departamentos dentro de una empresa donde se configurará una VLAN para cada departamento, los cuales cuentan con distintos equipos que utilizan conexión a internet mediante el uso de switches de capa 2, donde posteriormente se crearan las VLAN y un router donde se configurará lo necesario para implementar la calidad de servicios.

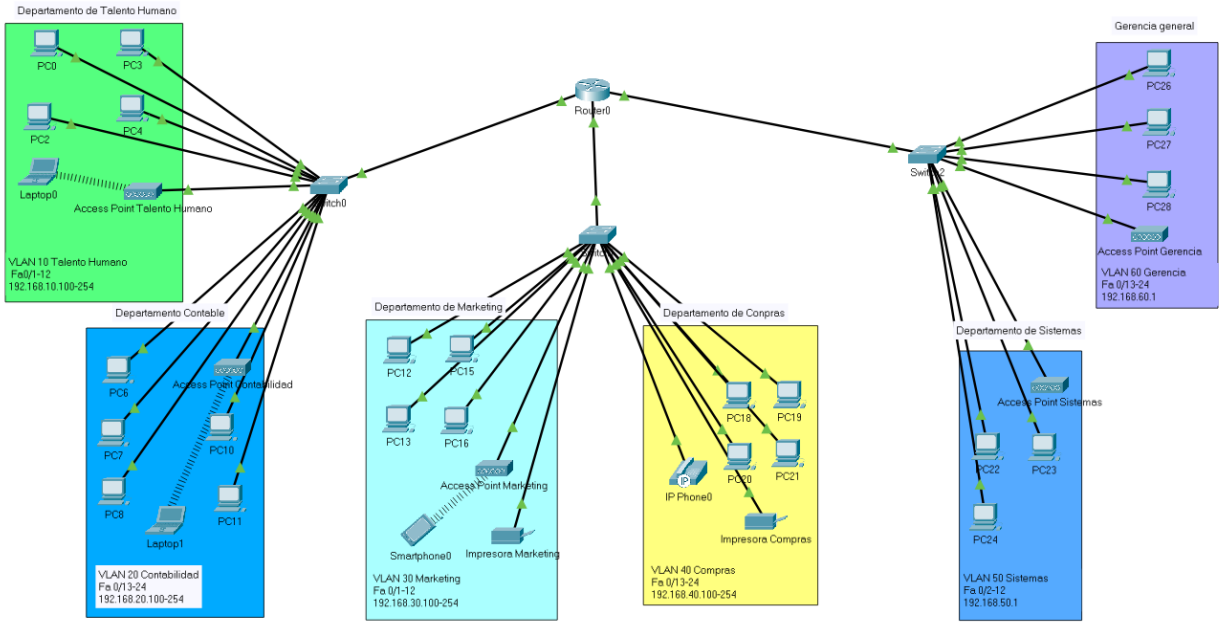
3.2. Topología de red

La topología que se empleará es una topología de tipo árbol, la cuál es la resultante de la combinación de la topología de bus y de estrella, en esta topología de red existe un nodo central al cuál se conectarán los demás dispositivos, que en este caso vendría a ser el switch.

En la topología de árbol se busca asemejarse a un modelo jerárquico, por lo que es recomendable el uso de esta topología debido a que los dispositivos a conectar se encuentran agrupados en diferentes áreas.

Figura 1.

Topología a ser usada en la red.



3.3. Configuración de equipos

Los equipos que van a ser utilizados, así como sus funciones se menciona en la siguiente tabla.

Tabla 1.

Tabla de equipos utilizados

Equipo	Nombre	Función
Switch 2960	Switch0	Alojamiento de VLAN 10, 20 y enlace troncal

Switch 2960	Switch1	Alojamiento de VLAN 30, 40 y enlace troncal
Switch 2960	Switch2	Alojamiento de VLAN 50, 60 y enlace troncal
Access Point	Access Point Talento Humano	Acceso inalámbrico a la red de VLAN correspondiente al departamento
Access Point	Access Point Contabilidad	Acceso inalámbrico a la red de VLAN correspondiente al departamento
Access Point	Access Point Marketing	Acceso inalámbrico a la red de VLAN correspondiente al departamento
Access Point	Access Point Compras	Acceso inalámbrico a la red de VLAN correspondiente al departamento
Access Point	Access Point Sistemas	Acceso inalámbrico a la red de VLAN correspondiente al departamento
Access Point	Access Point Gerencia	Acceso inalámbrico a la red de VLAN correspondiente al departamento
Router 4331	Router0	Pool de DHCP, comunicación entre VLANS por medio de Dot1Q, políticas de calidad de servicio

3.4. Configuración de VLANS

Una vez definida la topología de red que se va a emplear se procederá a configurar los respectivos switches que van a permitir que existan las VLANS respectivas para cada departamento, las cuáles se puede ver más detallada en la siguiente tabla.

Tabla 2

Nombre de la tabla

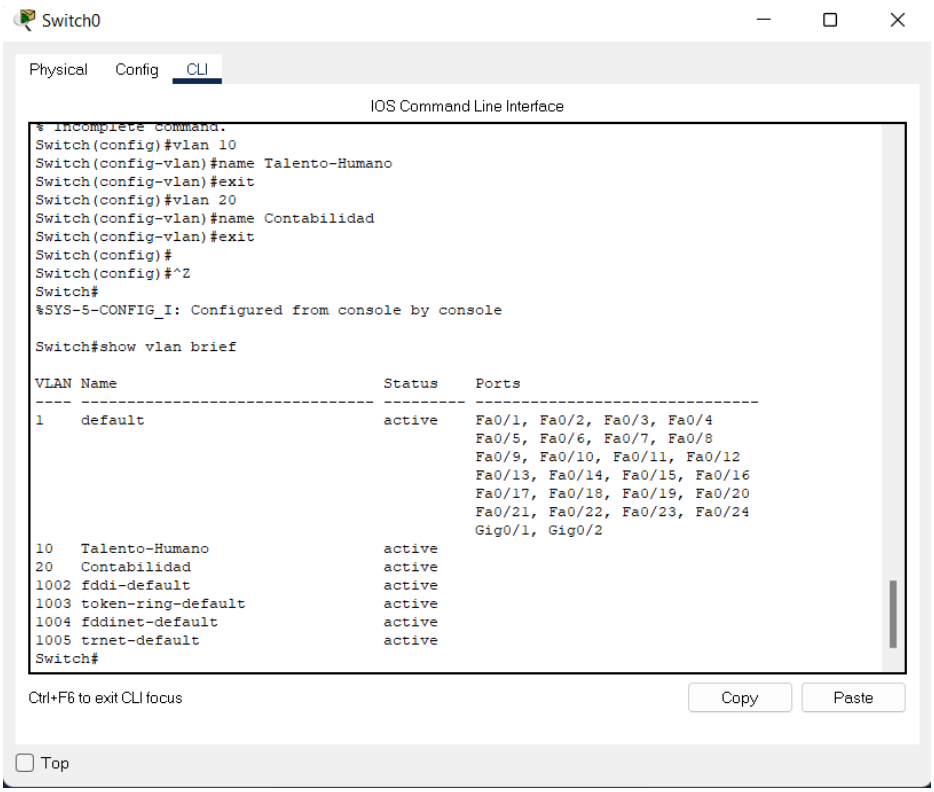
Departamento	Número de VLAN	Nombre de la VLAN	Interfaces en el switch	Rango de IP
Talento Humano	10	Talento Humano	SW0 Fa0/1-12	192.168.10.100-254
Contabilidad	20	Contabilidad	SW0 Fa0/13-24	192.168.20.100-255
Marketing	30	Marketing	SW1 Fa0/1-12	192.168.30.100-256

Compras	40	Compras	SW1 Fa0/13-24	192.168.40.100-257
Sistemas	50	Sistemas	SW2 Fa0/1-12	192.168.50.100-258
Gerencia	60	Gerencia	SW2 Fa0/13-24	192.168.160.100-259

En primer lugar, se va a empezar por la configuración de las VLAN respectivas para el switch0, sin asignar el rango de direcciones IP, ya que esta se la va a aplicar más adelante en la configuración del router.

Figura 2.

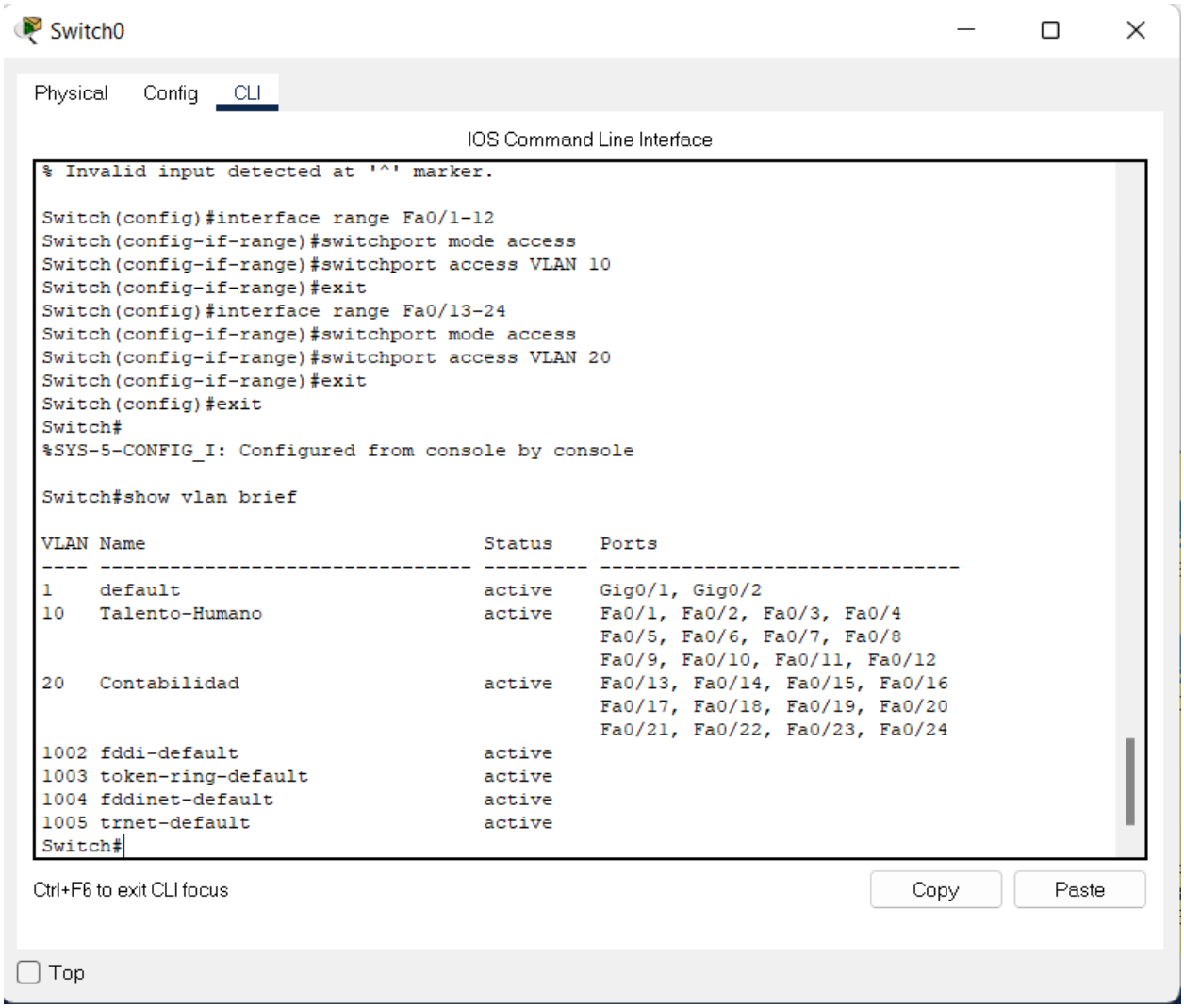
Creación de VLAN 10 y 20 en Switch 0.



Continuando con la configuración se procede a asignar las interfaces que posee el switch a las VLAN que se han creado dentro de este, siguiendo las especificaciones de la tabla

Figura 3

Asignación de VLANS a puertos de Switch0.



Seguido se debe realizar las mismas configuraciones en cada switch, teniendo en cuenta los requerimientos de la tabla para la creación de las VLAN

Figura 4.

Creación de VLANS 30 y 40 en Switch1.

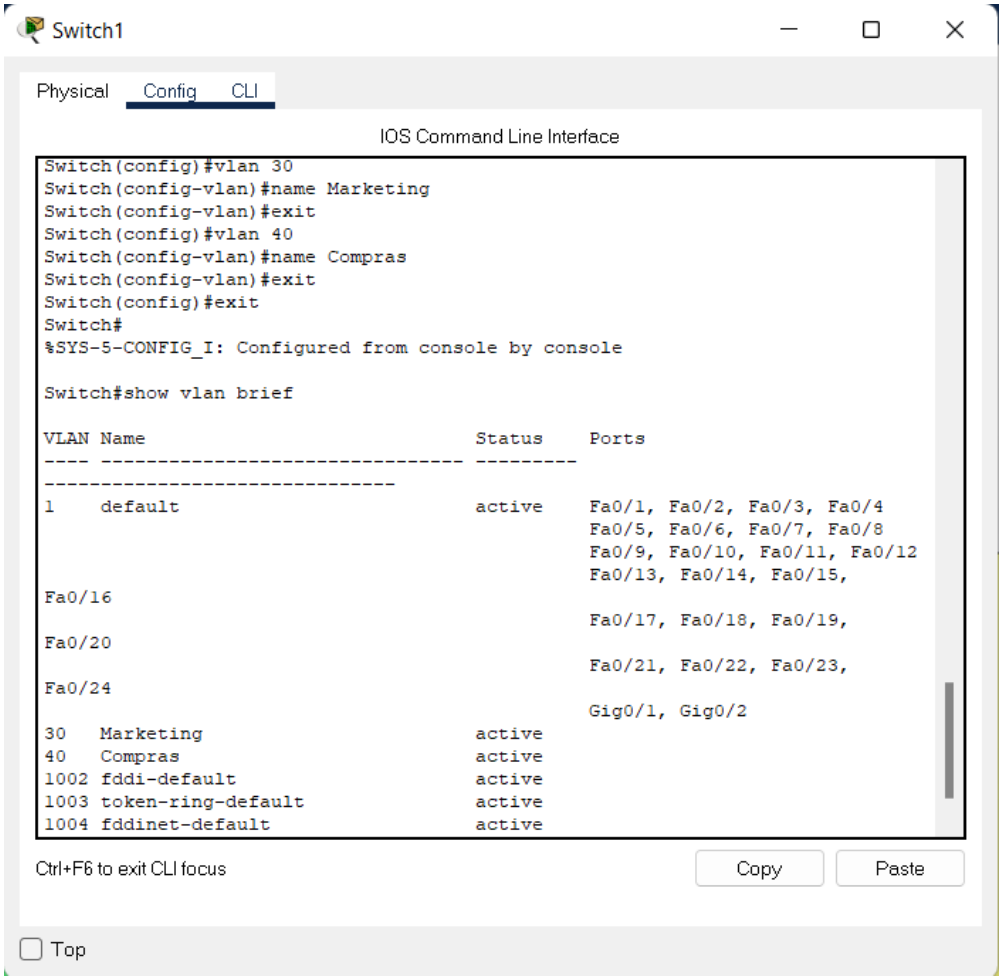


Figura 5

Asignación de VLANS a puertos de Switch1.

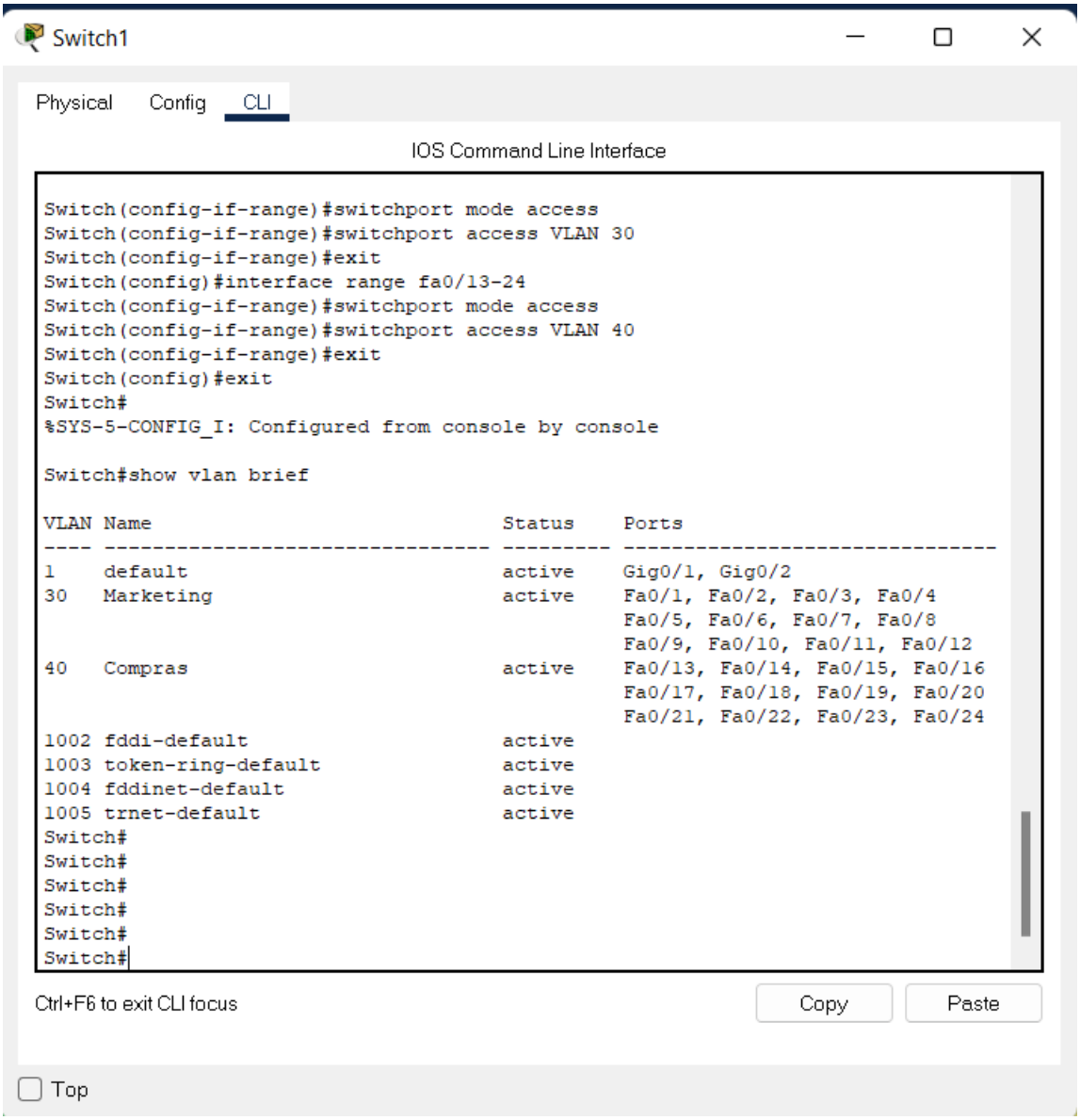


Figura 6

Creación de VLANS 50 y 60 en Switch2

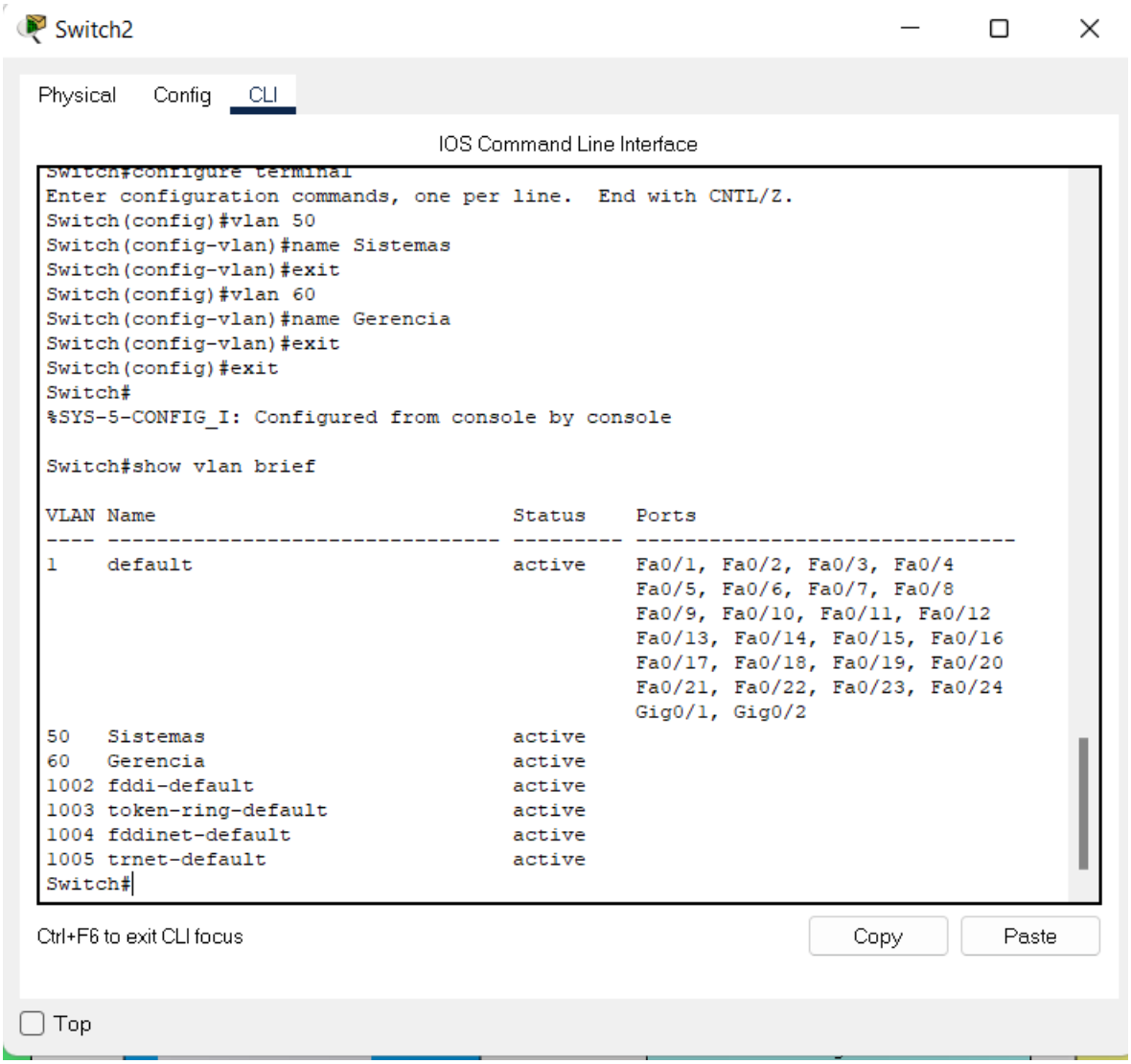
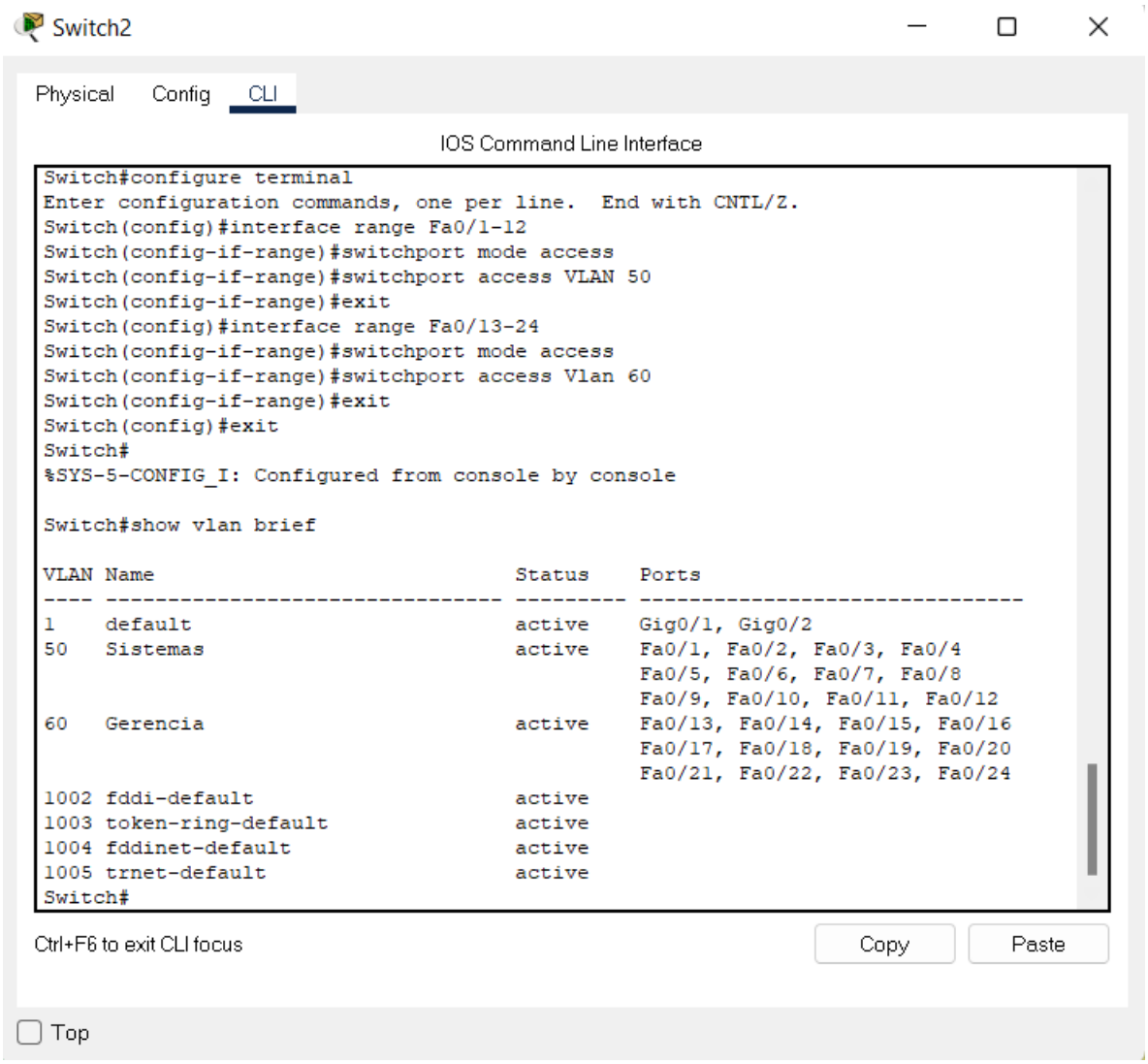


Figura 7

Asignación de VLANS a puertos del Switch2.



Una vez culminado con la configuración anterior se va a establecer la interfaz GigabithEthertnet0/1 como enlace troncal para permitir que el tráfico fluya en un mismo canal para distintas VLANS, para lo cual se va a configurar cada switch con la interfaz G0/1 como enlace troncal, al cual solo se permitirá el acceso al tráfico a las VLANS creadas en cada switch.

Figura 8

Asignación de enlace troncal en Switch0.

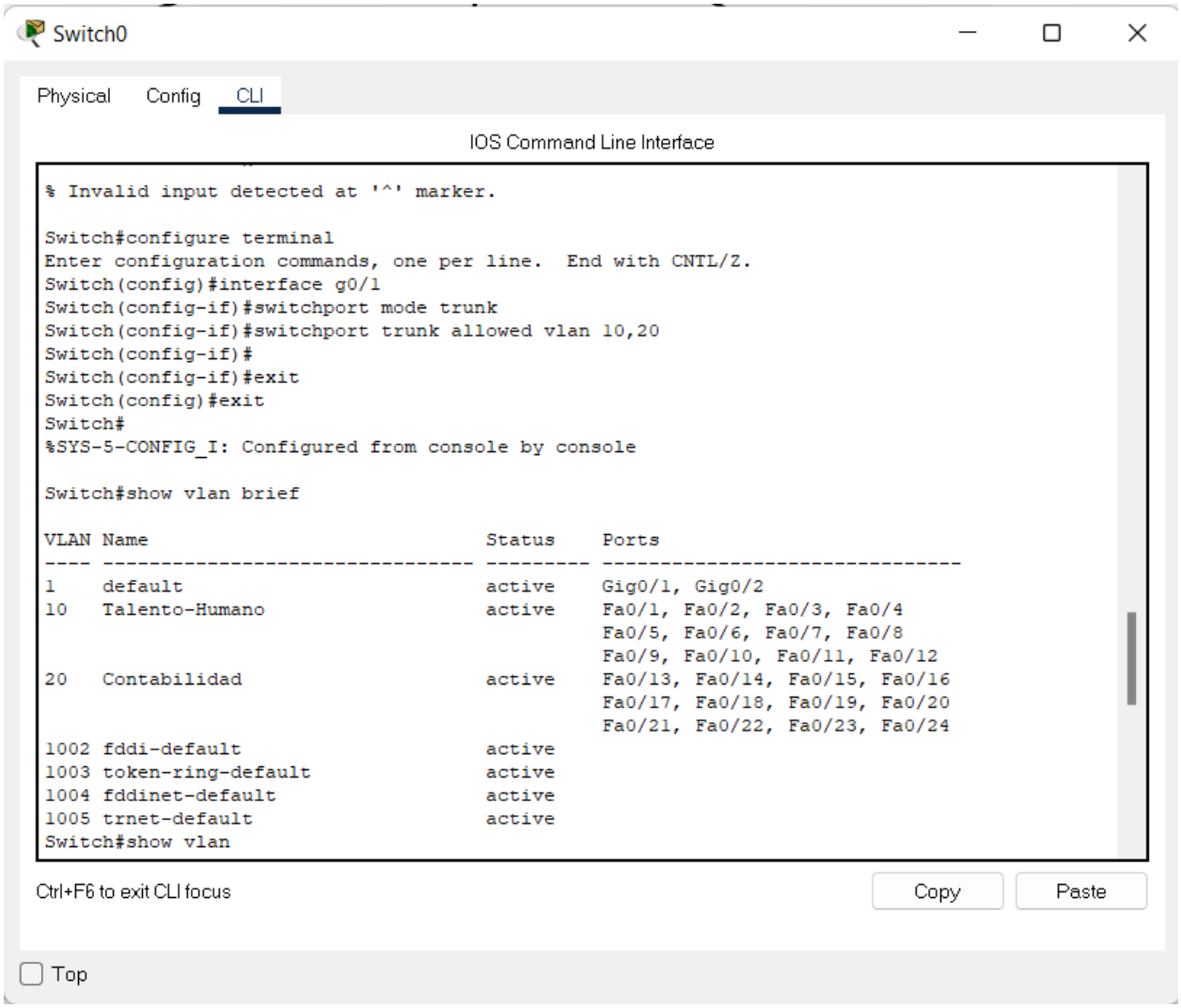


Figura 9

Asignación de enlace troncal en Switch1.

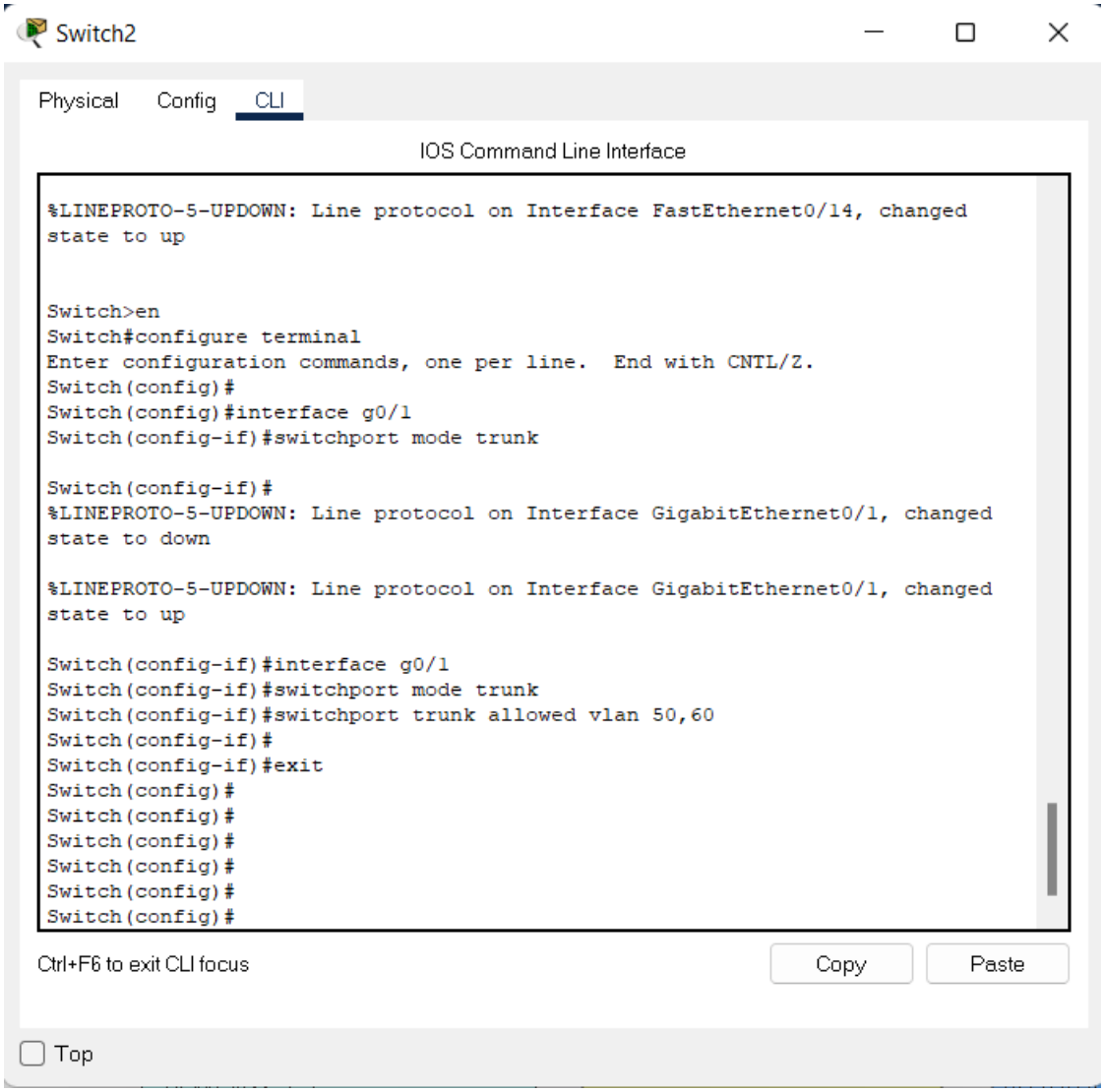
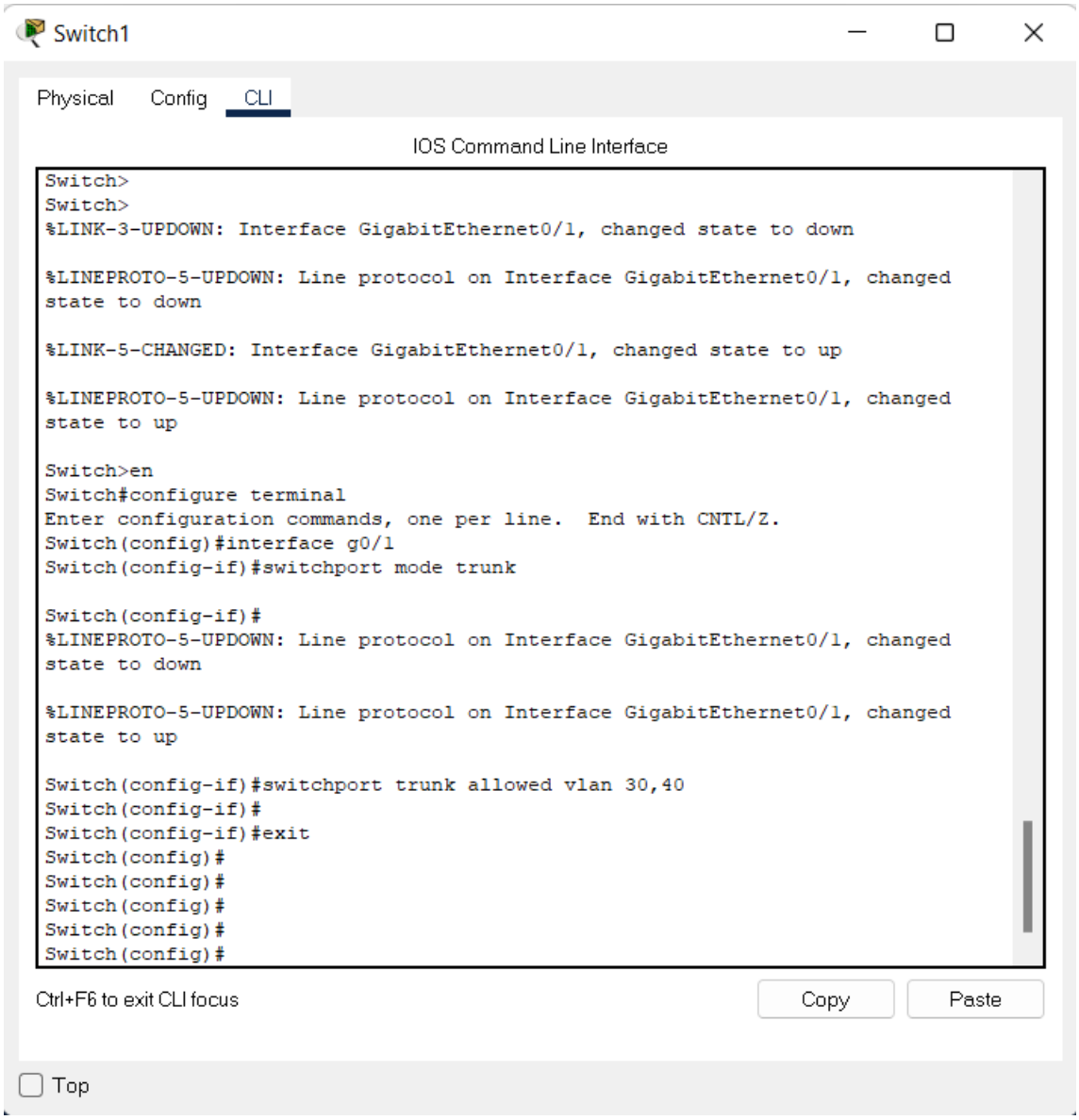


Figura 10

Asignación de enlace troncal en Switch1.



A continuación, se va a proceder con la configuración del router, para lo cual lo primero a realizar va a ser activar el protocolo de encapsulación dot1Q o también conocido como el protocolo IEEE 802.1Q, el cual va a ser el encargado del etiquetar los paquetes con la información de sus respectivas VLAN que se fueron creadas anteriormente con el fin de que el tráfico generado en los switches pueda ser procesado en el router.

Para configurar el protocolo dot1Q, se lo debe realizar creando subinterfaces que correspondan a cada VLAN, con el fin de poder comunicar los datos que envíe el switch al router, aquí también se procede a determinar una dirección IP para cada subinterfaz.

Figura 11

Asignación de enlace troncal en Switch1.

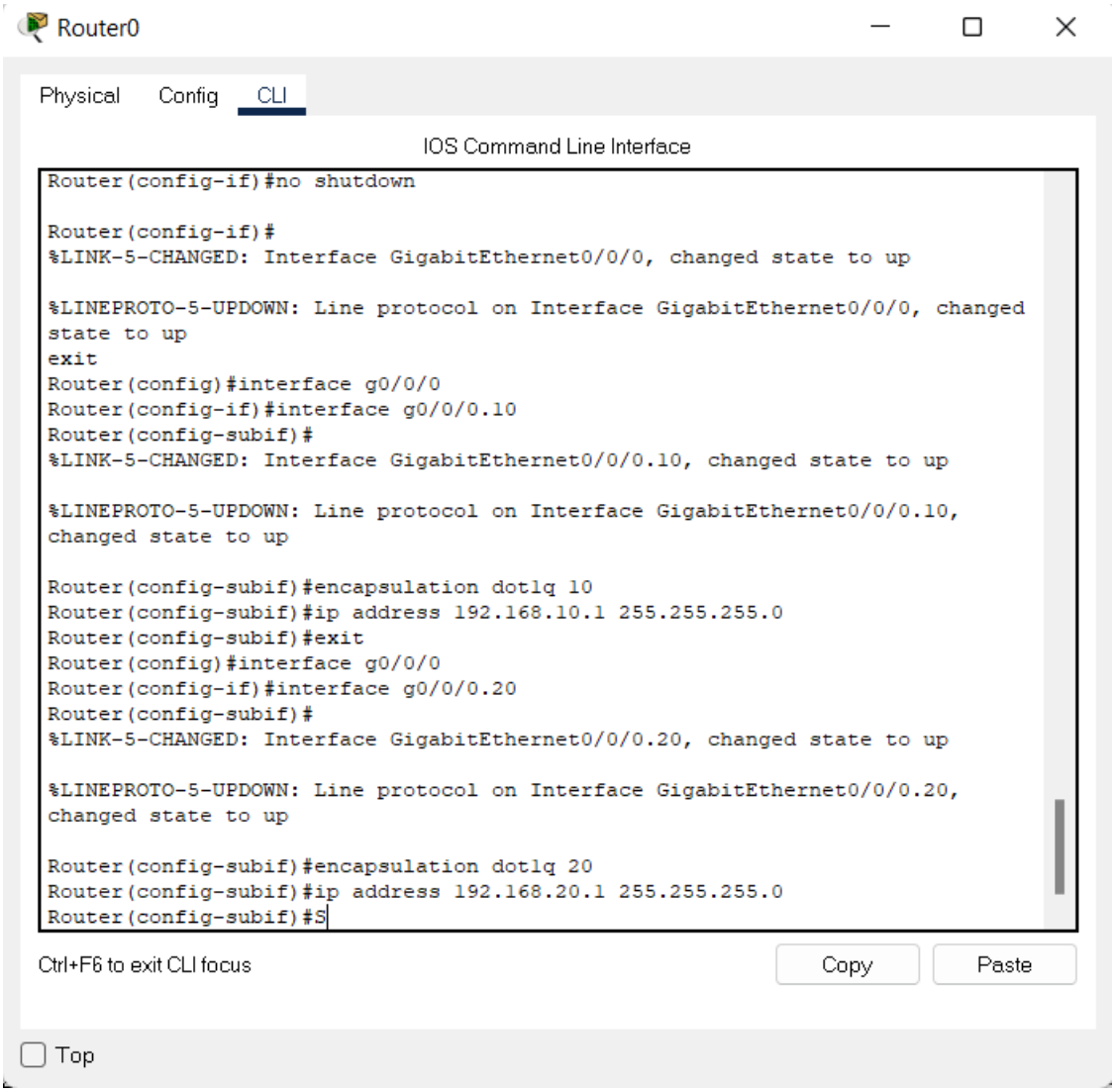


Figura 12

Asignación de enlace troncal en Switch1.

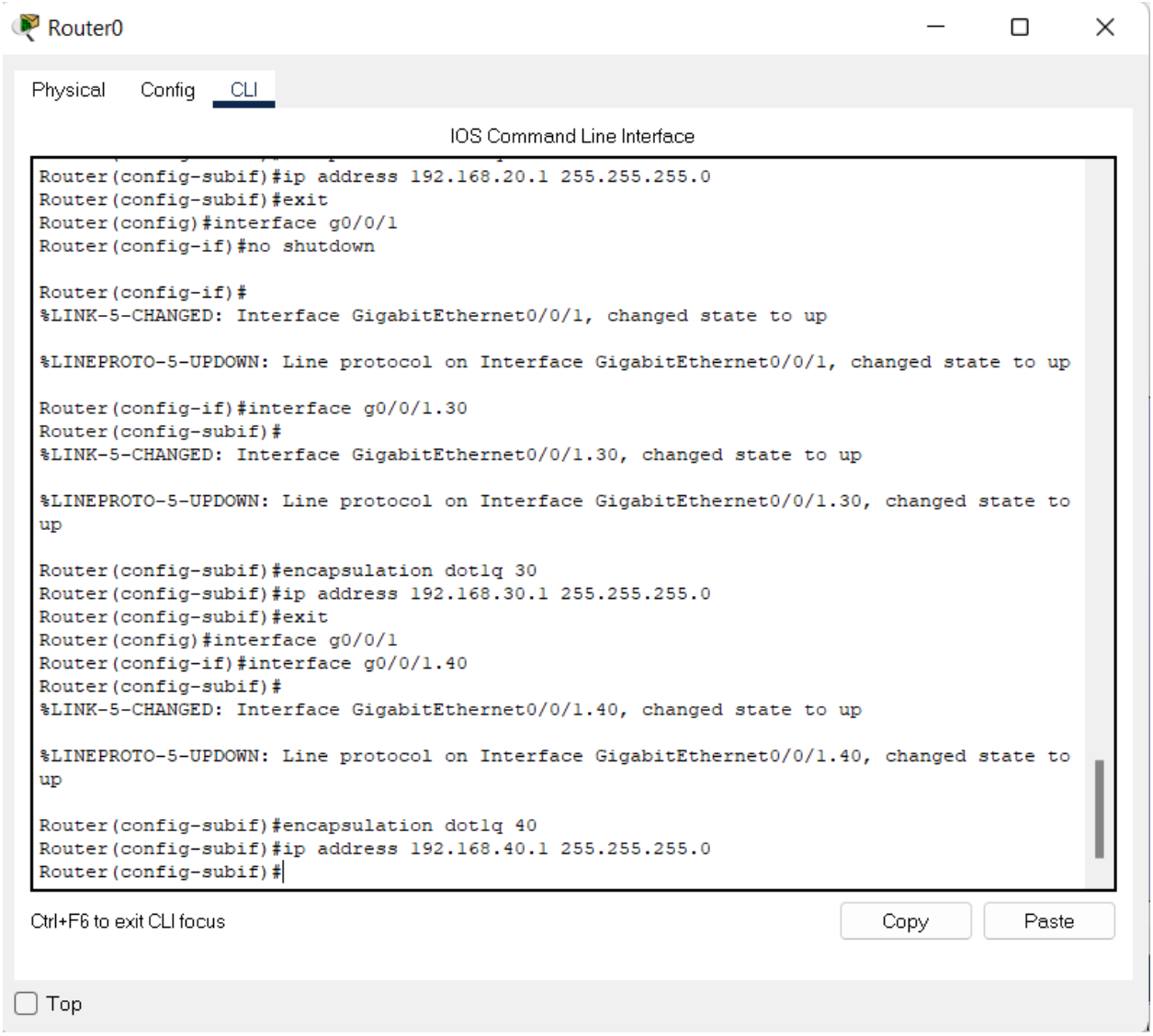
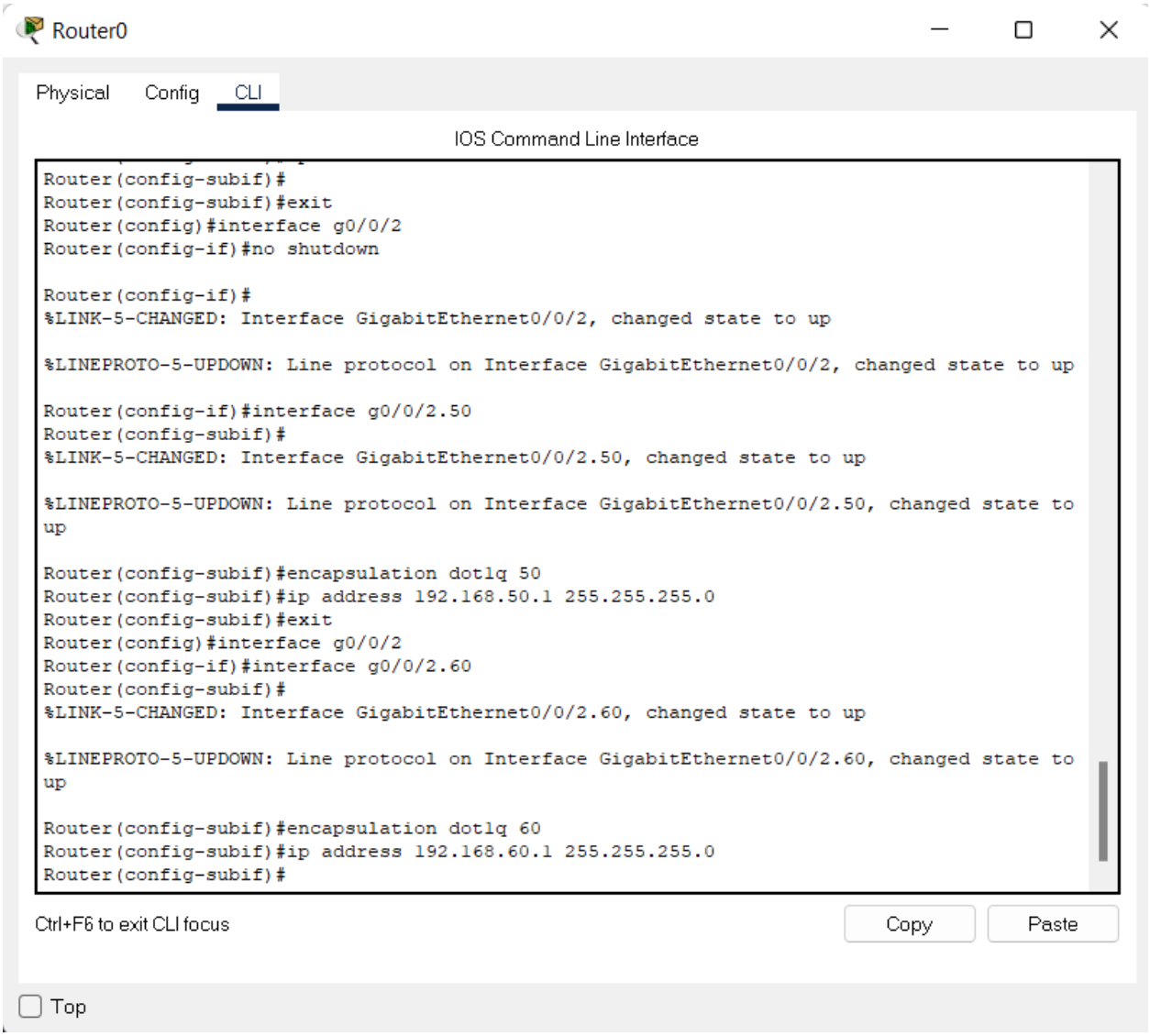


Figura 13

Asignación de enlace troncal en Switch2.



3.5. Configuración de DHCP

Se procede a configurar un pool de DHCP en el router con el fin de que cada VLAN pueda asignar direcciones IP a sus equipos de forma dinámica gracias a este protocolo, para lo cual se va a definir las direcciones correspondientes en la tabla 3.

Tabla 3.

Tabla de asignación de direcciones de red para las VLANS

Número de VLAN	Dirección de red	Servidor DNS	Default-router	Rango de IP
10	192.168.10.0	8.8.8.8	192.168.10.1	192.168.10.100-254
20	192.168.20.0	8.8.8.8	192.168.20.1	192.168.20.100-255
30	192.168.30.0	8.8.8.8	192.168.30.1	192.168.30.100-256
40	192.168.40.0	8.8.8.8	192.168.40.1	192.168.40.100-257
50	192.168.50.0	8.8.8.8	192.168.50.1	192.168.50.100-258
60	192.168.60.0	8.8.8.8	192.168.60.1	192.168.160.100-259

Figura 14

Asignación de DHCP para VLANS 10 y 20 en Router0.

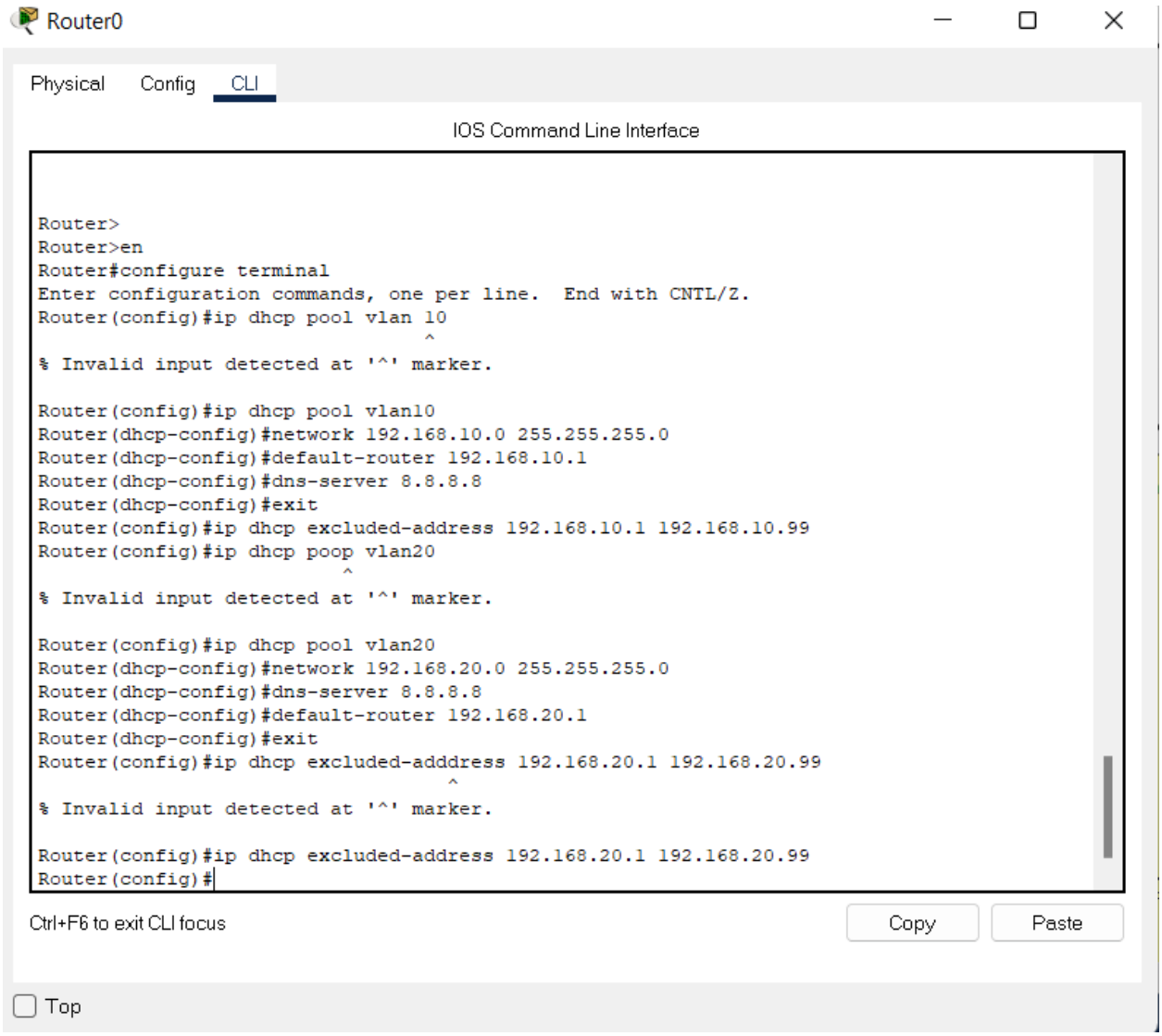
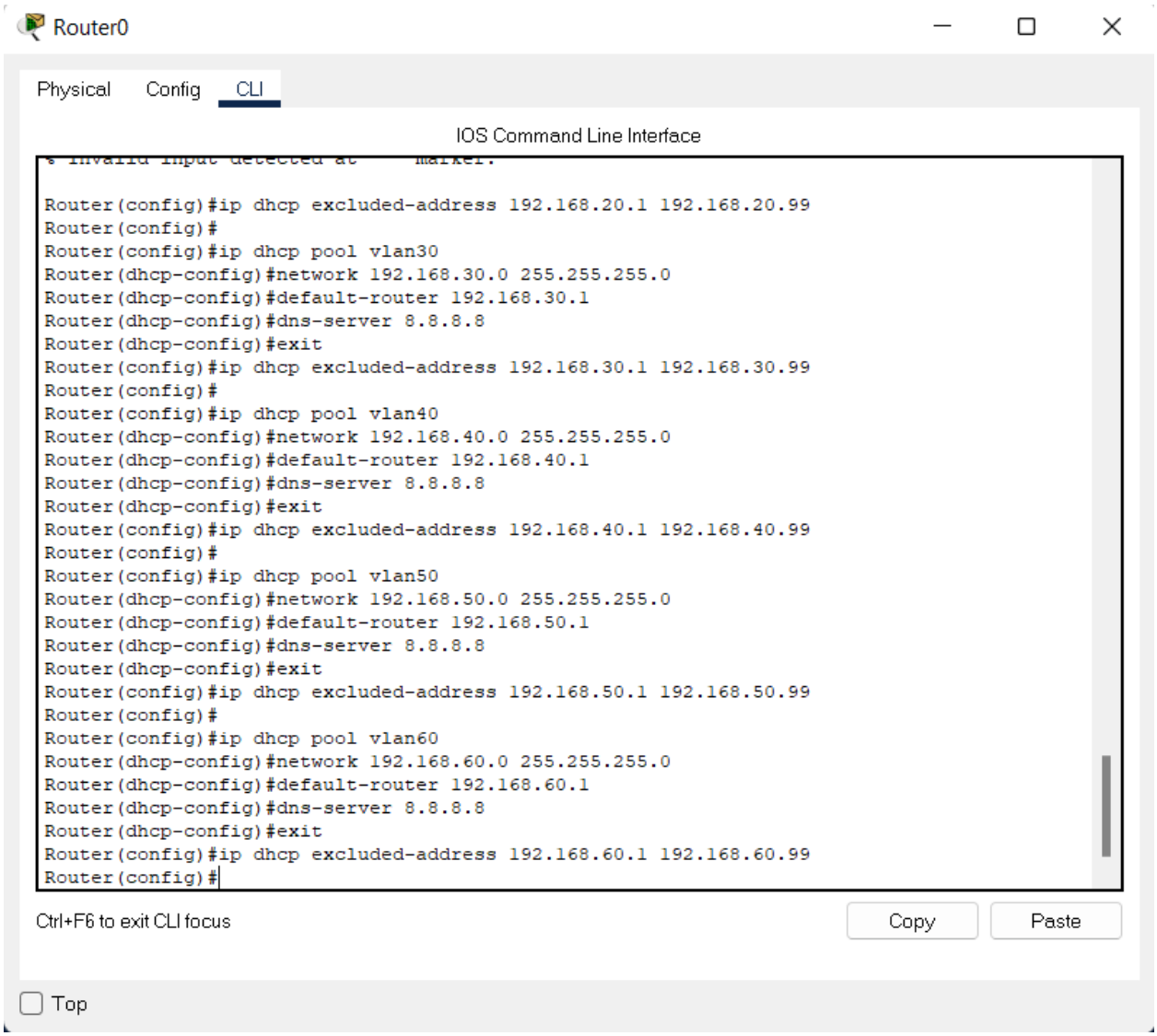


Figura 15

Asignación de DHCP para VLANS 30, 40, 50 y 60 en Router0.



3.6. Verificación de DHCP

Una vez culminada la asignación de direcciones IP se procede a verificar las direcciones IP que arrojan los equipos mediante DHCP.

Figura 16

Asignación de DHCP en PC3.

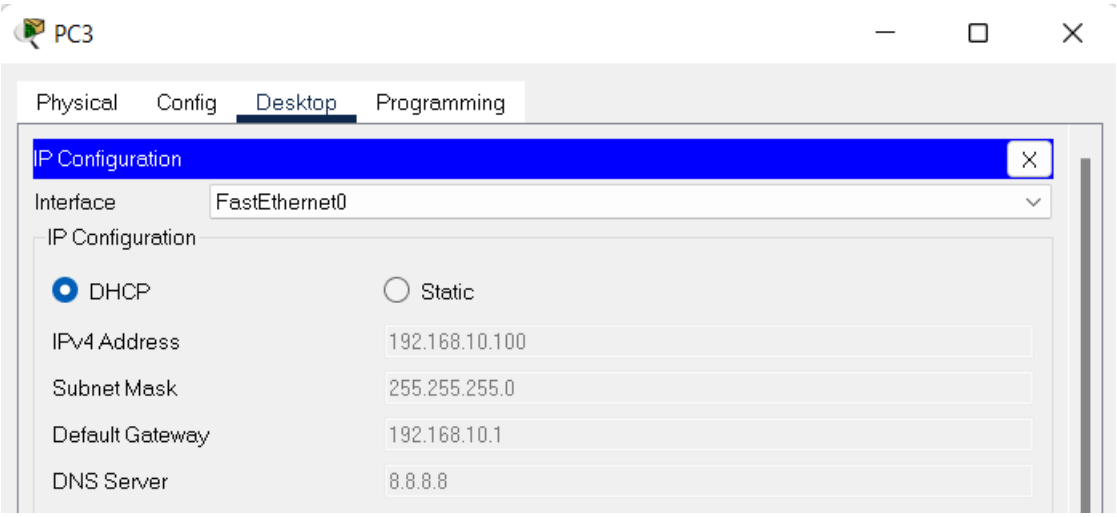


Figura 17

Asignación de DHCP en PC6.

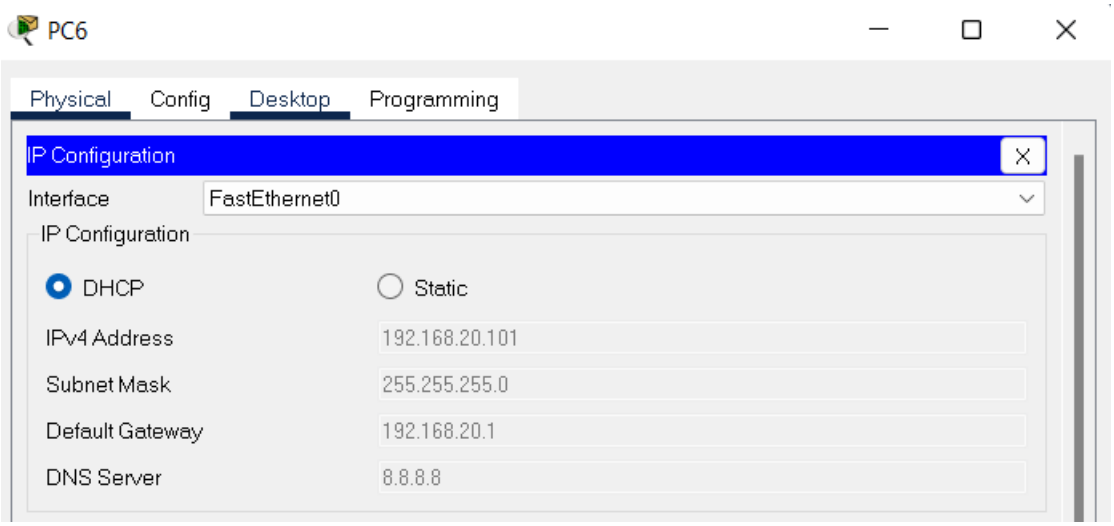


Figura 18

Asignación de DHCP en PC12.

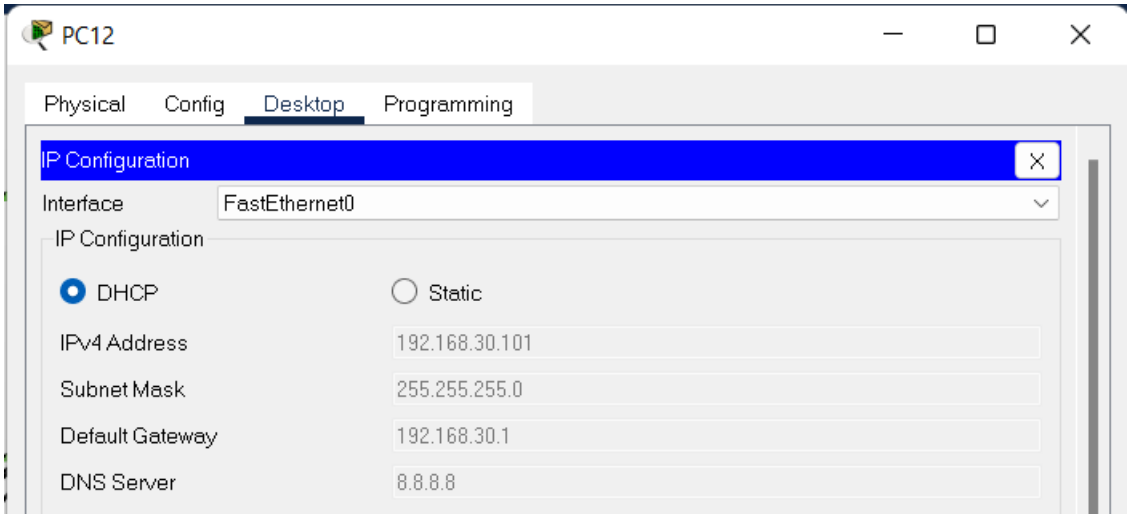


Figura 19

Asignación de DHCP en PC18.

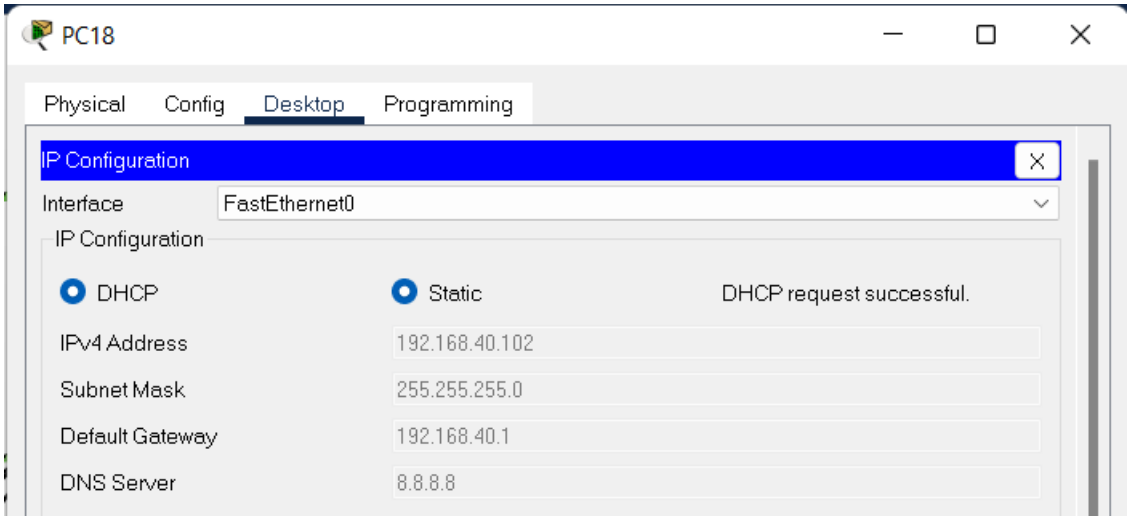


Figura 20

Asignación de DHCP en PC22.

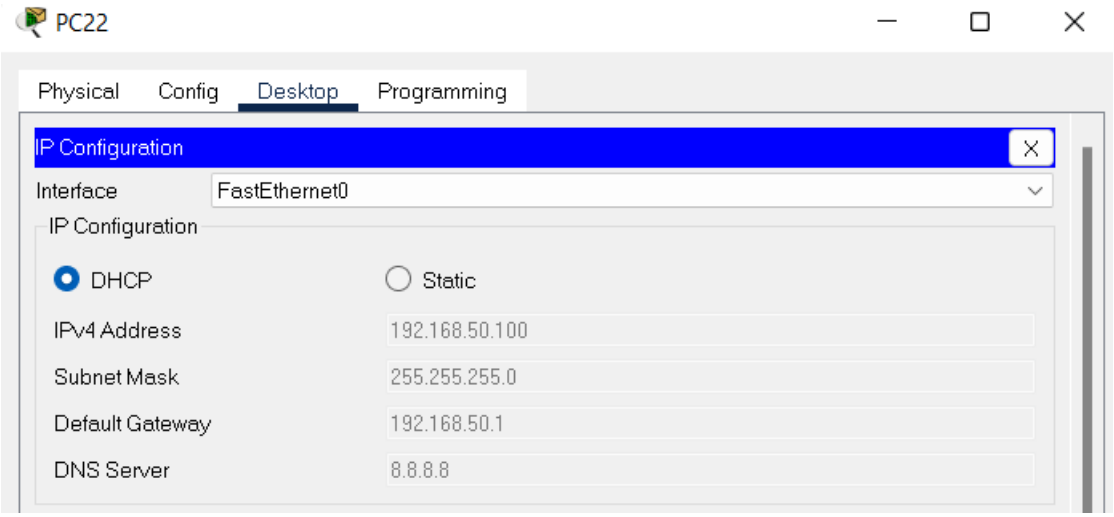
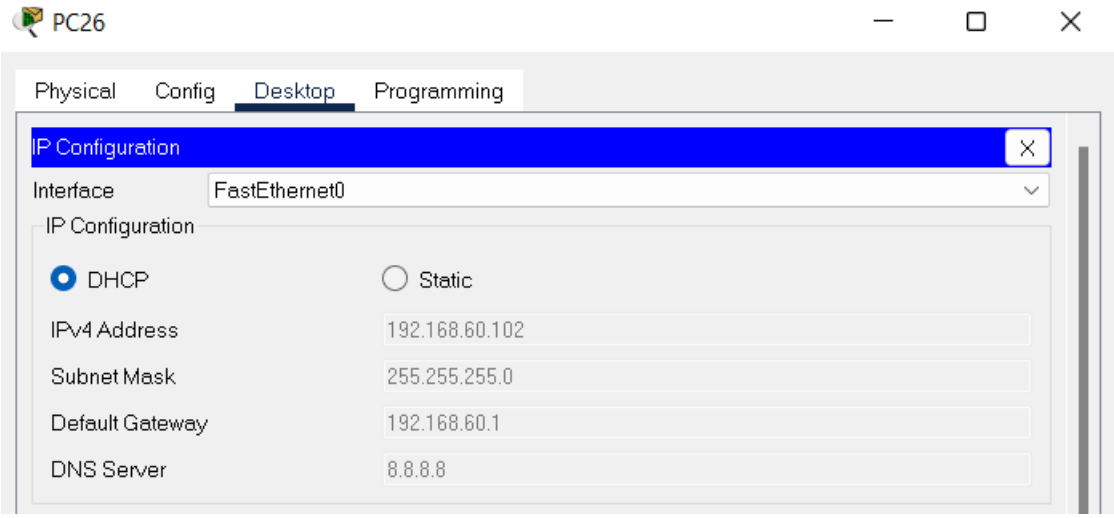


Figura 21

Asignación de DHCP en PC26.



3.7. Configuración de QoS

Para entender el funcionamiento de la calidad de servicios se va a crear class-map con el fin de explicar cómo configurar el router. Para lo cual se debe considerar que dentro del tráfico de red existen varios protocolos como el RTP para audio y video, el cual es usado comúnmente en

los servicios de VoIP, y se procede a tomar este protocolo como ejemplo, para el cual dentro del router se procede a crear una class-map con el nombre de “voice”, donde se debe asignar el tipo de protocolo que se quiere que reconozca esa clase, como en este caso el RTP.

Figura 22

Configuración de class-map para protocolo RTP en Router0.

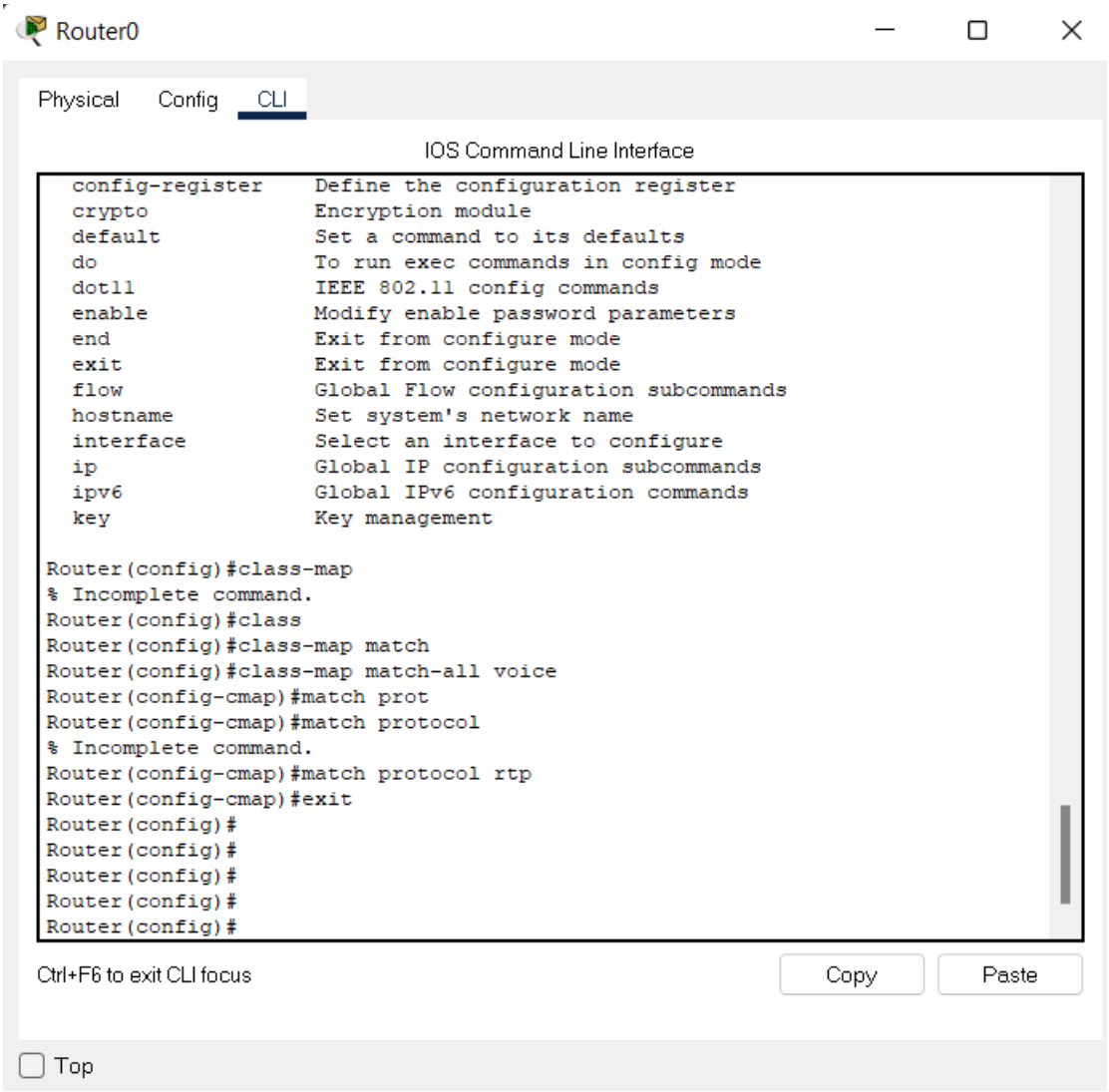


Figura 23

Configuración de class-map para protocolo http en Router0.

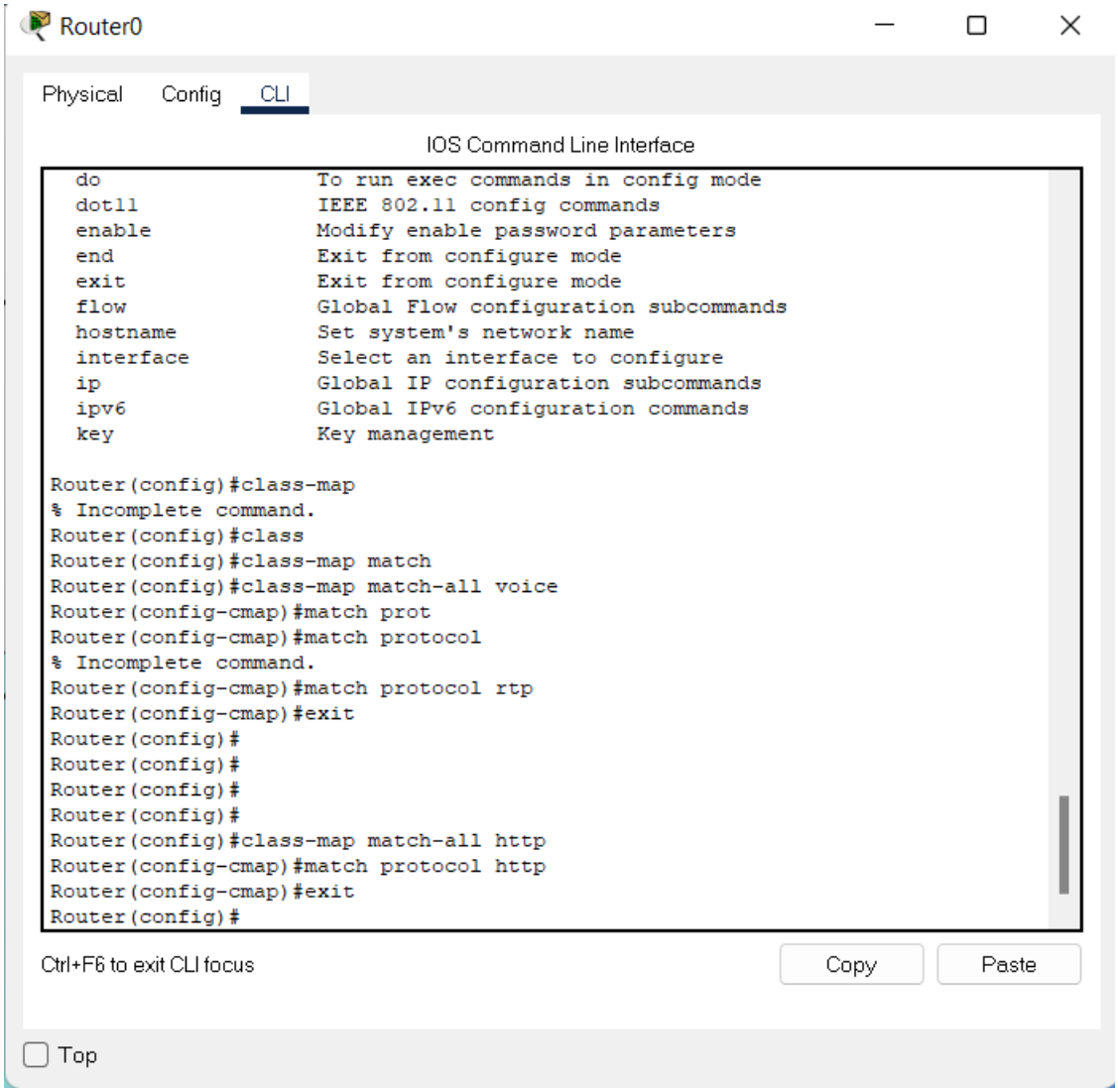
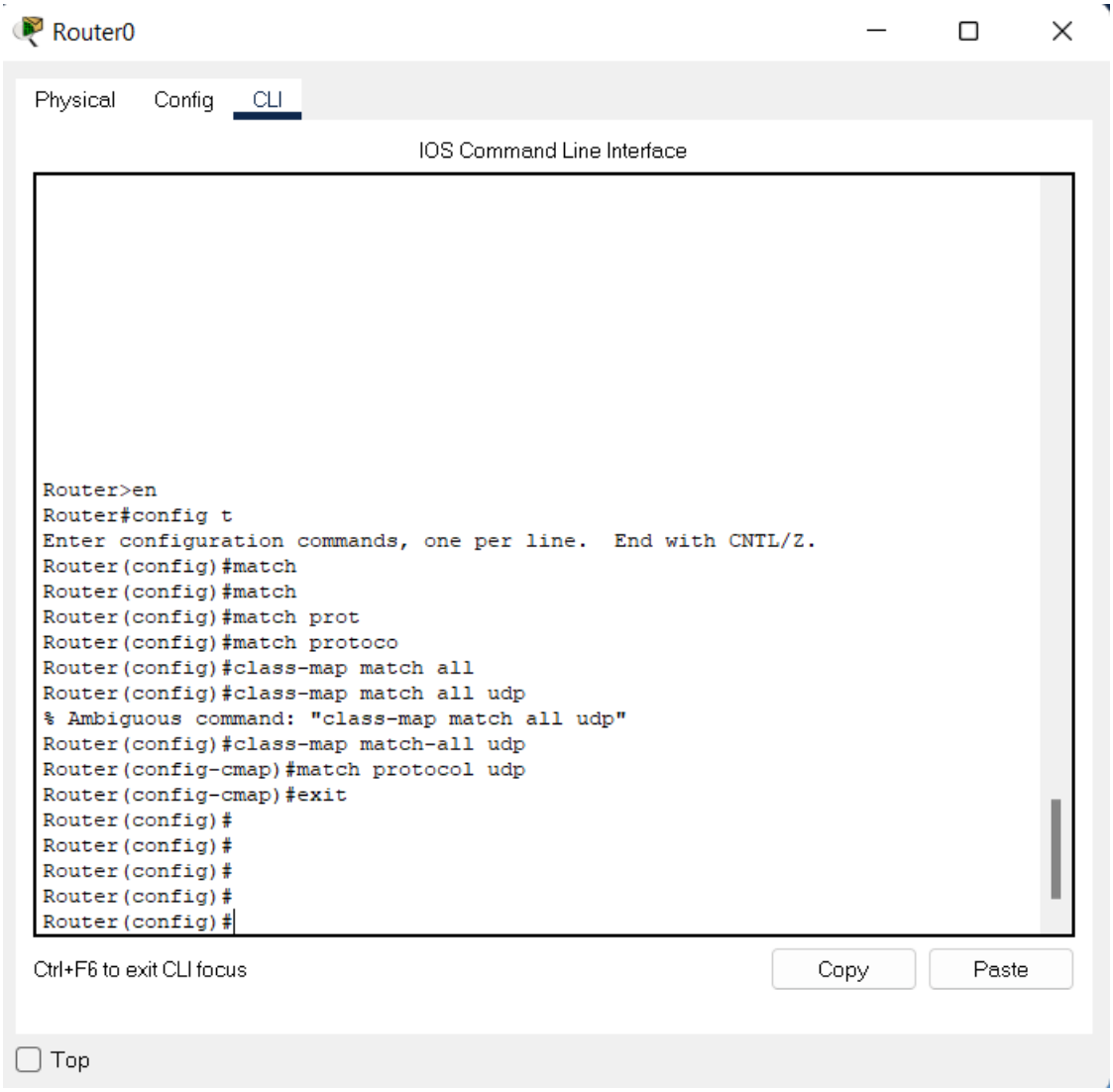


Figura 24

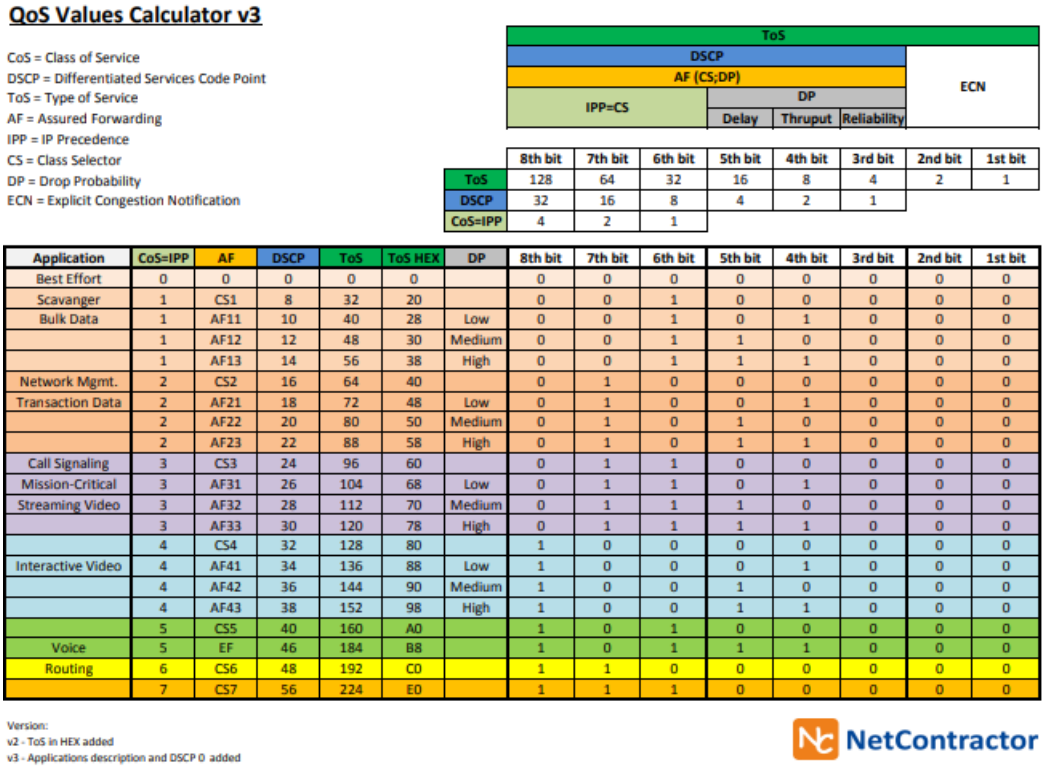
Configuración de class-map para protocolo UDP en Router0



Existe una tabla conocida como QoS Values Calculator, la cual especifica los valores de prioridad que tienen las aplicaciones, donde 0 son las menos importantes y 7 las más importantes o críticas.

Figura 25

QoS Values Calculator



QoS Values Calculator v3

CoS = Class of Service
DSCP = Differentiated Services Code Point
ToS = Type of Service
AF = Assured Forwarding
IPP = IP Precedence
CS = Class Selector
DP = Drop Probability
ECN = Explicit Congestion Notification

ToS								
DSCP							ECN	
AF (CS;DP)								
IPP=CS			DP					
			Delay	Thruput	Reliability			

	8th bit	7th bit	6th bit	5th bit	4th bit	3rd bit	2nd bit	1st bit
ToS	128	64	32	16	8	4	2	1
DSCP	32	16	8	4	2	1		
CoS=IPP	4	2	1					

Application	CoS=IPP	AF	DSCP	ToS	ToS HEX	DP	8th bit	7th bit	6th bit	5th bit	4th bit	3rd bit	2nd bit	1st bit
Best Effort	0	0	0	0	0		0	0	0	0	0	0	0	0
Scavanger	1	CS1	8	32	20		0	0	1	0	0	0	0	0
Bulk Data	1	AF11	10	40	28	Low	0	0	1	0	1	0	0	0
	1	AF12	12	48	30	Medium	0	0	1	1	0	0	0	0
	1	AF13	14	56	38	High	0	0	1	1	1	0	0	0
Network Mgmt.	2	CS2	16	64	40		0	1	0	0	0	0	0	0
Transaction Data	2	AF21	18	72	48	Low	0	1	0	0	1	0	0	0
	2	AF22	20	80	50	Medium	0	1	0	1	0	0	0	0
	2	AF23	22	88	58	High	0	1	0	1	1	0	0	0
Call Signaling	3	CS3	24	96	60		0	1	1	0	0	0	0	0
Mission-Critical	3	AF31	26	104	68	Low	0	1	1	0	1	0	0	0
Streaming Video	3	AF32	28	112	70	Medium	0	1	1	1	0	0	0	0
	3	AF33	30	120	78	High	0	1	1	1	1	0	0	0
	4	CS4	32	128	80		1	0	0	0	0	0	0	0
Interactive Video	4	AF41	34	136	88	Low	1	0	0	0	1	0	0	0
	4	AF42	36	144	90	Medium	1	0	0	1	0	0	0	0
	4	AF43	38	152	98	High	1	0	0	1	1	0	0	0
	5	CS5	40	160	A0		1	0	1	0	0	0	0	0
Voice	5	EF	46	184	B8		1	0	1	1	1	0	0	0
Routing	6	CS6	48	192	C0		1	1	0	0	0	0	0	0
	7	CS7	56	224	E0		1	1	1	0	0	0	0	0

Version:
v2 - ToS in HEX added
v3 - Applications description and DSCP 0 added

NetContractor

Fuente. http://www.netcontractor.pl/download/QoS%20Values%20Calculator%20v3.pdf

Para determinar que protocolos de red son los más críticos en una empresa, se lo realiza en base a la siguiente tabla, la cual muestra un análisis de uso de red por paquetes y que aplicaciones son las que más se usan dentro de la empresa Coltrans.

Figura 26

Top 10 aplicaciones usadas dentro de la empresa Coltrans

TOP10 Application Categories			
Total Packets: 1 015 259 877			
Total Traffic: 679.9 GB			
Application Category	**Packets**	**Traffic**	**%**
Web Services	551 505 219	385.5 GB	56.70
Unclassified	152 553 526	109.6 GB	16.12
Streaming Media	128 203 938	87.1 GB	12.81
Mail	69 136 609	45.6 GB	6.70
File Transfer	59 764 179	30.9 GB	4.54
Networking	26 173 011	8.6 GB	1.27
Messaging	6 401 147	3.4 GB	0.50
Database	4 409 330	2.3 GB	0.34
Social Networking	3 247 913	2.2 GB	0.33
Games	3 059 491	1.7 GB	0.25

Nota. Esta imagen es tomada de un estudio realizado para la empresa Coltrans. Tomado de Análisis de tráfico de red y reasignación del ancho de banda adecuado de la red de COLTRANS (p.54), por Hernández Cueto, C. C., & Vargas Galindo, D. E., 2018.

En esta figura se puede determinar que las aplicaciones web son las más usadas, para estas aplicaciones se determina que se utiliza los protocolos http, https para la navegación por internet. Los servicios de streaming, que están en tercer lugar en la figura 26, los servicios de streaming funcionan junto con el protocolo UDP, en estos tipos de servicios se encuentran las videoconferencias. Debido al alto valor de tráfico de red que tienen las aplicaciones, se los va a considerar como prioridad de tráfico de red.

En la mitad de la figura 26 se encuentra la transferencia de archivos, para esto se utiliza el protocolo FTP, por lo que se va a considerar a este tráfico con un nivel medio.

Por último, a pesar de que el tráfico de correos está en una posición alta en la figura 26, al no requerir muchos recursos de red para el envío, se procede a considerar los protocolos de correo POP3 dentro de una prioridad de red baja.

A continuación, se tiene la información de los protocolos a considerarse críticos en la siguiente tabla.

Tabla 4.

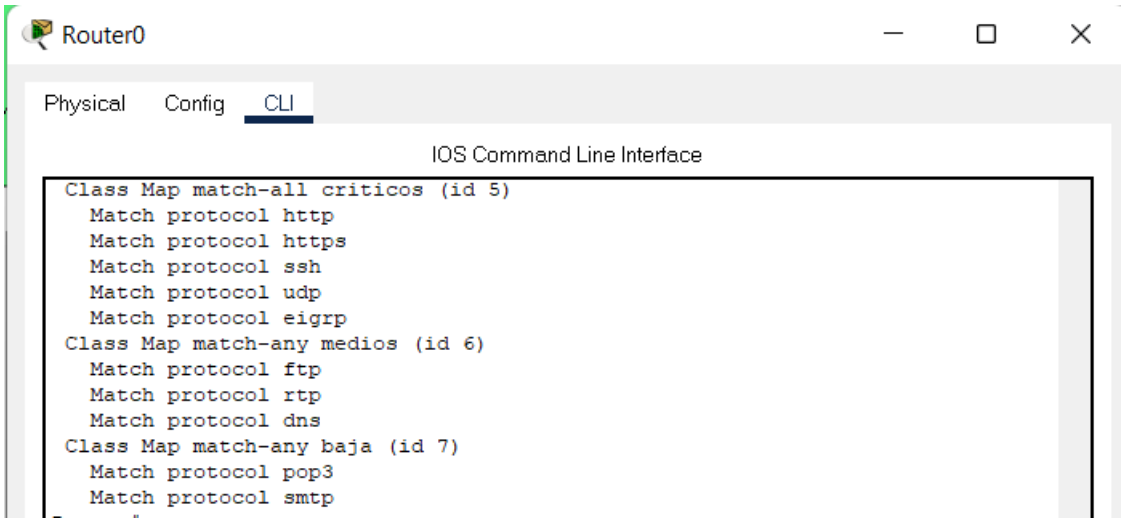
Tabla de asignación de protocolos según el nivel de importancia.

Nombre class-map	Especificación	Protocolos
Críticos	Prioridad de tráfico para procesos críticos de la empresa	SSH, EIRGP, UDP, HTTP, HTTPS
Medios	Tráfico de transmisión de medios como datos, voz y video.	FTP. RTP
Baja	Tráfico de transmisión de aplicaciones no críticas como el correo	POP3, SMTP

Se debe configurar las class-map junto con sus respectivos protocolos críticos para la empresa priorizando, que en este caso uno de ellos es el tráfico para videoconferencias por medio del protocolo UDP.

Figura 27

Configuración de class-map para protocolos críticos, medias, y baja.



Se va a crear una policy-map donde se van a establecer las class-map que se crearon anteriormente dándoles una prioridad de capa 2 a los protocolos críticos con el comando set precedence donde 7 representa la más alta prioridad y el 1 la más baja.

Figura 28

Configuración de set precedence en Router0.

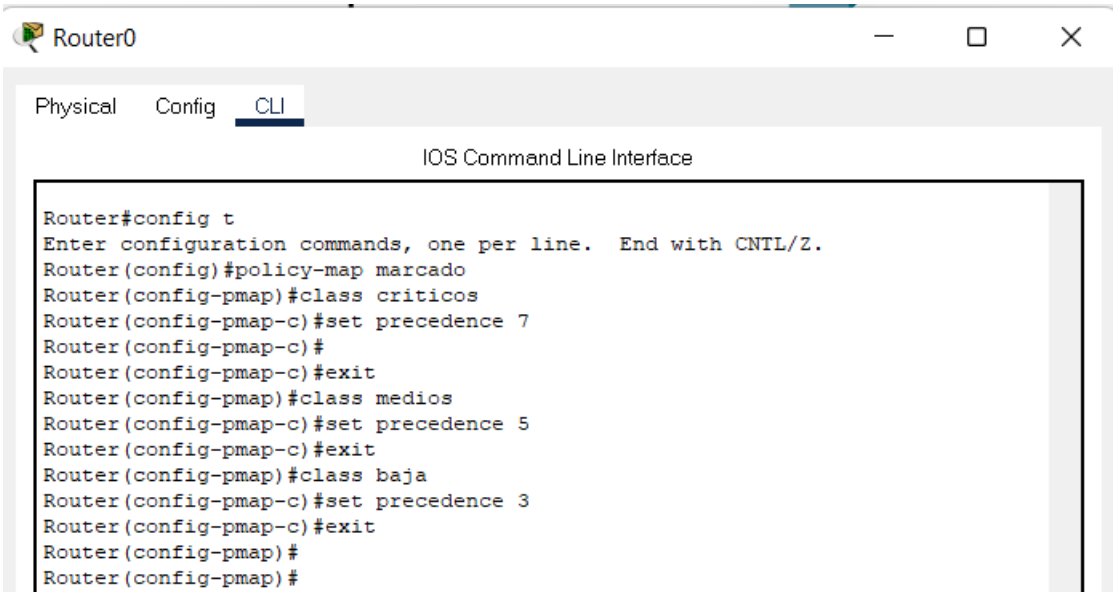
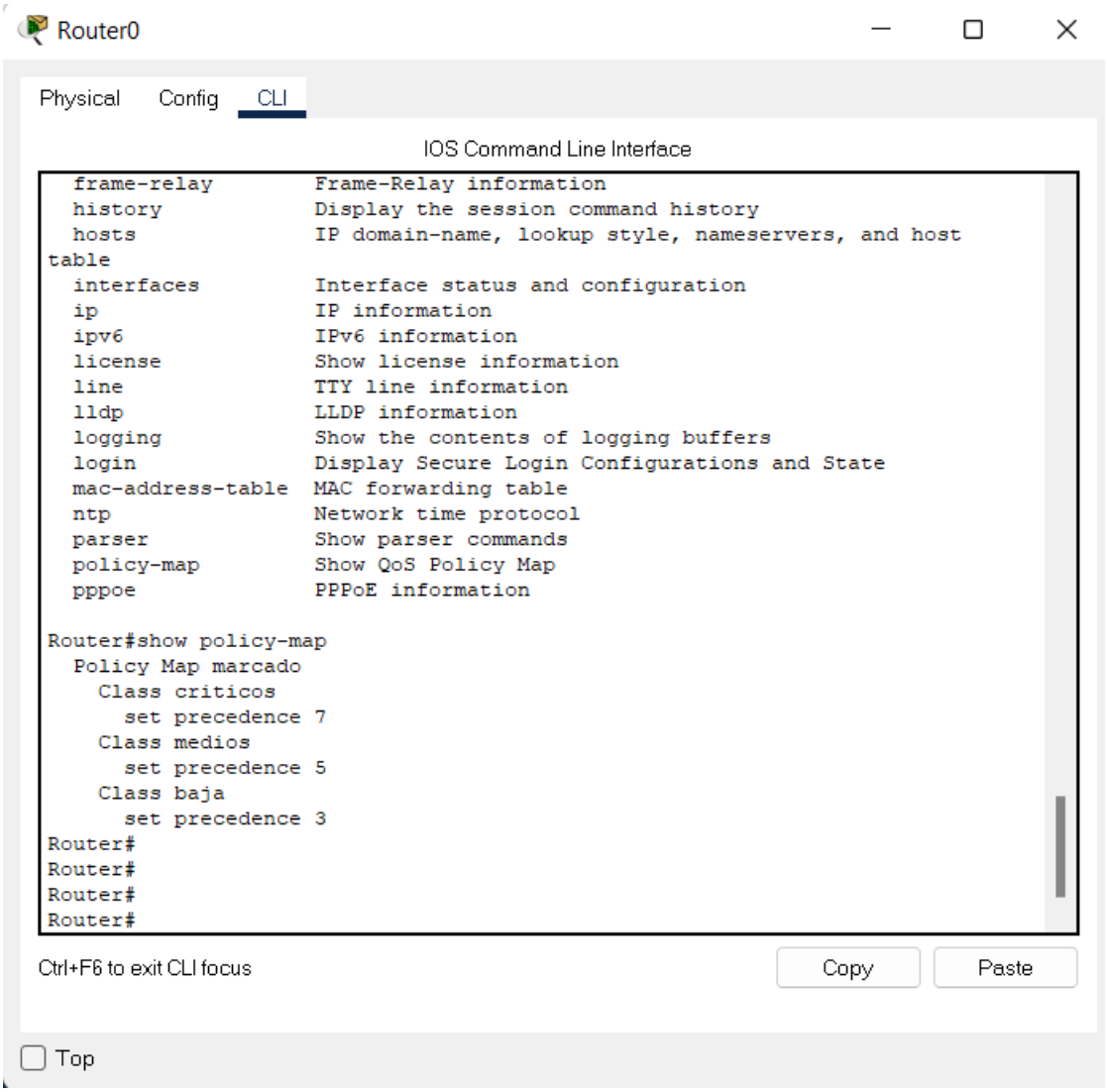


Figura 29

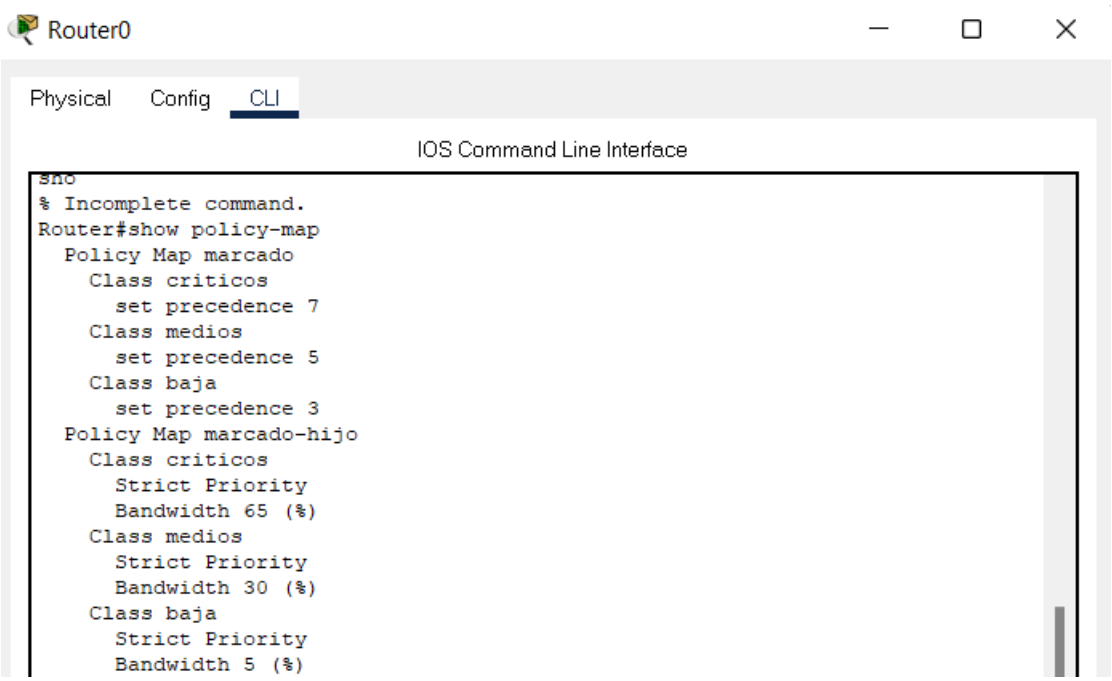
Verificación de policy-map creados.



Se asigna de igual forma otro policy-map que va a determinar el ancho de banda utilizado por la red para los distintos protocolos que hayan sido asignados a class-map, aquí se aplica el encolamiento de tipo WFQ, priorizando un porcentaje del ancho de banda a ser utilizado en los procesos críticos.

Figura 30

Verificación de ancho de banda asignado en Router0.

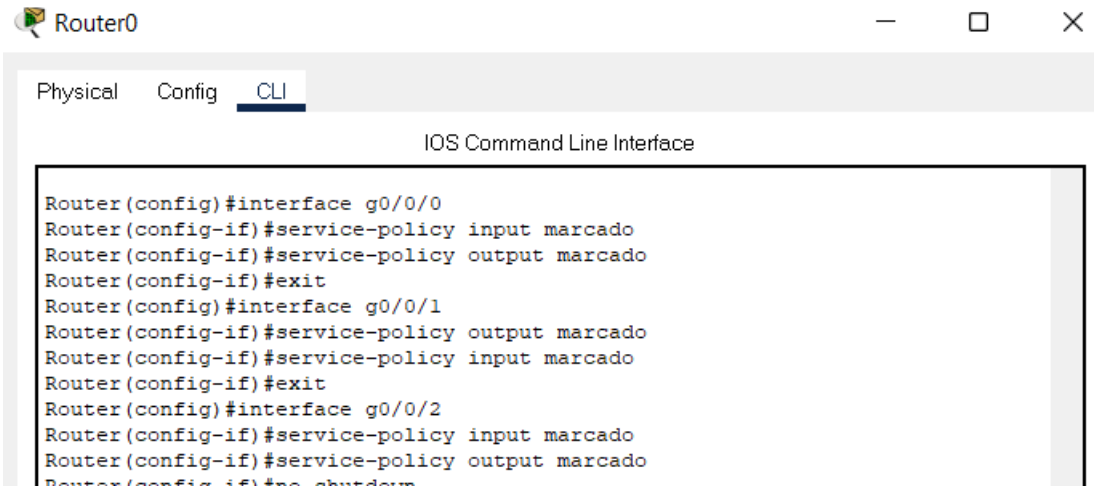


Cabe recalcar que la aplicación de encolamiento de tipo WFQ no está disponible para simulación en las subinterfaces del router, por lo que, se procede a trabajar con las políticas de capa 2 para priorizar los paquetes.

Las policy-map se proceden a asignar cada una de estas a la interfaz para que cumpla con las class-map establecidas.

Figura 31

Configuración de service-policy en Router0.


Router0
Physical
Config
CLI
IOS Command Line Interface
Router(config)#interface g0/0/0
Router(config-if)#service-policy input marcado
Router(config-if)#service-policy output marcado
Router(config-if)#exit
Router(config)#interface g0/0/1
Router(config-if)#service-policy output marcado
Router(config-if)#service-policy input marcado
Router(config-if)#exit
Router(config)#interface g0/0/2
Router(config-if)#service-policy input marcado
Router(config-if)#service-policy output marcado

CAPÍTULO IV: PRUEBAS DE FUNCIONAMIENTO

4.1. Pruebas de conectividad

Concluida la configuración de los equipos en la red se va a realizar pruebas de funcionamiento de la red. Empezando por comprobar que los dispositivos estén asignados a las VLANS correspondientes

Figura 32

Equipos dentro del departamento de Talento Humano

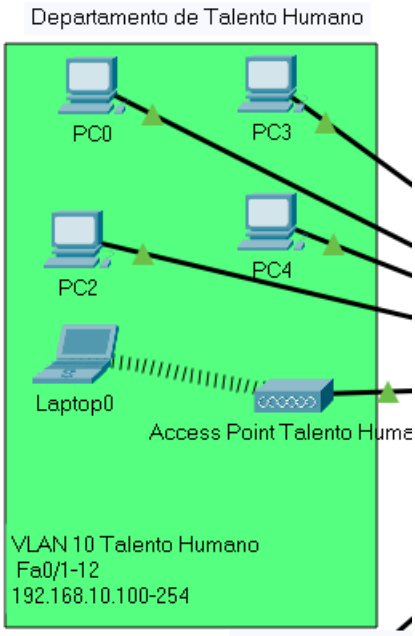
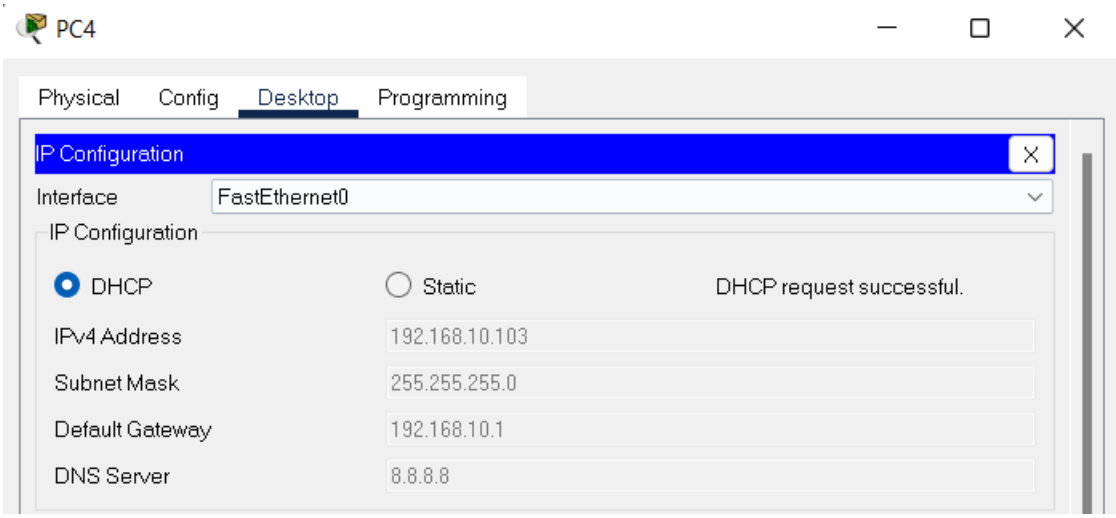


Figura 33

Verificación de DHCP en PC4.

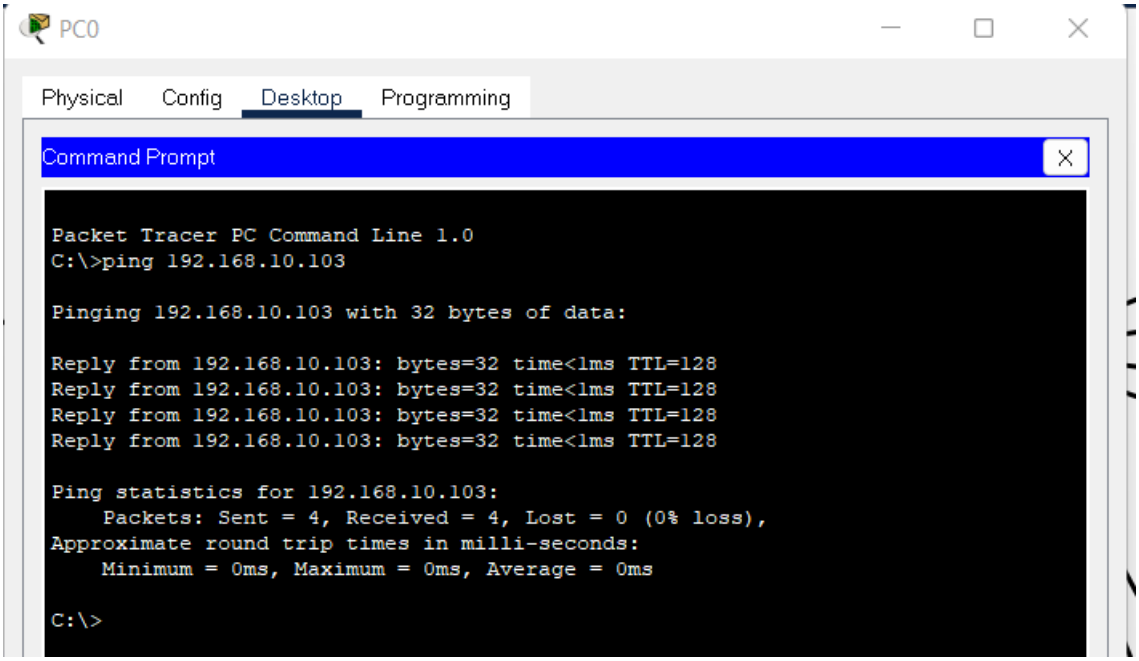


Se puede apreciar que la conectividad a la VLAN 10 es la correcta y se asigna una dirección IP por DHCP con la puerta de enlace que se pudo configurar en el router

Se revisa que exista conectividad entre dispositivos de la misma red mediante el comando ping desde la consola de un equipo

Figura 34

Prueba de ping entre PC´s de la VLAN 10.



Verificación de conectividad en el departamento contable mediante la verificación de asignación IP por DHCP y ping entre máquinas.

Figura 35

Equipos dentro del departamento contable.

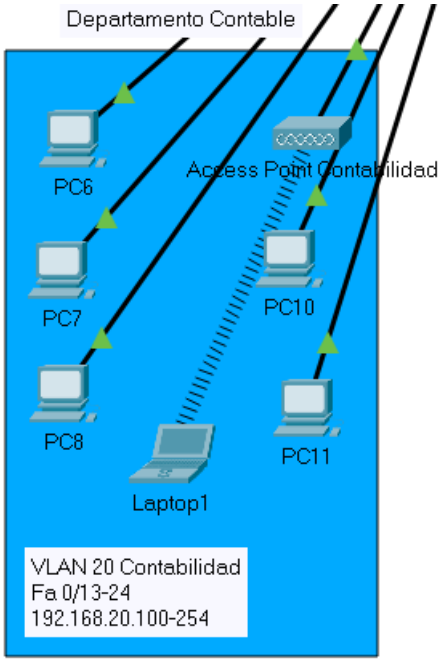


Figura 36

Verificación de DHCP en PC6.

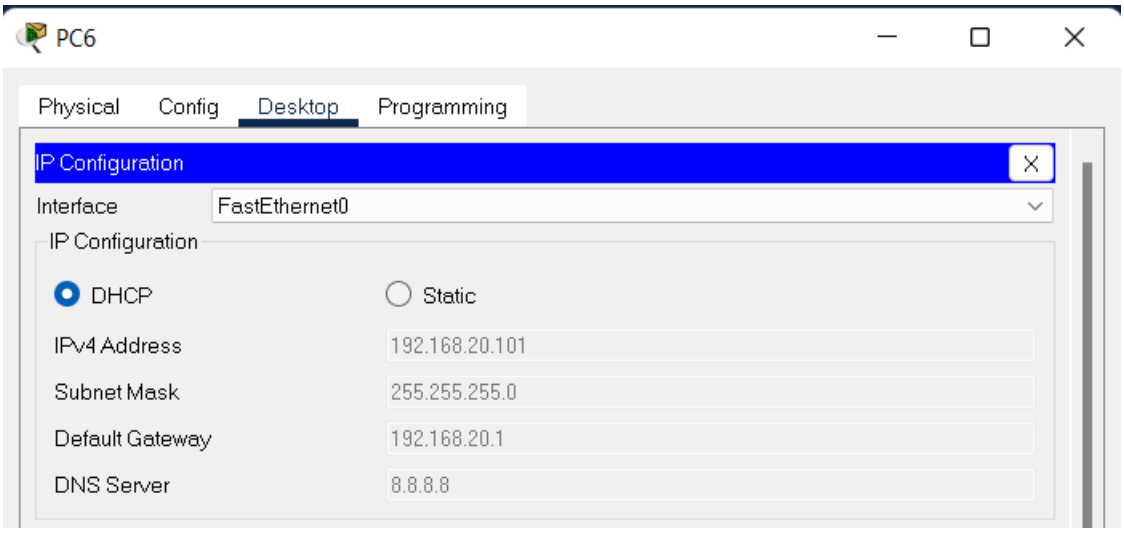
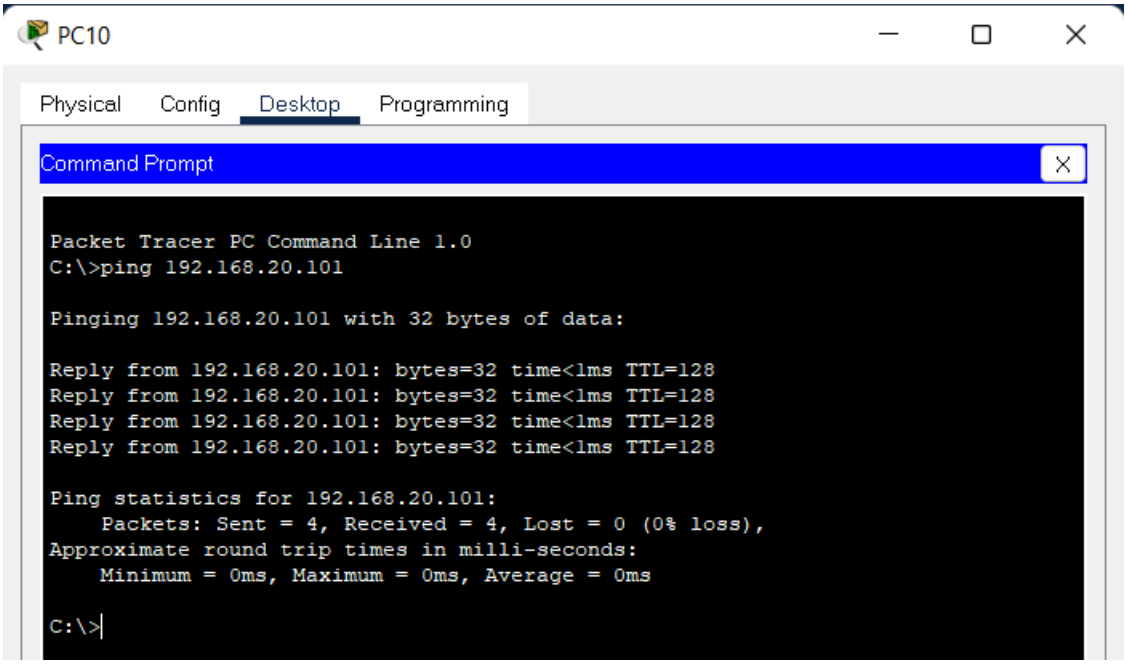


Figura 37

Prueba de ping entre PC´s de la VLAN 20.



Verificación de conectividad en el departamento de marketing mediante la verificación de asignación IP por DHCP y ping entre máquinas.

Figura 38

Equipos dentro del departamento de Marketing.

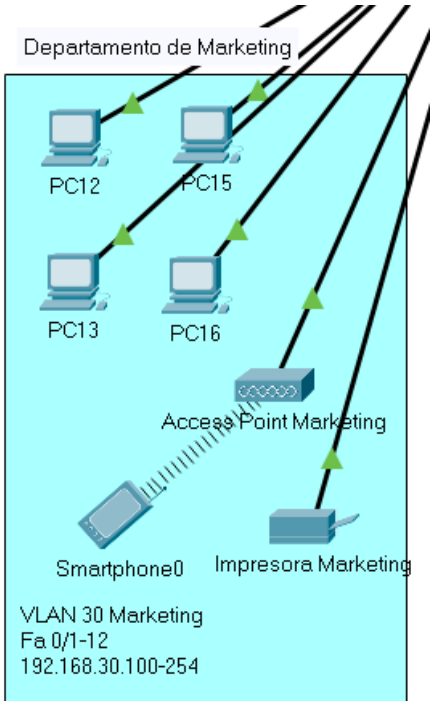


Figura 39

Verificación de DHCP en PC12.

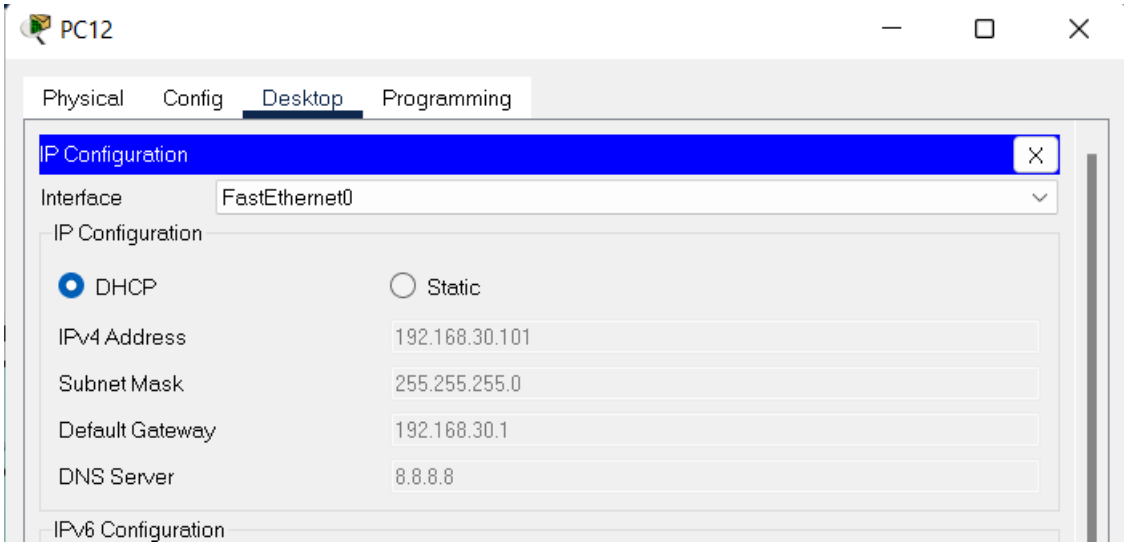
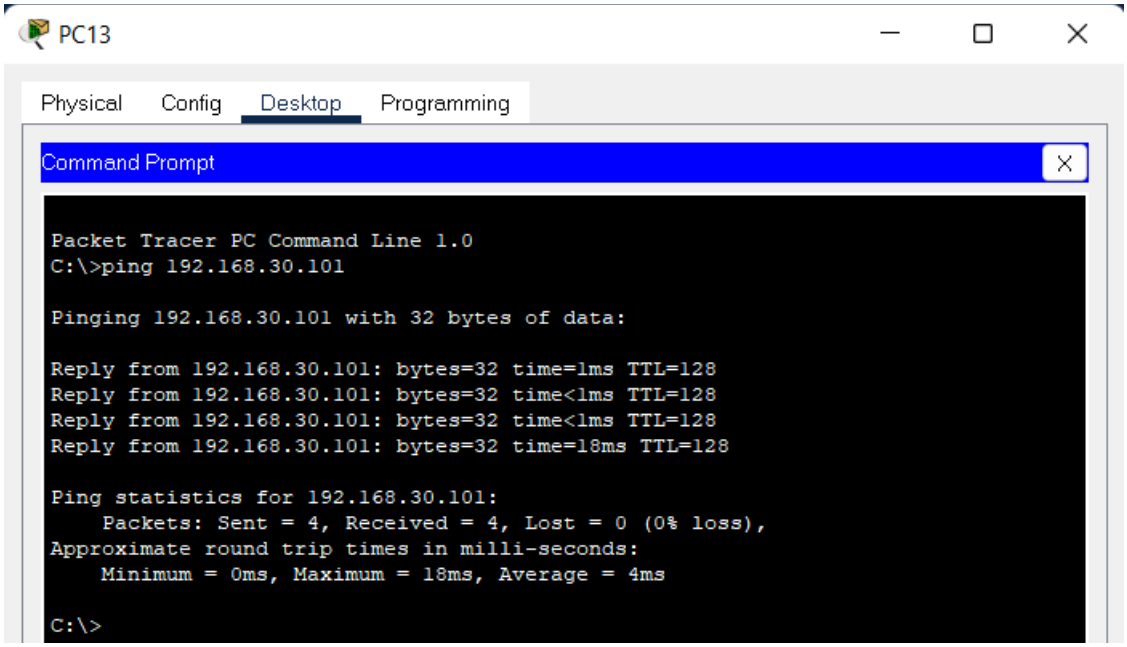


Figura 40

Prueba de ping entre PC´s de la VLAN 30.



Verificación de conectividad en el departamento de compras mediante la verificación de asignación IP por DHCP y ping entre máquinas.

Figura 41

Equipos dentro del departamento de Compras.

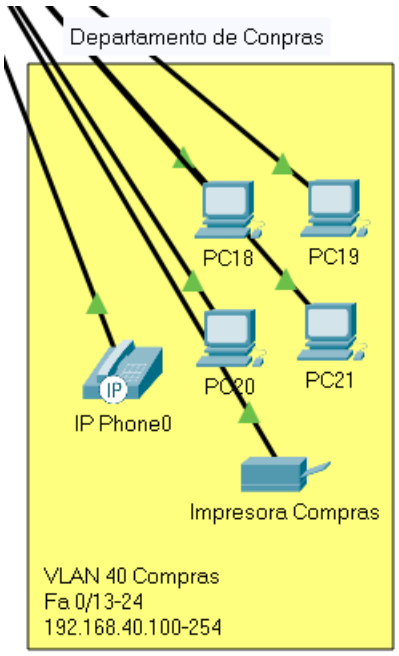


Figura 42

Verificación de DHCP en PC18.

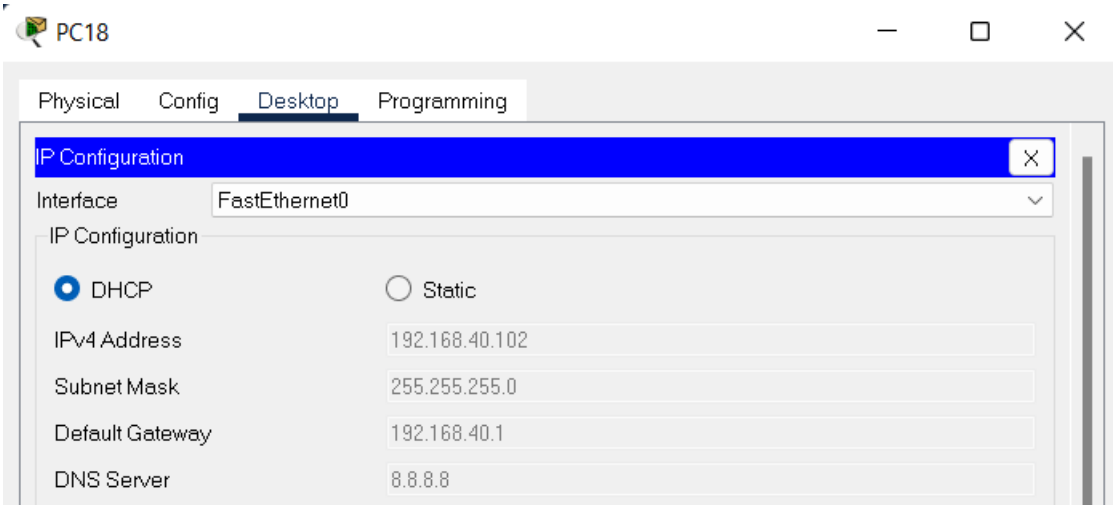
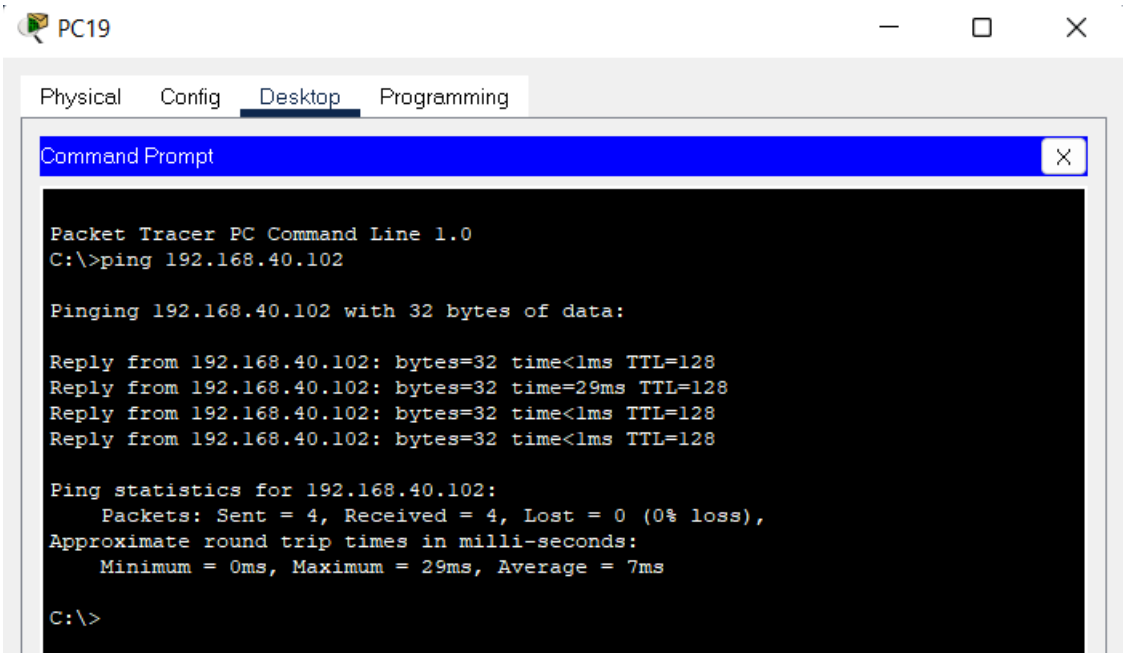


Figura 43

Prueba de ping entre PC´s de la VLAN 40.



Verificación de conectividad en el departamento de sistemas mediante la verificación de asignación IP por DHCP y ping entre máquinas.

Figura 44

Equipos dentro del departamento de sistemas.

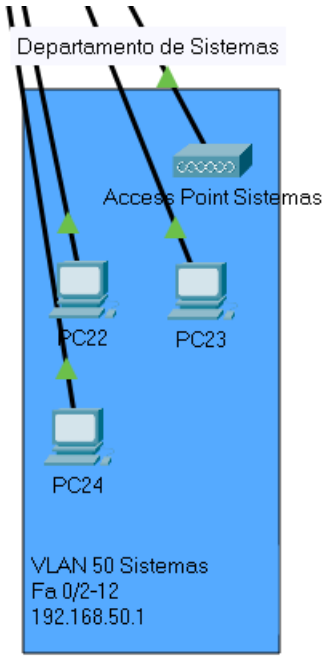


Figura 45

Verificación de DHCP en PC22.

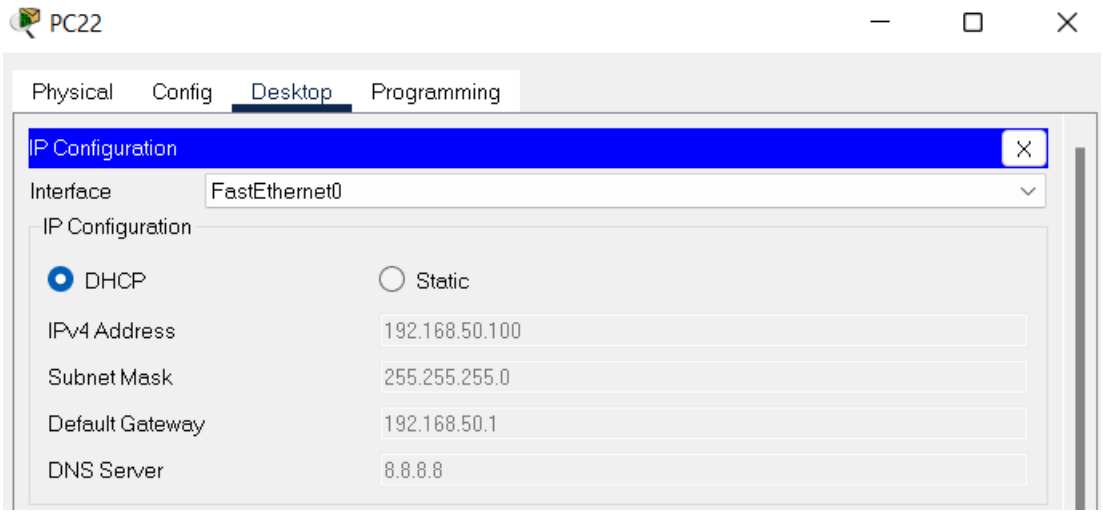
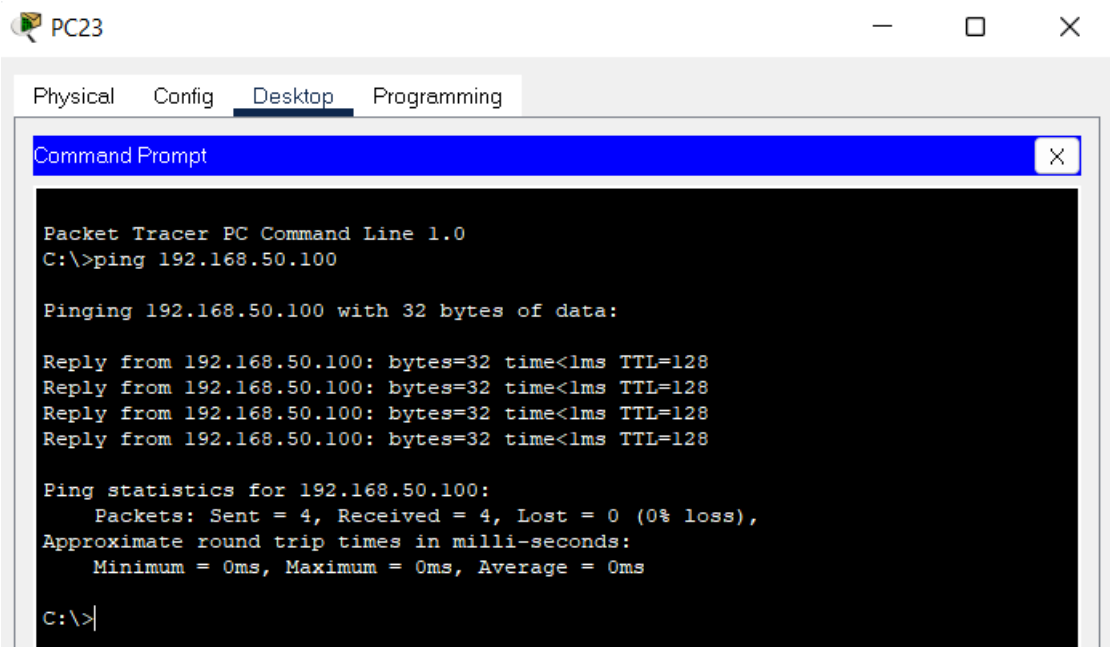


Figura 46

Prueba de ping entre PC´s de la VLAN 50.



Verificación de conectividad en el departamento de gerencia mediante la verificación de asignación IP por DHCP y ping entre máquinas.

Figura 47

Equipos dentro del departamento de gerencia general.

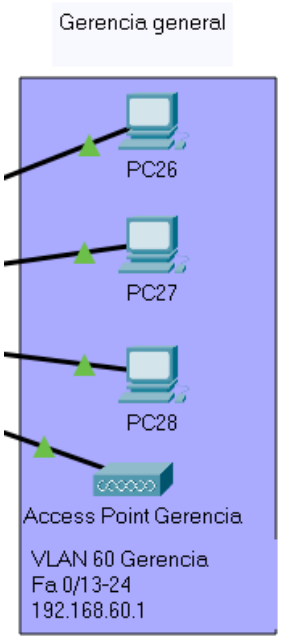


Figura 48

Verificación de DHCP en PC26.

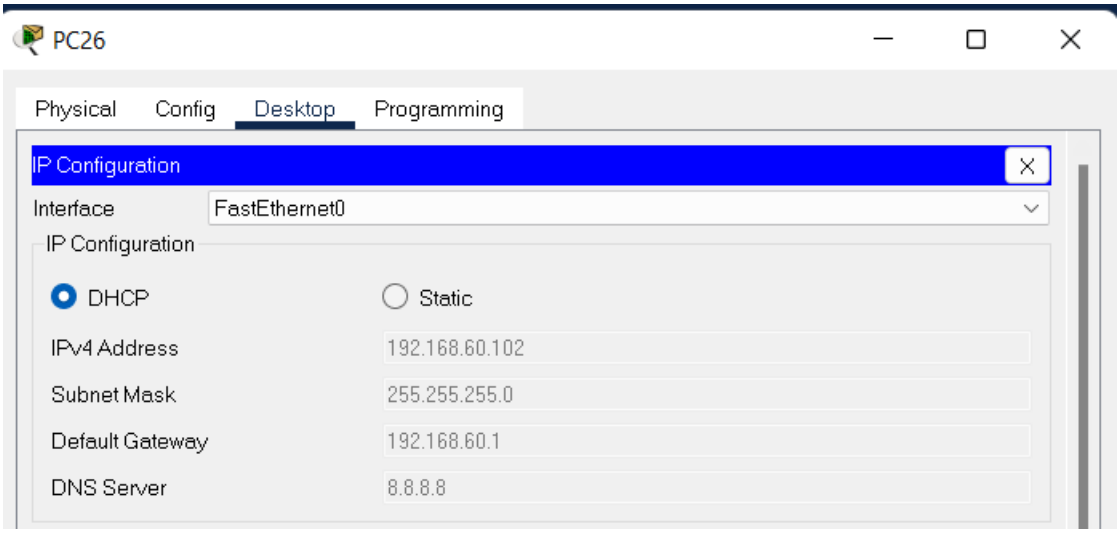
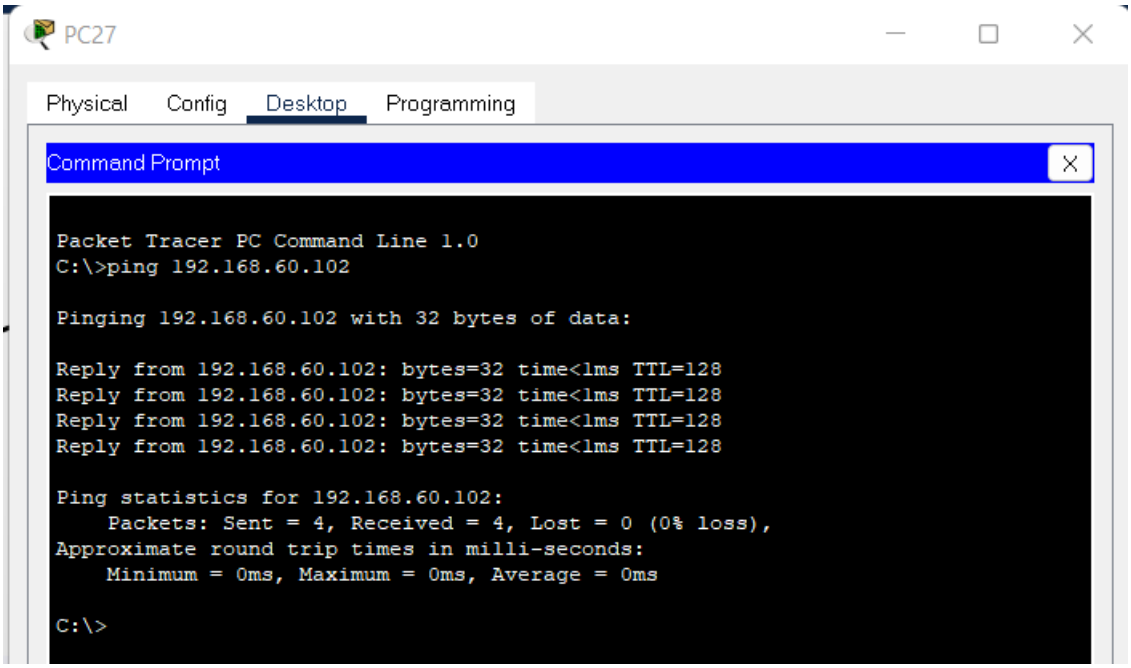


Figura 49

Prueba de ping entre PC´s de la VLAN 60.

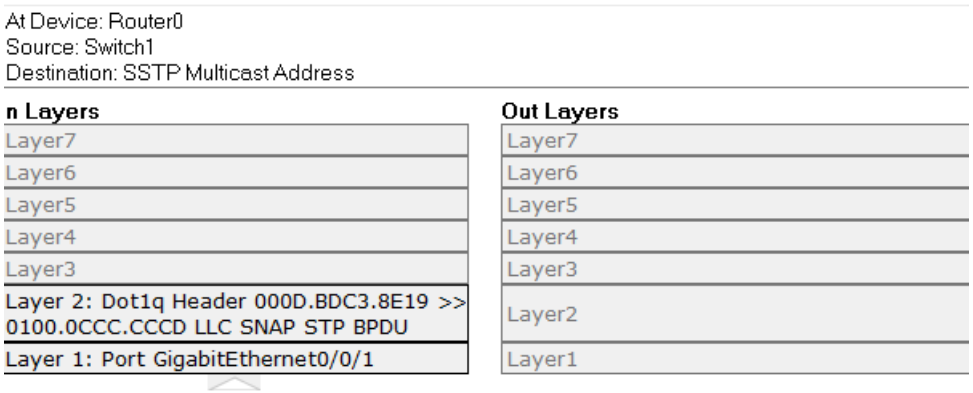


4.2. Pruebas de envío de paquetes

Enviando paquetes de datos en la simulación se puede apreciar que los paquetes que se envían van con el protocolo de marcado DOT1Q que contiene la información de la VLAN al router.

Figura 50

Envío de paquetes en el Router0.



CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Se diseñó y configuró de forma exitosa la red junto con sus respectivos equipos que permiten la priorización de un tráfico de red específico y la segmentación de la red por cada departamento mediante VLANS.
- El tipo de encolamiento WFQ o encolamiento controlado basado en pesos, permitió distribuir el ancho de banda de la red permitiendo dar prioridad al tipo de tráfico crítico que tiene una empresa.
- Las prioridades de red que tienen las empresas no siempre van a ser las mismas, por lo que, los protocolos de red que se consideren críticos para una empresa deben ser tomados en cuenta para poder asignar la prioridad necesaria.

Recomendaciones

- Utilizar el simulador Packet Tracer con las últimas actualizaciones debido a que se encontrarán dispositivos actualizados que permiten realizar más configuraciones en comparación con dispositivos antiguos.
- Entender el funcionamiento de los tipos de encolamiento que se utilizan para aplicar calidad de servicio para así poder tener una idea clara de que tipo de encolamiento resulta mejor utilizar.
- Se recomienda ir documentando las direcciones IP que vayan a ser utilizadas con el fin de no confundirlas.
- Realizar el diseño de la red en otros simuladores debido a que Packet Tracer solo cuenta con equipos Cisco, lo que puede limitar la investigación y futuras aplicaciones prácticas.

BIBLIOGRFÍA

- Martín, C. D. J., Evila, M. C. G., Avila, B. S., Sendy, P. C. S., & Dorie, C. R. Seguridad en redes LAN implementando VLAN.
- Mejía, M. J. O., Ortiz, C. A. A., Ramos, W. E. V., & Moscoso, L. E. P. (2022). Gestión del tráfico de red en la calidad de servicio "QoS" WAN en Tambopata-Perú 2021. *Revista de ciencias sociales*, *28*(2), 300-318.
- Aguilera Pino, F. Implementación de calidad de servicio (QoS) en redes tácticas de gran unidad.
- Rivera Zabala, J. C. Un sistema multi-agente para la auto-configuración de las operaciones de red en la subcapa MAC del modelo OSI. *Ingeniería de Sistemas*.
- Ortega Ureta, J. E. (2019). Diseño e Implementación de un sistema de control y balanceo de carga, en routers Mikrotik para mejorar la calidad de servicio (QoS) de la empresa zona vip, ubicada en el distrito de amarilis, provincia de Huánuco 2015.
- Castillo Porturas, A. N. (2019). Implementación de redes virtuales utilizando Vlan para reducir el tamaño del dominio de difusión de la red en el Inabib.
- Domínguez, J. M. C., Cárdenas, G. E. M., Sauza, A. B., Castañeda, S. S. P., & Ramírez, D. C. (2017). Seguridad en redes LAN implementando VLAN. *Ingenio y Conciencia Boletín Científico de la Escuela Superior Ciudad Sahagún*, *4*(8).
- Villamarín, E. J. A., Herrera-Tapia, J., & Felipe, M. D. R. C. (2022). Diseño de redes para Instituciones Académicas con criterios de QoS. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E47), 170-183.

- Salcedo Castillo, J. E. (2020). Diseño y emulación de una red de datos con priorización de servicios en la Unidad Educativa Suizo Ambato.
- Hernández Cueto, C. C., & Vargas Galindo, D. E. (2018). Análisis de tráfico de red y reasignación del ancho de banda adecuado de la red de COLTRANS.
- Dordoigne, J. (2015). *Redes informáticas-Nociones fundamentales (5ª edición):(Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6...)*. Ediciones Eni.

GLOSARIO DE TÉRMINOS

1.8. **Ping:** Utilidad de diagnóstico en redes de computadoras que se encargan de comprobar el estado de la comunicación entre el dispositivo anfitrión local con otros dispositivos.

1.9. **Broadcast:** Es la difusión masiva de información o paquetes de datos desde un nodo emisor a una multitud de nodos receptores.

1.10. **IEEE:** Instituto de ingenieros eléctricos y electrónicos.

ANEXOS

Anexo A: Configuración de Switch0

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
mls qos
!
!
!
!
spanning-tree mode pvst
```

```
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
```

```
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 10
```

```
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 20
 switchport mode access
!
```

```
interface FastEthernet0/14
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 20
```

```
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 20
 switchport mode access
!
```

```
interface FastEthernet0/23
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
```

```
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

Anexo B: Configuración del Switch1

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
```

```
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 30
```

```
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
!
```

```
interface FastEthernet0/7
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 30
```

```
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 40
 switchport mode access
!
```

```
interface FastEthernet0/16
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 40
```

```
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 40
 switchport mode access
!
```

```
interface GigabitEthernet0/1
 switchport trunk allowed vlan 30,40
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
```

login

!

!

!

!

end

Anexo C: Configuración de Switch2

!

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Switch

!

!

!

!

!

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 50
```

```
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 50
 switchport mode access
!
```

```
interface FastEthernet0/9
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 60
```

```
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 60
 switchport mode access
!
```

```
interface FastEthernet0/18
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 60
```

```
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 60
 switchport mode access
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 50,60
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
```

```
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

Anexo D: Configuración del Router0

```
!
version 15.4
```

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
ip dhcp excluded-address 192.168.10.1 192.168.10.99
ip dhcp excluded-address 192.168.20.1 192.168.20.99
ip dhcp excluded-address 192.168.30.1 192.168.30.99
ip dhcp excluded-address 192.168.40.1 192.168.40.99
ip dhcp excluded-address 192.168.50.1 192.168.50.99
ip dhcp excluded-address 192.168.60.1 192.168.60.99
!
ip dhcp pool vlan10
 network 192.168.10.0 255.255.255.0
```

```
 default-router 192.168.10.1
 dns-server 8.8.8.8
ip dhcp pool vlan20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 8.8.8.8
ip dhcp pool vlan30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 8.8.8.8
ip dhcp pool vlan40
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 8.8.8.8
ip dhcp pool vlan50
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.1
 dns-server 8.8.8.8
```

```
ip dhcp pool vlan60
 network 192.168.60.0 255.255.255.0
 default-router 192.168.60.1
 dns-server 8.8.8.8
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
```

```
!
!
!
spanning-tree mode pvst
!
class-map match-all voice
 match protocol rtp
class-map match-all http
 match protocol http
class-map match-all https
 match protocol https
class-map match-all udp
 match protocol udp
class-map match-all criticos
 match protocol http
 match protocol https
 match protocol ssh
 match protocol udp
```

```
 match protocol eigrp
class-map match-any medios
 match protocol ftp
 match protocol rtp
 match protocol dns
class-map match-any baja
 match protocol pop3
 match protocol smtp
!
policy-map marcado
 class criticos
  set precedence 7
 class medios
  set precedence 5
 class baja
  set precedence 3
!
!
```

```
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 service-policy input marcado
 service-policy output marcado
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
```

```
interface GigabitEthernet0/0/1
 no ip address
 service-policy input marcado
 service-policy output marcado
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
!
interface GigabitEthernet0/0/1.40
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.0
!
interface GigabitEthernet0/0/2
 media-type sfp
 no ip address
```

```
 service-policy input marcado
 service-policy output marcado
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/2.50
 encapsulation dot1Q 50
 ip address 192.168.50.1 255.255.255.0
!
interface GigabitEthernet0/0/2.60
 encapsulation dot1Q 60
 ip address 192.168.60.1 255.255.255.0
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
!
interface Serial0/1/1
```

```
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
```

```
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```