

Universidad Tecnológica de El Salvador

**FACULTAD DE INFORMATICA Y CIENCIAS APLICADAS
TECNICO EN INGENIERIA DE REDES COMPUTACIONALES**



TEMA:

“ELABORACIÓN DE MANUAL DE PRACTICAS DE LABORATORIO
PARA LA PREPARACIÓN DE LA CERTIFICACIÓN CCENT 100-105
CISCO CERTIFIED ENTRY CISCO NETWORKING TECHNICIAN”

TRABAJO DE GRADUACIÓN PRESENTADO POR:

Christopher Antonio Arévalo Meza

Melissa Stephanie Azucena Méndez

PARA OPTAR AL GRADO:

TECNICO EN INGENIERIA DE REDES COMPUTACIONALES

ABRIL, 2019

SAN SALVADOR, EL SALVADOR, CENTROAMERICA

AUTORIDADES ACADEMICAS

ING. NELSON ZARATE SANCHEZ

RECTOR

LIC. JOSE MODESTO VENTURA

VICERRECTOR ACADEMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

ING. OMAR OTONIEL FLORES CORTEZ

PRESIDENTE

LIC. NELSON OSWALDO LOPEZ CHAVEZ

PRIMER VOCAL

LIC. LUIS RODRIGO PALOMO QUIÑONEZ

SEGUNDO VOCAL

ABRIL, 2019

SAN SALVADOR, EL SALVADOR, CENTROAMERICA.

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:

Lic.Nelson Oswaldo López Chavez, Lic.Luis Rodrigo Palomo Quiñonez, Ing.Omar Otoniel Flores, a las 12:30p.m del día Viernes, 23 de Noviembre de dos mil dieciocho.
Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

- | | |
|--|----------------------------|
| 1- <u>Christopher Antonio Arévalo Meza</u> | <u>Carnet 26-3286-2015</u> |
| 2- <u>Melissa Stephanie Azucena Mendez</u> | <u>Carnet 26-2854-2013</u> |

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:

"Elaboración de manual de prácticas de Laboratorio para la preparación de la certificación CCENT 100-105 CISCO CERTIFIED ENTRY Cisco "Networking Technician"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES

Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

APROBADO

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 23 de Noviembre de dos mil dieciocho.

F. 
PRIMER VOCAL
Lic.Nelson Oswaldo López Chavez

F. 
SEGUNDO VOCAL
Lic.Luis Rodrigo Palomo Quiñonez

F. 
PRESIDENTE
Ing.Omar Otoniel Flores

Índice

Introducción.....	i
--------------------------	----------

Capítulo I

Planteamiento del Problema.....	1
--	----------

1. Objetivos.....	3
1.1 Objetivo general.....	3
1.2 Objetivo específico.....	3
2. Limitaciones.....	4
3. Justificación.....	4

Capítulo II

Marco Teórico.....	6
---------------------------	----------

1. Cisco Certified Entry Networking Technician (CCENT).....	6
2. Cisco Certified Network Professional (CCNP).....	16
3. Cisco Certified Internetwork Expert(CCIE).....	17

Capítulo III

Metodología.....	18
-------------------------	-----------

1. Recolección de Cotizaciones.....	20
-------------------------------------	----

Capítulo IV

Análisis de Resultados.....	22
------------------------------------	-----------

1.Preguntas de Encuesta.....	22
------------------------------	----

Capítulo V

Conclusiones y Recomendaciones.....	26
1. Conclusiones.....	26
2. Recomendaciones.....	27
Referencias.....	28
Anexos.....	29

Introducción

Las redes son, en la actualidad, una parte muy importante de nuestra vida personal y laboral. Tanto en nuestros hogares como en el trabajo, estamos inmersos en alguna red, aunque no seamos conscientes de ello. Con sólo conectarnos a Internet, estamos accediendo a una red, y lo mismo sucede si existe una impresora compartida entre varios equipos o si nos conectamos a otra PC para transferir archivos.

Todas ellas se crean para aprovechar las grandes ventajas que brindan, y todas deben ser sometidas a cuidados especiales para que no representen un problema debido a la falta de seguridad. Este avance de las redes dentro de todos los ámbitos genera un campo de trabajo en el que, primero, necesitamos saber qué son, cómo se constituyen, cuáles son las tecnologías y dispositivos que se encuentran detrás de ellas y de qué forma es posible diseñarlas y configurarlas de la manera más adecuada para cada caso y necesidad.

Por eso, en esta obra nos ocuparemos de hacer un recorrido que partirá desde los cimientos de una red básica y pequeña hasta llegar a convertirla en una red que incorpore las últimas tecnologías y, así, pueda brindar beneficios adicionales a los que comúnmente se implementan.

Capítulo I

Planteamiento del Problema

En San Salvador capital de El Salvador en la dirección 19 Av. Norte 19 AV Sur, Se ubica la Universidad Tecnológica de El Salvador la cual desde 1981 con innovación como su lema abre las puertas a todos los salvadoreños dentro como fuera del el país con el objetivo de que cada estudiante sea capaz de trabajar en el mundo laboral con carreras de gran importancia en el mercado laboral, dicha universidad en su Facultad de Informática y Ciencias Aplicadas ofrece varias carreras en el área de computación, específicamente podemos mencionar la carrera de técnico en ingeniería de redes computacionales, la cual imparte el fundamento y orientación a la implementación y administración de redes de comunicación de datos.

Esta carrera se apoya con los diplomados de Cisco Networking Academy, en los cuales los estudiantes pueden aprender desde los fundamentos de redes de datos hasta aspectos avanzados en interconexión y seguridad de redes.

En la universidad por medio de Cisco Networking Academy se brinda el diplomado CCNA “Routing and Switching”, el cual se imparte en la carrera de técnico en ingeniería de redes computacionales y como diplomado abierto para todos los alumnos interesados en cursar el diplomado.

El diplomado CCNA Routing and Switching, está conformado por 4 módulos los cuales son: Introducción a las Redes, Fundamentos de Routing y Switching, Redes Escalables e Interconexión de redes.

El estudiante luego de haber cursado estos 4 módulos puede optar a obtener certificaciones de Cisco, estas certificaciones son universalmente reconocidas como un estándar de la industria para el diseño y soporte de redes, garantizando altos niveles de conocimientos y credibilidad, esto permite al estudiante demostrar que domina las competencias y habilidades obtenidas en el diplomado CCNA "Routing and Switching", es de mencionar que las certificaciones tienen un costo adicional, no se realizan en la universidad sino en un centro de certificación autorizado por Cisco, los exámenes son en inglés y existe un tiempo específico para realizar la prueba.

Para el diplomado CCNA "Routing and Switching", Cisco ofrece la certificación CCENT "Cisco Certified Entry Networking Technician" con el examen 100-105 ICND1, la cual, valida las habilidades requeridas para las posiciones de soporte de red de nivel inicial, el punto de partida para muchas carreras exitosas en redes. Las personas certificadas con el CCENT tienen el conocimiento y las habilidades para instalar, operar y solucionar problemas una red de sucursales de pequeñas empresas, incluida la seguridad básica de la red, esta certificación contempla los temas que se estudian en los módulos: introducción a las redes y fundamentos de Routing & Switching, del CCNA "Routing and Switching".

La mayoría de los estudiantes que terminan de cursar el diplomado CCNA “Routing and Switching” no pican para realizar la certificación CCENT, el motivo es que no existe material didáctico acorde para realizar prácticas en los laboratorios de la universidad, el material que existe muchas veces esta en idioma inglés, esto dificulta el aprendizaje, tomando en cuenta además, que muchas prácticas son necesario que se desarrollen en tiempos específicos ya que el examen de certificación se realiza en un tiempo muy corto.

Además, mencionar que la metodología de Cisco Networking Academy exige al estudiante que el aprendizaje se autodidacta, esto es un problema para muchos estudiantes que quieren certificarse, porque muchos no cuentan con materiales didácticos que les permita desarrollar esta competencia.

1. Objetivos

1.1 Objetivo general.

Elaborar un manual de prácticas de laboratorio para la preparación de la certificación CCENT 100-105 “Cisco Certified Entry Networking Technician”, como apoyo de enseñanza y aprendizaje en la cátedra de redes de la Universidad Tecnológica De El Salvador.

1.2 Objetivo específico

- Realizar un análisis de los contenidos y de la importancia de tener la certificación CCENT 100-105 “Cisco Certified Entry Networking Technician”.
- Diseñar un modelo de prácticas de laboratorio para un dominio más práctico y claro para la preparación de la certificación CCENT 100-105 “Cisco Certified Entry Networking Technician”
- Crear un manual de prácticas de laboratorio para reforzar y fortalecer el conocimiento de los estudiantes para la preparación de la certificación CCENT 100-105 “Cisco Certified Entry Networking Technician”

2. Limitaciones

La falta de estudiantes y profesores que no poseen la certificación CCENT ni material acorde para el desarrollo de las competencias para lograr pasar el examen de certificación.

Otra limitante es el hecho de no contar con material de prácticas en español que permita reforzar contenidos y competencias para el examen CCENT, la mayoría de material que capacita en la certificación esta en inglés.

3. Justificación

En la Actualidad, existen muchos estudiantes que han cursado el diplomado CCNA “Routing and Switching” pero que no han logrado realizar el examen de certificación CCENT, Por lo cual se hace necesario e importante la creación de un manual de prácticas de laboratorio que oriente al estudiante en cómo viene el examen de certificación CCENT, con este manual se pretende que el estudiante cuente con un material didáctico realizado en la universidad para que le permita prepararse en la certificación y le permita desarrollar además la competencia de ser autodidactica desarrollando las prácticas en la universidad o en cualquier otra parte, con simuladores o con equipos físicos.

Es por todo lo anterior que se crear un manual de prácticas de laboratorio que facilite las competencias y habilidades para la aprobación del examen de certificación CCENT, además

Que permita generar competencias en el área de redes de datos y que puedan ser desarrolladas en el laboratorio de CISCO, ubicado en el edificio Francisco Morazán de dicha universidad, por si en algún momento al estudiante le quedan ciertas dudas, pueda ir a desarrollar las practicas nuevamente las veces que sean necesarias para aclarar y solventar dudas y así generando un aprendizaje significativo y autodidactica.

Capítulo II

Marco Teórico

El presente proyecto de investigación está basado en la necesidad de cada uno de los estudiantes de la Universidad Tecnológica de El Salvador siempre en la Facultad de Informática y Ciencias Aplicadas en la carrera de Técnico Ingeniera en Redes Computacionales la necesidad de obtener un material extra para su aprendizaje a la hora de realizar la certificación de CCENT 100-105 CISCO CERTIFIED.

La solución que le ofrece está basada en que los estudiantes de dicha carrera Técnica se puedan certificar ya que cada estudiante puede tomar la decisión de poder certificarse en Routing & Switching ya que sería una certificación de entrada ya que la certificación CCENT valida las habilidades requeridas para las posiciones de soporte de red de nivel inicial, el punto de partida para muchas carreras exitosas en redes.

Esta certificación abre las puertas a una carrera en el ámbito informático de Redes, tener un CCENT significa que el estudiante tiene lo que se necesita para poder administrar una pequeña red de sucursales empresariales.

1. Cisco Certified Entry Networking Technician (CCENT)

¿Qué es la certificación CCENT?

La Certificación Cisco Certified Entry Networking Technician (CCENT) valida la habilidad para instalar, operar y resolver problemas de una red corporativa pequeña, incluyendo una red de seguridad básica. Con la Certificación CCENT los profesionales de redes demuestran que poseen las habilidades requeridas para puestos básicos de soporte de redes - los puntos de inicio para futuras carreras exitosas en redes.

Esta Certificación cubre temas de fundamentos de redes, tecnologías WAN, seguridad básica y conceptos de wireless, fundamentos de routing y switching y configuración de redes simples. La Certificación CCENT es el primer paso en Cisco para posteriormente alcanzar la Certificación CCNA que cubre redes empresariales de tamaño mediano con conexiones complejas.

¿Ventaja de obtener CCENT?

Ventaja de obtener una certificación CCENT 100-105 es poder abrir las puerta a amplias certificaciones que posee la academia de Cisco como una de ellas y la siguiente después del CCENT es CCNA Routing and Switching.

¿Cuáles son los temas que contiene esta certificación de CCENT 100 - 105?

- Fundamentos de la red.

✓ Tecnologías de conmutación LAN.

✓ Tecnologías de enrutamiento.

✓ Servicios de infraestructura.

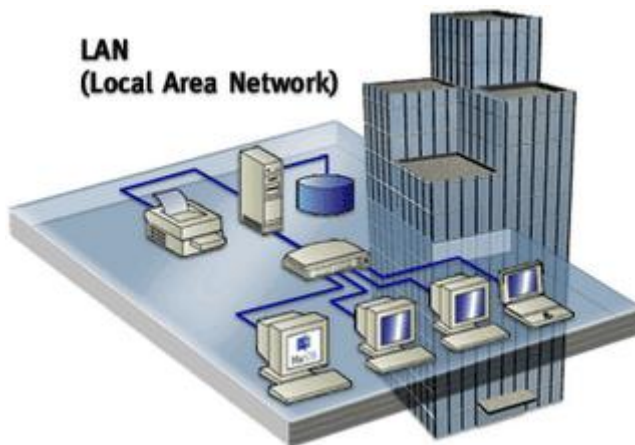
✓ Gestión de Infraestructura.

¿Qué son los Fundamentos de la Red?

Red es una interconexión de dos o más computadoras con el propósito de compartir información y recursos a través de un medio de comunicación, como puede ser el cable coaxial. El propósito más importante de cualquier red es enlazar entidades similares al utilizar un conjunto de reglas que aseguren un servicio confiable. Estas normas podrían quedar de la siguiente manera:

- La información debe entregarse de forma confiable sin ningún daño en los datos.
- La información debe entregarse de manera consistente. La red debe ser capaz de determinar hacia dónde se dirige la información.
- Las computadoras que forman la red deben ser capaces de identificarse entre sí o a lo largo de la red.
- Debe existir una forma estándar de nombrar e identificar las partes de la red

¿Conmutación LAN?



Una LAN o "red de área local," es un tipo de conexión de datos que funciona mediante ondas de radio. La tecnología LAN es usada habitualmente para conectar dispositivos móviles a Internet sin cables,

Permitiendo a los usuarios moverse libremente dentro del área de cobertura. Si bien el principio general sigue siendo el mismo, hay disponibles diferentes aplicaciones de la tecnología.

(Tutorialspoint.,2016)

¿Tecnologías de Enrutamiento?

ROUTER

Un router es un conmutador de paquetes que opera en el nivel de red del modelo OSI.

Sus principales características son:

- Permiten interconectar tanto redes de área local como redes de área extensa.
- Proporcionan un control del tráfico y funciones de filtrado a nivel de red, es decir, trabajan con direcciones de nivel de red, como por ejemplo, con direcciones IP.
- Las computadoras que forman la red deben ser capaces de identificarse entre sí o a lo largo de la red.
- Debe existir una forma estándar de nombrar e identificar las partes de la red

Son capaces de rutear dinámicamente, es decir, son capaces de seleccionar el camino que debe seguir un paquete en el momento en el que les llega, teniendo en cuenta factores como líneas más rápidas, líneas más baratas, líneas menos saturadas, etc.

Los routers son más "inteligentes" que los switches, pues operan a un nivel mayor lo que los hace ser capaces de procesar una mayor cantidad de información. Esta mayor inteligencia, sin embargo, requiere más procesador, lo que también los hará más caros.

A diferencia de los switches y bridges, que sólo leen la dirección MAC, los routers analizan la información contenida en un paquete de red leyendo la dirección de red. Los routers leen cada paquete y lo envían a través del camino

más eficiente posible al destino apropiado, según una serie de reglas recogidas en sus tablas.

Un router también sabe cuándo mantener el tráfico de la red local dentro de ésta y cuándo conectarlo con otras LANs. Dispondrá de una o más interfaces de red local, las que le servirán para conectar múltiples redes locales usando protocolos de nivel de red. Eventualmente, también podrá tener una o más interfaces para soportar cualquier conexión WAN.

(Tutorialspoint., 2016)

SWITCHES

Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).

Clasificación de Switches:

Atendiendo a la forma de segmentación de las sub-redes:

- Switches de Capa 2 o Layer 2 Switches

¿Infraestructura de red?

Se entiende como infraestructura de red a todos aquellos elementos básicos e imprescindibles para cualquier institución organización pública o privada (empresa, oficina o industria) que precise todos o algunos de los siguientes servicios de telecomunicaciones: teléfono, fax, ordenador, escáner, impresoras, TPV, cámaras de control y vigilancia, control de accesos, datafonos, climatización, incendio, etc.

Y los diferentes elementos que conforman

La Infraestructura de Red es:

- Cableado Estructurado
- Alimentación eléctrica equipos de comunicaciones
- Cuarto de Comunicaciones
- Seguridad y control
- Electrónica de Red

¿Qué es una gestión de infraestructura?

La gestión de redes abarca hoy en día muchos aspectos, que pueden

resumirse o sintetizarse en tareas de “despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos “de una red para conseguir niveles de trabajo y de servicio adecuados a los objetivos de una Instalación y de una organización.

(Tutorialspoint.,2016)

¿Qué es Cisco?

La palabra Cisco proviene del nombre de la ciudad San Francisco, lugar donde se fundó la empresa. El logotipo de esta es el Puente Colgante Golden Gate.

Hasta el 8 de junio de 2009 era considerada una de las grandes empresas del sector tecnológico y un importante miembro del mercado del NASDAQ o mercado accionario de tecnología. Posteriormente, gracias a su solidez, ingresó en el índice de industriales Dow Jones.

La empresa fue fundada en 1984 por el matrimonio de Leonard Bosack y Sandra Lerner, quienes formaban parte del personal de computación de la Universidad de Stanford. El nombre de la compañía viene de la palabra "San Francisco"; al mirar por la ventana había al frente un cartel que decía "San

Francisco" y un árbol se interponía la palabra separando San Fran Cisco, de ahí proviene el nombre de la empresa. Allí comenzó su despliegue como empresa multinacional.

Bosack adaptó el software para enrutadores multiprotocolo originalmente escrito por William Yeager, empleado de informática de la universidad. Cisco Systems creó el primer router comercialmente exitoso.

Hoy en día, otro gigante que le está intentando hacer sombra es la multinacional Juniper Networks, a la venta de routers para enlaces backbone (columna vertebral).

Además de desarrollar el hardware de sus equipos, Cisco Systems también se ocupa de desarrollar su propio software de gestión y configuración de los mismos. Dicho software es conocido como IOS, de código actualmente cerrado y totalmente propietario.

A través del IOS se consigue configurar los equipos Cisco mediante la denominada "Command Line Interface" (CLI) (Interfaz de Línea de Comandos), que sirve de intérprete entre el usuario y el equipo.

(Tutorialspoint., 2016)

¿Cuáles son las Certificaciones de Cisco?

Las certificaciones de la Plataforma de Cisco se dividen en 3 de menor a mayor dificultad como nombre de ellas son:

- Cisco Certified Network Associate
- Cisco Certified Network Professional
- Cisco Certified Internetwork Expert

Como mejores conocidas por sus siglas CCNA, CCNP y CCIE.

(Tutorialspoint., 2016)

¿Cisco Certified Network Associate (CCNA)?

CCNA (Cisco Certified Network Associate) es una certificación entregada por la compañía Cisco Systems a las personas que hayan rendido satisfactoriamente el examen correspondiente sobre infraestructuras de red e Internet. Está orientada a los profesionales que operan equipos para redes de datos. Otra vía para conseguir la certificación CCNA es a través de un curso oficial de Cisco con el mismo nombre, ofrecido en las academias de redes

Cisco en todo el mundo, dividido en cuatro módulos, la duración del

curso para lograr la certificación CCNA puede variar pues existen academias que dan las clases una vez por semana o dos veces por semana. En dicho caso, si una academia da dos lecciones semanales cada módulo tendría una duración de dos meses. La certificación completa duraría 8 meses.

2.Cisco Certified Network Professional (CCNP).

CCNP (Cisco Certified Network Professional) es el nivel intermedio de certificación de la compañía .3 Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 3 módulos.

Esta certificación, es la intermedia de las certificaciones generales de Cisco, no está tan valorada como el CCIE, pero si, mucho más que el CCNA.

El 25 de enero de 2010 se anunció la actualización del temario (anuncio oficial de Cisco) quedando de la siguiente manera:

- Enrutamiento (ROUTE)
- Conmutación (SWITCH)
- Resolución de problemas (TSHOOT)

Si bien se han producido ligeros cambios en los nuevos temarios de ROUTE y SWITCH, estos son convalidables por los anteriores BSCI y BCMSN

respectivamente. ISCW y ONT son eliminados, apareciendo el nuevo examen TSHOOT.

3. Cisco Certified Internetwork Expert (CCIE)

CCIE es una certificación de nivel avanzado para los profesionales que tienen “el entrenamiento, la experiencia y la confianza para abordar los problemas más desafiantes de su campo.” El CCIE “certifica así las habilidades de establecimiento de una red de un individuo en el nivel experto.” CCIE es un programa aparte que, hasta principios del 2009, no tenía un programa oficial de entrenamiento.

Para certificar al nivel experto no es prerequisite haber certificado otros niveles (CCNA, CCNP o equivalentes), pero tener una certificación de Cisco de nivel avanzado, tal como CCNP (Certificado Cisco de Profesional de Red), CCDP (Certificado Cisco de Profesional de Diseño), CCIP (Certificado Cisco de Profesional de Internet), o CCSP (Certificado Cisco de profesional en Seguridad) serían deseables antes de tomar el CCIE.

(Tutorialspoint., 2016)

Capítulo III Metodología

En este trabajo de Graduación se basa en la implementación de un manual de prácticas para estudiantes de la carrera Técnico Ingeniería en Redes Computacionales donde se puede visualizar ciertos ejemplos de configuraciones de equipos de redes tanto como routers y switches también su funcionalidad de cada uno de ellos para su preparación de la certificación CCENT 100-105.

Pasos a seguir en este proyecto de investigación son los siguientes:

- Creación de manual de practicas
- Realización de encuesta
- Compra de material para manual de practicas

Como primero punto para el análisis de esta creación de manual de prácticas ha sido la elección de los temas que estarán conformando dicho manual de prácticas observando cada uno de los temas principales para su formación los temas siguientes que estarán conformando este manual son:

- ✓ Fundamentos de la red.
- ✓ Tecnologías de conmutación LAN.
- ✓ Tecnologías de enrutamiento.
- ✓ Servicios de infraestructura.

✓ Gestión de Infraestructura.

Consecutivamente la realización de una encuesta dicha encuesta tiene un fin de recolectar datos de estudiantes de la carrera anteriormente mencionada para conocer por que lo estudiantes no optan por una certificación y quienes de dichos estudiantes si optan por un certificación al terminar la carrera de Técnico Ingeniería de Redes Computacionales

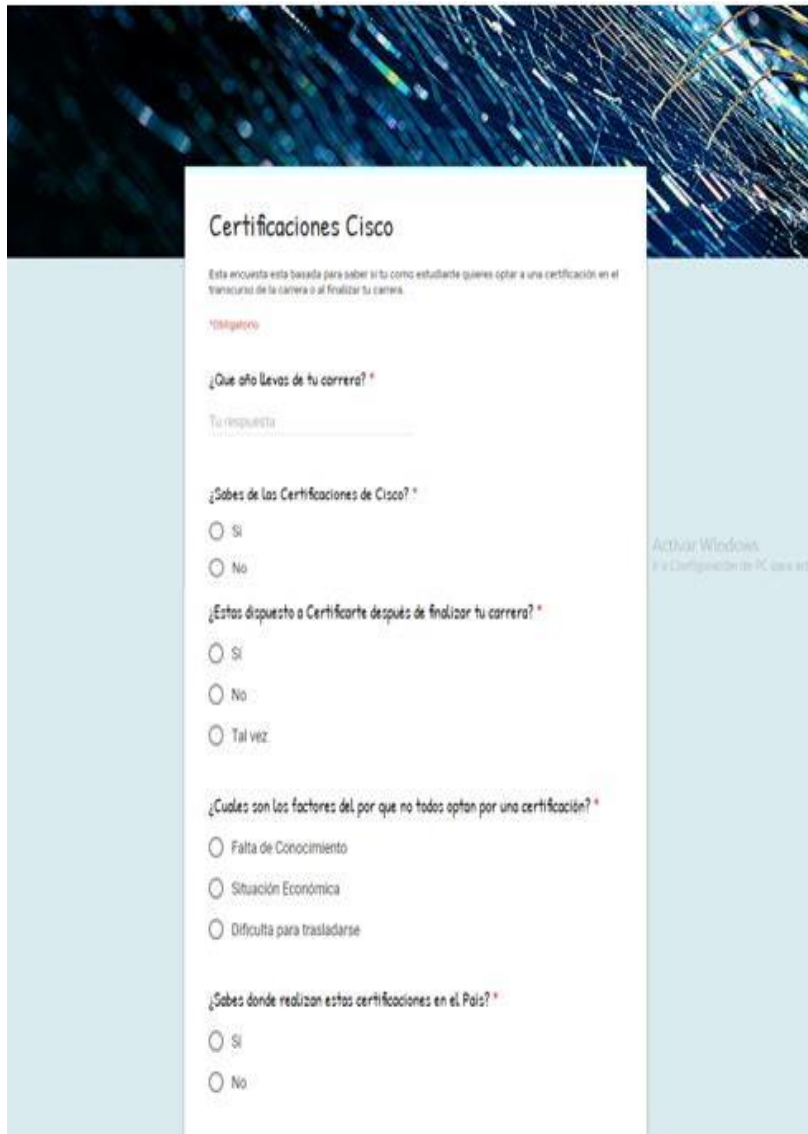


Figura 3

Portada de Manual

Dicha encuesta se realizó en Google Drive para la mayor comodidad del estudiante, la encuesta consta de 6 preguntas para saber si el estudiante optara por una certificación durante o al final de s carrera.

Figura 4



Certificaciones Cisco

Esta encuesta esta basada para saber si tu como estudiante quieres optar a una certificación en el transcurso de la carrera o al finalizar tu carrera.

***Obligatorio**

¿Que año llevas de tu carrera? *

Tu respuesta

¿Sabes de las Certificaciones de Cisco? *

☐ Si

☐ No

¿Estas dispuesto a Certificarte despues de finalizar tu carrera? *

☐ Si

☐ No

☐ Tal vez

¿Cuales son los factores del por que no todos optan por una certificación? *

☐ Falta de Conocimiento

☐ Situación Económica

☐ Dificulta para trasladarse

¿Sabes donde realizan estas certificaciones en el País? *

☐ Si

☐ No

Encuesta.

1. Recolección de Cotizaciones

Para el último punto se tomaron en cuenta costos para la elaboración de manual de prácticas debido a la alta competencia de imprentas así que se

tomaron los mejores costo, material con que se iba a imprimir dicho manual, durabilidad.

Tabla 1 Cotización

COTIZACION #1	PRECIO \$25
6 Manuales de Laboratorio	
COTIZACION #2	PRECIO \$35
6 Manuales de Laboratorio	
COTIZACION #3	PRECIO \$55
6 Manuales de Laboratorio	

Imagen 5

Figura de Cotización 1

	VENTAJAS	DESVENTAJAS
COTIZACION 1	Precio bajo	Material para la fabricación
DESCRIPCION: Páginas de manual de baja calidad precio bajo para su adquisición		
	VENTAJAS	DESVENTAJAS
COTIZACION 2	Precio Accesible	Envío adicional
DESCRIPCION: Material para la elaboración de dicho manual de muy buena calidad no incluye envío		
	VENTAJAS	DESVENTAJAS
COTIZACION 3	Material de Excelente Calidad	Precio Elevado
DESCRIPCION: Material de excelente calidad incluye envío y detalles que se le requieran agregar de último momento durabilidad de manual		

Tabla 2 Descripción de Cotización

Capítulo IV

Análisis de Resultados

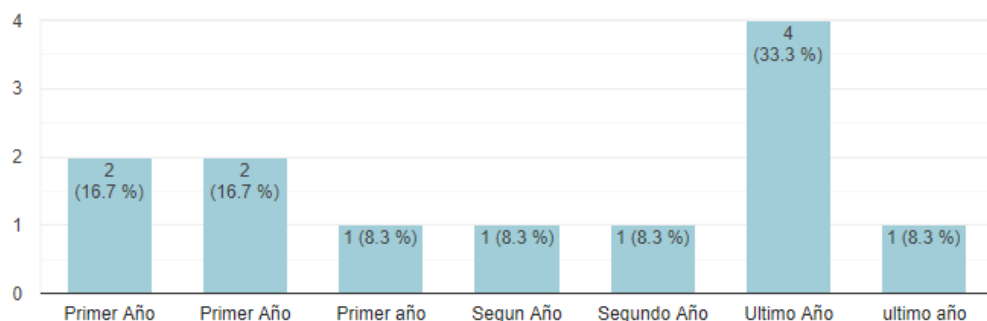
La implementación de un manual de laboratorio para los estudiantes de la carrera de Técnico Ingeniería en Redes Computaciones viene hacer una buena herramienta esencial en cuanto al aprendizaje de los estudiantes a la hora de emprender algún ejercicio.

Como tarea principal se realizó una encuesta para saber por qué algunos estudiantes no optan por tener una certificación en Cisco Networking y si tienen el conocimiento en qué lugar del país se realizaban dicha encuesta se realizó con una herramienta que la Universidad Tecnológica de El Salvador nos provee llamada Google Drive encuesta se mandó a estudiantes de la carrera anteriormente mencionada para que ellos en su tiempo libre pudieran realizar la encuesta.

1. Preguntas de encuesta:

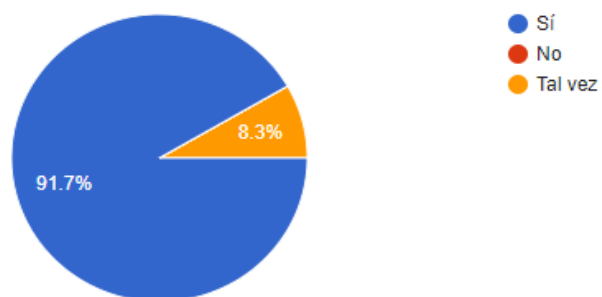
¿Que año llevas de tu carrera?

12 respuestas



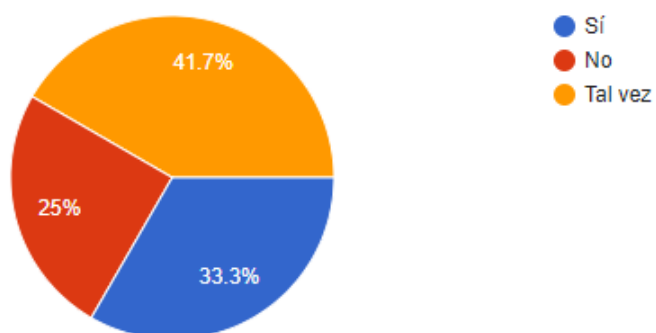
¿Te facilitaría un Manual de practicas de laboratorio a la hora de ejercer cualquier tipo de ejercicio lógico?

12 respuestas



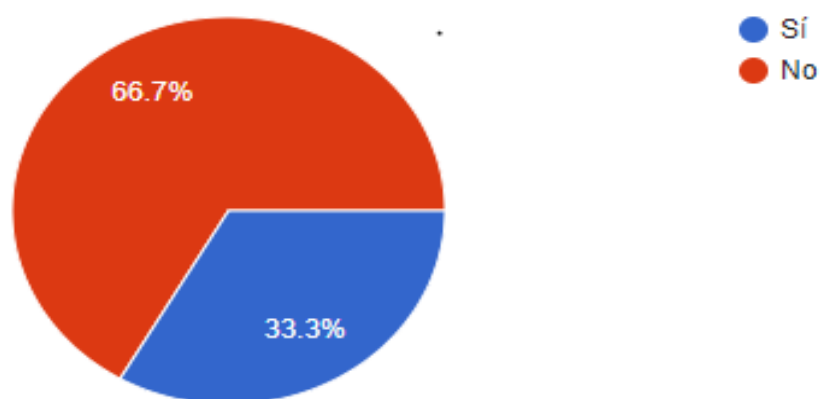
¿Estas dispuesto a Certificarte después de finalizar tu carrera?

12 respuestas



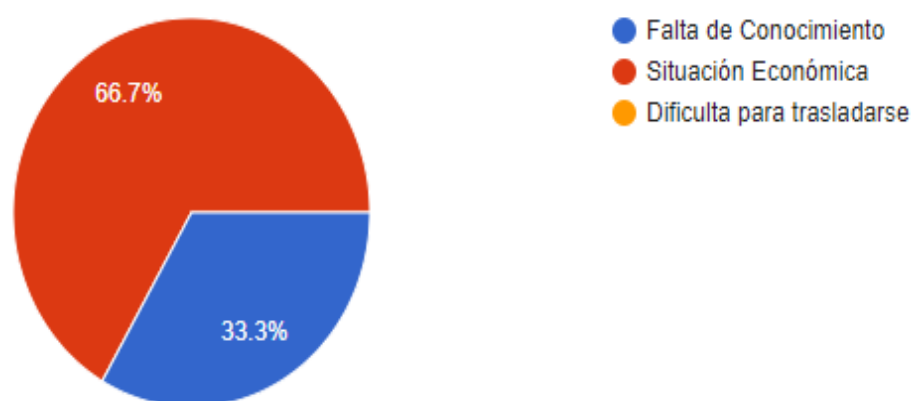
¿Sabes donde realizan estas certificaciones en el País?

12 respuestas



¿Cuales son los factores del por que no todos optan por una certificación?

12 respuestas



Creamos un manual con dichos temas de la Certificación CCENT 100-105 el manual se conforma por 9 temas los cuales son:

- Direccionamiento Ipv4
- Direccionamiento Ipv6
- Configuraciones Básicas
- VLAN
- VLSM Ipv4
- Enrutamiento de protocolo OSPFv2
- DHCP
- ACL
- NAT

En el diseño del manual de prácticas de laboratorio se tomó como base principal el aprendizaje de cada uno de los estudiantes de la carrera Técnico Ingeniería en Redes Computacionales para que a ellos se les facilite la realización de cada desafío que se les presente en la carrera o en cada práctica que ellos realizan.

Como resultado de la investigación mostramos de forma clara y concisa que el manual de prácticas de laboratorio fue creado con la finalidad de ayudar y facilitar al estudiante de dicha carrera antes mencionada para las distintas prácticas o ejercicios pero sobre todo para que el estudiante tenga mejor conocimiento a la hora de desempeñarse laboralmente.

Capítulo V

Conclusiones y Recomendaciones.

1. Conclusiones.

El manual de prácticas de laboratorio será una herramienta básica para el aprendizaje de los que se forman en la carrera Técnico en Ingeniería de Redes Computacionales basado en temas que se le hace difícil a el estudiante su comprensión en el momento de realizar las practicas o ejercicios que se desarrollan en clase.

Además de que es una ayuda en clase el manual también es un apoyo en el momento que el estudian tenga la determinación y el interés de certificarse como CCEN 100-105, debido a que el libro se encuentra basado en la temática de la certificación.

Se tiene claro con este proyecto que existen diferentes tipos de manuales de acorde a la necesidad de los estudiantes. Surgió la idea de un manual debido a las innumerables dificultades que existen al momento de la certificación, las limitantes más comunes son la falta de interés que hay en la certificación debido a que no hay mucho material de apoyo, la limitante de tiempo en prácticas que están restringidas por la hora clase, la falta de comprensión del estudiante en temas que son complicados entre otros motivos que surgen mediante el proceso.

Algo para destacar es que el manual se encontraría al alcance del estudiante solventando la problemática de la deficiencia que hay en el momento de realizar sus prácticas.

En la investigación se ha tomado en cuenta una de las primeras certificaciones que el estudiante de la carrera de Técnico en Ingeniería de Redes Computacionales podría optar como primer paso para una mejor formación académica, luego de este primer paso la academia de CISCO posee otras certificaciones más avanzadas que ayudan a una mejor formación Para la competencia de los estudiantes.

2. Recomendaciones

El estudiante de la carrera Técnico en Ingeniería de redes Computacionales tiene que seguir buscando la manera de innovarse con nuevos manuales debido que la tecnología avanza a pasos a agigantados y es por eso que el estudiante tiene que velar por su conocimiento para poder tener mejores Oportunidades laborales al culminar su carrera.

Realizar cada cierto tiempo test de conocimiento general debido a que las versiones de las certificaciones pueden tener ciertos cambios cada tiempo y poder estar al día con esos cambios que surjan es necesario que cada los estudiantes se sometan a estas certificaciones y especializarse cada vez más en área de redes informáticas.

Referencias

Mikroways. (2010). *Tipos de Nat*. Recuperado de <https://www.mikroways.net/2010/06/06/tipos-de-nat-y-configuracion-en-cisco/>

Rosales, D. (2015, octubre 2015). *Configuraciones básicas de router o switch*. [Registro web]. Recuperado de <https://delfirosales.blogspot.com/2011/02/configuraciones-basicas-de-un-router-o.html>

Tutorialspoint.(2011). *VLSM*. Recuperado de https://www.tutorialspoint.com/es/ipv4/ipv4_vlsm.htm

Tutorialspoint. (2013). *Direccionamiento Ipv4*. Recuperado de https://www.tutorialspoint.com/es/ipv4/ipv4_addressing.htm

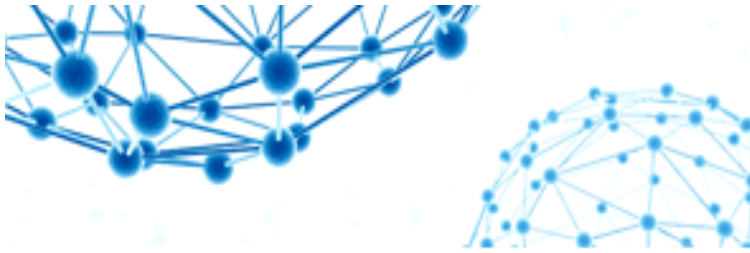
Tutorialspoint. (2016). *Todo sobre redes descripción general*. Recuperado de https://www.tutorialspoint.com/es/ipv4/ipv4_overview.htm



MANUAL PARA LA PREPARACION DE LA CERTIFICACION CCENT 100-105

...

CHRISTOPHER MEZA & MELISSA MENDEZ



Indice

Introducción.....	3
Direccionamiento Ipv4.....	6
Direccionamiento Ipv6.....	17
VLSM IPV4.....	27
Configuraciones básicas de router y swichts.....	33
Banners.....	39
VLAN.....	43
OSPFv2.....	52
NAT.....	60
DHCP.....	85



Introducción

Las redes son, en la actualidad, una parte muy importante de nuestra vida personal y laboral. Tanto en nuestros hogares como en el trabajo, estamos inmersos en alguna red, aunque no seamos conscientes de ello. Con sólo conectarnos a Internet, estamos accediendo a una red, y lo mismo sucede si existe una impresora compartida entre varios equipos o si nos conectamos a otra PC para transferir archivos. El tamaño de las redes es variable, pero en todos los casos sus fundamentos son los mismos. Todas ellas se crean para aprovechar las grandes ventajas que brindan, y todas deben ser sometidas a cuidados especiales para que no representen un problema debido a la falta de seguridad. Este avance de las redes dentro de todos los ámbitos genera un campo de trabajo en el que, primero, necesitamos saber qué son, cómo se constituyen, cuáles son las tecnologías y dispositivos que se encuentran detrás de ellas y de qué forma es posible diseñarlas y configurarlas de la manera más adecuada para cada caso y necesidad. Por eso, en esta obra, nos ocuparemos de hacer un recorrido que partirá desde los cimientos de una red básica y pequeña hasta llegar a convertirla en una red que incorpore las últimas tecnologías y, así, pueda brindar beneficios adicionales a los que comúnmente se implementan. En nuestro camino, conoceremos conceptos teóricos y realizaremos las tareas prácticas necesarias para comprender cada tema en particular; también, analizaremos la conveniencia de utilizar cada una de las alternativas que tenemos disponibles. Así, aprenderemos a elegir los dispositivos adecuados para cada red, basándonos en sus temas o, en sus perspectivas de crecimiento y en las necesidades que tendrán sus usuarios.

A la hora de elegir dispositivos, en general, optaremos por alguno de los que nos ofrece Cisco, una de las empresas más importantes en hardware de conectividad. Entre sus productos, encontraremos soluciones ideales para diferentes tamaños de red y para resolver los distintos aspectos que hay que cubrir en ella. Comencemos, entonces, el aprendizaje que nos convertirá en especialistas en el armado y configuración de redes que cubran las necesidades de cualquier potencial del estudiante

Direccionamiento Ipv4

Ejemplo de una dirección IP:

192.168.10.10

Las direcciones IPv4 se expresan mediante un número binario de 32 bits permitiendo un espacio de direcciones de hasta 4.294.967.296 (2³²) direcciones posibles, se dividen los 32 bits de la dirección en cuatro partes divididas por un punto y cada parte posee 8 bits expresados en binario.

Ejemplo.

192	.	168	.	10	.	10
11000000		10101000		00001010		00001010

Una dirección IP está formada por un conjunto de uno a tres números en cada octeto de los cuales puede ser entre 0 y 255.

Para poder comunicarse en una red, cada equipo debe tener una dirección IP exclusiva. En el direccionamiento IP en clases, existen tres clases de dirección primordiales que se utilizan para asignar direcciones IP a los equipos. El tamaño y tipo de la red determinará la clase de dirección IP que se aplique cuando proporcionemos direcciones IP a los equipos y otros hosts de nuestra red.

Clase A

Las direcciones de clase A se asignan a redes con un número muy grande de hosts. Esta clase permite 126 redes, utilizando el primer número para el ID de red. Los tres números restantes se utilizan para el ID de host, permitiendo 16.777.214 hosts por red.

Clase B

Las direcciones de clase B se asignan a redes de tamaño mediano a grande. Esta clase permite 16.384 redes, utilizando los dos primeros números para el ID de red. Los dos números restantes se utilizan para el ID de host, permitiendo 65.534 hosts por red.

Clase C

Las direcciones de clase C se utilizan para redes de área local (LANs) pequeñas. Esta clase permite aproximadamente 2.097.152 redes utilizando los tres primeros números para el ID de red. El número restante se utiliza para el ID de host, permitiendo 254 hosts por red.

Clases D y E

Las clases D y E no se asignan a hosts. Las direcciones de clase D se utilizan para la multidifusión, y las direcciones de clase E se reservan para uso futuro.

Clase IP	Rango
A	0.0.0.0 - 127.255.255.255
B	128.0.0.0 – 191.255.255.255
C	192.0.0.0 – 223.255.255.255
D	224.0.0.0 – 239.255.255.255
E	240.0.0.0 247.255.255.255

Estos son los rangos a los que pertenecen las IP:

En el método de clases, cada clase de dirección tiene una máscara de subred predeterminada.

- Clase A: 255.0.0.0
- Clase B: 255.255.0.0
- Clase C: 255.255.255.0

Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Una vez establecida una red, todos los equipos que se encuentran en ella necesitan una dirección IP. Sin una dirección IP, un equipo no recibe los datos que van dirigidos a él, el formato de la dirección IP debe seguir

ciertas directrices para garantizar que los datos se transmiten al equipo correcto.

- El primer número del ID de red no puede ser 127. Este número de ID está reservado para pruebas de conexión, como realizar un bucle local.
- Los números del ID de host no pueden ser todos 255, ya que esta dirección se utiliza como dirección de difusión IP.
- ID de host no puede ser todo ceros (0s), ya que esta dirección se utiliza para indicar un ID de red.
- El ID de host debe ser exclusivo para el ID de red local.

Luego de haber identificado los componentes, del direccionamiento de una red IPv4, es importante hacer uso del proceso Denominado "Subneteo". El subneteo es la sistematización que nos ayuda a determinar la ip de los equipos utilizados en una red, ya sea una red muy grande o una red pequeña.

Ejemplo:

En esta ocasión utilizaremos una ID de red clase C, 192.168.1.0 con la mascara de subred /24 debido a que la dirección de Red o (ID de host) es clase C, Nos piden obtener las direcciones accionables para una red que posee 13 computadoras y un router.

Paso 1.

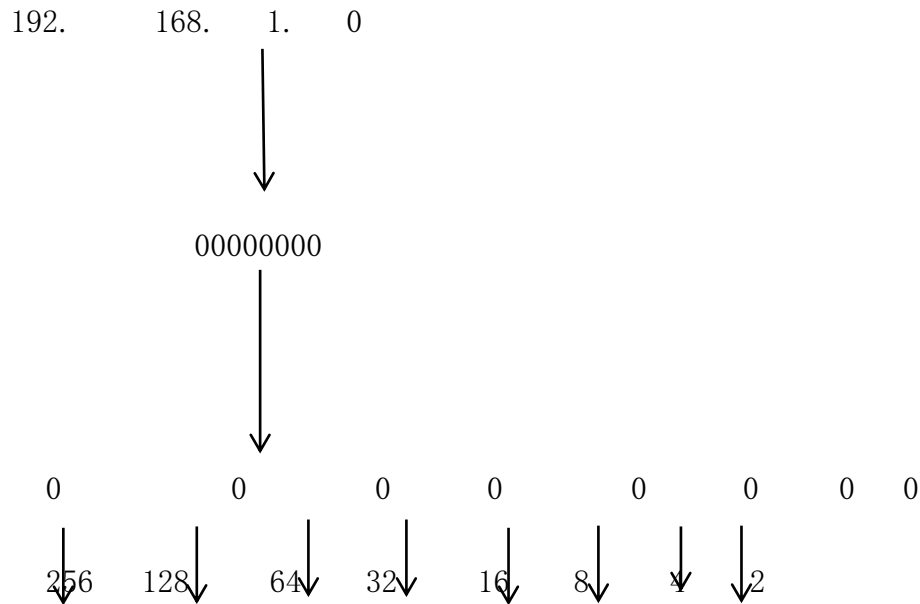
Debemos convertir el ID de Red en binario, el binario es un conjunto de 1 y 0, los 1 representan los bits que se han utilizado en un ID de host o de Red, Y los 0 representan los bits que aún se encuentran libres para utilizar, cada numero binario es un bits, que tiene una valor asignado, ahora convertiremos a binario el ultimo octeto que se encuentra en el ID de red 192.168.1.0.

192.	168.	1.	0
		↓	
		00000000	

Como podemos observar en el ejemplo todos los numero se encuentran en cero significa que ningún bits ha sido utilizando de los ocho que se compone cada decimal en el ID.

Paso 2.

Ahora de haber convertido el decimal que se utilizar de el ID, hay que definir el varlo que posee cada bits, este es el valor que posee cada bits ya de manera predeterminada, según los estándares.



Paso 3.

Una vez realizados el paso 1 y 2, para encontrar las direcciones de asignables que le colocaremos a los host, debemos utilizar la formula $2^n - 2$ (dos elevado a la "n" potencia menos 2), el valor de "n" depende de la cantidad de IP que necesitamos, en el ejercicio nos señala, que estaríamos utilizando un total de 13 de host, entonces debemos elevar el 2 a la potencia que creamos correspondiente que nos de un numero resultado de acorde a la cantidad de IP que necesitamos en este caso seria 4, si elevamos 2 a la cuarta potencia, nos da un total de 16, que es el número de IP que podemos utilizar, y la formula nos indica que al resultado debemos restarle 2 digitos, que seria la primer IP asignable y el broadcast.

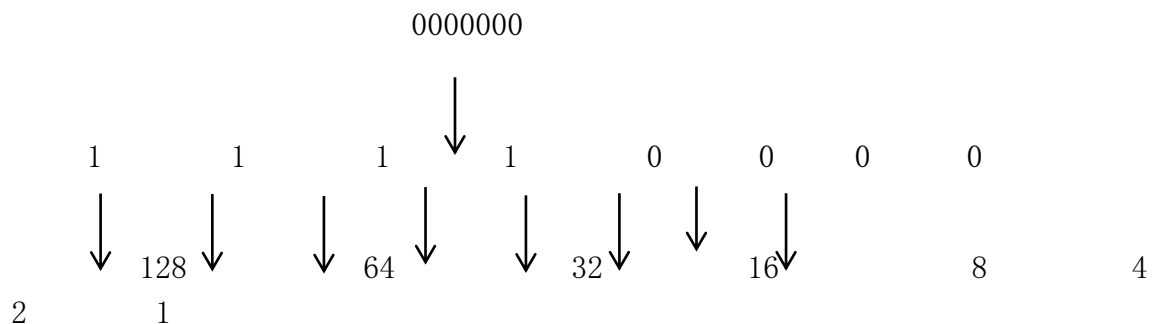
Entonces la formula quedaría de la siguiente manera:

$$2^4 - 2 = 14$$

Y el resultado es 14, que es el número de IP asignable que obtendremos, siempre que realicemos el subneteo de una red debemos tomar en cuenta que la cantidad de bits que decidamos encender debe ser mayor a la cantidad de Host.

Paso 4.

Ya que encontramos cual sería la cantidad de IP asignables, ahora debemos encontrar la máscara de subred, debido a que hemos encendido los últimos 4 bits la máscara de subred ya no es la misma, para encontrar la máscara de subred, debemos manejar una tabla distinta, en donde el cero es tomando un bit, que significa esto, que si en algún momento elevamos el 2 a la cero debe darnos como resultado 1. Entonces esta sería el desarrollo para encontrar la máscara.



Tenemos 4 bits que se encuentran encendidos en esta fórmula ¿Qué significa?, son los bits que no se utilizaron en la fórmula anterior para encontrar la cantidad de host, entonces los bits que no se utilizan para encontrar host, esos bits que sobran son utilizados en la fórmula de la subredes que es la siguiente, $2^n - 2$ en donde "n" es el número de bits que se utilizaron para la subred, entonces esa fórmula quedaría de la siguiente manera:

$$2^4 - 2 = 16$$

En donde 16 es la cantidad de subredes que pueden utilizarse, y para encontrar la máscara que utilizaremos de ahora en adelante con los ID de red, debemos realizar la suma de todos los bits que fueron utilizados para red. Entonces debemos sumar, $128 + 64 + 32 + 16 = 240$

Entonces si la antigua máscara de red era 255.255.255.0 ahora debido a que solo se ha tocado el último octeto sería la siguiente, 255.255.255.240.

Entonces el resultado de todo seria, el siguiente

La direcciones 192.168.1.0 con una máscara de 255.255.255.240.

Direccionamiento Ipv6

El Protocolo de Internet versión 6, en inglés: Internet Protocol version 6 (IPv6), es una versión del Internet Protocol (IP), y diseñada para reemplazar a Internet Protocol version 4 (IPv4) que a 2016 se está implementando en la gran mayoría de dispositivos que acceden a Internet.

Una dirección IPv6 tiene un tamaño de 128 bits y se compone de ocho campos de 16 bits, cada uno de ellos unido por dos puntos. Cada campo debe contener un número hexadecimal.

Ejemplo:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

La mayoría de las direcciones IPv6 no llegan a alcanzar su tamaño máximo de 128 bits. Eso comporta la aparición de campos rellenos con ceros o que sólo contienen ceros.

La mayoría de las direcciones IPv6 no llegan a alcanzar su tamaño máximo de 128 bits. Eso comporta la aparición de campos rellenos con ceros o que sólo contienen ceros.

La arquitectura de direcciones IPv6 permite utilizar la notación de dos puntos consecutivos (:) para representar campos contiguos de 16 bits de ceros. Por ejemplo, la dirección IPv6 de la Figura 3-2 se puede abreviar reemplazando los dos campos contiguos de ceros del ID de interfaz por dos puntos. La dirección resultante es 2001:0db8:3c4d:0015::1a2f:1a2b. Otros campos de ceros pueden representarse como un único 0. Asimismo, puede omitir los ceros que aparezcan al inicio de un campo, como por ejemplo cambiar 0db8 por db8.

Así pues, la dirección 2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b se puede abreviar en 2001:db8:3c4d:15::1a2f:1a2b.

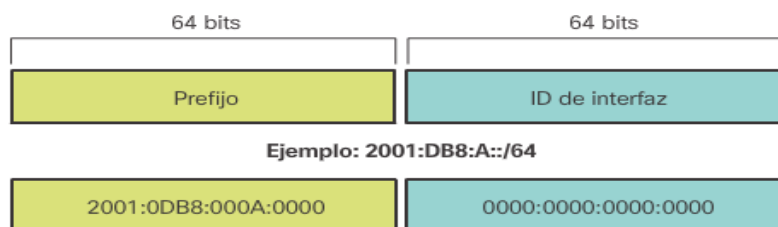
La notación de los dos puntos consecutivos se puede emplear para reemplazar cualquier campo contiguo de ceros de la dirección IPv6. Por ejemplo, la dirección IPv6 2001:0db8:3c4d:0015:0000:d234::3eee:0000 se puede contraer en 2001:db8:3c4d:15:0:d234:3eee::.

Los campos que están más a la izquierda de una dirección IPv6 contienen el prefijo, que se emplea para enrutar paquetes de IPv6.

El tamaño del prefijo se expresa en notación CIDR (enrutamiento entre dominios sin clase). La notación CIDR consiste en una barra inclinada al final de la dirección, seguida por el tamaño del prefijo en bits

IPv6 utiliza la longitud de prefijo para representar la porción de prefijo de la dirección. IPv6 no utiliza la notación decimal punteada de máscara de subred (en otras palabras ya no se verán mascarar similares a esta 255.255.255.0). La longitud de prefijo se utiliza para indicar la porción de red de una dirección IPv6 mediante el formato de dirección IPv6/longitud de prefijo.

La longitud de prefijo puede ir de 0 a 128. Una longitud de prefijo IPv6 típica para LAN y la mayoría de los demás tipos de redes es /64. Esto significa que la porción de prefijo o de red de la dirección tiene una longitud de 64bits, lo cual deja otros 64bits para la ID de interfaz (porción de host) de la dirección.



Y para obtener las direcciones asignab

les en la red y las subredes debemos entender cómo funciona.

Las direcciones en IPv6 están armadas con números en hexadecimal, que es el mismo que usamos para montar las direcciones MAC (dirección física de la computadora).

En cuanto los decimales van de 0 hasta 9 las hexadecimales van de 0 a F, así que tenemos:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Una dirección IPv6 está formada por 128 bits, que se representa mediante ocho grupos de cuatro dígitos hexadecimales, cada grupo representando 16 bits (dos octetos).

Los grupos se separan mediante dos puntos (:). Un ejemplo de dirección IPv6 podría ser:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Separemos un grupo:

2001 = 4 hexadecimales 2, 0, 0, 1

La creación de subredes en IPv6, sigue el mismo principio de la creación de subredes en IPv4, la única diferencia está en la representación de la dirección.

En general las direcciones en IPv6 son pensadas para que los primeros 64 bits sean la red y los segundos 64 bits sean el host.

Ejemplo:

El proveedor de Internet nos brinda la siguiente dirección de IPV6, 2001:DB8::/32 y debemos encontrar cuantos host tendríamos asignables al elevar esta dirección IPV6 al prefijo 48. Iniciaremos explicando lo siguiente.

En la dirección 2001:DB8:: solo tenemos 2 hextetos que ya han sido utilizados y nos restan 5 hextetos más para la red, de los cuales para este ejemplo solo estaríamos utilizando 1 debido a que cada exteto posee 16 bist.

Para identificar la parte de la red que debemos utilizar es recomendable descomprimir la red:

2001:DB8::0000

Entonces con respecto a el prefijo si sumamos 32 bits que se encontraban en uso en el prefijo de la dirección IPV6 original más los 16 que estaríamos tomando darían un total de 48 bist.



$$\begin{array}{ccccc}
 2001: & & \text{DB8::} & & 0000 \\
 \downarrow & & \downarrow & & \downarrow \\
 16 & + & 16 & + & 16 = 48
 \end{array}$$

Ahora para encontrar las direcciones de host, descomprimos el bloque de 16 bits que estaríamos utilizando (el tercer hexeto). Recordando que cada dígito que ocupamos puede llegar de el cero hasta la letra "f"

2001:	DB8::	0000	
		↓	
			0001
			0002
			0003
	...		
	...		000F
			0010
			0011
			0012
	...		...
			FFF

Y esas serían las direcciones, recordando que cuando en el primer dígito hasta llegado hasta "f", entonces debemos continuar con el siguiente dígito. Pero para saber exactamente cuántas direcciones son asignables solamente elevamos 2 a la 16 que es el número de bits que posee el hexeto que nos daría un total de 65,536 direcciones para host.

Ahora que ya sabemos cuáles son los ID de host, estos serían los ID de red.

Tomando en cuenta que el número que ha cambiado para obtener los ID de host, es el último hexeto y que no hemos utilizado los 16 hexetos que se encuentran a la par y que daría de la siguiente manera.

2001:DB8:0000::/48

2001:DB8:0001::/48

2001:DB8:0002::/48

2001:DB8:0003::/48

Y así sucesivamente hasta llegas a "F", ahora tomaremos la segunda red para saber como se colocaríamos las IP asignables.

2001:DB8:0002::1/48

2001:DB8:0002::2/48

2001:DB8:0002::3/48

Esas serían las direcciones asignables que podemos utilizar para los host, El cambio para saber que direcciones podemos asignar a los equipos siempre debe colocarse en el octavo hexeto.

EJERCICIO.

Utilizar la dirección 2001:BABA:CAFE::/48, Y elevarla hasta el prefijo /56 y calcular cuántos host tendríamos por cada red y cuáles serían las siguiente 3 redes a utilizar.

VLSM IPV4

Objetivo: Brindar mayor flexibilidad a las aplicaciones de subredes, este método se implementó con la finalidad de poder evitar la debilidad de las direcciones.

VLSM es la sigla de Variable Length Subnet Masks o, en español, máscara de subred de longitud variable o máscara variable. Básicamente es la técnica por la cual se diseña un esquema de direccionamiento usando varias máscaras en función de la cantidad de hosts, es decir, la cantidad de hosts determina la longitud de la máscara o longitud del prefijo de red.

Características VlsM Ipv4

- I. Se permite solo una máscara de subred para todas las redes.
- II. Es el enrutamiento de Classless.
- III. Es el proceso de dividir una subred en subredes

Ejemplo de VlsM Ipv4

Paso - 1

Hacer una lista de subredes.

Paso - 2

Ordenar los requisitos de IPs en orden descendente (de mayor a menor).

Ventas 100

Adquirir 50

25 Cuentas

5 Gestión

Paso 3

Asignar la más alta gama de IPs a la más alta exigencia, por lo que vamos asignarle 192.168.1.0 /25 (255.255.255.128) en el departamento de ventas. Esta subred IP 192.168.1.0 con número de red dispone de 126 direcciones IP de host válidos que cumplan con el requisito del departamento de ventas. La máscara de subred que se utiliza para esta subred tiene 10000000 como el último octeto.

Paso - 4

Asignar la próxima gama más alta, por lo que vamos asignarle 192.168.1.128 /26 (255.255.255.192) en el departamento de compras. Esta subred IP 192.168.1.128 con número de red válido tiene 62 direcciones IP de Host que se pueden asignar fácilmente a todos los equipos de del departamento de compras. La máscara de subred que se utiliza tiene 11000000 en el último octeto.

Paso - 5

Asigne el siguiente rango más alto, es decir, las cuentas. El requisito de 25 IPs puede ser cumplido con 192.168.1.192 /27 (255.255.255.224) subred IP, que contiene 30 host IPs. El número de red del departamento de contabilidad será 192.168.1.192. El último octeto de máscara de subred es 11100000.

Paso - 6

Asigne el siguiente rango más alto en la administración. El departamento de gestión contiene sólo 5 equipos. La subred 192.168.1.224 /29 con la máscara 255.255.255.248 tiene exactamente 6 válida direcciones IP de host. Por lo tanto, esta puede ser asignado a la gestión. El último octeto de la máscara de subred contendrá 11111000.

Con VLSM, el administrador puede subred la subred IP de tal manera que un menor número de direcciones IP se desperdician. Incluso después de asignar IPs a cada departamento

Ejercicio de práctica de laboratorio VlsM Ipv4

Dada la red 192.168.0.0/24, desarrolle un esquema de direccionamiento que cumpla con los siguientes requerimientos. Use VLSM, es decir, optimice el espacio de direccionamiento tanto como sea posible.

- I. Una subred de 20 hosts para ser asignada a la Aula de Profesores
- II. Una subred de 80 hosts para ser asignada a la Aula de Estudiantes
- III. Una subred de 20 hosts para ser asignada a la Sala de Invitados

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Configuraciones básicas de router y swichts

Se mostrara como realizar las siguientes configuraciones básicas de un Router Cisco o Switch

- Configurar un Nombre al Router
- Configurar los Passwords
- Proteger los Puertos de Consola y el Auxiliar
- Configurar un Banner
- Encriptar Passwords
- Como guardar la Configuración

También quiero mencionar que los comandos que se utilizaran para configurar el Router son los mismos para un Switch Cisco.

Para configurarle un nombre al router se utiliza el comando `hostname`.
Escribimos enable para entrar a Modo Privilegiado (Privilege Exec Mode)

```
Router> enable
```

Escribimos Configure Terminal para entrar a Modo de Configuración

```
Router# configure terminal
```

Global (Global Configuration Mode)

```
Router(config)# hostname nombredelrouter
```

Ejemplo

```
Router>  
Router> enable  
Router# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)# hostname delfirosales  
delfirosales(config)#
```

Una vez en configuración global escribimos el comando hostname y el nombre del router.

Configuración de las Contraseñas

Son cinco las contraseñas que se utilizan para asegurar nuestros router Cisco.

1. Consola
2. Auxiliar
3. Telnet (vty)
4. Enable Password
5. Enable Secret

El enable secret y enable password se utilizan para asegurar con una contraseña al modo privilegiado. Esto hará que un usuario escriba el comando enable le pida una contraseña y así entrar a modo privilegiado. Los otros tres se utilizan para configurar una contraseña cuando el modo de usuario (User Exec Mode) se accede a través del puerto de consola, a través del puerto auxiliar o a través de Telnet.

Enable Password y Enable Secret

Para habilitar el enable password y el enable secret tenemos que estar en modo de configuración global, como se muestra a continuación.

```
delfirosales# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
delfirosales(config)# enable ?
last-resort Define enable action if no TACACS servers respond
password    Assign the privileged level password
secret      Assign the privileged level secret
use-tacacs   Use TACACS to check enable passwords

delfirosales(config)# enable password delfirosales
delfirosales(config)# enable secret delfirosales
The enable secret you have chosen is the same as your enable password.
This is not recommended. Re-enter the enable secret.
```

Hemos configurado los el enable password y enable secret, pero hemos recibido un mensaje en consola de que la contraseña utilizada para el enable password y enable secret es la misma, así que lo recomendable es cambiarla, utilizar contraseñas diferentes

Configurar una contraseña al Puerto Auxiliar

Para configurar una contraseña al puerto auxiliar tenemos que estar en modo

```
delfirosales# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
delfirosales(config)# line aux 0
delfirosales(config-line)# password passaux
delfirosales(config-line)# login
delfirosales(config-line)#
```

de configuración global.

```
delfirosales(config)# line console 0
delfirosales(config-line)# password passconsole
delfirosales(config-line)# login
delfirosales(config-line)#
```

Configurar un Password para la Consola

Configurar un Password a Telnet

Para configurar un password a telnet necesitamos estar en modo de configuración global y utilizar el comando line vty. Todos los router que no estén ejecutando la edición Enterprise del IOS por defecto solo tienen cinco líneas vty, de la 0 a la 4. Pero si nuestro router está ejecutando un IOS de la edición Enterprise, tendremos más líneas vty. La mejor manera de averiguar el número que tiene el router utilizaremos el signo de interrogación como se muestra a continuación.

```
delfirosales(config)# line vty ?
<0-1276> First Line number

delfirosales(config)# line vty 0 1276
delfirosales(config-line)# password passtelnet
delfirosales(config-line)# login
delfirosales(config-line)#
```

Banners

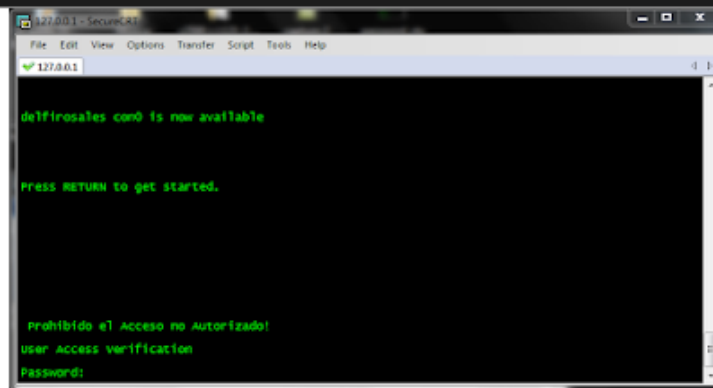
Los banners son mensajes de advertencia que se muestran cuando alguien quiera establecer una sesión de telnet. Para configurar el banner mas utilizado, el banner MOTD (Message of the day) escribimos en consola el siguiente comando.

```
(config)# banner motd x Aquí el mensaje del Banner motd x
```

Por ejemplo

```
delfirosales(config)# banner motd x Prohibido el Acceso no Autorizado! x
```

```
delfirosales(config)#  
delfirosales(config)# ^Z  
*Mar 1 00:45:21.963: %SYS-5-CONFIG_I: Configured from console by console  
delfirosales# exit
```



Cerramos sesión y al tratar de iniciar una sesión nueva nos saldrá el mensaje motd como se muestra a continuación.

Encriptar los Passwords

Debido a que solo la contraseña de enable secret se encripta de forma predeterminada, tendremos que encriptar las contraseñas manualmente utilizando el comando `service password-encryption` desde configuración global.

```
delfirosales# config t
Enter configuration commands, one per line. End with CNTL/Z.
delfirosales(config)# service password-encryption
```

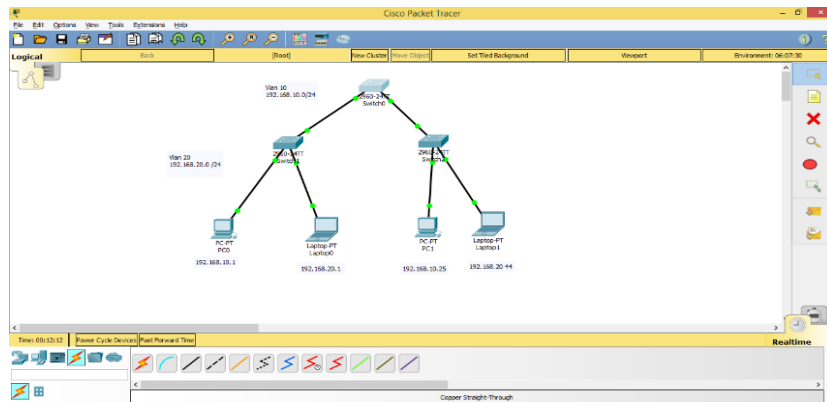
Guardar la Configuración

Finalmente después de configurar nuestro router ahora toca guardar la configuración de la running-config a la startup-config.

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

VLAN

Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios



(MAC, números de puertos, protocolos, etc.).

Ejemplo

Paso 1

Entrar a configurar y colocar los comandos

Switch#enable

Switch#Configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with

Switch(config)#vlan 10

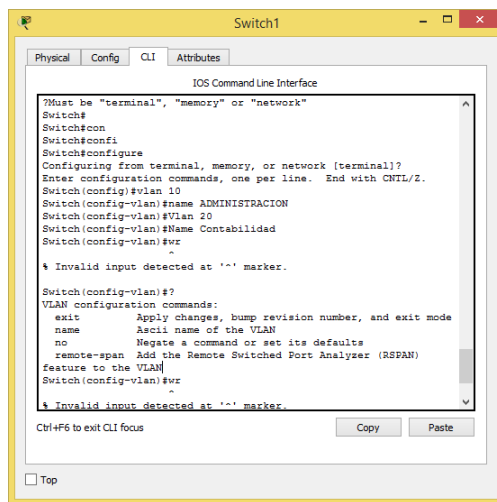
Paso 2

Le pondremos nombres a las Vlan como Vlan 10 Administracion y la Vlan 20 como Contabilidad

Switch(config)#vlan 10

Switch(config-vlan)#name ADMINISTRACION

Switch(config-vlan)#Vlan 20

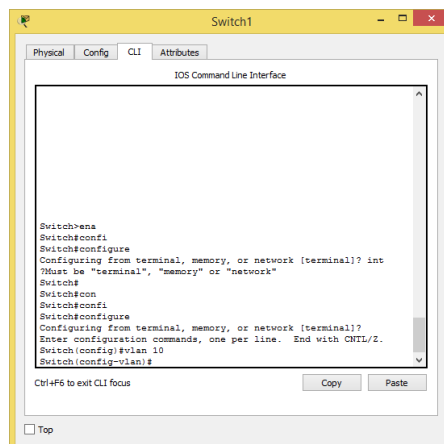


Switch(config-vlan)#Name Contabilidad

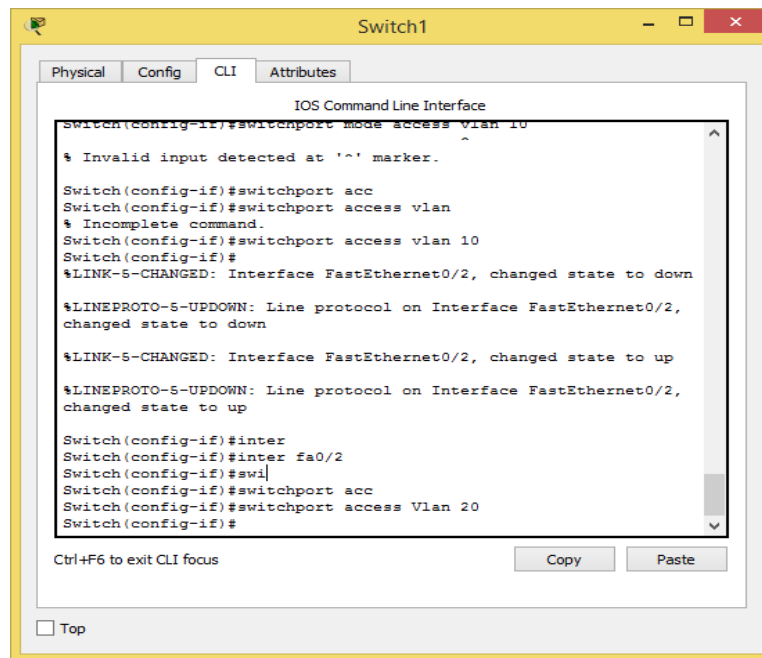
En todos los Switch tendr íamos que ubicar los comandos

Switch(config)#vlan 10

Switch(config-vlan)#name ADMINISTRACIO



Switch(config-vlan)#Vlan 20
Switch(config-vlan)#Name Contabilidad

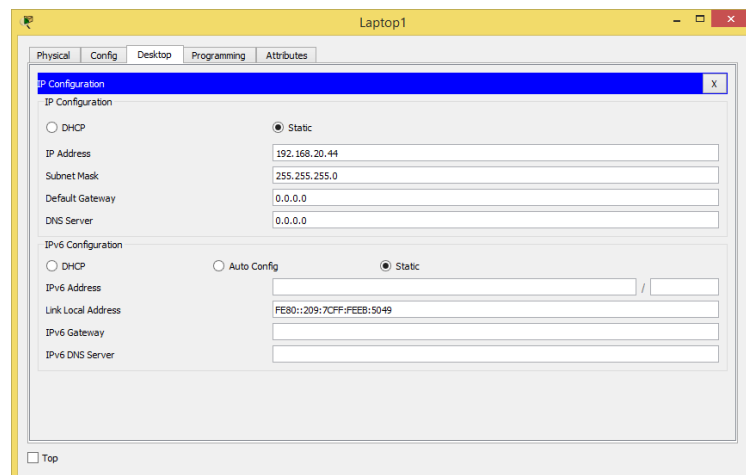
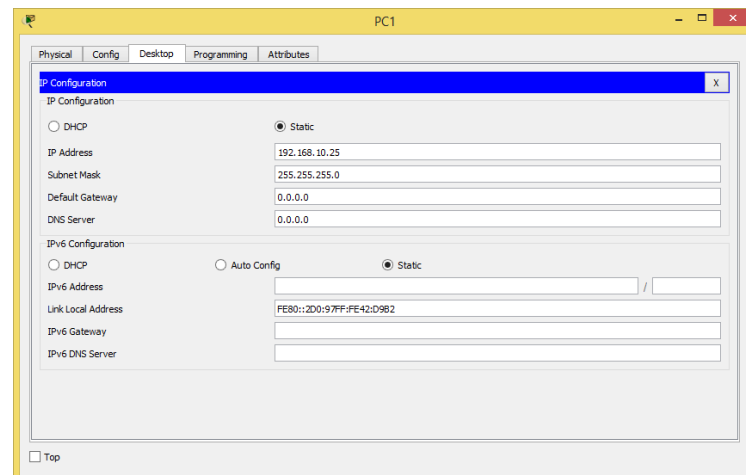
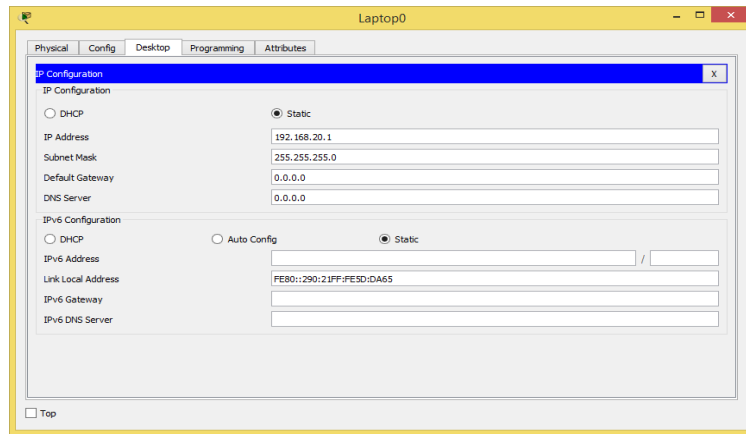


Paso 3

Pasaremos a colocar las interfaces de cada uno de los Switch

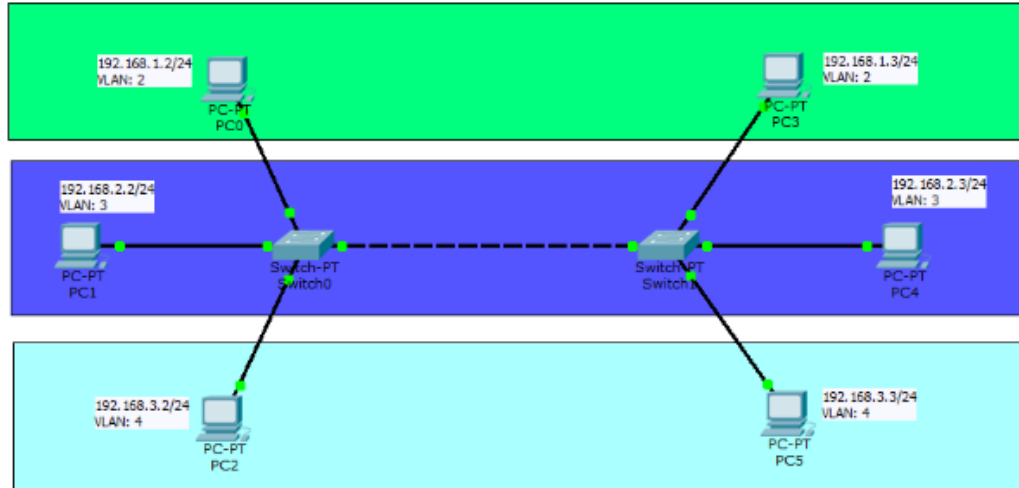
Paso 4

Colocaremos las Ip estáticas a cada una de las Pcs que están en el ejercicio



Al tenerlas configuradas nos vamos a lo que es podremos probar con un ping dentro de las pcs para ver si tienen comunicación entre cada Vlan

Ejercicio a realizar



OSPFv2

OSPFv2 es la versión del protocolo OSPF que actualmente utilizamos en redes IPv4.

Un enrutador OSPFv2 envía un mensaje especial, denominado paquete de saludo, a cada router configurado con OSPFv2.

Por medio de las Interfaz para descubrir otros routers vecinos OSPFv2. Una vez que se descubre un vecino, los dos enrutadores

Comparan la información en el paquete de saludo para determinar si los enrutadores tienen configuraciones compatibles.

Los enrutadores vecinos intentan establecer adyacencia, lo que significa que los enrutadores sincronizan sus bases de datos de estado de enlace para garantizar que tengan información de enrutamiento OSPFv2 idéntica.

Enrutadores adyacentes

Comparten anuncios de estado de enlace (LSA) que incluyen información sobre el estado operativo de cada enlace,

El costo del enlace, y cualquier otra información del vecino. Los enrutadores luego inundan estos LSA recibidos a cada interfaz habilitada

para OSPF, de modo que todos los enrutadores OSPFv2 eventualmente tengan bases de datos de estado de enlace idénticas.

Cuando todos los enrutadores OSPFv2 tienen bases de datos de estado de enlace idénticas, la red está convergente

Cada enrutador utiliza la ruta más corta primero de Dijkstra (SPF) Algoritmo para construir su tabla de rutas.

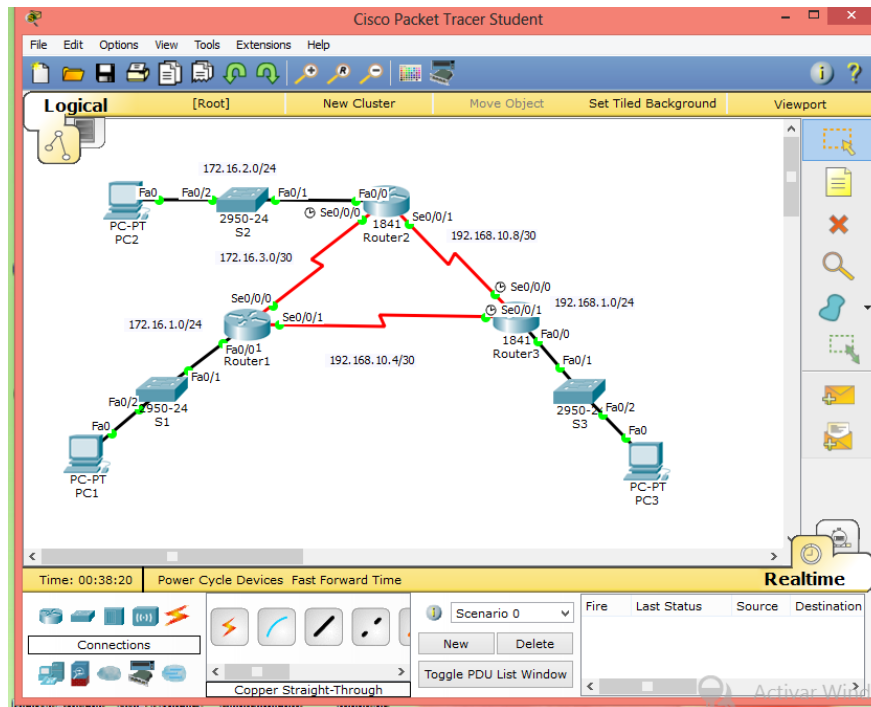
Puede dividir las redes OSPFv2 en áreas. Los enrutadores envían la mayoría de los LSA solo dentro de un área, lo que

Reduce los requisitos de CPU y memoria para un enrutador habilitado para OSPF.

Paso. 1

Se le asigna ID a cada red, utilizando VLSM y se coloca la ip correspondiente a los Host. Para el desarrollo de OSPFv2.

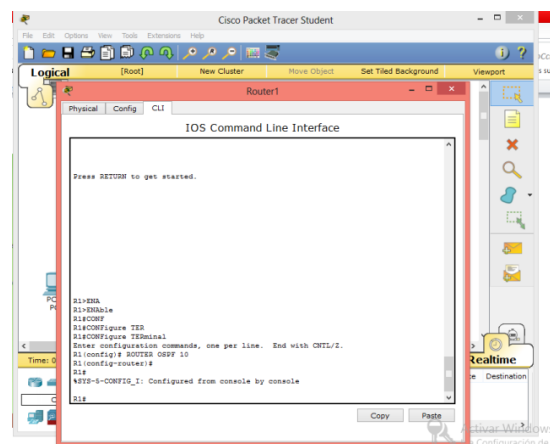
Paso 2 comenzamos las configuraciones en el router 1, colocando el comando.



R1(config)# ROUTER OSPF 10... en el modo de configuración global.colocando el numero 10 como el ID de proceso

Paso 3

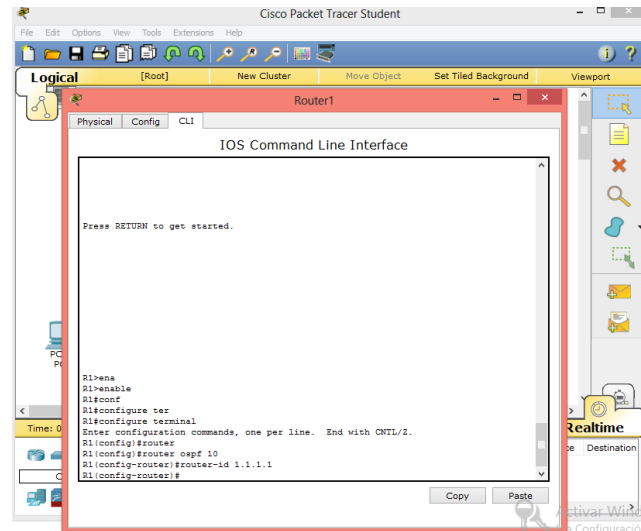
Estando ya en el modo de configuración de OSPFv2, configuramos el ID que



tendría a el dispositivo R1 con el comando R1(config-router)#router-id y seguido del número de ID 1.1.1.1

Paso N° 4

Debemos colocar las interfaces en modo pasivo, para que no se realicen



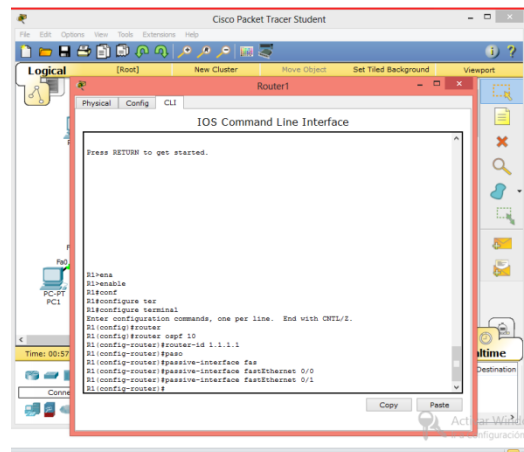
publicaciones en las LAN que se encuentran conectadas.

Con el siguiente comando.

R1(config-router)#passive-interface

Paso N° 5.

Y para finalizar con el Router N° 1, publicaremos todas las direcciones ID



[illegible]

correspondiente con el siguiente comando.

Luego de haber realizado esa configuración, hacemos lo mismo en el R2 y R3. Siempre guardando todo en cada router.

Ejercicio a realiza

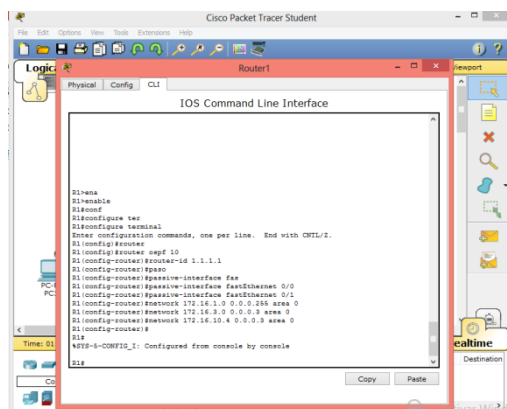
NAT

La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés Network Address Translation), es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

El tipo más simple de NAT proporciona una traducción una-a-una de las direcciones IP. La RFC 2663 se refiere a este tipo de NAT como NAT Básico, también se le conoce como NAT una-a-una. En este tipo de NAT únicamente las direcciones IP, las sumas de comprobación (Checksums) de la cabecera IP y las sumas de comprobación de nivel superior, que se incluyen en la dirección IP, necesitan ser cambiadas.

Cuando el cliente envía paquetes fuera de la red, NAT traduce la dirección IP interna del cliente a una dirección externa.

Existen 3 clases de NAT:



NAT Estática.

Conocida también como NAT 1:1, es un tipo de NAT en el que una dirección IP privada se traduce a una dirección IP pública, y donde esa dirección pública es siempre la misma. Esto le permite a un host, como un servidor

Web, el tener una dirección IP de red privada pero aun así ser visible en Internet.

NAT Dinámica

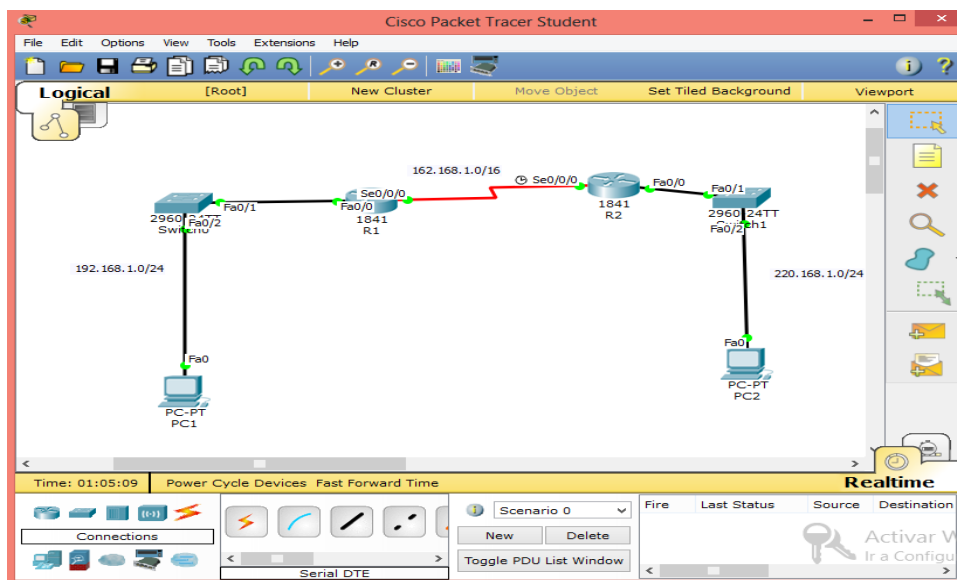
Es un tipo de NAT en la que una dirección IP privada se mapea a una IP pública basándose en una tabla de direcciones de IP registradas (públicas). Normalmente, el router NAT en una red mantendrá una tabla de direcciones IP registradas, y cuando una IP privada requiera acceso a Internet, el router elegirá una dirección IP de la tabla que no esté siendo usada por otra IP privada. Esto permite aumentar la seguridad de una red dado que enmascara la configuración interna de una red privada, lo que dificulta a los hosts externos de la red el poder ingresar.

Para este método se requiere que todos los hosts de la red privada que deseen conectarse a la red pública posean al menos una IP pública asociadas.

NAT con sobrecarga

El caso de NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos y el más usado en los hogares. Consiste en utilizar una única dirección IP pública para mapear múltiples direcciones IPs privadas. ventajas, el cliente necesita contratar una sola dirección IP pública para que las máquinas de su red tengan acceso a Internet, lo que supone un importante ahorro económico y ahorra un número importante de IPs públicas, lo que demora el agotamiento de las mismas.

En una única dirección IP pública se mapeen múltiples IPs privadas. Con PAT el hace uso de múltiples puertos para manejar las conexiones de cada host interno.

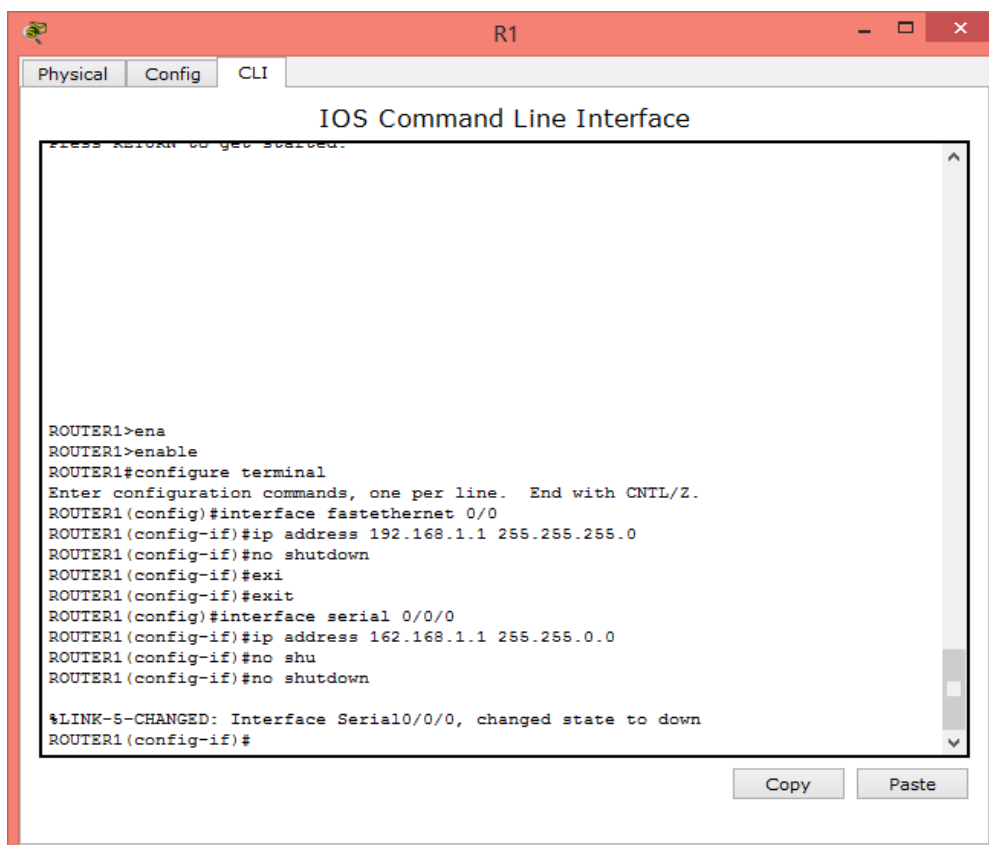


Ejemplo de Nat Estático

Vamos a realizar la configuración de las interfaces de los router de la topológica anterior.

Paso2.

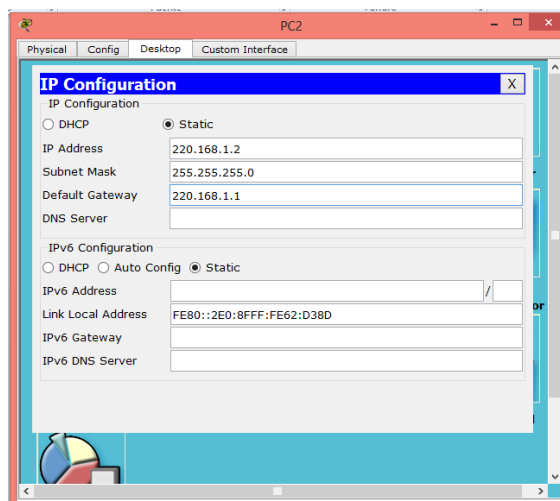
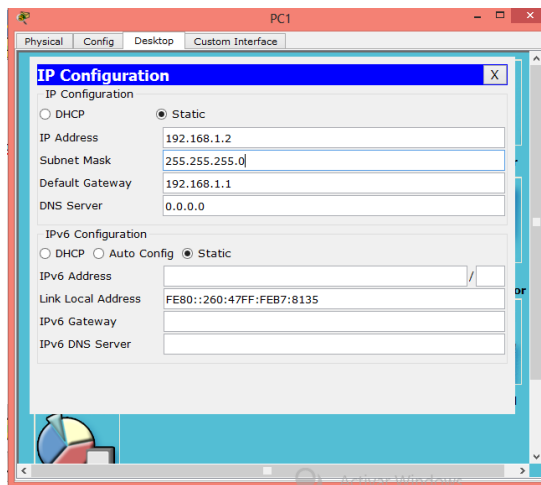
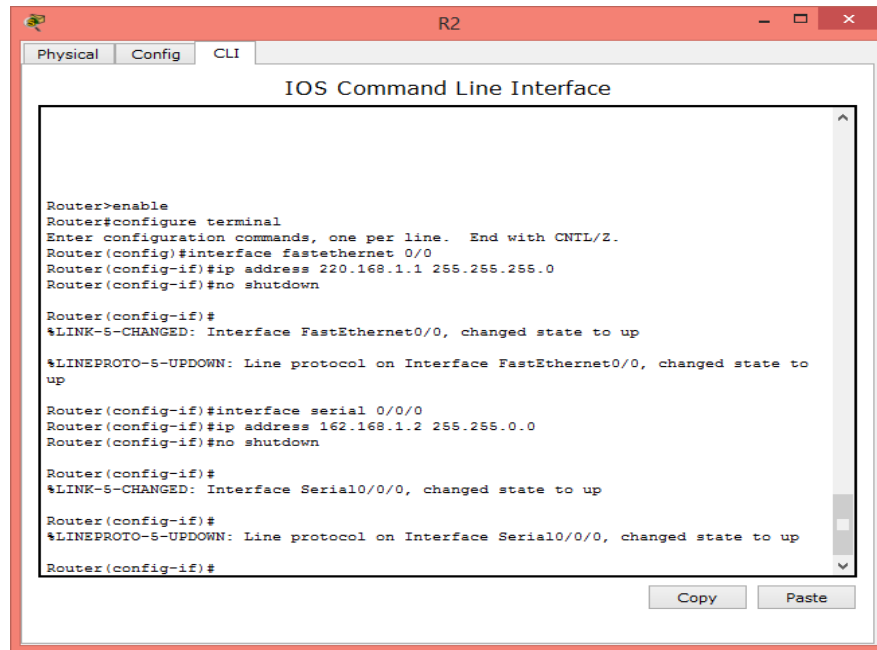
Ahora realizaremos la configuración de las direcciones IP en los host.



The screenshot shows a window titled "R1" with tabs for "Physical", "Config", and "CLI". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and responses:

```
ROUTER1>ena
ROUTER1>enable
ROUTER1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER1(config)#interface fastethernet 0/0
ROUTER1(config-if)#ip address 192.168.1.1 255.255.255.0
ROUTER1(config-if)#no shutdown
ROUTER1(config-if)#exi
ROUTER1(config-if)#exit
ROUTER1(config)#interface serial 0/0/0
ROUTER1(config-if)#ip address 162.168.1.1 255.255.0.0
ROUTER1(config-if)#no shu
ROUTER1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
ROUTER1(config-if)#
```

At the bottom of the window, there are "Copy" and "Paste" buttons.

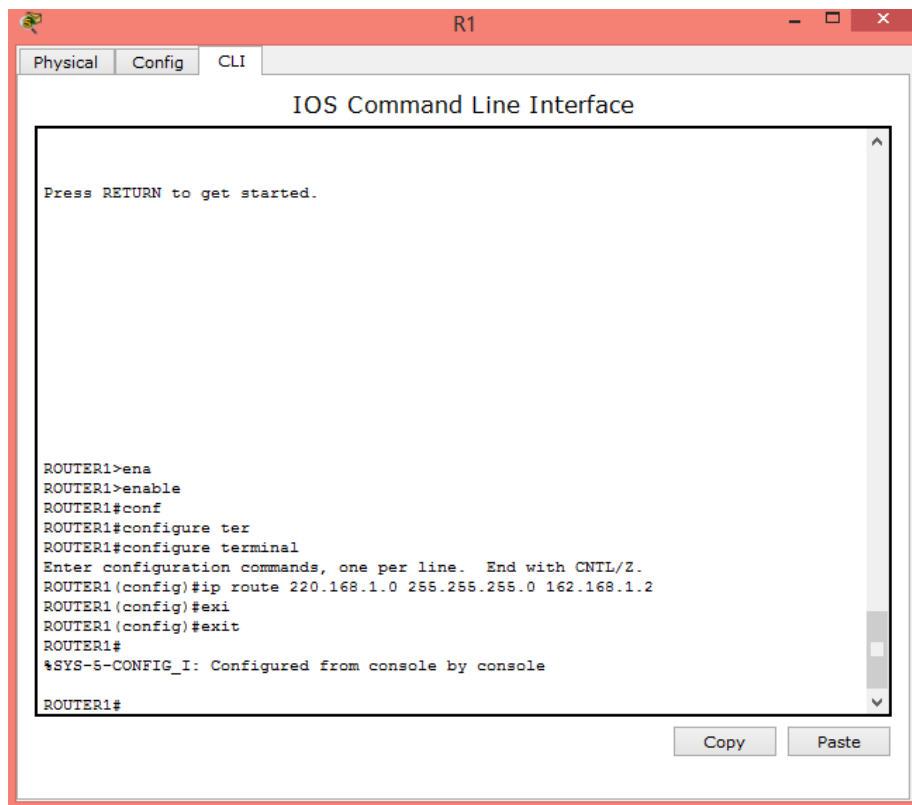


PASO 3.

Ahora realizaremos la configuración de NAT Estático con el siguiente comando.

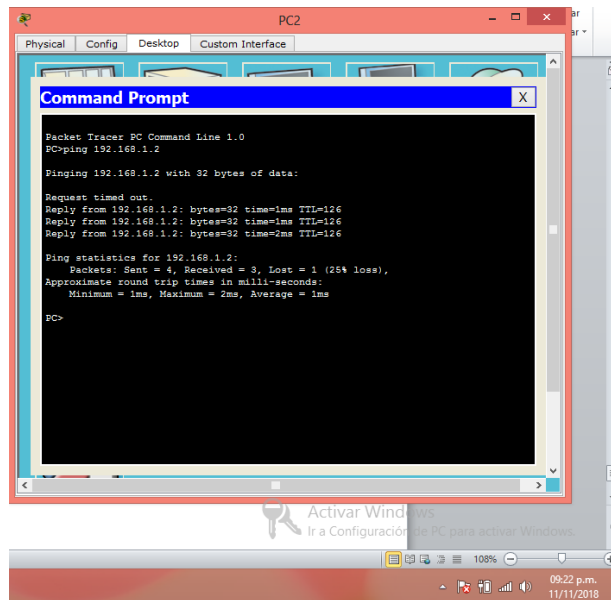
Router1.

ROUTER1(config)#ip (ID del Router2 que no conoce) (mascara de la red que no conoce) (ip de la serial donde tendr ía la comunicaci ón).

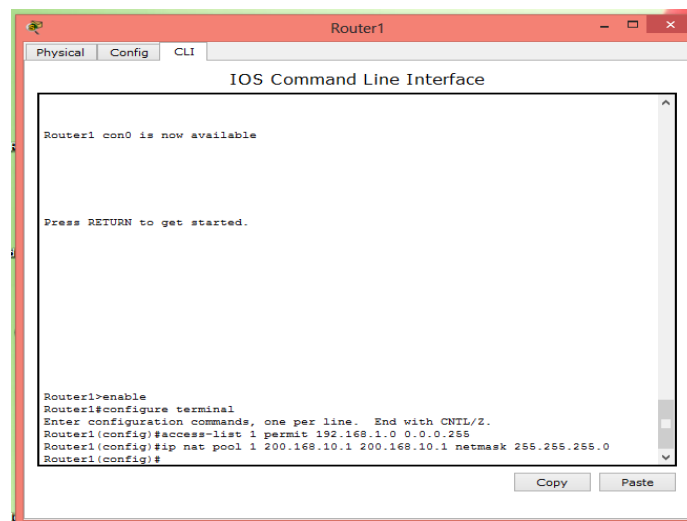


Luego realizamos el mismo procedimiento el Router2.

Para comprobar su funcionabilidad haremos ping desde la Pc2 a la Pc1



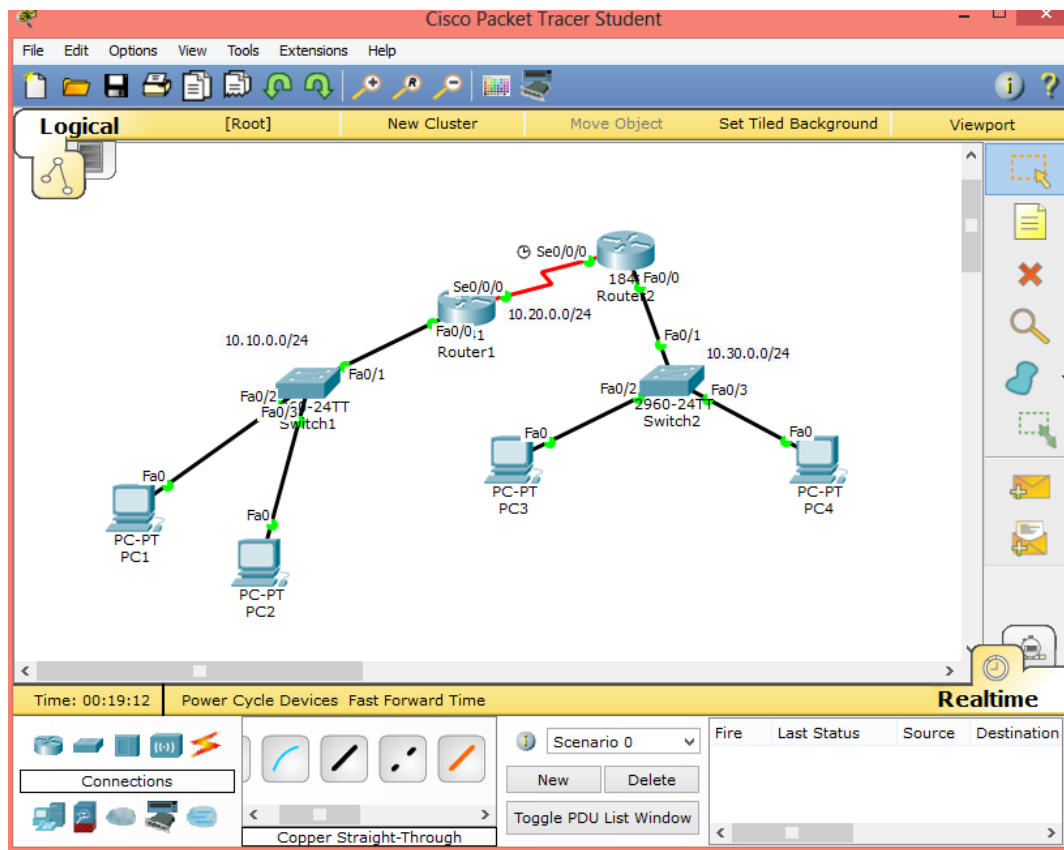
Ejercicio de Nat Estatico



Ejemplo de Nat Dinamico

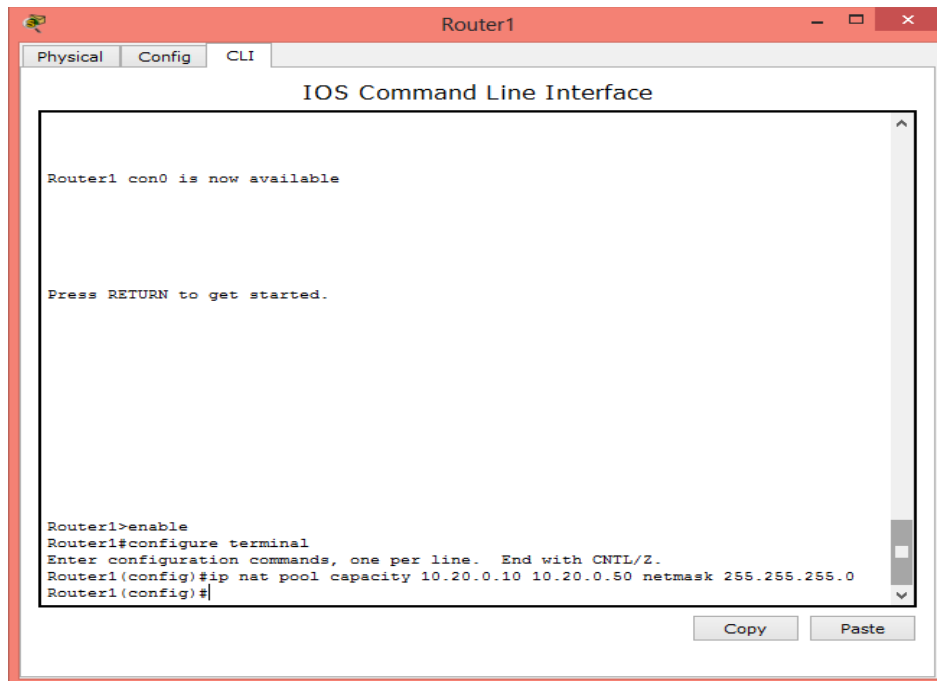
Paso 1.

Con la siguiente topología vamos a encender las interfaces de los equipos, y realizaremos la configuración de las IP en los host y equipos para que puedan tener comunicación.



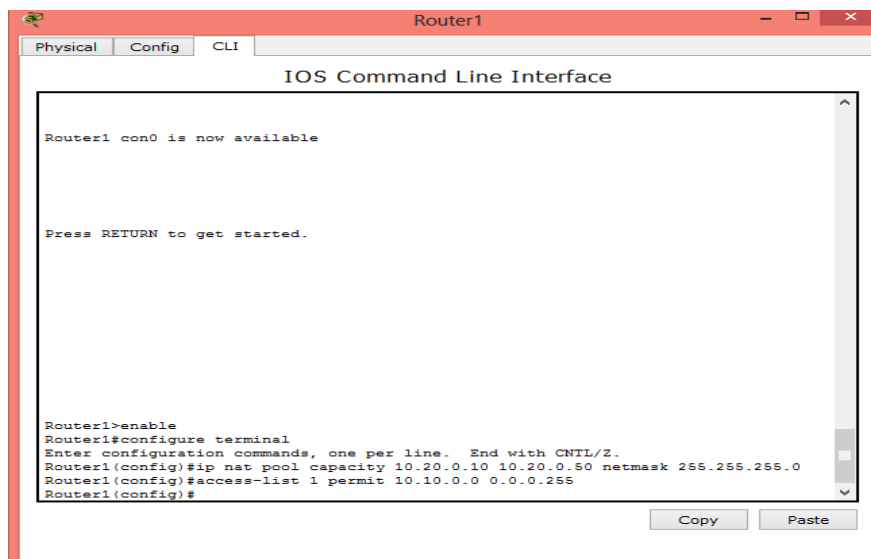
Paso 2.

Luego de eso realizaremos la configuración de NAT Dinamico en el Router1 con el, lo primero que debemos hacer es crear un pool de direcciones, un pool es una cantidad de dirección que el router sabe que tiene disponibles para intercambiarlas con la dirección de destino original, crearemos el pool con el comando Router1(config)#ip nat pool (el nombre de el pool) (la ip desde donde tenemos disponible el rango de direcciones) (la ip hasta donde tenemos disponible en el rango de direcciones) netmask (la máscara de red de el rango de direcciones).



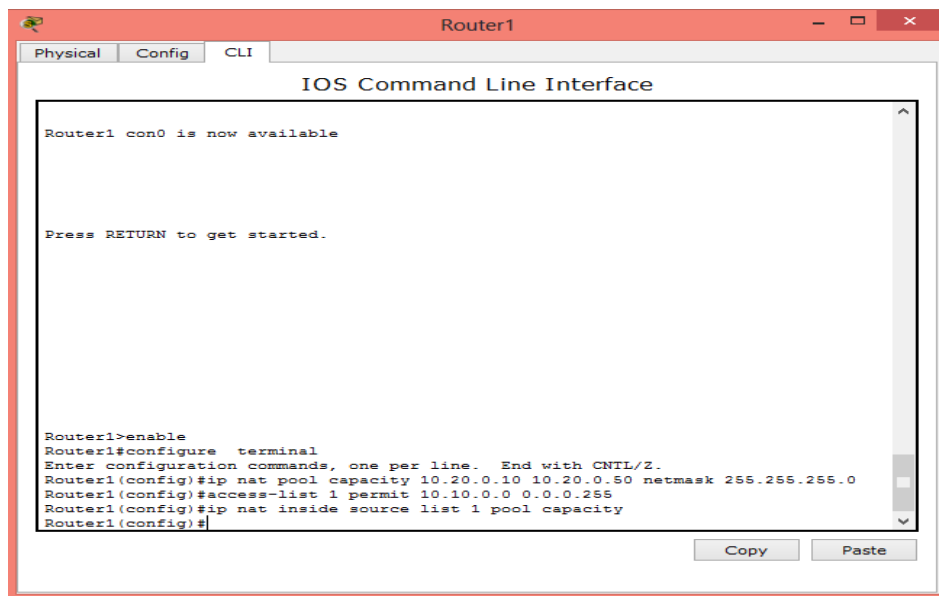
Paso 3.

Luego de haber creado el pool de direcciones y de haberle colocado un nombre con el rago de direcciones, crearemos una ACL que le permita el paso a la red a la que queremos realizar el cambio de direcciones, con la máscara reversible de la red a la que queremos realizarle el cambio.



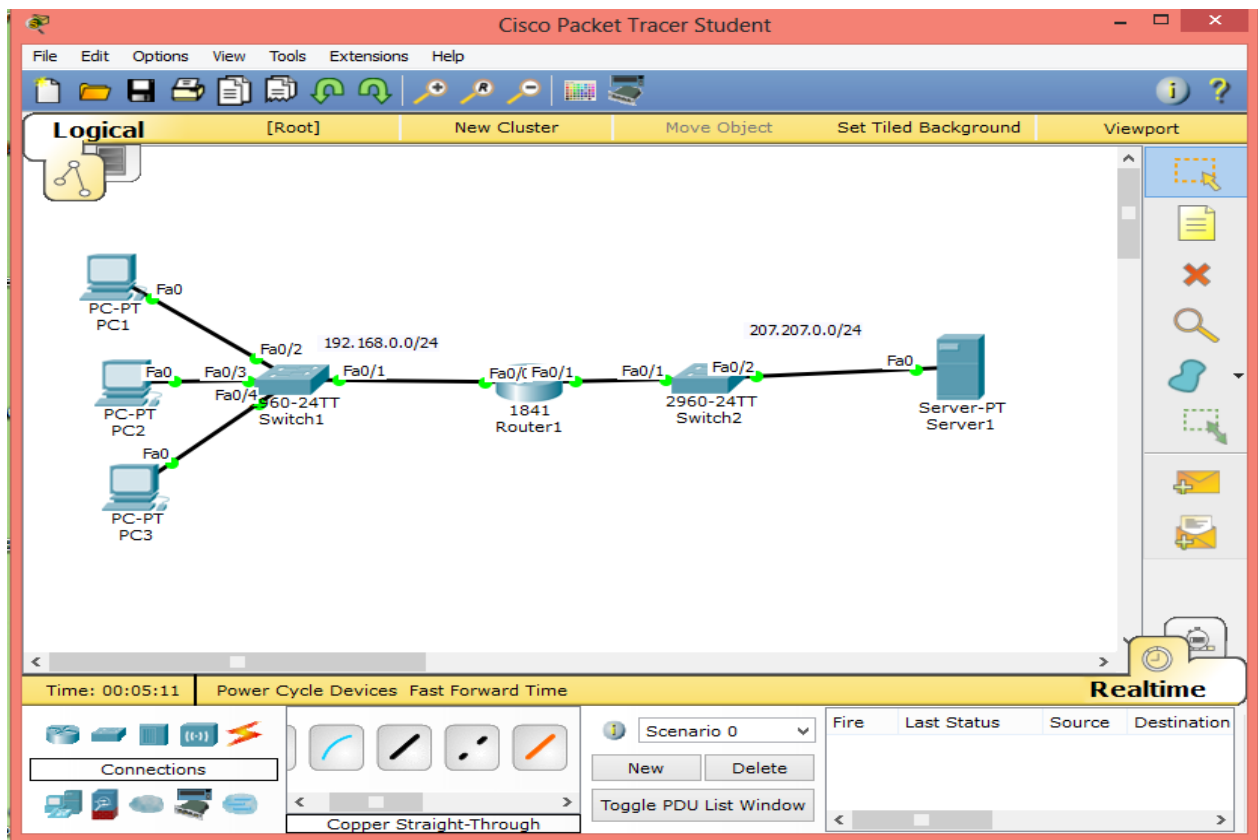
Paso 4.

Después de haber realizado los pasos anteriores debemos crear una regla en NAT que debe indicar cuál es la el ID de origen de la Red el auténtico y que pool es el que estaría utilizando para definir el rango con el siguiente comando, Router1(config)#ip nat inside source list (el numero de lista que es la ACL que se creo) pool (el nombre que le colocamos a el pool).



Paso 5.

Ahora finalizaremos la configuración de NAT Dinámico configurando las interface de manera que se haga saber cuál es la interface que utilizaría el router para salga la información y cual interface utilizaría para que entre la información.

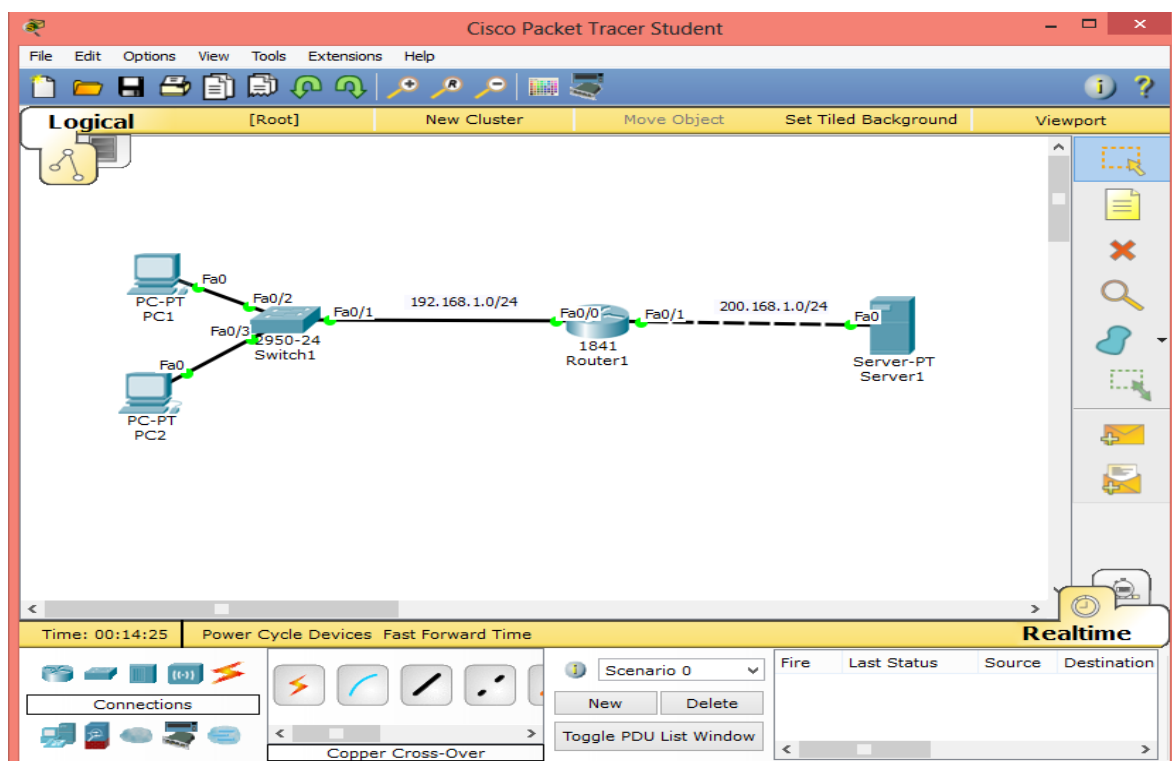


Ejercicio de Nat Dinámico

EJEMPLO DE NAT CON SOBRECARGA.

Paso 1.

Encender ambas Fastethernet en los Routers y colocarles el número de IP correspondiente.

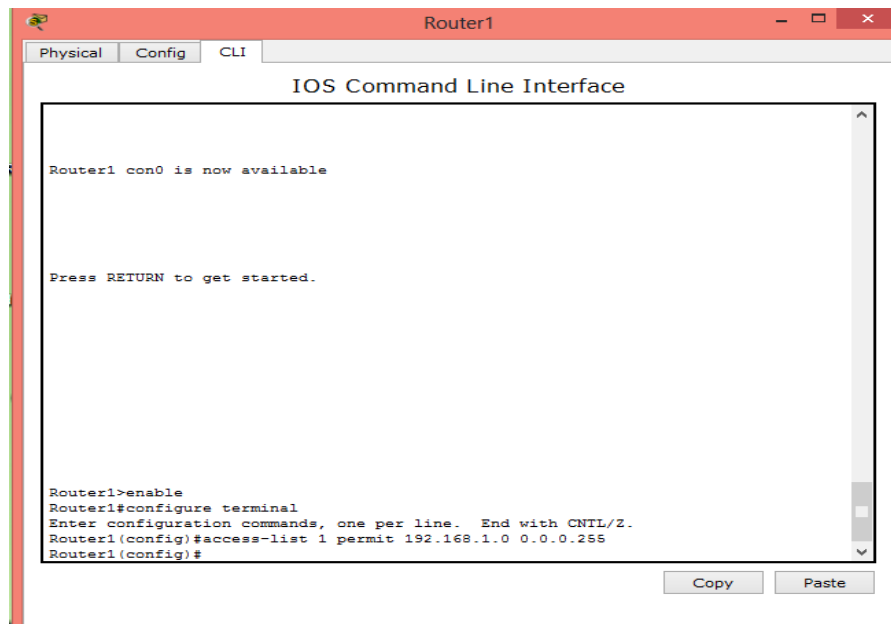


Paso 2.

Los comandos que se utilizan para realizar la configuración NAT con sobrecarga son muy similares a los que se utilizan para configurar NAT Dinámico, y se comienza creando una lista de acceso seguido del ID de la red de la que queremos cambiar la IP y la wildcard.

Paso 3.

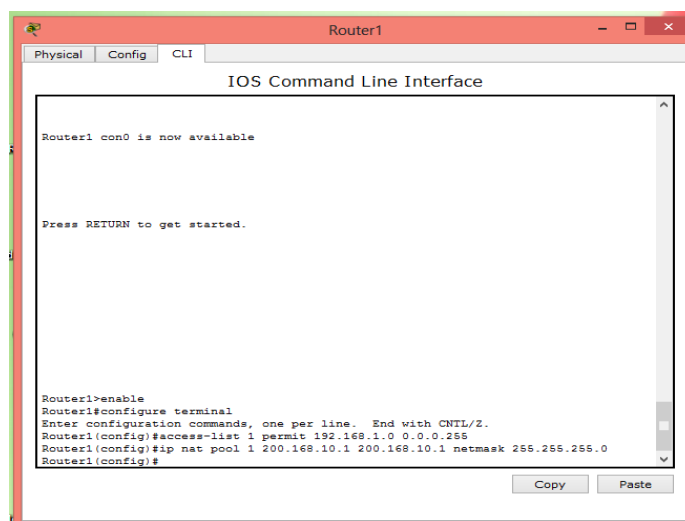
Luego de crearemos el pool de direcciones con el rango que se estaría utilizando para intercambiar las direcciones, que en este caso utilizaríamos solo una dirección pública para convertir todas las direcciones privadas, así que en el rango en donde colocamos la direcciones desde y hasta sería la misma, así se observa en la configuración.



```
Router1 con0 is now available

Press RETURN to get started.

Router1>enable
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router1(config)#
```



```
Router1 con0 is now available

Press RETURN to get started.

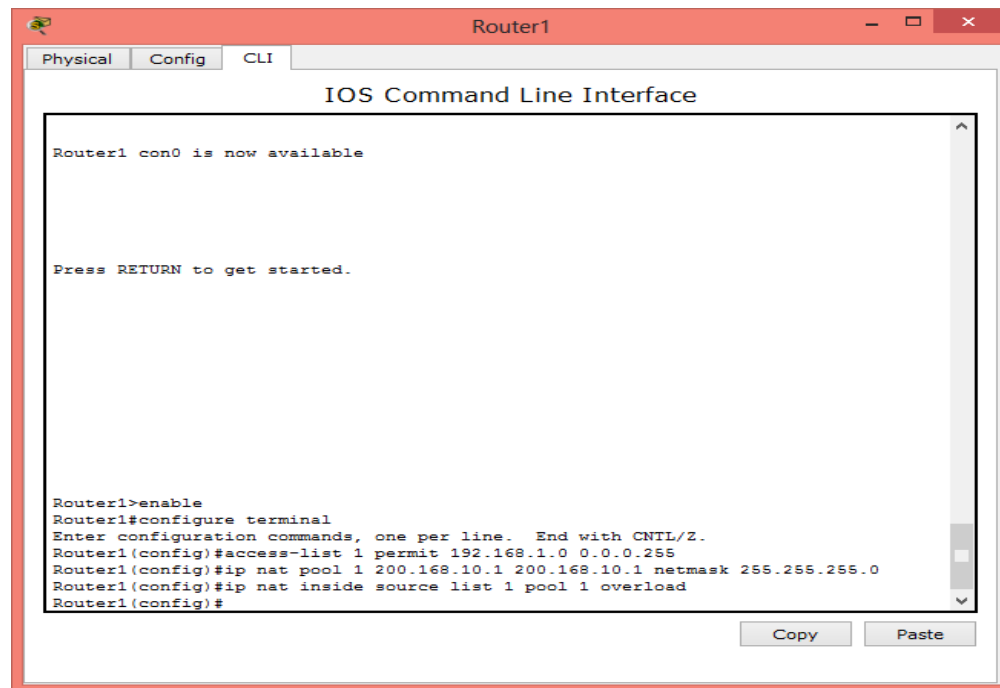
Router1>enable
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router1(config)#ip nat pool 1 200.168.10.1 200.168.10.1 netmask 255.255.255.0
Router1(config)#
```

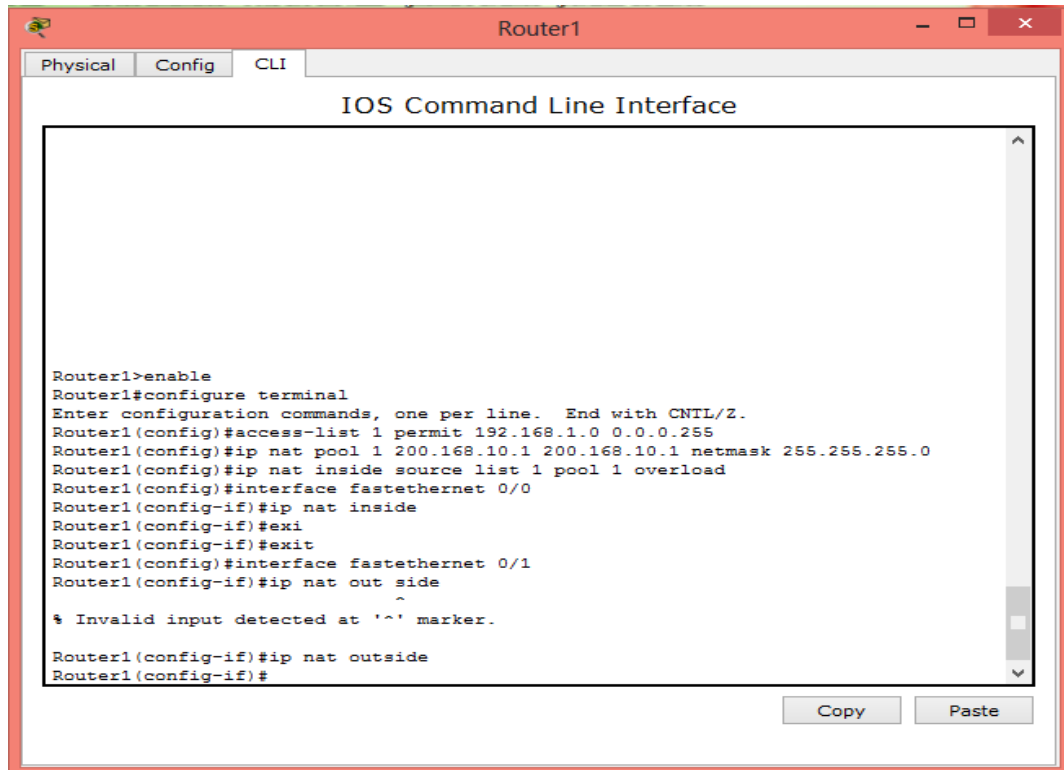
Paso 4.

Después de haber realizado los anteriores pasos, asignamos la lista de acceso a el pool de direcciones, con el mismo comando que se utilizó en la configuración de NAT Dinámico, pero le agregaremos la palabra "overload".

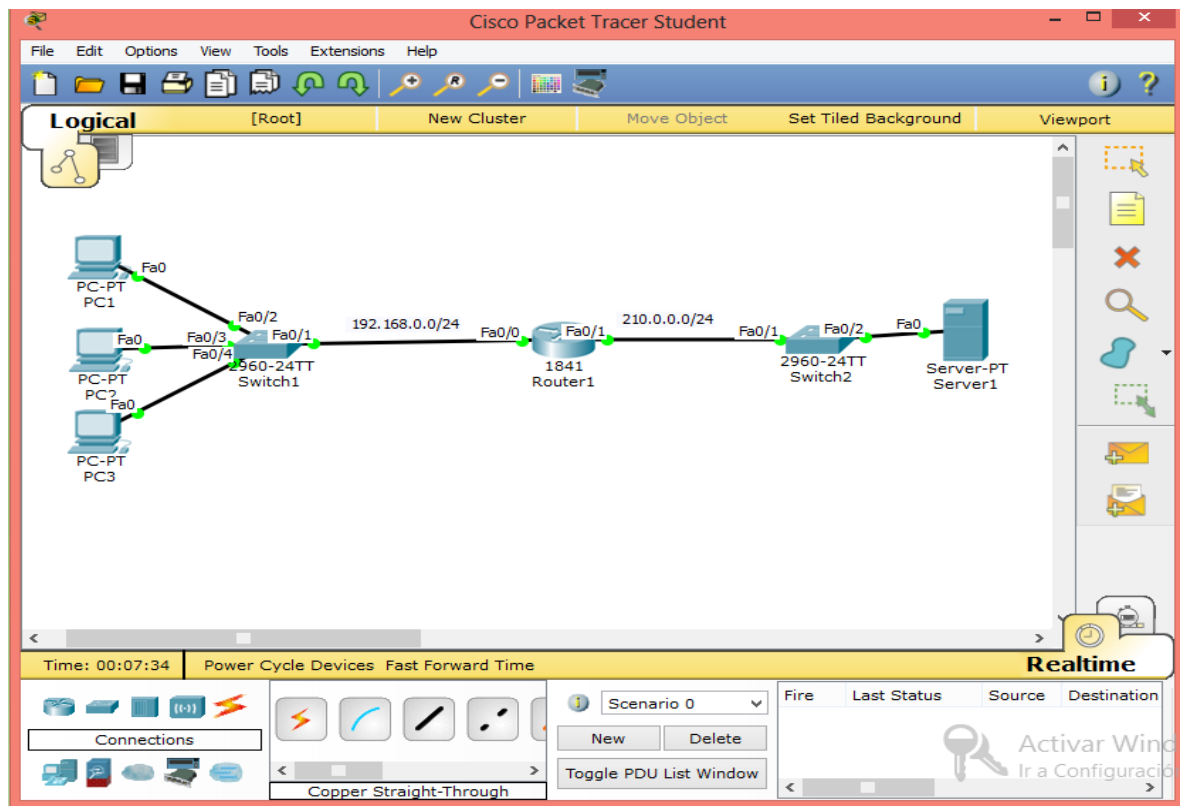
Paso 5.

Y como último paso realizaremos la configura de las interfaces que serán las internas de donde salen los paquetes y cuáles serán las externas.





Ejercicio de Nat de Sobrecarga

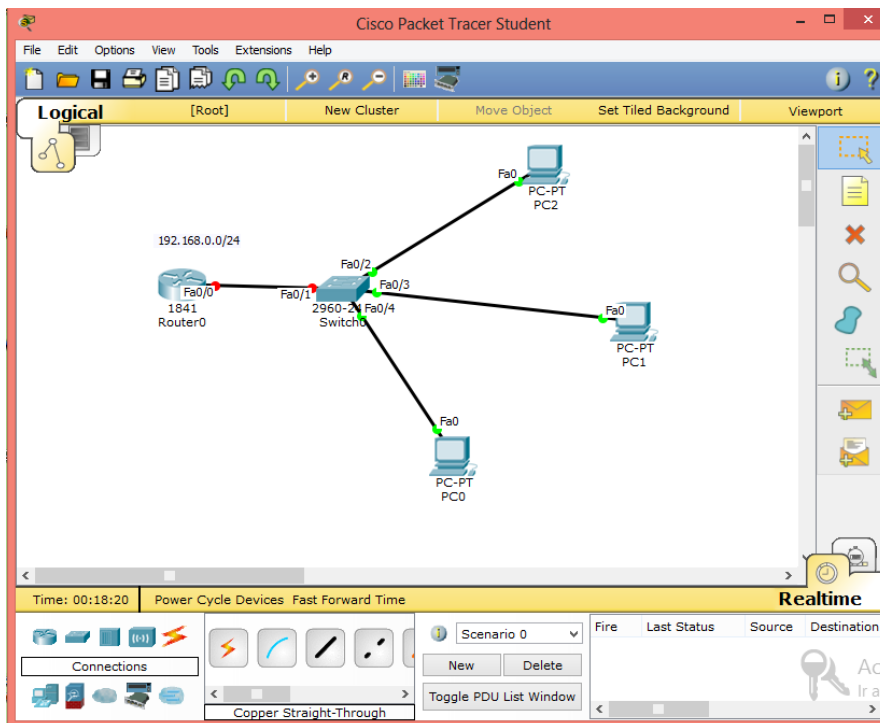


DHCP

El protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP) es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP. Este servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente.

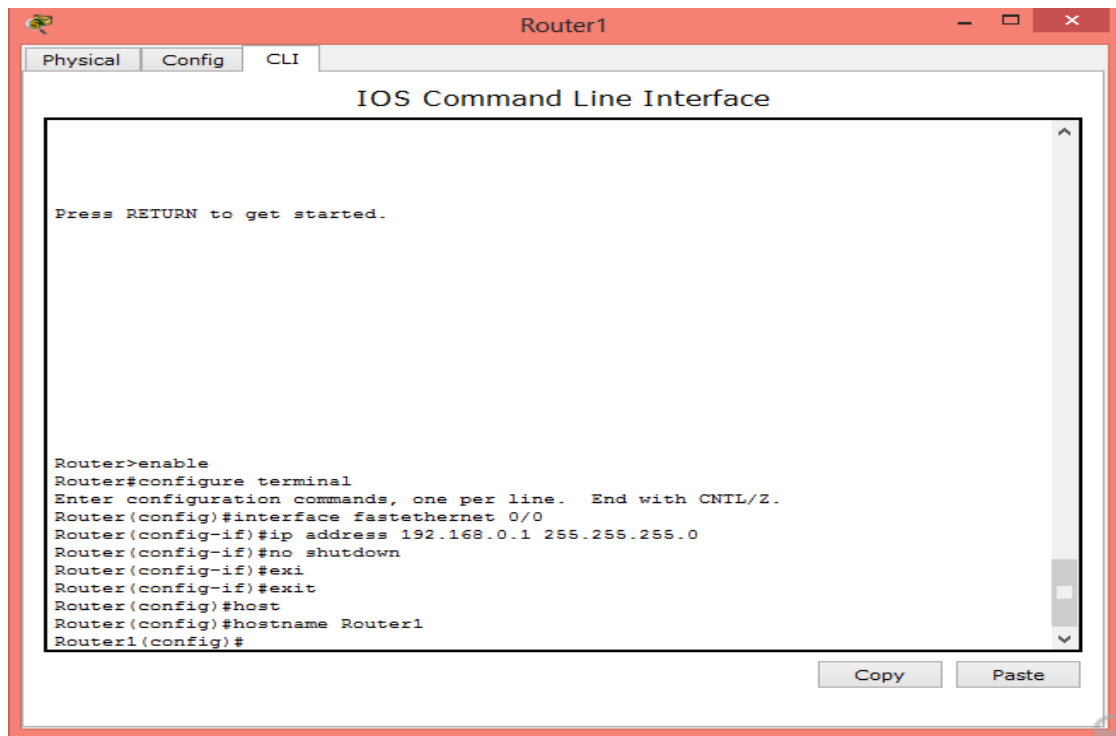
EJERCICIO.

Realizar la configuración de la siguiente topología con los comandos de DHCP.



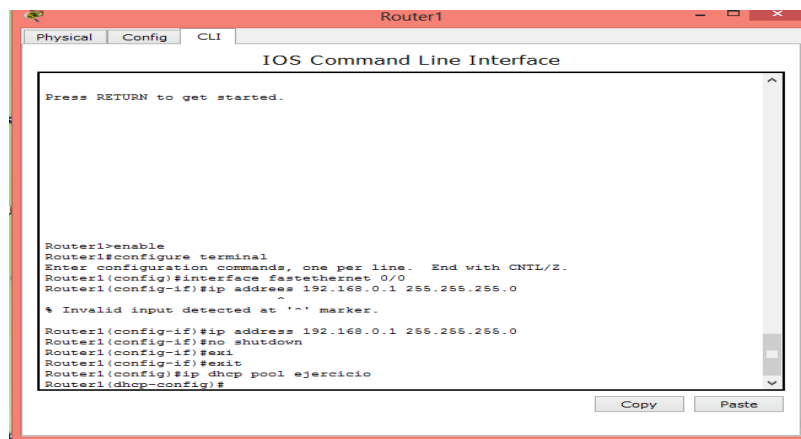
Paso 1.

Le colocamos una IP a la interface de el router y la encenderemos, luego de eso le cambiaremos el nombre a Router1.



Paso 2.

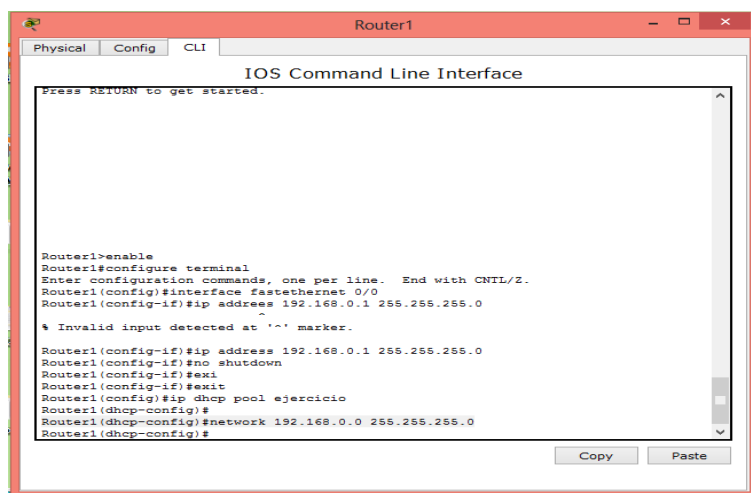
Crearemos un pool de direccion con el siguiente comando, Router1(config)#ip dhcp pool (el nombre que le colocaremos a el pool).



```
Router1>enable
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip address 192.168.0.1 255.255.255.0
~
% Invalid input detected at '^' marker.
Router1(config-if)#ip address 192.168.0.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#ip dhcp pool ejercicio
Router1(dhcp-config)#
```

Paso 3.

Luego de eso le configuraremos a el pool de direcciones de el DHCP el ID de red que se estaría utilizando con el siguiente comando, Router1(dhcp-config)#network 192.168.0.0 255.255.255.0

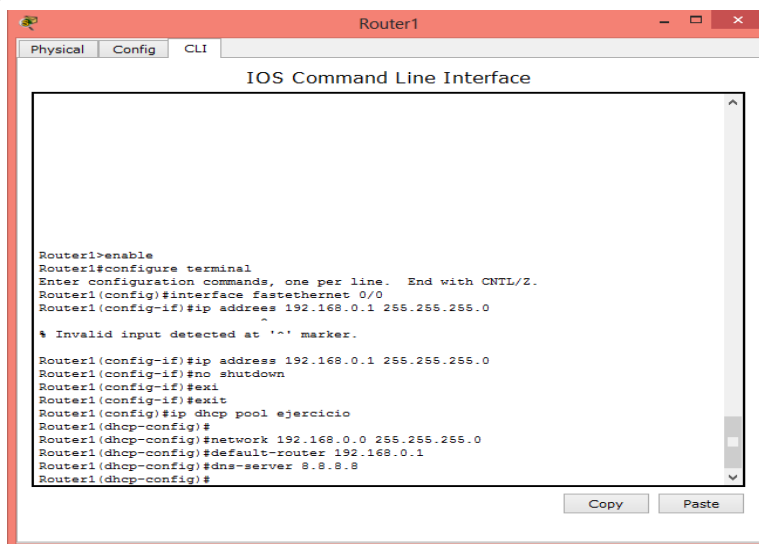


```
Router1>enable
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip address 192.168.0.1 255.255.255.0
~
% Invalid input detected at '^' marker.
Router1(config-if)#ip address 192.168.0.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#ip dhcp pool ejercicio
Router1(dhcp-config)#
Router1(dhcp-config)#network 192.168.0.0 255.255.255.0
Router1(dhcp-config)#
```

Paso 4.

Le coloramos a el pool, cuál será el enlace predeterminaron que utilizara, en este caso será el mismo router que estariamos utilizando por lo tanto le colocaremos la IP de la interface 0/0 del router, pero en otra clase de red, que se desee configurar y desee ocupar otra clase de equipo,

como un servidor o un firewall, se deberá colocar la IP del equipo que vamos a utilizar como DHCP con el siguiente comando Router1(dhcp-config)#default-router (la ip de el quipo que se estar ía utilizando como DHCP).



```
Router1>enable
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip address 192.168.0.1 255.255.255.0

% Invalid input detected at '^' marker.

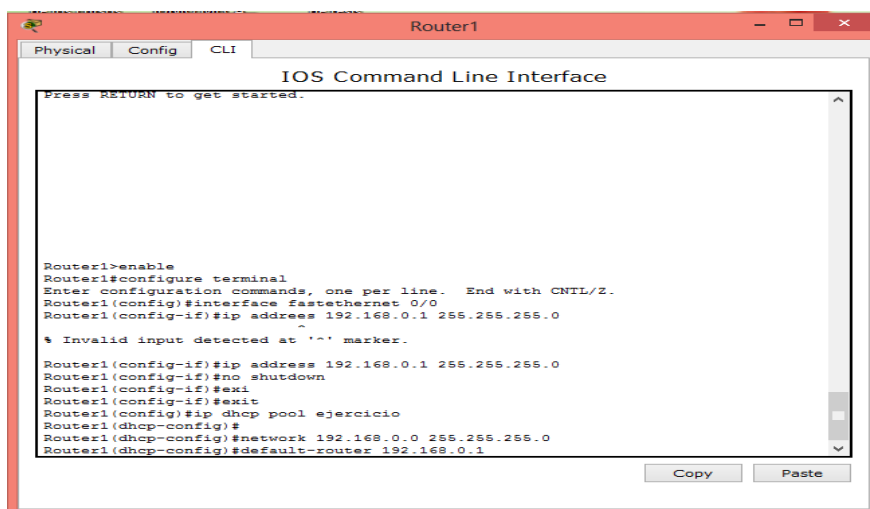
Router1(config-if)#ip address 192.168.0.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#ip dhcp pool ejercicio
Router1(dhcp-config)#
Router1(dhcp-config)#network 192.168.0.0 255.255.255.0
Router1(dhcp-config)#default-router 192.168.0.1
Router1(dhcp-config)#dns-server 8.8.8.8
Router1(dhcp-config)#
```

Paso 5

Colocaremos una dirección de un servidor DNS.

Paso 6.

El paso 6 es opcional, este se configura si en algún momento queremos que



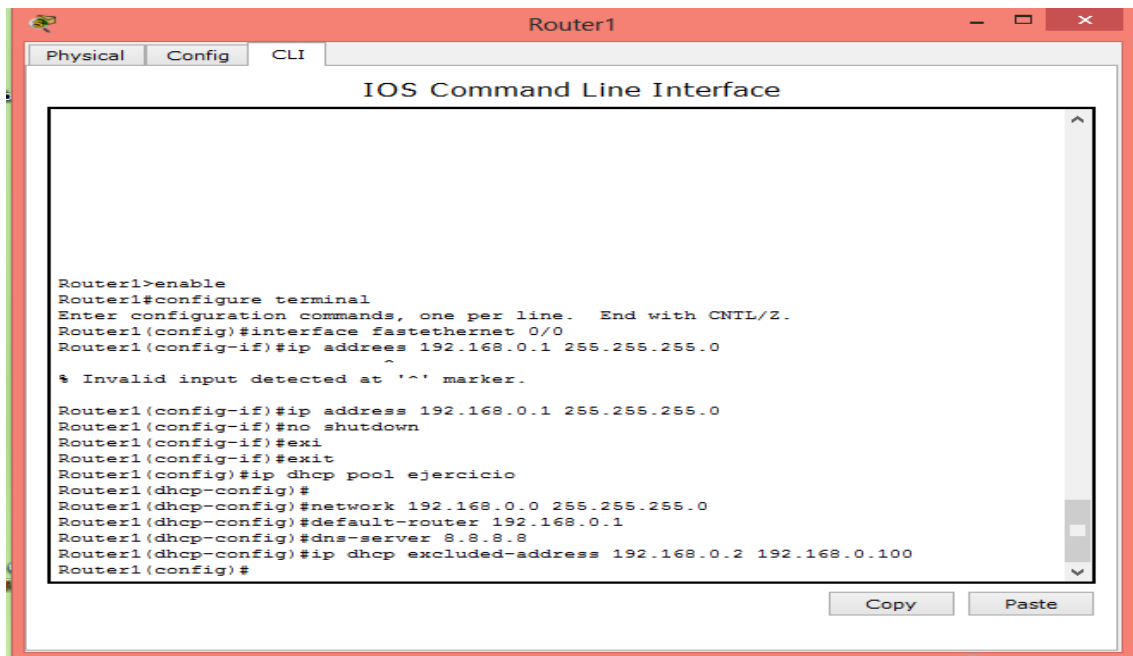
```
Press RETURN to get started.

Router1>enable
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip address 192.168.0.1 255.255.255.0

% Invalid input detected at '^' marker.

Router1(config-if)#ip address 192.168.0.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#ip dhcp pool ejercicio
Router1(dhcp-config)#
Router1(dhcp-config)#network 192.168.0.0 255.255.255.0
Router1(dhcp-config)#default-router 192.168.0.1
```

el DHCP no le asigne IP a los host con un rango predeterminado de direcciones con el siguiente comando Router1(dhcp-config)#ip dhcp excluded-address (ip desde donde no quieres que asigne el DHCP) (IP hasta donde quieres que DHCP puede asignar direcciones).



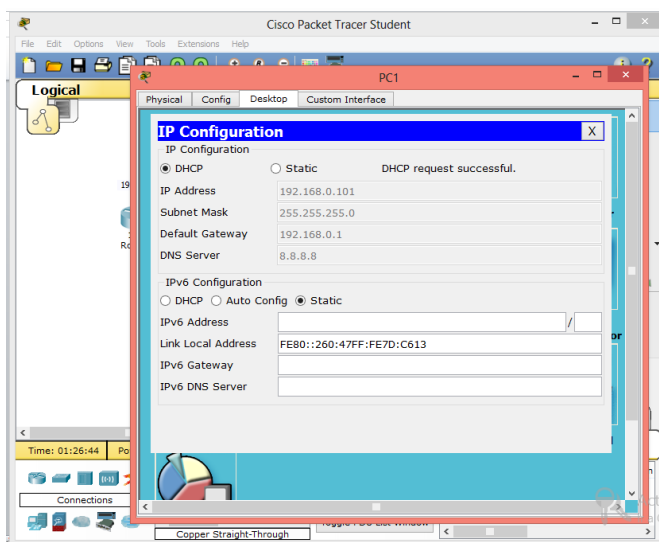
```
Router1>enable
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip address 192.168.0.1 255.255.255.0

% Invalid input detected at '^' marker.

Router1(config-if)#ip address 192.168.0.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#ip dhcp pool ejercicio
Router1(dhcp-config)#
Router1(dhcp-config)#network 192.168.0.0 255.255.255.0
Router1(dhcp-config)#default-router 192.168.0.1
Router1(dhcp-config)#dns-server 8.8.8.8
Router1(dhcp-config)#ip dhcp excluded-address 192.168.0.2 192.168.0.100
Router1(config)#
```

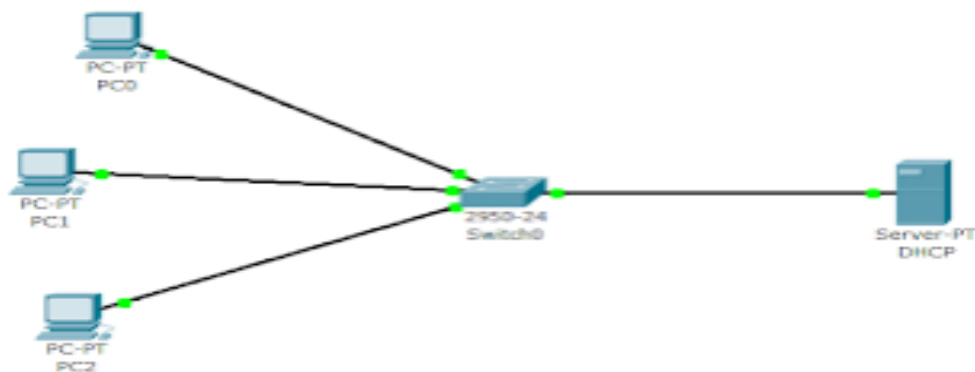
Paso 7.

Ahora configuraremos las maquinas para que acepten DHCP cambiando la manera en la toman las IP de forma statica a DHCP.



Como vemos el DHCP le ha asignado un IP fuera de el rango que le hemos solicitado no asignar.

Ejercicio a realizar



Los pasos son los siguientes:

1. Se construye la topología indicada.
2. Se configura manualmente el servidor DHCP con la dirección 172.16.1.254
3. Se asume que el gateway o la puerta de enlace para la red es 172.16.1.1 y que el servidor DNS es 172.16.1.100.
4. Se configura el rango y el número máximo de conexiones.

ACL

Una Lista de Control de Acceso o ACL (de la inglé, Access Control List) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACLs permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en IDS.

Ejemplo de Acl

PC3

Physical Config Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.2.3

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::20C:85FF:FE07:8238

IPv6 Gateway

IPv6 DNS Server

☐ Top

PC1

Physical Config Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.1.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

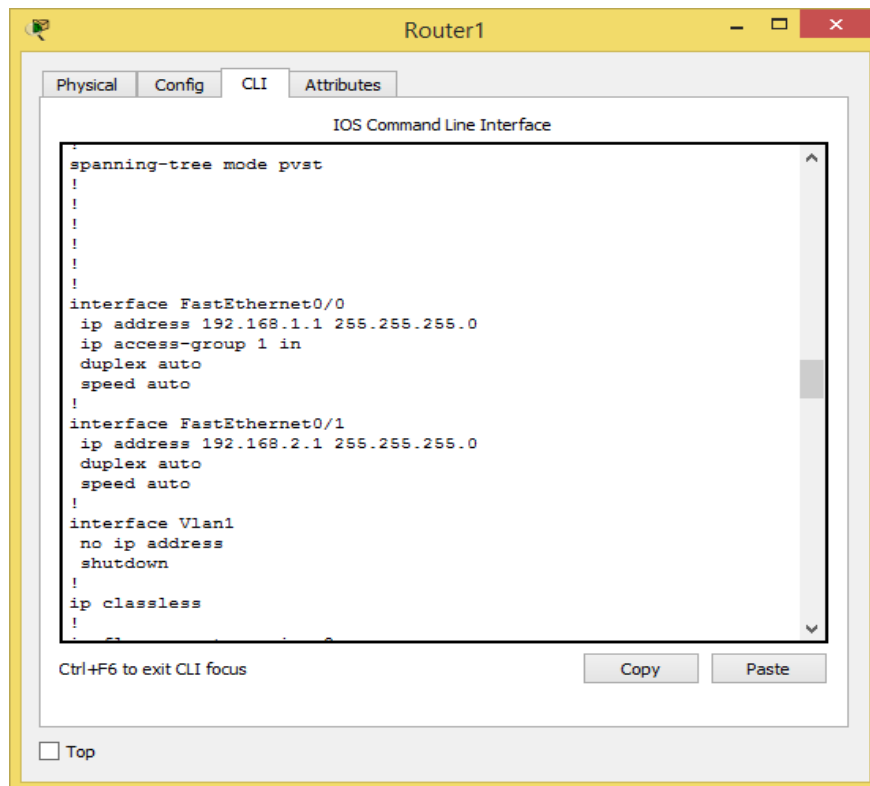
Link Local Address FE80::260:2FFF:FE65:B90B

IPv6 Gateway

IPv6 DNS Server

☐ Top

Paso 1 Configura las ips en las Pcs



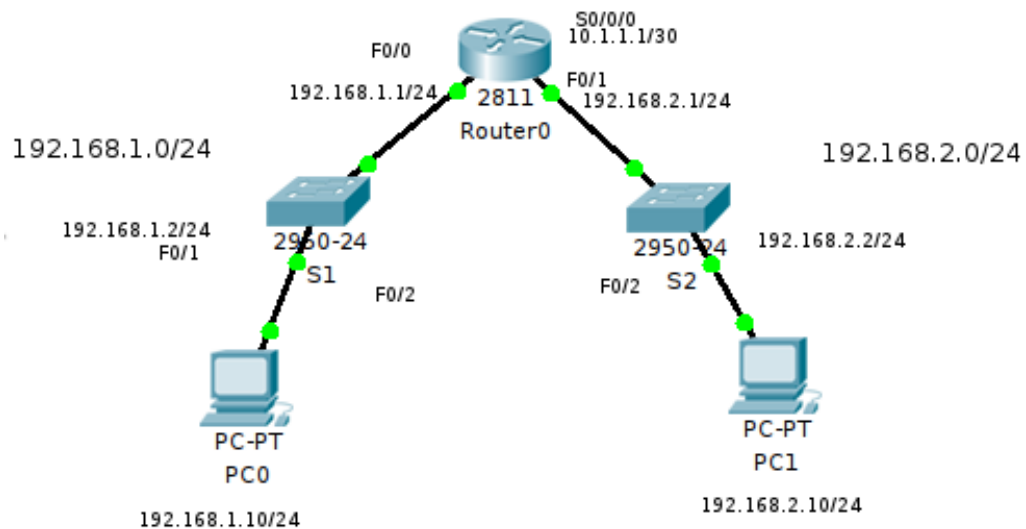
Paso 3

Configuración de router para colocar las ips y verificar cual será denegada y permitida

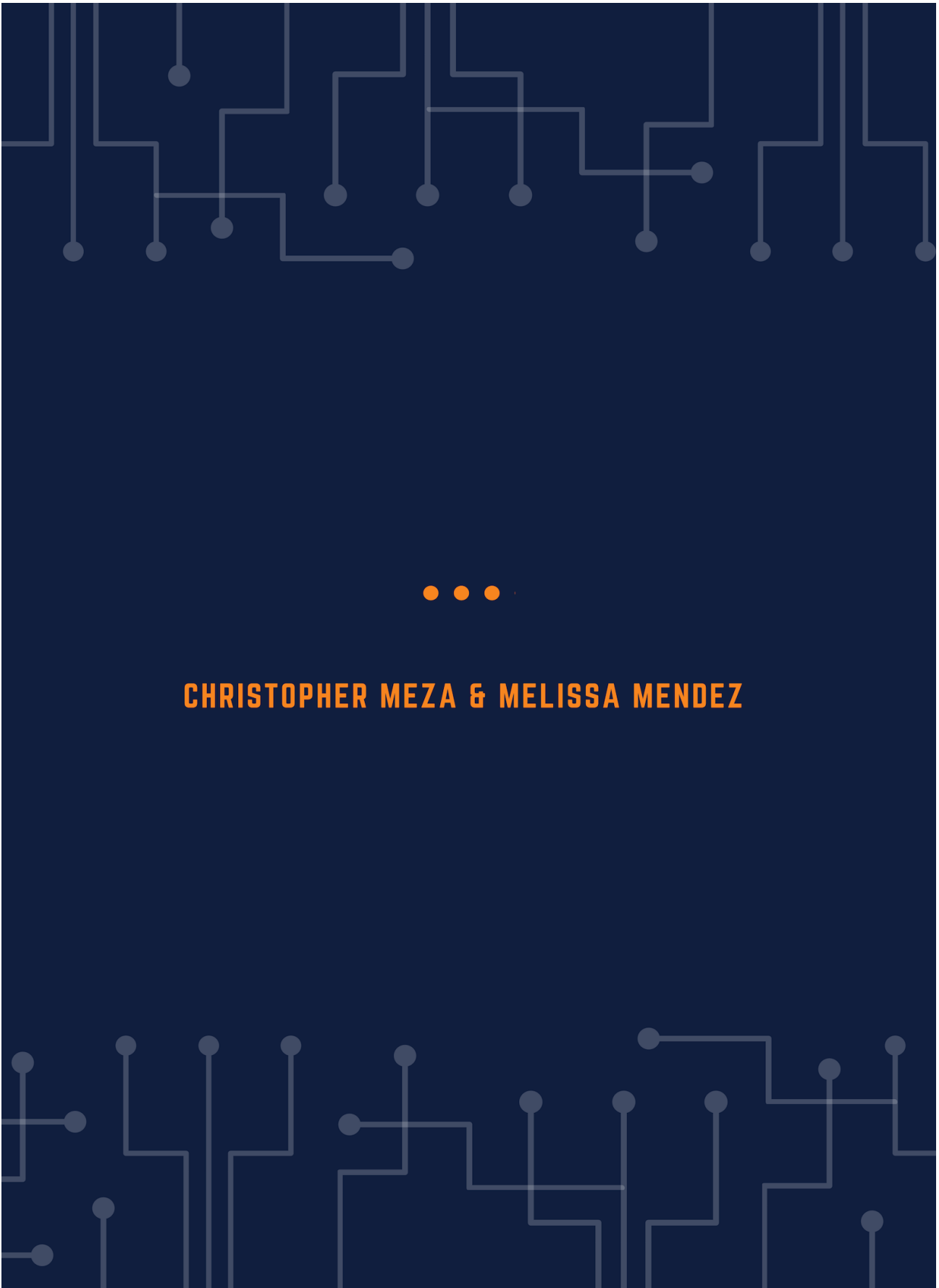
Paso 4

Entramos a una de las Pcs para realizar un Ping y veremos si hay o no respuesta

Ejercicio de Acl



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Request timed out.
Ping statistics for 192.168.2.2:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
~C
C:\>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=2ms TTL=255
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
[ ] Top
```



CHRISTOPHER MEZA & MELISSA MENDEZ