Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

MANUAL DE CONFIGURACIÓN DE ENRUTAMIENTO ESTÁTICO Y DINÁMICO PARA DISPOSITIVOS CISCO, BASADO EN CCNA VERSIÓN 7

Héctor Abraham Chen Ramos

Asesorado por la Inga. Ana María Navarro Orozco

Guatemala, abril 2023

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

MANUAL DE CONFIGURACIÓN DE ENRUTAMIENTO ESTÁTICO Y DINÁMICO PARA DISPOSITIVOS CISCO, BASADO EN CCNA VERSIÓN 7

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA
DE LA FACULTAD DE INGENIERÍA
POR:

HÉCTOR ABRAHAM CHEN RAMOS
ASESORADO POR LA INGA. ANA MARÍA NAVARRO OROZCO

AL CONFERIRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, ABRIL 2023

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Vladimir Armando Cruz Lorente
VOCAL V	Br. Fernando José Paz Gonzáles
SECRETARIA	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICO EL EXAMEN PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADOR	Ing. Brian Enrique Chicol Morales
EXAMINADOR	Ing. Hugo Leonel Tiul Valenzuela
EXAMINADOR	Ing. José Aníbal Silva de los Ángeles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En el cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

MANUAL DE CONFIGURACIÓN DE ENRUTAMIENTO ESTÁTICO Y DINÁMICO PARA DISPOSITIVOS CISCO, BASADO EN CCNA VERSIÓN 7

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería de Mecánica Eléctrica, el 26 de julio de 2022

Héctor Abraham Chen Ramos

Guatemala, 09 de febrero de 2023

Ingeniero
Julio César Solares Pañete
Coordinador de área, Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería
Universidad de San Carlos de Guatemala.

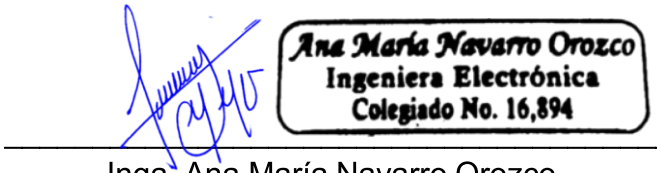
Estimado Ingeniero Solares:

Hago de su conocimiento por este medio que he concluido la revisión del trabajo de graduación del estudiante Héctor Abraham Chen Ramos, titulado:

MANUAL DE CONFIGURACIÓN DE ENRUTAMIENTO ESTÁTICO Y DINÁMICO PARA DISPOSITIVOS CISCO, BASADO EN CCNA VERSIÓN 7

El cual cumple plenamente el propósito para el que fue concebido. Por lo que, en mi calidad de ASESORA nombrada por la escuela de Ingeniería Mecánica Eléctrica, doy mi aprobación al mismo. Indicando que tanto la suscrita como el estudiante Chen Ramos somos responsables por el contenido del trabajo referido.

Reciba un cordial saludo,



Inga. Ana María Navarro Orozco
Colegiado No. 16,894
ASESORA.

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 13 de febrero de 2023

Señor director
Armando Alonso Rivera Carrillo
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC

Estimado Señor director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **MANUAL DE CONFIGURACIÓN DE ENRUTAMIENTO ESTÁTICO Y DINÁMICO PARA DISPOSITIVOS CISCO, BASADO EN CCNA VERSIÓN 7,** desarrollado por el estudiante **Héctor Abraham Chen Ramos**, ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio César Solares Peñate
Coordinador de Electrónica

ESCUELA DE INGENIERÍA MECÁNICA ELÉCTRICA
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

REF. EIME 18.2023.

1. El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante Héctor Abraham Chen Ramos: **MANUAL DE CONFIGURACIÓN DE ENRUTAMIENTO ESTÁTICO Y DINÁMICO PARA DISPOSITIVOS CISCO, BASADO EN CCNA VERSIÓN 7**, procede a la autorización del mismo.

Ing. Armando Alonso Rivera Carrillo

Guatemala, 9 de marzo de 2023.

Decanato
Facultad de Ingeniería
24189101- 24189102
secretariadecanato@ingenieria.usac.edu.gt

LNG.DECANATO.OI.413.2023

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **MANUAL DE CONFIGURACIÓN DE ENRUTAMIENTO ESTÁTICO Y DINÁMICO PARA DISPOSITIVOS CISCO, BASADO EN CCNA VERSIÓN 7**, presentado por: **Héctor Abraham Cifuentes Ramos**, después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, abril de 2023

AACE/gaoc

ACTO QUE DEDICO A:

Mis padres

Lesley Ramos y Jorge Chen, quienes con su esfuerzo me apoyaron y guiaron para seguir adelante, soportando el ruido en las madrugadas y acompañándome en cada proyecto, por lo cual son lo mejor que tengo en esta vida.

Mis hermanos

Josué, Félix Chen, quienes son personas fundamentales en mi vida de los cuales estoy muy agradecido ya que gracias a su ayuda los proyectos, fueron más fáciles de realizar.

Mis abuelos

Rodrigo Chen (q.e.p.d.), Luisa Cortez (q.e.p.d.), Héctor Ramos (q.e.p.d.) y Ninnette Juárez**,** quienes me brindaron a tan grandes padres, también gracias a las enseñanzas trasmitidas a mis padres logran formarme para ser mejor cada día.

Mi 2do Abuelo

Reginaldo Mancilla, quien me ha apoyado en el trascurso de mi vida, brindándome su sabiduría y su cariño, con quien siempre que lo necesito puedo contar con él y al cual le tengo mucho cariño y respeto.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por darme el privilegio de ser parte de tan admirable institución, en la cual me permite formarme como profesional.
Facultad de Ingeniería	Por exigirme la superación personal en cada labor que deba realizar.
Mis catedráticos	A cada uno de los docentes que tuve en el trascurso de mi vida académica, pues gracias a ellos y al conocimiento que me otorgaron, es posible este logro.
Mis compañeros de catedra	Por los consejos, apoyo y ayuda mutua en cada elaboración de proyectos, ya que entre risas y desvelos la carga de los trabajos fue más fácil de lleva.
Mis compañeros de Facultad	Por estar siempre allí en los momentos más difíciles, con quienes, a pesar de estar en escuelas distintas, siempre nos apoyábamos.

INDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

ADSL	Línea de abonado digital asimétrica.
Atenuación	Perdida de potencia ocasionada al transitar por cualquier medio de transmisión.
CLI	*Command Line Interface* o interfaz de comandos en línea.
Comunicación	Se le conoce a la transferencia de información desde un remitente hacia un receptor.
Diafona	Interacción o acoplamiento entre señales cercanas.
GUI	*Graphical User Interface* o interfaz gráfica de usuario.
IP	Protocolo de Internet.
NIC	Tarjeta de Interfaz de Red.
Nodo	Puntos en los cuales se entrelazan 2 o más conexiones de red.
NOS	Sistema Operativo de Red**.**

Nvram	Memoria no volátil de acceso aleatorio, esta nos indica que no pierde la información, al interrumpirse la alimentación eléctrica.
Omnidireccional	Orienta la señal en todas direcciones con un haz pleno de corto alcance, envían la información en un radio de 360 grados.
Rack	Se le conoce a la estructura en la cual está diseñada para albergar dispositivos de redes informáticas como por ejemplo routers, servidores, entre otros.
RAM	Memoria de acceso aleatorio, al apagase el equipo o perder alimentación eléctrica, se pierde la información.
Redundante	Consiste en asegurar la supervivencia de la red ante un fallo, proporcionándole rutas de datos alternativas cuando se produce un fallo de enlace.
Refracción	Cambio de dirección y lentitud que experimenta una onda al pasar de un medio a otro.
Servidor	Dispositivo conectado a internet que su función es la de almacenar información, administrar bases de datos y responder a las solicitudes de los navegadores de los internautas.
Splitter	Dispositivo encargado de recibir una señal para luego distribuirla en varios canales.

TCP	Protocolo para el Control de Transmisión.

RESUMEN

En este punto en el que nos encontramos actualmente el uso de redes es indispensable para la población, ya que se puede utilizar para realizar redes para hogares, redes de oficinas (LAN) e igualmente redes empresariales entre otras.

El seguimiento de redes se puede afirmar que es la manera más eficiente para el envío y recepción de datos de manera confiable y esto se logra a través de la configuración que se le otorgué a los equipos en cuestión.

Las redes son la forma de comunicación para el envío de datos de un hogar, realizar una búsqueda en algún servidor o estar en contacto con algún pariente lejano, si esto se lleva a cabo en una empresa puede servir para tener comunicados a los empleados entre sí, contar con distintas subdivisiones para mantener un control de la información con la que cuenta cada departamento, entre otros beneficios, aunque en este documento se especializara en los enrutamientos para contar con interconexión en la red otorgada por el proveedor, se sabe que se pueden implementar métodos de seguridad en nuestra red esto con el fin de hacerla más confiable así como segura para nosotros mismos pero este tema de ciber seguridad no se llevara a cabo de forma detallada en este escrito.

Gracias a los avances en la información otorgada por CCNA se cuenta con la última versión para la enseñanza de este tipo de configuraciones de la cual se tomará la base de este trabajo.

Por lo cual el presente documento brindara de forma ilustrativa ejemplos de configuraciones para poder realizar la comunicación entre los dispositivos siendo esta la configuración estática y dinámica de los equipos, lo que podemos utilizar para las clases laboratorio de redes en la escuela de mecánica eléctricas, o bien para trabajo de técnico en redes.

OBJETIVOS

General

Que el practicante cuente con las herramientas y el conocimiento necesario para la elaboración de un enrutamiento ya sea para una red local o empresarial.

Específicos

1. Brindar apoyo para el proceso de instalación de las herramientas virtuales para la realización de las practicas.

2. Detallar los conceptos necesarios para otorgar de manera factible el conocimiento para la elaboración de redes de forma práctica.

3. Indicar con ejemplos los procesos necesarios para cada uno de los temas abarcados en la teoría.

4. Crear un sistema grafico donde el practicante se sienta a gusto con lo aprendido.

INTRODUCCIÓN

El presente trabajo se realiza con el fin de poder brindar un apoyo para las configuraciones en los dispositivos cisco, se toma como base la información otorgada por CCNA, el tema principal es el enrutamiento estático y dinámico adaptado y enfocado en la práctica de cada tema, detallado en este escrito.

Se abordarán temas de suma importancia antes de realizar ejercicios prácticos ya que contar con información puntual de ciertos temas como son topologías básicas, conceptos básicos, entre otros temas fundamentales otorgaran el soporte para facilitar el aprendizaje y dar un cimiento balanceado entre la práctica y la teoría.

Se utilizará la herramienta *Cisco Packet Tracert*, para la realización de los ejemplos prácticos dando un aporte grafico de cómo se deben configurar los equipos, ya que esta herramienta está dotada con una interfaz amigable, así también se adapta a la configuración de un equipo real, además se explicará la forma de realizar dicha programación al contar con equipo de manera física.

El método empleado para la preparación de este trabajo de graduación contará con pequeñas prácticas para que el estudiante pueda tener la confianza y poder llevar a cabo las configuraciones necesarias en los equipos de trabajo de manera fluida.

1. CONCEPTOS BÁSICOS DE REDES

1.1. ¿Qué son las redes?

Para el ámbito de la informática, se les conoce a las redes como enlace de datos.

En la forma más básica de su definición se puede encontrar que las redes tienen el propósito fundamental de comunicar dos o más dispositivos, uniendo la infraestructura de software y hardware, para realizar enlaces de datos se necesita en este sistema el apoyo de una NIC (*Network Interface Target*).

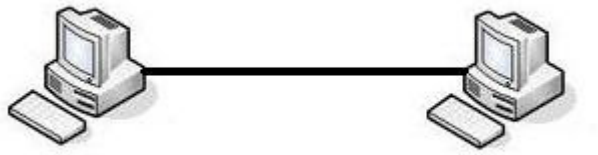
Para la conexión de una red se requiere de la instalación de NOS (*Network Operating System*), el cual es diseñado para soportar el flujo de operación en una red de trabajo.

- Existen 2 tipos de NOS los cuales son:

    - Punto a punto: Estos permiten al usuario compartir y acceder a la información desde cualquier dispositivo que se encuentre conectado en él, ya que esta arquitectura permite que los dispositivos se visualicen de la misma manera en términos de funcionalidad.

      En este tipo de arquitectura es más eficiente para redes pequeñas o medianas y su costo en más económico

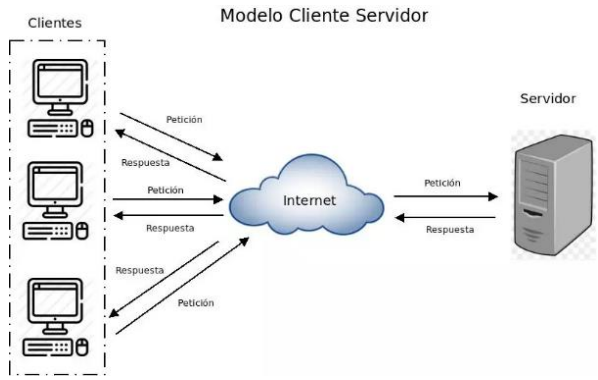
Figura 1. **Red punto a punto**



Fuente: Casillas Sergio y Rodríguez Felipe (2014). *Topología y arquitectura de red.* Consultado el 26 de abril de 2022. Recuperado de https://sites.google.com/site/605bredesdecomputadoras/home/*6.*

- Cliente / Servidor: Esta configuración brinda al usuario acceso a todos los recursos a través de un servidor, este tipo de arquitectura su costo es más elevado puesto que se pueden ejecutar acciones no importando la ubicación física del operador, por otra parte, este también requiere mantenimiento técnico de mayor grado, así también una de sus ventajas es que facilita la incorporación de cambios en el sistema.

Figura 2. **Red cliente / servidor**



Fuente: Schiaffarino Andres (2019). Modelo cliente servidor. Consultado el 26 de abreil de 2022. Recuperado de https://blog.infranetworking.com/modelo-cliente-servidor/.

1.1.1. Las redes nos conectan

Las redes nos mantienen conectados, nos brindan una comunicación de manera instantánea, conocer las noticias, descubrimientos e incluso emprender en algún negocio de manera virtual.

Internet realiza un cambio significativo en la forma de las interacciones comerciales, sociales políticas entre otros.

El hablar de redes nos lleva también a conocer que son las telecomunicaciones y la diferencia que se cuenta con el significado de comunicación; La comunicación es la transferencia de información ya que es la transmisión de un mensaje, pero al momento de establecer una comunicación entre sistemas o personas que se encuentran distantes es lo que conocemos como telecomunicaciones.

1.1.2. Redes en la actualidad

Los avances que se han realizado con esta tecnología son los más significativos, pues con el conocimiento en redes se puede hacer que las fronteras, las distancias geográficas además de las limitaciones físicas no tengan mucha importancia ya que no se convierten en obstáculos para la comunicación.

Gracias a la información que se ha logrado conocer y actualizar en los procesos de redes, se crean comunidades en línea para llevar a cabo intercambio de información e ideas para otorgar un aumento de oportunidades y de productividad en las diferentes ramas de empleos a nivel mundial.

Un ejemplo de dichos avances se puede conocer mediante el servidor conocido como la nube, la cual es una herramienta de almacenamiento (documentos, imágenes, videos, entre otros.), esto con el fin de poder tener acceso en cualquier parte del mundo y en cualquier horario, con cualquier dispositivo en el cual tengamos acceso a la red ya sea con nuestros datos o bien con alguna aplicación.

Figura 3. **Interconexión de redes**

Fuente: Matago Franklin (2016). *Que es VoIP en red de interconexión.* Consultado el 27 de abril de 2022. Recuperado de http://www.servervoip.com/blog/que-es-voip-en-red-de-interconexion/.

1.2. Componentes de la red

Las redes se componen por tres tipos de componentes los cuales son dispositivos, medios y servicios, los cuales al operar en conjunto crean la infraestructura de red en la cual la información puede transportarse de un sitio a otro.

En la red de datos la parte de los dispositivos y medios son los elementos físicos (*Hardware*), este como bien es conocido es lo que se encuentra de manera visible de la infraestructura de una red.

1.2.1. Dispositivos finales

Los componentes con los que las personas interactuamos constantemente son conocidos como dispositivos finales o *Host*, a estos al estar conectados en la red reciben un número o bien una dirección conocida como IP con el fin de distinguir un dispositivo final de otro y la red en la cual se encuentra. Estos dispositivos pueden ser computadoras, teléfonos, TV, impresoras, entre otros.

Al momento de iniciar un intercambio de paquetes el dispositivo final emisor utiliza la dirección de destino del dispositivo al cual se necesita enviar el paquete para especificar la entrega del paquete.

Figura 4. **Dispositivos finales**

Fuente: Competencia digital. *Como funciona el internet.* Consultado el 27 de mayo de 2022. Recuperado de https://competenciadigital542370443.wordpress.com/2017/12/15/como-funciona-el-internet/.

1.2.2. Dispositivos intermediarios

Son los dispositivos cuya funcionalidad se basa en la conexión de los dispositivos finales dentro de la red, de igual forma pueden realizar la conexión entre múltiples redes para formar una red interna. Los dispositivos que se conocen bajo este nombramiento proporcionan conectividad y garantizan el flujo correcto de los datos que viajan a través de la red.

Estos dispositivos utilizan la dirección de del dispositivo final, junto a la información sobre las interconexiones de la red, con el fin de validar la mejor ruta para él envió de paquetes a través de la red. Algunas funciones que pueden admitir estos componentes son:

- Regenerar y retransmitir la información.

- Conservar información sobre las rutas que existen a través de la red y dirigir los datos por las rutas alternativas en dado caso encuentre alguna falla en él enlace principal.

- Notificación de errores y fallas a otros dispositivos.

- Clasificación de mensajes de acuerdo con su prioridad, así también permitir o negar el flujo de datos esto conforme sus parámetros de seguridad.

Figura 5. **Dispositivos intermediarios**

Fuente: CCNAIT. *Dispositivos intermediarios. Consultado el 27 de abril de 2022. Recuperado de* https://www.uv.mx/personal/angelperez/files/2019/02/CCNA_ITN_Chp1.pdf.

1.2.3. Medios de red

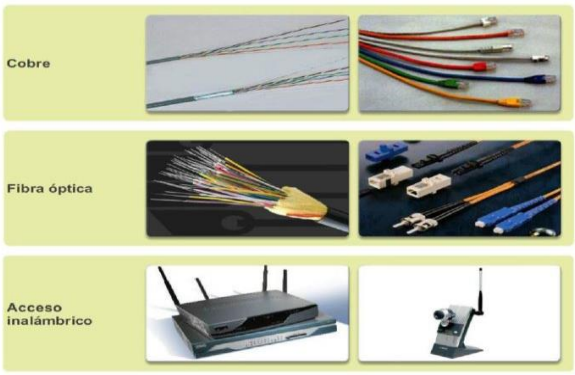
Son los canales por donde viaja la información desde el origen hacia su destino o mejor conocidos como los medios por en donde se trasmite la comunicación a través de una red, existen varios tipos los cuales pueden ser cobre o hilos metálicos, fibra óptica, transmisión inalámbrica, entre otros.

- Hilos metálicos o cobre: Datos los cuales se codifican por medio de impulsos eléctricos.

- Fibra óptica: Son fibras de plástico o vidrio que codifican los datos con impulso luminosos.

- Transmisión inalámbrica: Su codificación es a través de modulación de frecuencias de las ondas electromagnéticas.

Figura 6. **Medios de red**



Fuente: Ingeniería Systmes. *Medios y representaciones de res.* Consultado el 28 de abril de 2022. Recuperado de https://www.ingenieriasystems.com/2016/06/Medios-y-representaciones-de-red-CCNA1-V5-CISCO-C1.html.

1.2.3.1. Hilos metálicos

Este es uno de los medios de transmisión más antiguos y comunes llamado par trenzado, el cual consta de dos cables de cobre asilados. El trenzado se debe a que dos cables constituyen a una antena simple, al momento de contar con el cable trenzado las ondas irradiadas por otros cables de cancelan y este irradia con menos efectividad, por lo general una señal se trasmite como la diferencia de voltaje entre los dos cables en el par, en consecuencia, este ofrece mejoría en la inmunidad al ruido externo.

En la actualidad su utilidad se puede encontrar en la conexión del sistema telefónico de un hogar ya que estos se conectan hacia la central telefónica sin embargo también se cuenta con el acceso ADSL (Permite la separación entre los canales de transmisión de voz y datos). Para lograr esta comunicación se debe conectar un *SPLITTER* o DIVISOR a la toma telefónica.

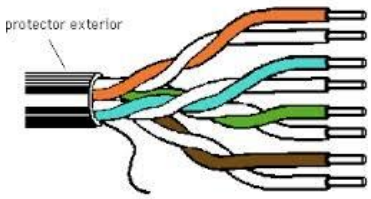
Figura 7. **Splitter ADSL**

Fuente: Made in China. *Splitter ADSL RJ11.* Consultado el 28 de abril de 2022. Recuperado de https://es.made-in-china.com/co_solitone/product_Rj11-ADSL-Splitter-of-High-Quality_enueshuog.html.

Podemos agregar que para este tipo de conexión se pueden tener varios kilómetros sin necesidad de instalar un amplificador, sin embargo, en distancias demasiado extensas es necesario colocar un repetidor, esto por la atenuación que sufre la conexión.

Una función importante del par trenzado es que pueden transmitir señal análoga y digital, y su ancho de banda depende del grosor del cable y la distancia que recorre, pero uno de sus mejores beneficios es su bajo costo.

Figura 8. **Par trenzado**



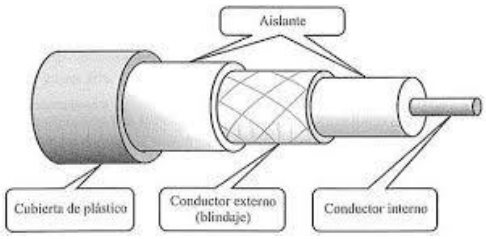
Cable UTP (4 pares)

Fuente: WikiCableado. *Cable de par trenzado.* Consultado el 29 de abril de 2022, Recuperado de https://sites.google.com/site/wikicableadodered/cableado-de-red/cable-de-par-trenzado.

El cable coaxial es otro medio de transmisión común en la trasferencia de datos, este contine un mejor blindaje y trabaja con un mayor ancho de banda que los pares trenzados, por lo que en general puede abarcar distancias más extensas y velocidades más elevadas.

Con este tipo de cable se puede tener tanta trasmisión de tv análoga así también de datos, este cable consiste en alambre de cobre como su núcleo, el cual lo rodea un material aislante que este forrado de un conductor cilíndrico que por lo general es una malla de tejido fuertemente trenzado.

Figura 9. **Cable coaxial**



Fuente:Velez Andres (2012). *Cable coaxial*. Consultado el 29 de abril de 2022, Recuperado de http://mecanicasvelez.blogspot.com/2012/02/cable-coaxial.html.

Este componente es menos susceptible a diafonías e interferencias que el par trenzado, sus principales limitaciones son la atenuación el ruido térmico y el ruido de intermodulación, el cual solamente ocurre cuando se utilizan simultáneamente varios canales o bandas de frecuencia.

Las desventajas que presenta frente al par trenzado son: Es más grueso, su precio es más elevado, la soldadura es más compleja ya que se debe dar continuidad al conductor interno y a la malla, por lo que es este no suele soldares sin embargo se colocan conectores.

En resumen, se suelen utilizar estos medios de transmisión como última milla, es decir en el interior del hogar dando como resultado el cable coaxial para la conexión de tv e internet y el par trenzado para la telefonía, aunque con las tecnologías xDSL como bien se ha mencionado se podrá emplear para otro tipo de transmisión ambos para distancias no muy extensas.

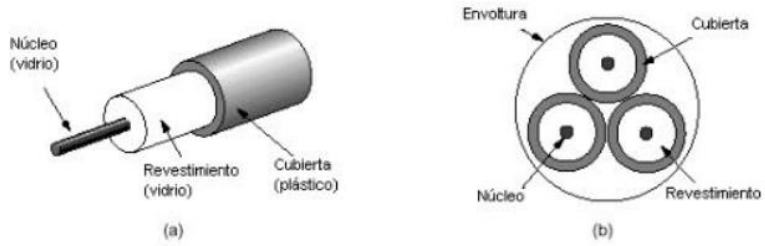
1.2.3.2. Fibra óptica

Este medio en relación con su historia es relativamente corta ya que hasta el año 1977 no se instaló un sistema de prueba en Inglaterra; sin embargo, dos años después, se producían cantidades importantes de este material.

Como derivación de los estudios realizados en física enfocados en la óptica, fue posible descubrir una nueva manera de utilizar la luz, la cual se denomina rayo láser, el cual se aplica en telecomunicaciones esto para que los mensajes se transmitieran a velocidades inusuales y con amplia cobertura, sin embargo se determinó un inconveniente y fue que el láser era demasiado limitado esto a razón de no contar con los conductos y canales adecuados para el viaje de las ondas electromagnéticas provocadas por la lluvia de fotones.

De esta manera para poder contrarrestar este inconveniente se realiza la implementación de un conducto o canal al cual se nombra fibra óptica. Actualmente una fibra óptica es un hilo de vidrio puro, fino en su diámetro, y por el exterior se coloca un revestimiento de vidrio, pero este no conduce la luz; estas dos partes se fabrican a propósito con diferente índice de refracción, de tal forma que, si la luz intenta salir, el vidrio exterior actúe como espejo y así la luz retorne al núcleo.

Figura 10. **Estructura de fibra óptica**

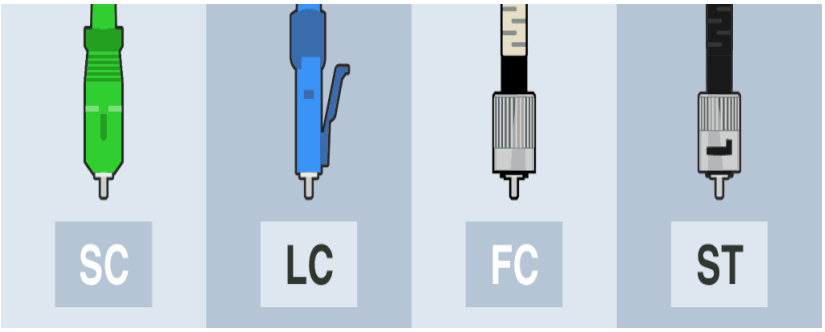


Fuente: Huidobro, José (2014). *Telecomunicaciones tecnologías, redes y servicios*.

Como se puede visualizar en la imagen anterior este medio contiene cierta similitud con los cables coaxiales, con la diferencia que este no contiene trenzado.

La fibra óptica puede trasmitir datos a cientos de kilómetros sin necesidad que la luz sea convertida en electricidad para ser amplificada, puesto que ya existen amplificadores ópticos, adicional a ello este medio permite la transferencia de mayor cantidad de datos.

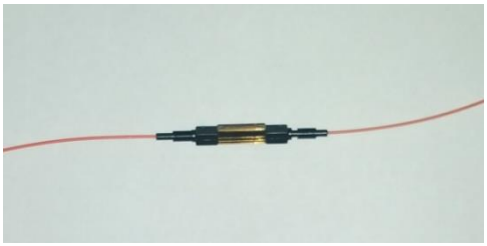
Figura 11. **Conectores de fibra óptica**



Fuente: Promax. *Tipos de conectores de fibra óptica*. Consultado 29 de abril de 2022 Recuperado de https://www.promax.es/esp/noticias/578/tipos-de-conectores-de-fibra-optica-guia-sencilla/.

Las fibras se pueden conectar de tres maneras diferentes. Primera, pueden conectarse mediante a conectores e insertarse en clavijas de fibra, pero estos tienen una pérdida de 10 y 20 % de la luz, sin embargo, facilitan la reconfiguración de los sistemas.

Figura 12. **Empalme mecánico**

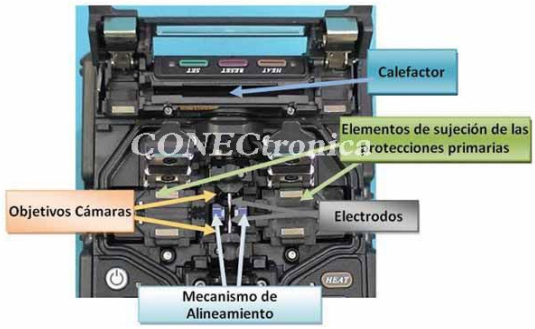


Fuente: el blog de fibra óptica hoy. *Evolución de los empalmes mecánicos. Consultado el 29 de abril de 2022. Recuperado de* https://www.fibraopticahoy.com/blog/evolucion-de-los-empalmes-mecanicos/.

Segunda, se puede realizar empalmes de manera mecánica, estos se refieren a la alineación de los dos extremos cortados esto con extremo cuidado, en una manga especial así sujetando la conexión, para contar con mejor alineación se puede atravesar la unión con luz para después realizar pequeños ajustes, un defecto de este modo de conexión al ser manual es el tiempo y la experiencia que posee el técnico y adicional a ello se produce una pérdida de luz de 10 %.

Tercera, se puede fusionar dos piezas para contar con una conexión sólida, el empalme por fusión es casi tan bueno como una sola fibra, pero de igual forma esta tiene una pequeña cantidad de atenuación, para este tipo de empalme se requiere una máquina especial la cual realizará dicha conexión.

Figura 13. **Máquina de fusión y empalme**



Fuente: Conectronica. *Empalmes de fibra óptica.* Consultado el 1 de mayo de 2022. Recuperado de https://www.conectronica.com/fibra-optica/ftth-fftx-fibra-optica/empalmes-de-fibra-optica-segun-la-nueva-normativa-de-icts.

Tabla I. **Diferencias entre fibra de hilos metálicos y fibra óptica**

Hilos metálicos o cobre	Fibra óptica
Depende de tipo de cable utilizado	Maneja anchos de banda mayores al cobre
Repetidores cada 5Km	Repetidores cada 50 Km
Se afecta al contar con sobrecargas de energía	Sin afectación a sobrecargas de energía
Susceptible a cambios de temperatura y cambios ambientales	No es susceptible a cambios de temperatura y cambios ambientales
Empalme más sencillo y a bajo costo	Empalme de mayor dificultad y costo más elevado

Fuente: elaboración propia, realizado con Excel.

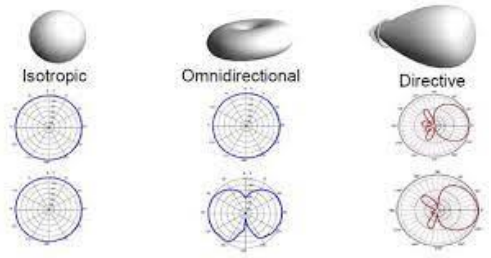
En resumen, se puede validar que la fibra óptica es la mejor opción para la elaboración de una conexión de red externo, pero para una red de menor tamaño o bien conocida como una red de oficina u hogar es más conveniente utilizar hilos metálicos o cobre.

1.2.3.3. Transmisión inalámbrica

Para los usuarios móviles no es de utilidad utilizar par trenzado, cable coaxial o fibra óptica, para estos dispositivos se necesita obtener datos sin estar atados a la infraestructura terrestre, es por esta razón que se formula el medio de transmisión inalámbrica las que mejor adaptación han tenido son los o radiotransmisión y las microondas.

Las ondas de radio frecuencia (RF), son fáciles de generar y pueden recorrer distancias largas así también logran penetrar con facilidad las estructuras, por lo que son muy utilizadas tanto en interiores como exteriores, la forma en la que estas irradian es omnidireccional

Figura 14. **Gráfica de comportamiento de antenas horizontal y vertical**



Fuente: Huidobro, José (2014). *Telecomunicaciones tecnologías, redes y servicios.* Consultado el 1 de mayo de 2022.

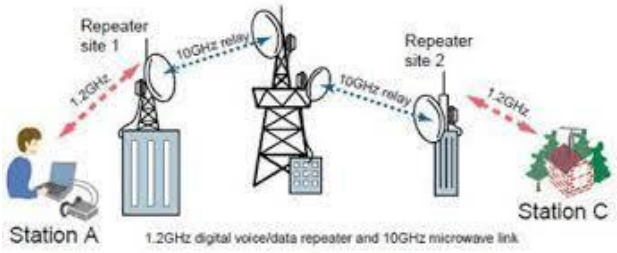
Este tipo de antenas trabajan bajo ciertas bandas de frecuencia HF y VHF, estas ondas forman parte del espectro electromagnético.

Por otra parte, para las señales de radio de alta frecuencia se conoce el enlace de microondas, como se menciona este medio es para frecuencias de 100 MHz, en este enlace se debe de tener extremo cuidado ya que tanto la antena emisora y receptora deben tener la mayor precisión en su alineación. Entre más elevada la antena se puede tener mayor distancia entre las antenas.

Así también este enlace Puede ser terrestre que es el mencionado en el texto anterior; como espacial (se utiliza un satélite de comunicaciones como repetidor intermedio de la señal). Las microondas se suelen utilizar para la sustitución del cable coaxial o fibra óptica, esto ya que no se necesitan demasiados repetidores y amplificadores.

La atenuación es una de las mayores debilidades de este enlace ya que este aumenta con las lluvias.

Figura 15. **Ejemplo de enlace de Microondas**



Fuente: RED Tauros. *Redes de transmisión.* Consultado el 1 de mayo de 2022. Recuperado de http://www.redtauros.com/Clases/Medios_Transmision/04_Radioenlaces_Terrestres_Microondas_.pdf.p.6.

Tabla II. **Diferencias entre enlaces físicos e inalámbricos**

ENLACES FÍSICOS	ENLACES INALÁMBRICOS
Dependido el medio utilizado depende del clima y la temperatura	Los datos viajan a través del medio por radiofrecuencia u ondas de microonda
Utiliza repetidores o amplificadores de señal cada cierta distancia	Cobertura depende del tipo de enlace y de antena utilizada
Se utiliza principalmente en el área urbana contemplando combinación de F.O y ADSL	Es más utilizado en el área rural donde se cuenta con difícil acceso de cableado

Fuente: elaboración propia, realizado con Excel.

1.3. Topologías y modelos de arquitectura de red

Los diagramas de topológicos son informes ilustrativos, ya que sirven como mapa visual que indica cómo se encuentran los equipos conectados en una red para el intercambio de datos, ya sean en diagramas físicos o bien en diagramas lógicos.

Estos diagramas se encuentran entrelazados por un conjunto de nodos, por los cuales viajan los datos.

Para los administradores de redes deben ser capaces de mostrar el aspecto final que tendrá su red, el poder visualizar me manera eficiente como se interconectan todos los dispositivos y saber la ubicación de cada componente.

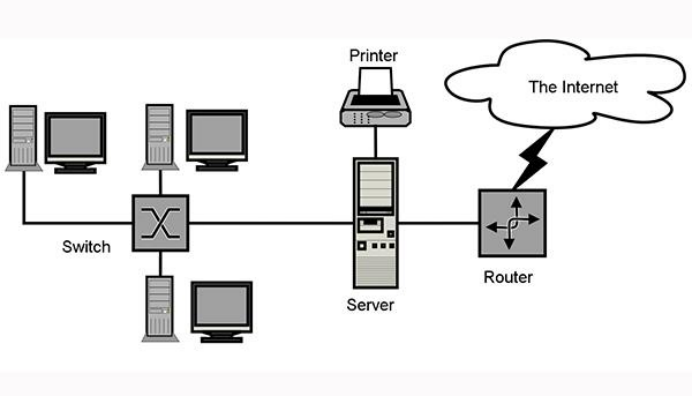
Para el análisis de la trayectoria que se tiene al instante en el cual se envía o recibe los datos se fundamenta por los modelos de referencia de red los cuales son 2 uno de ellos es el protocolo TCP/IP y el segundo es el modelo OSI, los cuales se explicaran más adelante.

1.3.1. Diagramas de topologías fiscas

Este tipo de ilustración indica la ubicación física de los dispositivos y la instalación por cable, de igual manera se tiene identificado por medio de etiquetas cada sitio en el cual se encuentran los dispositivos.

Este tipo de topología es utilizado entre los profesionales de redes para el monitoreo de gestión de redes locales otra utilidad es para saber la jerarquía de cada dispositivo en la red, tanto para conocer sus funciones y responsabilidades.

Figura 16. **Diagrama topológico físico**



Fuente: Helmut SyCorvo 2019. *Topologías físicas.* Consultado el 1 de mayo de 2022 Recuperado de https://www.lifeder.com/topologias-de-red/.

Para este tipo de diagramas se cuenta con cinco formas o topologías diferentes los cuales son:

- Topología de anillo
- Topología de malla
- Topología de bus
- Topología de estrella
- Topología de árbol

1.3.1.1. Topología de Anillo

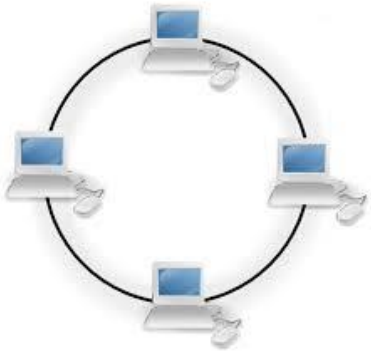
Para esta conexión cada nodo se conecta con el nodo siguiente y el anterior creando así solo una única ruta para la transferencia de datos.

Los anillos puedes se de forma unidireccional y la comunicación se puede establecer en sentido horario o bien antihorario, pero este tiene una gran

deficiencia ya que por contar solo con ruta estas pueden verse interrumpidas por fallas en su enlace, esto ocasionado por el corte o falla de un nodo.

La solución a este inconveniente es que en algunos casos se coloca un anillo de antirrotación (*C-ring*), para la creación de una topología redundante

Figura 17. **Topología de Anillo**



Fuente: Rivera Helen 2017. *Topología en anillo.* Consultado el 2 de mayo de 2022, recuperado de https://clasificaciondelasredesblog.wordpress.com/2017/05/09/topologia-anillo/.

- Ventajas
    - Fácil instalación.
    - Fácil resolución de problemas.
    - Rápida trasferencia de datos entre dispositivos.
- Desventajas
    - Un solo corte puede afectar la red completa.
    - Los datos se transfieren atreves de toda la red.

1.3.1.2. Topología de Malla

Para este tipo de topología se interconectan todos los nodos, de tal manera que los datos pueden utilizar rutas alternas para llegar a su destino, si la red está completamente conectada no debe existir ninguna falla en la comunicación.

Esta topología no necesita de un nodo central, como ya se ha mencionado al realizar un mantenimiento en algún nodo este no sería impedimento para que las tramas de otros dispositivos no tendrían fallos en llegar a su destino. Su mayor implementación se realiza con el enrutamiento dinámico.

La cantidad de conexiones se pueden calcular con la siguiente formula

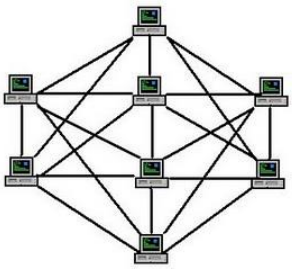
$$N = \frac{n * (n - 1)}{2}$$

Siendo:

N: Cantidad de conexiones.

n: Número de computadoras conectadas en la red.

Figura 18. **Topología Malla**



Fuente: Rivera Helen 2017. *Topología en maya.* Consultado el 2 de mayo de 2022, recuperado de https://clasificaciondelasredesblog.wordpress.com/2017/05/09/topologia-en-maya/.

- Ventajas

  - Sin problemas para tráfico de datos.
  - Fácil identificación de fallas.
  - Mayor facilidad para adaptar más dispositivos.

- Desventajas

  - Una de las topologías más costosas.
  - Difícil instalación.

1.3.1.3. Topología de Bus

Topología en la cual todos los nodos están contados hacia un mismo enlace y no existe otra forma de conexión entre los nodos. La conexión de cada host es en un mismo cable, por lo que la comunicación es más directa sin embargo la ruptura de este cable se pierde la comunicación hacia los hosts.

Este cable que une el host es conocido como troncal, se pueden conectar una cantidad considerable de host, si una host falla no pierde la transmisión de datos, al contrario, como se ha mencionado anteriormente si se corta el Bus físicamente.

Para la transmisión de datos este envía el mensaje a todos los hosts, la tarjeta NIC examina cada dirección del mensaje para determinar hacía que host va dirigido el mensaje.

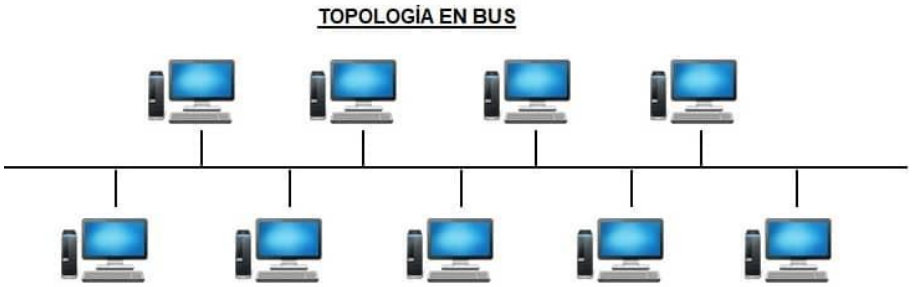
- Ventajas

    - Fácil y simple en solucionar problemas.
    - Fácil adaptación.
    - Facilidad de crecimiento.
    - No ocupa demasiado espacio.

- Desventajas

    - La calidad de la señal determina el límite de hosts.
    - Si el canal presenta falla afecta toda la red.
    - Perdidas de paquetes por colisiones.

Figura 19. **Topología de Bus**



Fuente: Areatecnologia. *Topologías de red.* Consultado el 2 de mayo de 2022. Recuperado de https://www.areatecnologia.com/informatica/topologias-de-red.html.

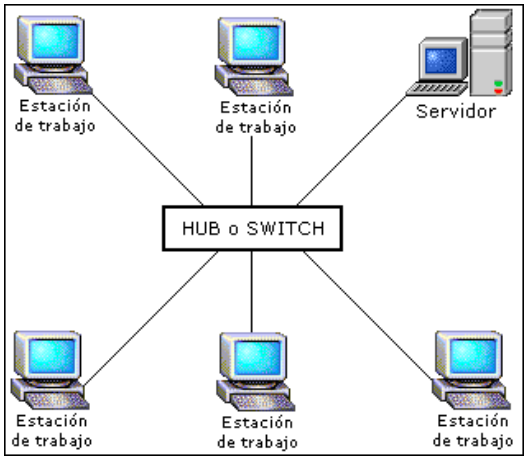
1.3.1.4. Topología de Estrella

Este tipo de topología las conexiones de los hosts se dirigen hacia el servidor, las conexiones se originan del centro hacia el host, sin embargo, los hosts no están conectados entre sí.

La conexión central o también llamado nodo central por lo regular se encuentra ocupado por un *HUB*, el cual distribuye la información hacia los hosts. En esta tipología no se permite demasiado tráfico de información, así también el HUB actúa como un intercambiador, ya que un host al enviar datos a otro envía los datos al controlador, el cual retrasmite la información hacia el dispositivo final.

Se cuenta con un similar funcionamiento que la topología de *BUS* ya que el mensaje que el *HUB* reenvía es trasmitido hacia todos los hosts, pero la tarjeta *NIC* de cada host es el que realiza el trabajo.

Figura 20. **Topología Estrella**



Fuente: Anitha. *Topologías.* Consultado el 2 de mayo de 2022. Recuperado de https://anitha98.tripod.com/Topologias1.HTML.

- Ventajas

  - Estructura simple.
  - Cada host es independiente.
  - Control de tráfico centralizado.
  - Permite agregar más dispositivos fácilmente.

- Desventajas

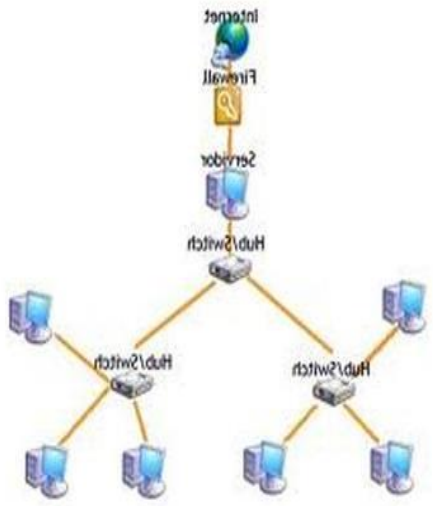
  - Costoso, ya que requiere de más cable.
  - Los dispositivos no están enlazados entre sí.
  - Su funcionamiento depende del servidor central.

1.3.1.5. Topología de Árbol

Es muy similar a la topología de Estrella, la diferencia es que esta topología no necesita un nodo central, este cuenta con un nodo de enlace central, el cual está siendo ocupado por lo regular por un *HUB* o un *SWITCH*, del cual emergen las ramificaciones hacia otros nodos.

Podemos afirmar que es una variación de la red de BUS con la diferencia que un fallo en un nodo no interrumpe la totalidad de la comunicación. La conexión se forma de manera jerárquica.

Figura 21. **Topología Árbol**



Fuente: Anitha. *Topologías.* Consultado el 2 de mayo de 2022. Recuperado de https://anitha98.tripod.com/Topologias1.HTML.

- Ventajas
    - Mayor rapidez en trasmisión de datos.

- Facilidad para resolución de problemas.
- Permite el crecimiento de la red.

- Desventajas

  - Mas costosa ya que requiere demasiado cableado.
  - Si el segmento central cae se tiene pérdida total.

1.3.2. Modelos de arquitectura de red

Los modelos se basan en la forma de visualizar los protocolos de red, ya que un protocolo es un conjunto de reglas que han sido acordadas por las organizaciones de normalización, él envió de un mensaje contine estas reglas para poder llegar de un punto a otro.

Las comunicaciones aparte de identificar el origen y el destino también definen detalles en la manera que se trasmiten los datos a través de la red, lo más común que incluyen estos protocolos son:

- Codificación del mensaje.
- Formato y encapsulamiento del mensaje.
- Tamaño del mensaje.
- Sincronización del mensaje.
- Opciones de entrega del mensaje.

1.3.2.1. Codificación del mensaje

El primer paso es convertir el mensaje en otra forma de escritura la cual al ser enviado por el canal este no corra riesgo de que cualquier persona pueda leer

su contenido, ya que solamente el destino tendrá la forma de decodificar el mensaje.

1.3.2.2. Formato y encapsulamiento del mensaje

Desde que se envía el mensaje este debe de contener un formato o estructura, esto dependerá del tipo de mensaje y el canal a utilizar para él envió de datos.

1.3.2.3. Tamaño del mensaje

Esto dependerá del tipo de mensaje ya que si es demasiado grande este será enviado en forma de paquetes los cuales dividirán el mensaje completo, y al llegar a su destino este unirá nuevamente todos los paquetes para tener el mensaje de manera completa.

1.3.2.4. Sincronización del mensaje

Cuando hablamos de sincronización nos referimos al tiempo que le toma a nuestro mensaje viajar por toda la red y así también obtener una respuesta del destino; en este tema se adjuntan los siguientes datos:

- Control de flujo: Es la velocidad a la cual se trasmiten los datos. Esto afecta a la cantidad de datos que se pueden enviar y la velocidad que tardara en entregar dicha información.
- Tiempo de respuesta (*Response Timeout*): Se refiere al momento en que es entregado el mensaje, el destino envía una respuesta de recibido, de no recibir esta respuesta dependiendo la configuración puede realizar un segundo envió o bien se contara como paquetes perdidos.

- Método de acceso: Determina el mejor momento para el envío de paquetes por la red, esto para evitar colisiones dentro de la red.

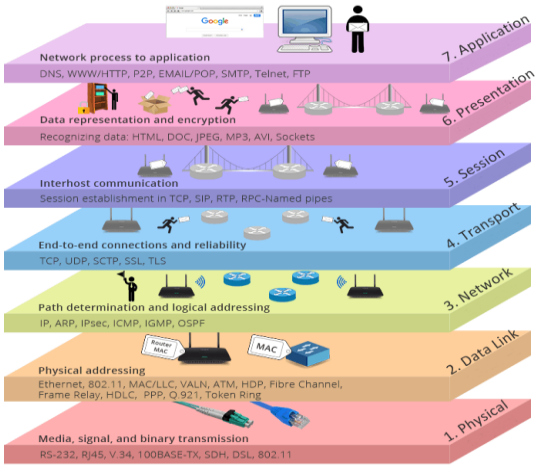
Para estas implementaciones en red contamos con un modelo y un protocolo los cuales de detallaran siendo estos:

- Modelo OSI
- Protocolo TCP/IP

1.3.2.5. Modelo OSI

Se compone por 7 capas o niveles de proceso, para empaquetar y trasmitir el mensaje a través de los medios físicos hasta su llegada al destino. Este tipo de modelo es coherente con todos los tipos de servicios y protocolos de red.

Figura 22. **Modelo OSI**



Fuente: Sheldon 6 de agosto 2021. *Capas del modelo OSI.* Consultado el 3 de mayo de 2022. Recuperado de https://community.fs.com/es/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html.

- Las capas con las cuales este modelo trabaja son:

    - Física: Describe los componentes mecánicos, funciónales, eléctricos para mantener, activar o desactivar una transmisión de datos o bits desde su origen hacia su destino.

    - Enlace de datos: Se basan en el intercambio de datos, conocidos como tramas entre dispositivos a través del mismo canal, utiliza el direccionamiento físico dentro de cualquier topología de red.

    - Red: Otorga el servicio de intercambiar piezas individuales por medio de la red entre dispositivos, ya que es el camino por el cual se enviarán los datos.

    - Transporte: Parte en la que se segmenta, transfiere y vuelve a construir los datos de la comunicación.

    - Sesión: organiza el diálogo y administra la capa de datos.

    - Presentación: Es la representación común de los datos enviados ente los servicios, este es el formato en el cual los datos se intercambiarán.

    - Aplicación: Contiene los protocolos usados para las comunicaciones proceso a proceso, proporciona los servicios de aplicaciones para que el usuario final pueda acceder a la red.

Para referirnos a los niveles del modelo OSI se nombran por capas iniciando como CAPA 1: FISICA y siendo la ultima la CAPA 7 APLICACIÓN.

1.3.2.6. Protocolo TCP / IP

El modelo de protocolo *TCP/IP* es también llamado modelo de internet, su función es describir las funciones en cada capa o protocolo determinado para la transmisión de datos, toma la referencia del modelo *OSI* sin embargo este contiene solamente cuatro capas.

- Capa de aplicación: Define los protocolos usados por las aplicaciones que proporcionaran gestión por parte del usuario final, algunos ejemplos son *HTTP, DNS, DHCP, FTP*.

- Capa de transporte: Son los puertos lógicos que permiten la trasferencia de datos por medio de la red, se define como será la conexión entre host activando los canales básicos que utilizará la capa de aplicación. Se encarga de la segmentación, control de errores y el control de flujo de los paquetes enviados, acá encontramos los protocolos *TCP y UDP*.

- Capa de internet: Su función es la estructura del paquete que circula por medio de la red y como será enviado, en otras palabras, es el enrutamiento que surge de las direcciones IP, para tener en cuenta hacía que destino será trasmitido, en este punto encontramos el protocolo I*P, ARP o ICMP y IGMP*.

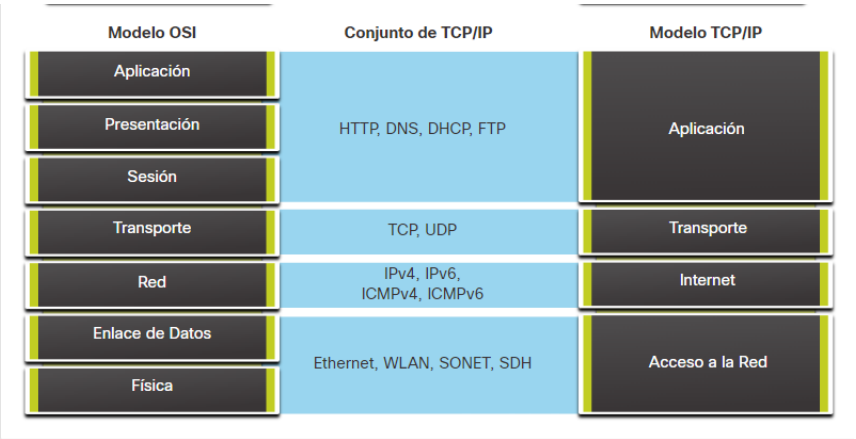
- Capa de acceso a la red: Es la capa que contiene el acceso físico de los hosts conectados en la red, se conoce que en esta capa se encuentran las

topologías de red ya descritas anteriormente así también al tipo de red *WAN*.

Como se puede observar la base de este protocolo es la reducción del modelo OSI, por lo que podemos afirmar que, el modelo *OSI* nos brinda el ejemplo más detallado de cómo es la estructura de red, sin embargo, el protocolo *TCP/IP* nos demuestra cómo es la operatividad y lo más exacto del trayecto que presenta una trasmisión de datos.

Por otra parte, la organización ISO (*Internal Organization for Standarization*) tiene como referencia es el modelo OSI.

Figura 23. **Comparación de modelo OSI y protocolo TCP / IP**



Fuente: CCNA 200-301. *Modelos y Protocolos.* Consultado el 3 de mayo de 2022. Recuperado de https://ccnadesdecero.es/modelos-tcp-ip-osi-caracteristicas/.

1.4. Tipos de redes

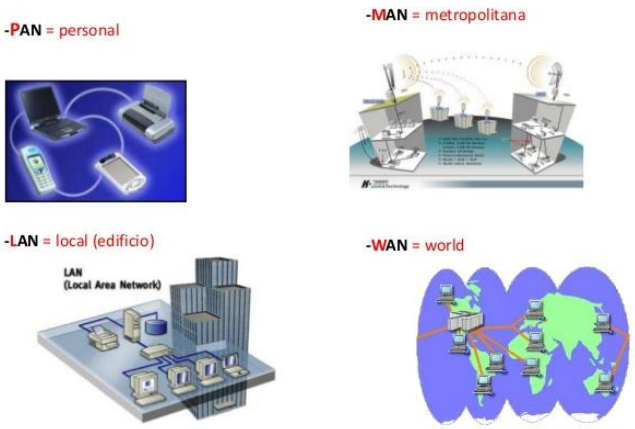
Ya que tenemos conocimiento de los componentes y así también de los modelos que se utilizan debemos conocer los diferentes tipos de redes que

existen en informática. Hay redes de diferentes tamaños pueden ser simples desde dos hosts hasta redes que interconectan un sinfín de hosts.

Existen redes domésticas las cuales pueden compartir distintos recursos entre dispositivos finales como por ejemplo música, videos, documentos, entre otros. Así también existen las redes de oficina o redes SOHO, que permiten al usuario compartir información desde su hogar desde una oficina remota.

Empresas grandes y organizaciones usan las redes para proporcionar almacenamiento y acceso a los servidores de la red, en las cuales proporcionan correos electrónicos, mensajería instantánea ente empleados

Figura 24. **Tipos de red por tamaño**



Fuente: Google. *Tipos de redes.* Consultado el 3 de mayo de 2022. Recuperado de https://sites.google.com/site/redesdecomputadora3/home/tipos-de-redes.

- Por tamaño contamos con los siguientes tipos de redes:
    - PAN
    - LAN

- MAN
- WAN
- VLAN

- Existe también las redes por su forma de conexión a internet y estas pueden ser:

  - INTRANET
  - EXTRANET

1.4.1. Tipos de redes por tamaño

En redes existen varios tipos de redes las cuales pueden variar según su tamaño ya sea por alcance territorial, la cantidad de equipos conectados o bien el uso que se le tenga a la red.

1.4.1.1. Red PAN

Por sus siglas en inglés (*Personal Area Network*), es la red de área personal, este tipo de red es el más pequeño ya que suele conectar todo tipo de aparato electrónico domestico ya sea tables, tv, computadas, impresoras entre otros., su alcance es no mayor a 10 metros por lo que se puede considerar como una red solamente domestica sin embargo es utilizado en algunas oficinas pequeñas.

No debemos confundirla con la red *LAN* ya que es similar en algunos aspectos, pero es de mayor tamaño.

Figura 25. **Red PAN**

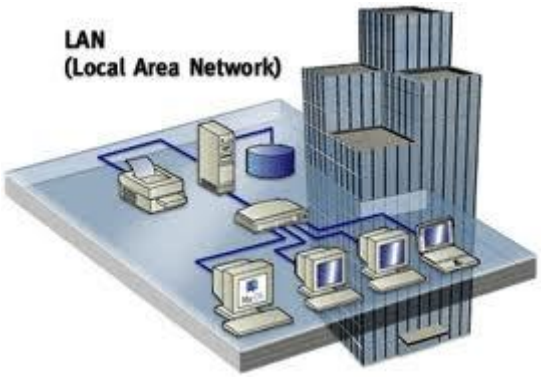
Fuente: Timetoast. *Redes de comunicación.* Consultado el 3 de mayo de 2022. Recuperado de https://www.timetoast.com/timelines/redes-de-comunicacion-21843c1b-b258-4a4c-8f20-f542f9a3a92d.

1.4.1.2. Red LAN

Conocida como Red de Área Local (*Local Área Network*), es la que permite la interconexión entre distintos nodos para compartir recursos y datos, pero esto siempre a una distancia corta, su conexión le permite contar desde 10 hasta 1000 dispositivos esto basado en áreas de trabajo como son casas, oficinas, hoteles, edificios, entre otros.

Cada ordenador conectado en este tipo de red es llamado nodo y cada uno de los nodos conectados cuenta con protección y su propio *CPU*. Por lo general la administración está a cargo de una sola organización o de una persona, ya que por su tamaño no es demasiado complicado su organización y expansión. Los anchos de banda con los que trabaja son de alta velocidad.

Figura 26. **Red LAN**

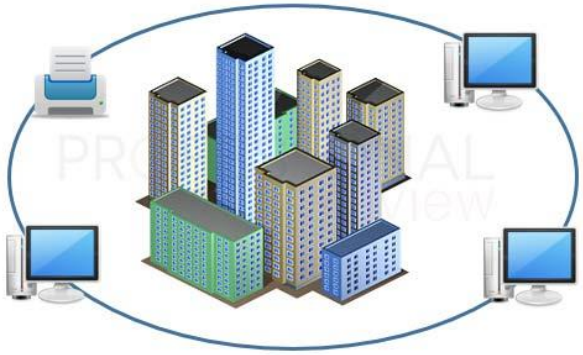


Fuente: Documentos Google. *Tipos de redes.* Consultado el 3 de mayo de 2022. Recuperado de https://sites.google.com/site/oscarcadenaslopez/tema-1/subtema-1.

1.4.1.3. RED MAN

Es la red de área metropolitana (*Metropolitan Área Network*), permite el intercambio de datos entre ciudades y pueblos esta red es más grande que una red *LAN*, pero más pequeña que una red *WAN*, su conexión es a base de fibra óptica y es de alta velocidad, también contine en si mima dos o más redes *LAN*, contiene mayor seguridad una red *MAN* privada que una red *WAN*, es por ello que suelen utilizarse en sistemas de vigilancia; su alcance no supera los 50 Km de diámetro.

Figura 27. **Red MAN**

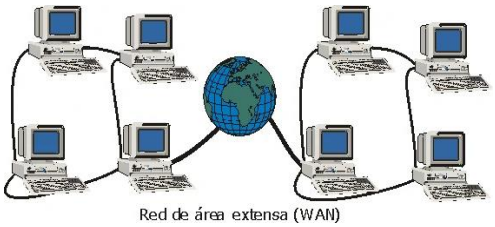


Fuente: Proreview. *Que son las redes.* Consultado el 4 de mayo de 2022, recuperado de https://www.profesionalreview.com/2018/12/09/redes-lan-man-wan/.

1.4.1.4. RED WAN

Este tipo de red abarca una mayor extensión geográfica y se conoce como la red de área amplia (*Wide Area Network*), regularmente son administradas por Proveedores de Servicio (*SP*), o bien proveedores de internet (*ISP*), las velocidades que proporciona a sus enlaces son lenta entre *LAN*; puede cubrir ciudades, pueblos, países o continentes, sin embargo, una deficiencia con la que estas redes cuentan es la poca seguridad que ofrecen.

Figura 28. **Red WAN**



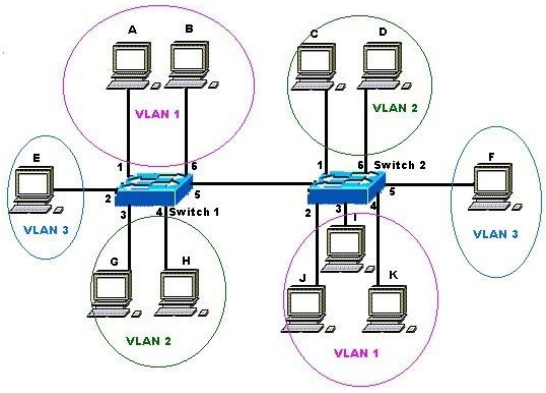
Fuente: InfonicWiki. *Red WAN. Consultado el 4 de mayo de 2022. Recuperado de* https://infotic.fandom.com/es/wiki/Red_WAN.

Puede tener una red WAN administrada por un ISP o bien puede contar con una red WAN privada como por ejemplo la nube ya que es para uso empresarial solamente, el medio por el cual se trasmiten sus datos es por fibra óptica sobre tierra y agua.

1.4.1.5. RED VLAN

Red *LAN* virtual o lógica (*Virtual Local Area Network*), son creadas a partir de una topología física, su mayor utilización es para segmentar la red por departamentos con el fin de que no se tenga colisiones en el tráfico ya que se reduce el área en el cual viajara nuestro paquete por la red puesto que no podrá interactuar con otros usuarios dentro de la red que no pertenezcan a su conjunto, es muy confiable en lo que respecta a su seguridad y cuentan con una considerable reducción de costes, facilitan su administración y su rendimiento.

Figura 29. **Red VLAN**



Fuente: Documentos Google. *Red vlan.* Consultado el 4 de mayo de 2022. Recuperado de https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/4-redes-de-area-local-virtuales-vlans/1-uso-de-las-vlan?tmpl=%2Fsystem%2Fapp%2Ftemplates%2Fprint%2F&showPrintDialog=1.

1.4.2. Internet y tipos de red por su conexión

Para el intercambio de datos existen también diferentes tipos ya que se puede contar con acceso interno o bien acceso externo a nuestra red, con los cuales se debe generar permisos.

1.4.2.1. Internet

Es la colección global de redes interconectada por sus siglas en inglés (*Intenetworks*), ya que se une a redes *LAN* Y *WAN*; El Internet no pertenece a ninguna persona o servidor, pero si necesita de una gran variedad de aplicaciones y estándares, así como cooperación de agencias de administración, algunos de estos entes que regulan los protocolos y procesos son:

- Grupo de trabajo de ingeniería de internet (*IETF*).
- Corporación de internet para la asignación de nombres (*ICANN*).
- Consejo de arquitectura de internet (*IAB*).

Este utiliza el Modelo *TCP/IP* para su funcionamiento, ya que es un enlace mundial, uno de los servicios más grande con el que cuenta es WWW (*World Wide Web*), este es un conjunto de protocolos que permite la consulta de archivos de hipertexto

Por su forma de conexión existen dos tipos de red:

1.4.2.2. Intranet

Término utilizado para la conexión que es privada de las redes *LAN* y *WAN* que son pertenecientes a una organización, modo de implementación es solo

para que los empleados o personal autorizado puedan acceder a los servidores o datos de la empresa.

Conecta distintos servidores web esto a través del acceso a internet público, pero el ingreso se realiza por medio de cortafuegos o firewalls que su función es la de analizar los mensajes de ambas partes tanto del emisor como la del receptor, ejemplos claros de intranet podemos encontrar en las redes escolares ya que solamente el profesor, estudiantes y personal administrativo contaría con acceso.

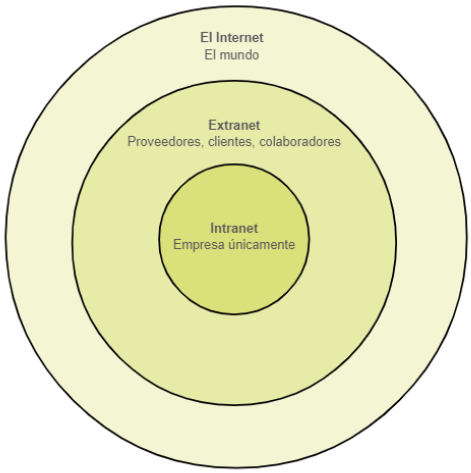
1.4.2.3. Extranet

Este concepto que indica ser una red privada a la que restringe al público en general con lo que solo permite comunicación entre usuarios que formen parte de la institución o que tengan algún vínculo con ella. En otras palabras, se puede afirmar que la Extranet es la unión de dos o más Intranets. Algunos ejemplos podemos encontrar.

- Hospitales
- Secretaria de educación

Ya que este se basa a proveedores, clientes o colaboradores.

Figura 30. **Tipos de red por su conexión**



Fuente: Linares Kevin (2017). *Internet, intranets y extranet.* Consultado el 4 de mayo de 2022. Recuperado de https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-LAN-WAN-e-Internet-internet-intranets-y-extranets.html.

1.5. Redes confiables

Ahora que tenemos conocimiento de los tipos de redes que existen, sus componentes, los modelos y los medio por los cuales viaja nuestro mensaje debemos preguntarnos como realizar una red de manera que esta cumpla con todas las expectativas y sea segura además de ser también eficaz.

Para responder a esta interrogante contamos con una serie de fundamentos los cuales debe contar nuestra red para que trabaje de manera óptima, la forma en la que estructuraremos nuestra red debe ser capaz de tener los siguientes principios:

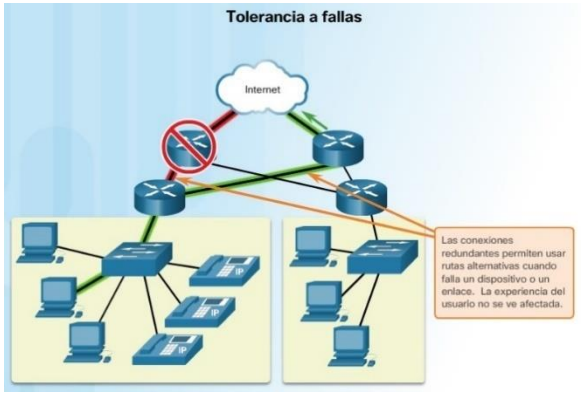
- Tolerancia a fallas

- Escalabilidad
- Calidad de servicio (*QoS*)
- Seguridad

1.5.1. Tolerancia a fallas

Este concepto se basa en la limitación de dispositivos afectados mientras una falla este en proceso, es la recuperación de la manera más rápida y efectiva, un ejemplo de ello son los enlaces redundantes ya que, si el enlace principal por el cual viaja la paquetería se ve afectado, el enlace redundante ingresa para que no se pierda la conexión mientras de restablecer el enlace principal.

Figura 31. **Tolerancia a fallas**



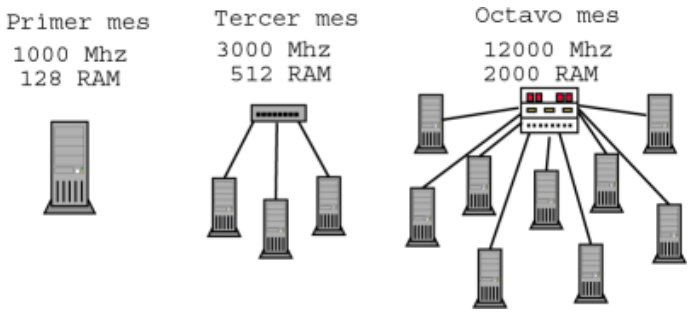
Fuente: CCNA20-301. *Tolerancia a fallas.* Consultado el 5 de mayo de 2022, recuperado de https://ccnadesdecero.es/redes-confiables/.

1.5.2. Escalabilidad

Termino que aplica para la expansión de manera segura y confiable de una red tanto para admitir nuevos dispositivos como implementar nuevas

aplicaciones, siempre sin degradar el rendimiento del servicio, esto se logra al seguir los modelos y los protocolos adecuados, por lo que los proveedores pueden realizar mejoras sin tener que realizar nuevos conjuntos de reglas para que logre operar la red de manera correcta

Figura 32. **Escalabilidad**



Fuente: Internet paso a paso. *Calidad de servicio.* Consultado el 5 de mayo de 2022, Recuperado de https://internetpasoapaso.com/qos-rou.

1.5.3. Calidad de servicio

Por sus siglas en ingles QoS (*Quality of Service*), se trata de mantener el rendimiento de los equipos ya sea si se trasmite voz, datos, videos, entre otros. Por ejemplo, sabemos que para envío de un video se necesitara más ancho de banda que enviar un mensaje de texto por la red, sin embargo, la calidad de servicio hará que estos lleguen en el menor tiempo posible y sin fallos o perdida de paquetes, puesto que para él envió de datos usa una segmentación de datos enviándolos por distintas rutas para no congestionar la red así también para no crear colisiones.

Garantiza que dos o más usuarios realicen tareas en simultaneo sin afectarlos, ya que para la trasmisión se medirá en bits por segundo.

Figura 33. **Calidad de servicio QoS**

Fuente: Internet paso a paso. *Calidad de servicio.* Consultado el 5 de mayo de 2022, Recuperado de https://internetpasoapaso.com/qos-rou.

1.5.4. Seguridad

Sabemos que para las organizaciones o bien redes pequeñas tenemos servicios e información que es muy delicada o importante, la cual solo el personal autorizado puede tener acceso, por lo que el personal de administración debe de tener al pendiente la seguridad de la infraestructura y la seguridad de la información.

Para que una rede sea segura se debe de asegura los dispositivos de manera física y los softwares que se utilizan.

2. INSTALACIÓN Y MODO DE UTILIZACIÓN DE HERRAMIENTA CISCO PACKET TRACERT

2.1. Descarga e instalación de herramienta de trabajo

Contamos con los conceptos básicos sobre las redes, es momento de iniciar con el proceso de configuración de los equipos, para poder realizar estas configuraciones utilizaremos un simulador de redes el cual la misma plataforma de estudio de cisco nos ofrece, la cual es una herramienta muy completa, ya que se asemeja en un buen porcentaje a estar haciendo conexiones de manera física. La herramienta a utilizar es *Cisco Packet Tracert*.

- Paso No. 1: debemos dirigirnos a la página oficial de CISCO, https://www.netacad.com, en este enlace encontraremos varias subsecciones de las cuales destacan:

    - Cursos: En esta sección encontraremos todos los cursos que podemos optar el tiempo total de duración de curso, también si es necesario contar con un instructor o seguir la secuencia de videos.

    - Carreras profesionales: Apartado que nos puede ser de utilidad para nuestra carrera profesional, puesto que cuenta con oportunidades de empleo, asesoramiento profesional y al completar un curso en esta sección encontraremos las insignias y los certificados obtenidos al completar un curso de marera exitosa.

- Apoyo: En esta sección nos redireccionara a la página de soporte y preguntas frecuentes.

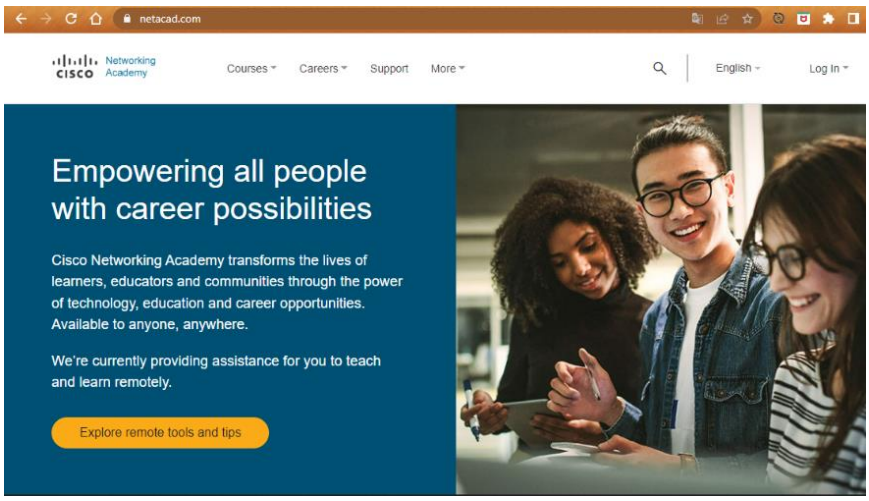
- Más: Nos direcciona a páginas indicando quien es cisco, que podemos aprender así también, nos puede direccionar a un podcast.

- Búsqueda

- Idioma

- Iniciar sesión

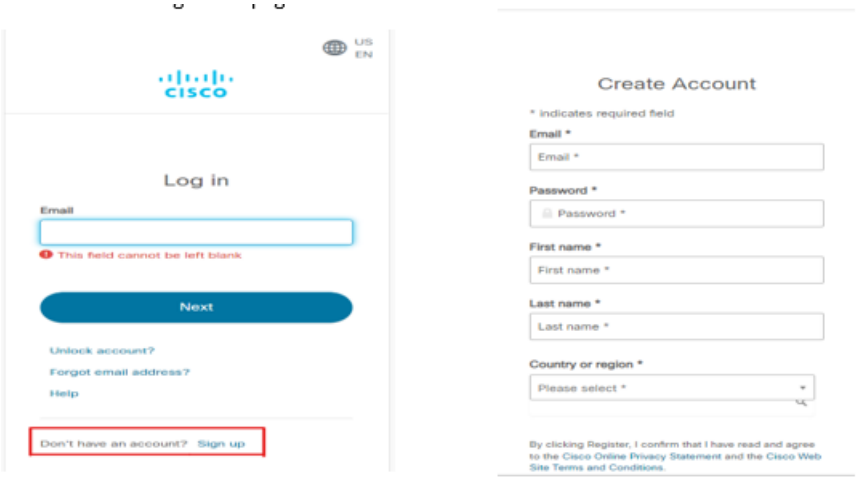
Figura 34. **Plataforma Oficial de Cisco**



Fuente: Cisco. *Plataforma networking academy.* Consultado el 5 de mayo de 2022, recuperado de https://www.netacad.com/es.

- Paso No. 2: Se debe crear una cuenta, esto ingresando al apartado de *Login* o inicio de sesión, el cual nos direccionara a la siguiente página.

Figura 35. **Creación de usuario**



Fuente: Cisco. *Login.* Consultado el 8 de mayo de 2022 recuperado de https://id.cisco.com/.

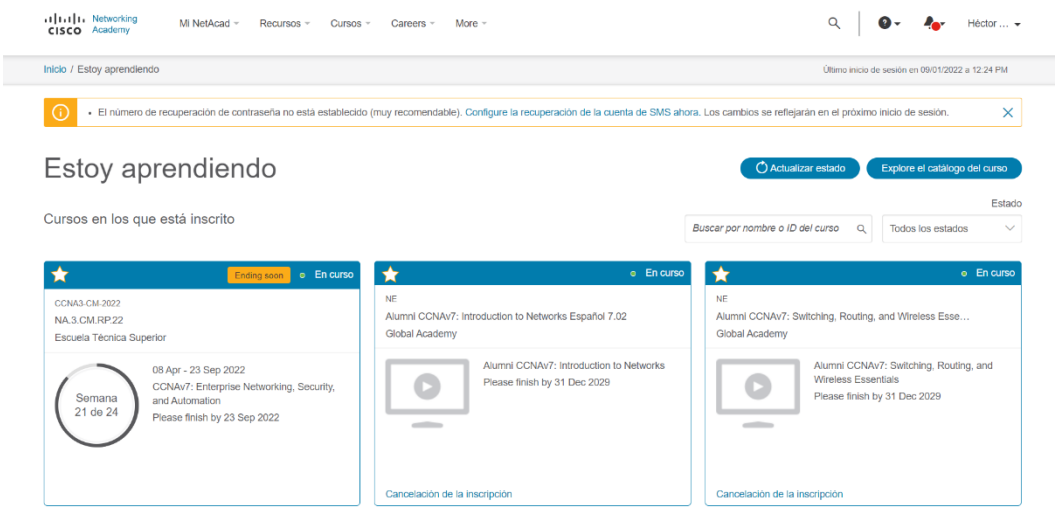
Seleccionaremos la frase que dice *Sign up* lo cual nos direccionará a una nueva página en la cual debemos de llenar con nuestros datos, esto no servirá para tener acceso a todas las herramientas y a las opciones vistas en el paso anterior, ya que de no hacerlo no tendremos accesos a los cursos y los beneficios de cisco.

Una vez creado nuestro usuario procederemos a ingresar en *Log In*, con los datos que establecimos en el paso anterior. Al tener acceso en la pantalla principal podremos observar los cursos a los cuales nos hemos asignado y el avance en el que estamos.

Podemos visualizar que tenemos una figura en forma de campana la cual nos indica noticias importantes sobre cursos o bien mensajes de nuestro instructor si es el caso de ya estar inscrito en algún curso.

También tiene nuestro nombre de usuario en el cual podemos modificar nuestro perfil, descargar insignias y certificados, obtener vales de descuento y finalizar nuestra sesión.

Figura 36. **Página principal de Cisco**



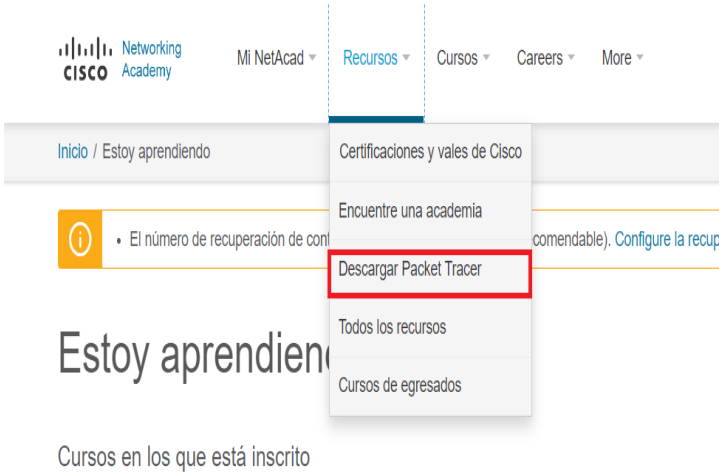
Fuente:Cisco. Pagina de inicio. Consultado el 8 de mayo. Recuperado de https://www.netacad.com/portal/learning.

- Paso No. 3: En el apartado de recursos ingresaremos a la opción que indica Descargar *Packet Tracert*.

Al ingresar en este apartado figura 37 podremos visualizar varias opciones, de las cuales encontramos información sobre el simulador y para que cursos nos podría ayudar. De igual forma nos recomienda realizar unos cursos

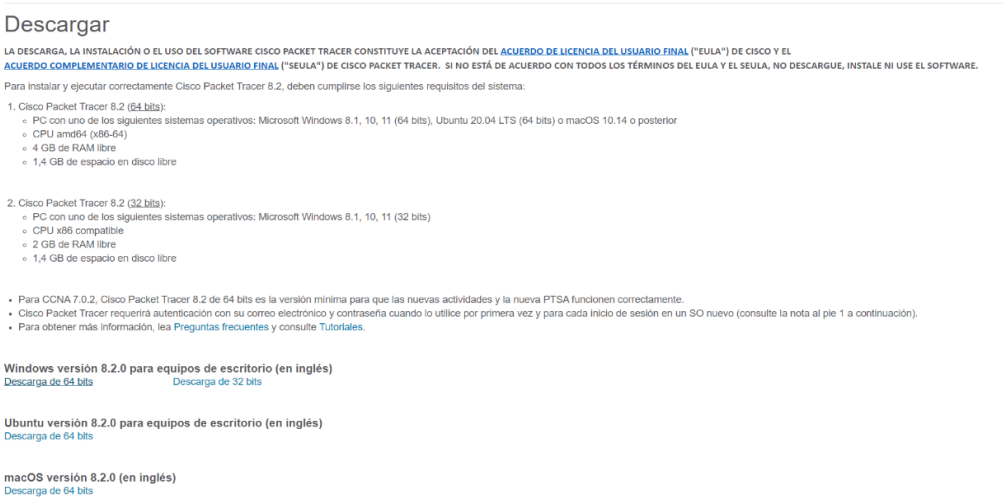
para tener el máximo provecho de la herramienta y por último nos indica que requerimientos se necesitan para la instalación.

Figura 37. **Descarga de simulador Packet Tracert**



Fuente: Cisco. *Recursos.* Consultado el 10 de mayo de 2022. Recuperado de https://www.netacad.com/portal/learning.

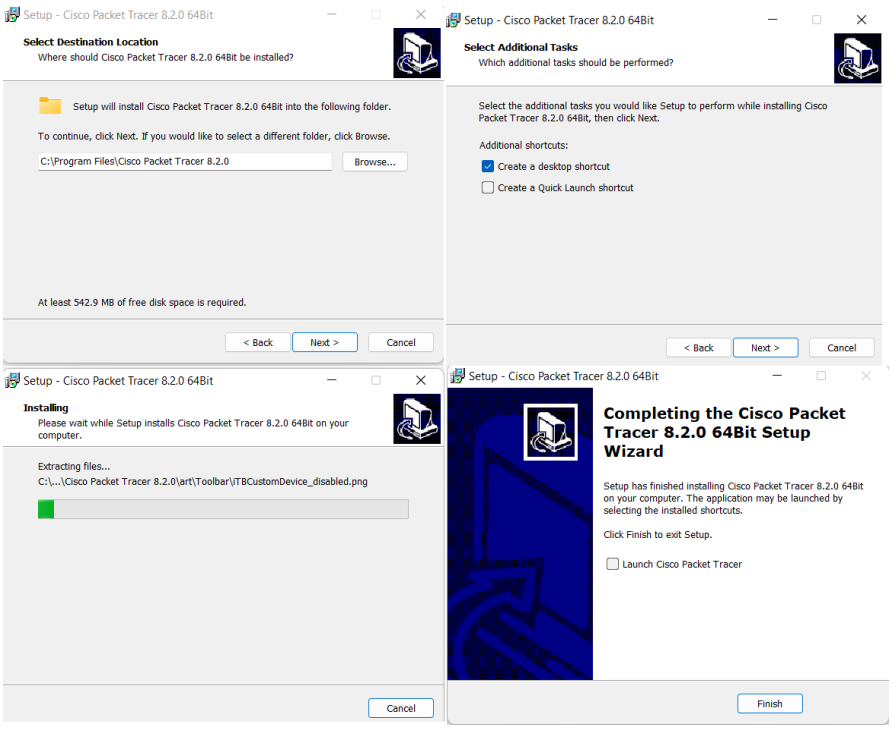
Figura 38. **Requerimientos de software para instalación**



Fuente: Cisco. *Cisco packet tracert.* Consultado el 10 de mayo 2022. Recuperado de https://www.netacad.com/portal/resources/packet-tracer.

- Paso No.4: Para la instalación se debe de seguir los pasos.
    - Aceptamos los acuerdos de licencia
    - Colocamos la ubicación en la cual se instalará el simulador o bien dejamos la ubicación por defecto
    - Decidimos si queremos acceso rápido en nuestro escritorio
    - Esperamos que finalice la instalación
    - Damos finalizar y listo ya tendríamos instalado nuestro simulador.

Figura 39. **Proceso de instalación**



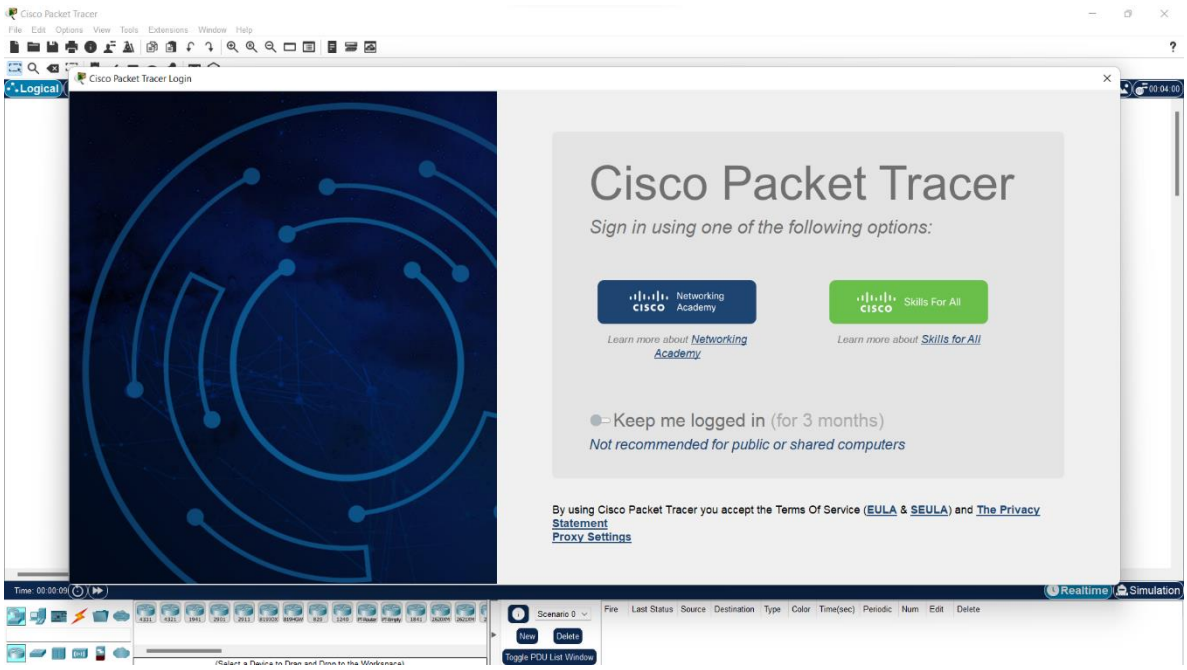
Fuente: elaboración propia, realizado con cisco *packet tracert*.

2.2. Introducción a Simulador Cisco Packet Tracert

Como hemos logrado la descarga e instalador de nuestro simulador avanzaremos al siguiente paso el cual consta de conocer nuestra herramienta y también saber cómo utilizarla, esto nos ayudara a mejorar en la programación hacia los equipos ya que se tiene un buen porcentaje de similitud con la programación en equipos reales.

Como dato importante debemos tener conocimiento que este simulador no remplazara la práctica de enrutadores, conmutadores, firewalls y servidores, ofrece muchos beneficios.

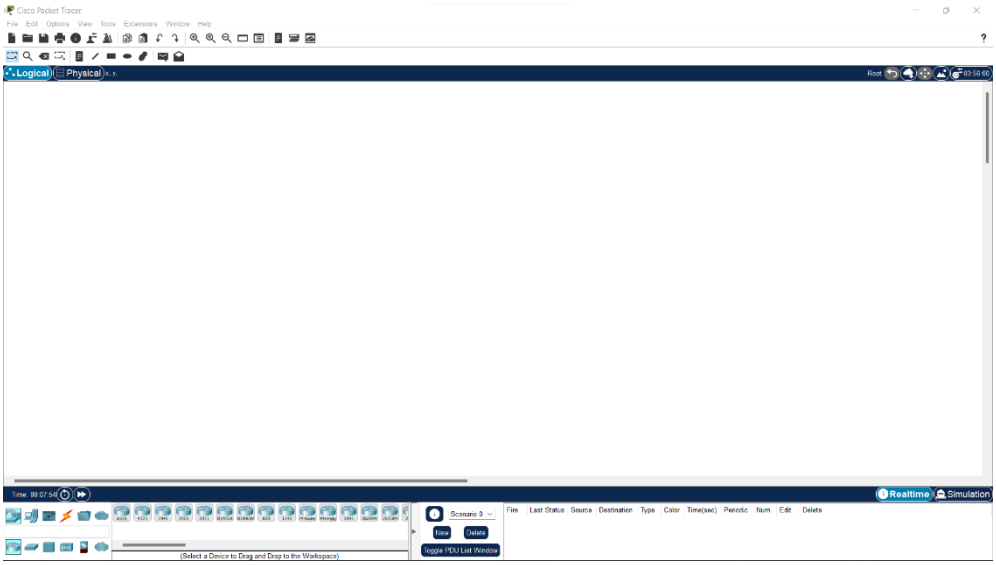
Figura 40. **Página de ingreso a simulador**



Fuente: elaboracion propia, realizado con cisco packet tracert.

Como podemos observar en la imagen anterior al abrir nuestro simulador nos solicita que ingresemos con una de las dos opciones mostradas, usaremos el ingreso por medio de *Networking Academy*, debemos ingresar nuestros datos de usuario de la plataforma www.netcad.com, con lo cual nos otorgara el acceso a la pantalla de configuraciones.

Figura 41. **Página principal de simulador Packet Tracert**



Fuente: elaboración propia, realizado con cisco *packet tracert*.

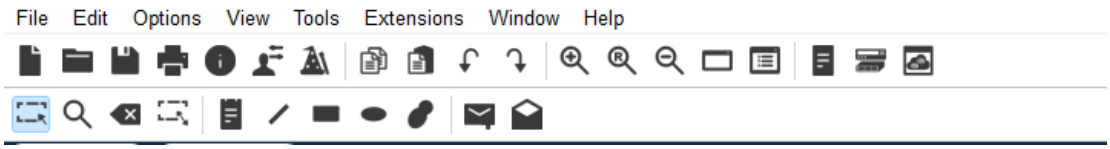
2.2.1. Menú de simulador Cisco Packet Tracert.

La herramienta a utilizar cuenta con 3 menús o barra de opciones en las que se puede realizar configuraciones, como vemos la pantalla de nuestro simulador, en las primeras opciones podemos realizar configuraciones sobre como guardar el archivo realizado, abrir archivos, ver etiquetas del dispositivo, seleccionar auto guardado, entre otros.

En la segunda barra de opciones podres realizar configuraciones sobre la pantalla en la cual colocaremos nuestros dispositivos, crear un nuevo archivo, ampliar la imagen, disminuir la imagen guardar avances, copiar algún dispositivo, entre otros.

En la tercera barra de opciones encontraremos las herramientas para modificar la red que hemos creado, como seleccionar un dispositivo, eliminar dispositivos.

Figura 42. **Barra de Opciones**



Fuente: elaboración propia, realizado con cisco *packet tracert.*

No se entrará mayor detalle en estos menús ya que este documento se especializa en las configuraciones de dispositivos, como se ha mencionado con anterioridad se puede ingresar a los cursos de la plataforma cisco para tener mayor documentación e información.

2.2.2. Tipos de vistas de configuración

Para esta parte contamos con dos formas de visualizar nuestros diagramas uno es la vista lógica y el segundo es la vista física, para cambiar de una vista a otra nos dirigiremos a la parte superior en el recuadro azul.

Figura 43. **Barra de cambio de vista**

Fuente: elaboración propia, realizado con cisco packet tracert.

La única diferencia que encontraremos en estas dos opciones es la forma de ver nuestro diagrama ya que para la realizar alguna configuración en los equipos de realizará de la misma manera.

Cada vista tiene sus propias opciones como por ejemplo para colocar más Racks opción de agregar o mover componentes, escala a la cual deseamos ver los equipos entre otras opciones que como ya se ha mencionado no se tendrá mayor detalle de ello.

Figura 44. **Vista física y vista lógica**

Fuente: elaboración propia, realizado con cisco *packet tracert*.

2.2.3. Guía de componentes y forma de simulación

En la parte inferior nos encontraremos con los componentes que tendremos disponibles como por ejemplo se cuenta con:

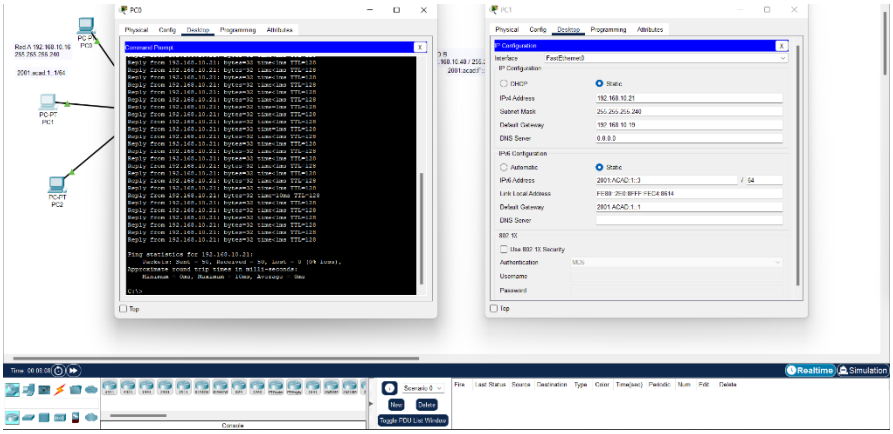
- Dispositivos de red: *Router*, *switch*, *hubs*, dispositivos wifi, dispositivos de seguridad, emulador de red *WAN*, entre otros.
- Dispositivos finales: *PC*, *laptop*, cámaras, dispositivos industriales, entre otros.
- Componentes: Actuadores, Tarjetas de redes, sensores, entre otros.
- Conexiones: Diferentes tipos de cables (directos, cruzados, seriales, de fibra, coaxial, entre otros).

Figura 45. **Menú de componentes**

Fuente: elaboración propia, realizado con cisco packet tracert.

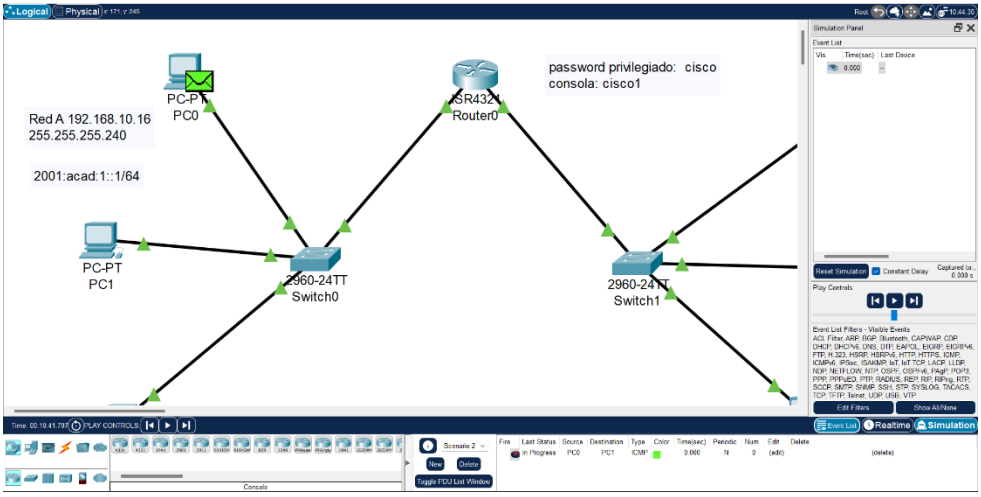
Para la simulación se cuenta con dos opciones una es en tiempo real y la otra forma es en simulación, la primera no podremos ver el viaje del paquete desde su origen hacia su destino a diferencia de la forma de simulación, en la cual podremos seguir el trayecto de nuestro paquete. Esta opción se encuentra en la parte inferior derecha.

Figura 46. **Simulación en modo Real Time**



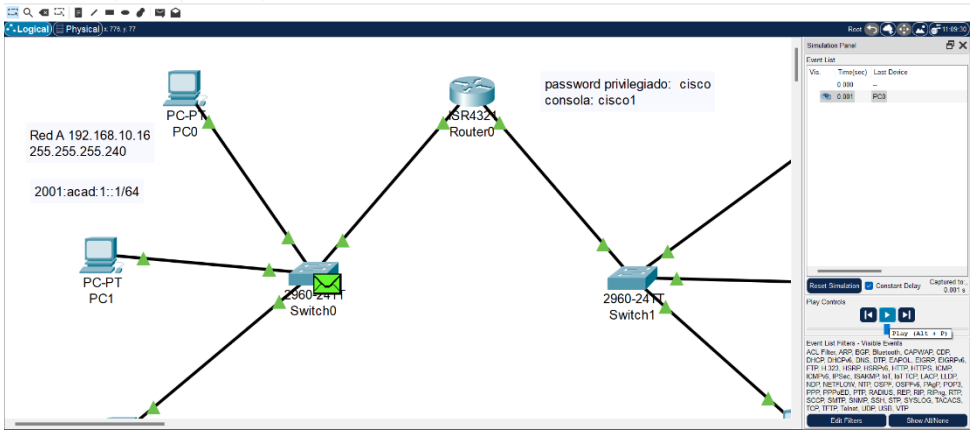
Fuente: elaboración propia, realizado con cisco *packet tracert*.

Figura 47. **Simulación desde su origen**



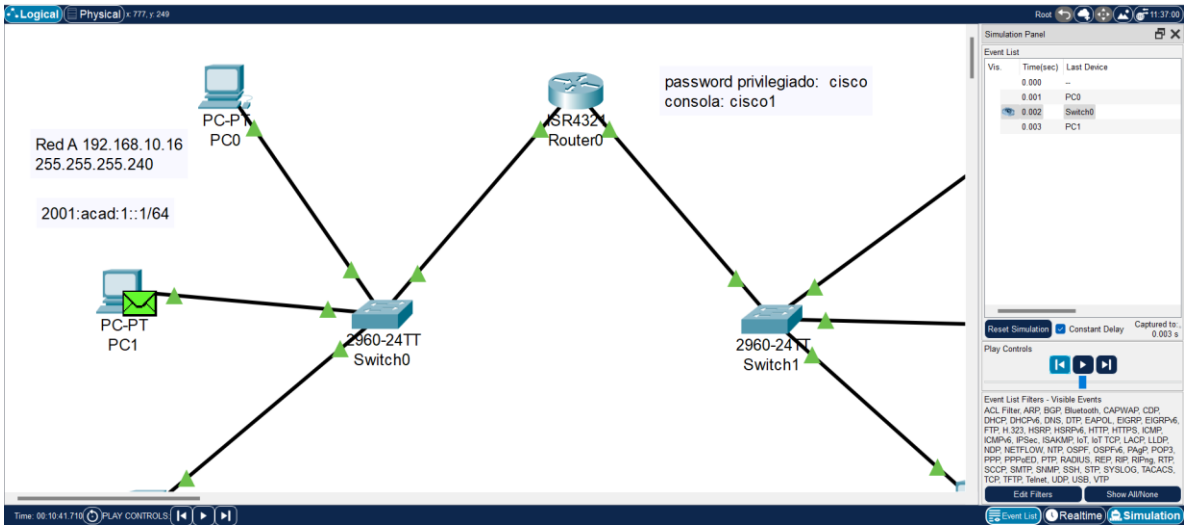
Fuente: elaboración propia, realizado con cisco *packet tracert*.

Figura 48. **Enrutamiento del mensaje hacia su destino**



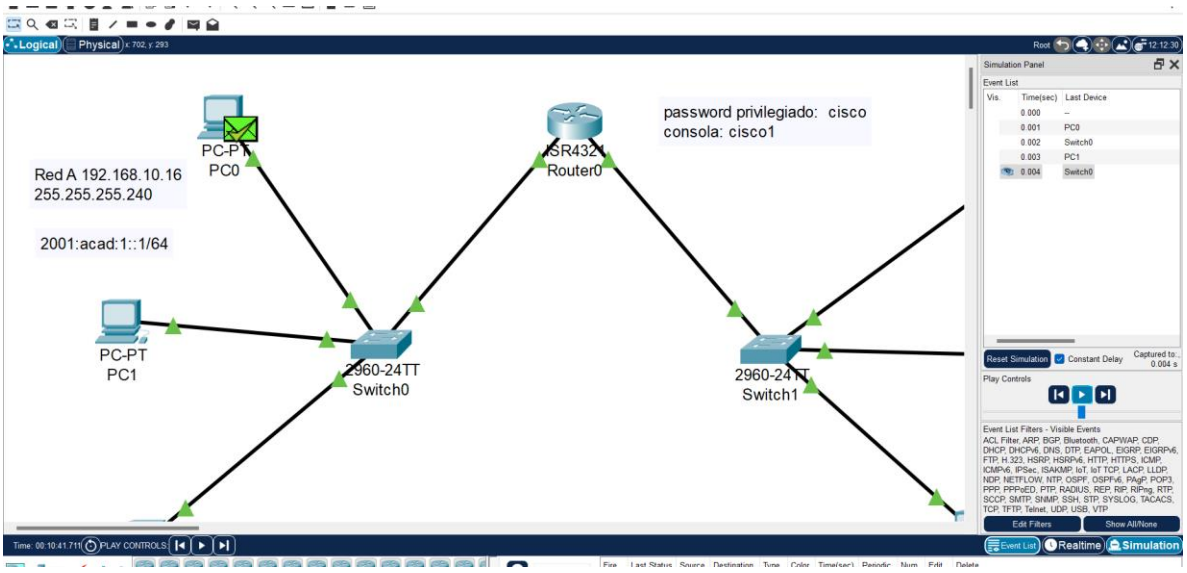
Fuente: elaboración propia, realizado con cisco *packet tracert*.

Figura 49. **Recepción del mensaje y envió de respuesta**



Fuente: elaboración propia, realizado con cisco packet tracert.

Figura 50. **Respuesta del mensaje, finalización de ciclo**



Fuente: elaboración propia, realizado con cisco packet tracert.

El ejemplo visto anteriormente se realizó en modo simulación en el cual se tomó de la 3er barra de menús de la parte superior la figura de un sobre con el signo más y se da clic primero en el dispositivo que será el origen y dando un segundo clic en el dispositivo que será el destino; luego en la parte derecha podemos ver un recuadro en el cual se presionará *play* o *next step*, para poder observar el recorrido de nuestro paquete.

2.3. Introducción a conexiones y configuraciones entre dispositivos

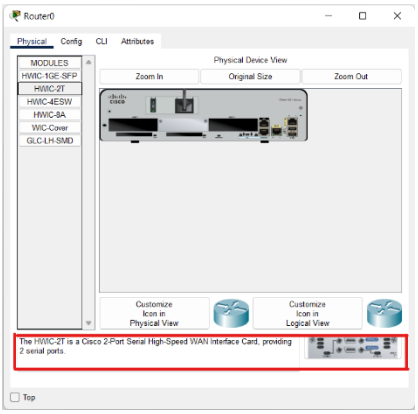
Ya que hemos visto cómo funciona nuestra herramienta de trabajo es momento de realizar conexiones para las cuales se cuenta con una gama muy amplia de dispositivo y cables para su conexión, en este capítulo se detallará la forma de cambio de tarjetas de los dispositivos como por ejemplo colocar tarjeta Wifi a una *laptop* o bien una tarjeta de entradas seriales a un *router*.

Se explicará también los diferentes tipos de cableado que existen para los dispositivos así también como su función esto para la realización de conexiones de manera física, ya que con el simulador se podrá evidenciar que se pueden utilizar los mismos cables para distintas conexiones.

2.3.1. Cambio de tarjetas en dispositivos

Una vez tengamos seleccionados los dispositivos a utilizar podremos cambiar las tarjetas para las diferentes conexiones, en cada dispositivo se encontrarán en el *GUI*, para acceder a esta debemos dar un clic sobre nuestro componente, al realizar este paso se abrirá una ventana nueva la cual contara con tres opciones (*PHYSICAL, CONFIG, CLI, ATTRIBUTES*), por lo cual necesitamos estar en la primer pestaña *Physical* y de lado izquierdo encontraremos las tarjetas que nos permite agregar a nuestro dispositivo, y en la parte inferior nos dará una breve descripción de la tarjeta así también como una imagen de cómo es físicamente la tarjeta.

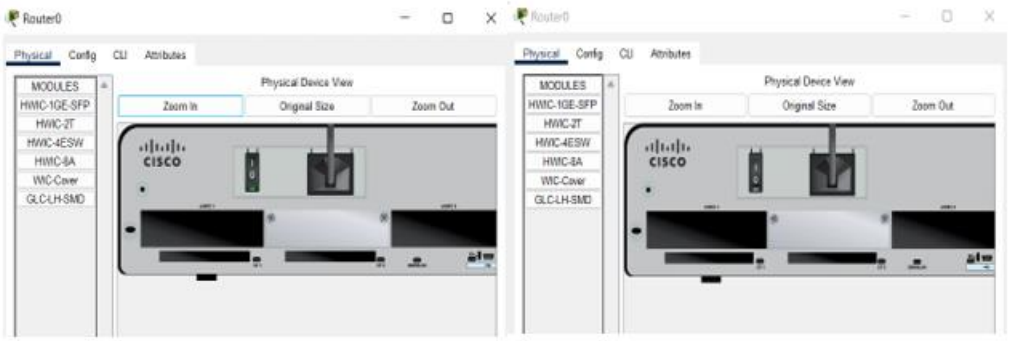
Figura 51. **Ventana de configuración de dispositivos**



Fuente: elaboración propia, realizado con cisco packet tracert.

Al seleccionar la tarjeta que utilizaremos debemos apagar nuestro equipo podemos dar en el botón de *ZOOM IN* para agrandar la imagen y encontraremos este botón en cada componente el botón puede estar en diferente parte, cuando el indicador está en verde es porque nuestro equipo se encuneta encendido, y al apagarlo se tornara en un color gris.

Figura 52. **Apagado de equipos**

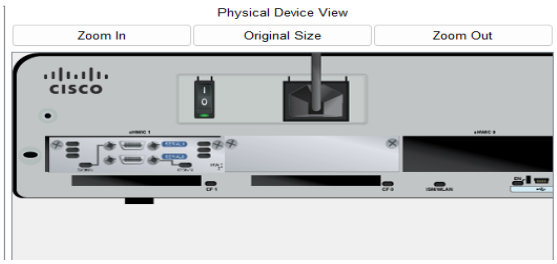


Fuente: elaboración propia, realizado con cisco packet tracert.

Como último paso es arrastrar la tarjeta deseada hacia las terminales vacías de nuestro componente, una vez colocado se procede a encender nuevamente el dispositivo.

En algunos dispositivos trae instalada una tarjeta por defecto para estos casos solo debemos quitarla antes de colocar la nueva, esto igualmente se realiza con el dispositivo apagado, se toma la tarjeta por defecto y se arrastra hacia el lado izquierdo lo cual dejara el terminal vacío para la colocación de la nueva tarjeta.

Figura 53. **Tarjeta instalada**



Fuente: elaboración propia, realizado con cisco packet tracert.

2.3.2. Cables más utilizados en conexiones de redes

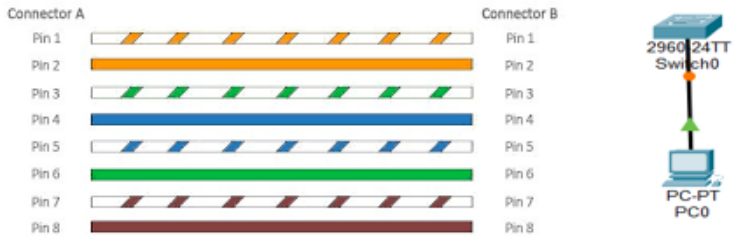
En las conexiones de redes contamos con diferentes tipos de cables en este capítulo daremos a conoces las más utilizadas para la intercomunicación de los dispositivos de red.

2.3.2.1. Cable LAN directo

Este tipo de cable está conformado por un cable *Ethernet* que tiene la misma configuración de sus hilos tanto en el lado a como en el lado b, mayormente es utilizado para conexiones de diferentes dispositivos como por ejemplo de *router* a *switch* o de *switch* a pc.

En el simulador lo podemos encontrar como el cable de color negro continuo, regularmente conectado a las entradas *FastEthernet*.

Figura 54. **Configuración y conexión de cable directo**



Fuente: Nuevos soportes tecnológicos. Cable directo o cruzado. Consultado el 28 de mayo de 2022. Recuperado de https://www.gruponst.es/cable-directo-cruzado/.

2.3.2.2. Cable LAN Cruzado

Este cable al igual que el anterior se compone con igualmente que el anterior por un cable Ethernet con la diferencia que este no es idéntico en sus extremos ya que cambia algunos hilos de su posición en el punto A hacia el punto B. Es utilizado para la conexión de dispositivos similares como ejemplo de *router* a *router* o bien de pc a pc.

En nuestro simulador lo encontraremos como un cable de color negro sin embargo este será intermitente.

Figura 55. **Configuración y conexión de cable cruzado**

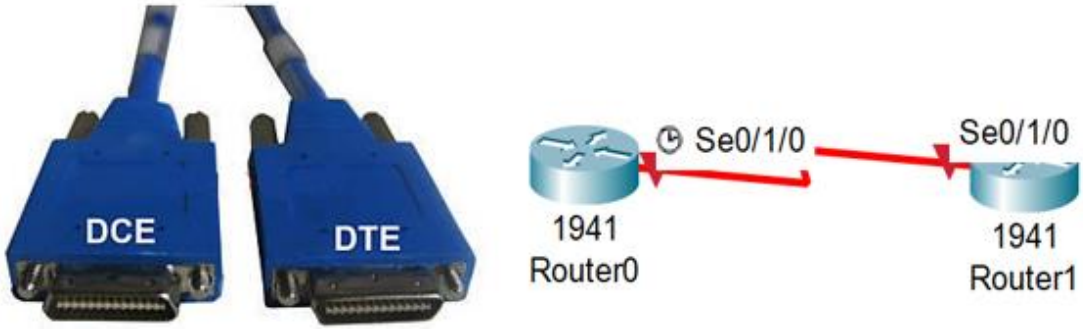
Fuente:Nuevos soportes tecnologicos. *Cable directo o cruzado*. Consultado el 28 de mayo de 2022. Recuperado de https://www.gruponst.es/cable-directo-cruzado/.

2.3.2.3. Cable serial DCE y DTE

Estos cables como su nombre lo indica son de tipo serial siendo el DCE, Equipo de Comunicaciones de Datos (el equipo que trasmite) y DTE es por Equipo Terminal de Datos (el equipo que recibe), para su configuración estos cuentan con él envió de datos mediante una secuencia de reloj. Al igual que el cable cruzado lo solemos utilizar para conectar dispositivos similares en especial conexión de *router* a *router*.

En nuestro simulador encontramos estos cables de color rojo y al momento de conectarlos aparecerá un símbolo de reloj a la par del nombre de la entrada de nuestro dispositivo con el cual sabremos que este será el DCE.

Figura 56. **Serial DCE y DTE, conexión en simulador**



Fuente: ¿Qué es un cable DCE? *Consultado el 28 de mayo de 2022. Recuperado de* Huawei. https://forum.huawei.com/enterprise/es/%C2%BFqu%C3%A9-es-un-cable-dce/thread/1029054-100237.

2.3.2.4. Cable de consola

Es el cable que nos permite configura nuestros dispositivos de red desde nuestra computadora, estos en un extremo son de entrada *USB* y en su según extremo son de entrada RJ-45, esto de manera fisca. Ya que hay que seguir una serie de pasos para establecer esta comunicación lo cual se detallara más adelante.

La forma en el que podemos encontrar estos cables en nuestro simulador es sencilla ya que es un cable de color celeste, y la forma de conexión es en la *PC* se debe seleccionar la entrada RS232 y en nuestro dispositivo de red a configurar se debe seleccionar la entrada de consola. Como se mencionó anteriormente más adelante se enseñará como configurar los dispositivos también en el simulador, pero desde cable de consola ya que no es muy necesario en el simulador.

Figura 57. **Conexión por cable de consola**

Fuente: Amazone. *Cable de consola USB a RJ45*. Consultado el 1 de septiembre de 2022. Recuperado de https://www.amazon.com/-/es/consola-accesorio-esencial-Ubiquity-Switches/dp/B01AFNBC3K.

2.3.3. Configuraciones en interfaz de dispositivos

Como se pudo observar en las secciones anteriores se cuenta con una interfaz para la configuración de los dispositivos en la cual podemos realizar cambios de tarjetas, pero también en este gestor se puede realizar cambio de direcciones *IP*, configuraciones de equipos, ingresar a la consola, entre otros.

Por lo que en esta sección se detallarán las opciones que utilizaremos para este proyecto de tesis, por lo que no se realizarán algunas opciones.

2.3.3.1. Cambio de dirección IP

Esta opción es más utilizada en las configuraciones propias de la *PC* para cuando no contamos con un servidor *DHCP* que nos otorgue una dirección *IP* de forma remota y sea el operador el que debe realizar el ingreso de forma manual. Para esta configuración explicaremos como realizarla en el simulador.

Para realizar este proceso en *Packet Tracert* debemos dar *click* en la PC a configurar y nos dirigiremos a la opción *DESKTOP*, seguido de eso ingresaremos en *IP CONFIGURATION*, una vez ingresemos nos aparecerá en la ventana una venta en la cual estará por seleccionada la opción *STATIC*, solo debemos llenar los espacios en blanco.

- *IPv4 Address*: Acá colocamos el número de *IP* de versión 4 que deseamos que tenga nuestra computadora.

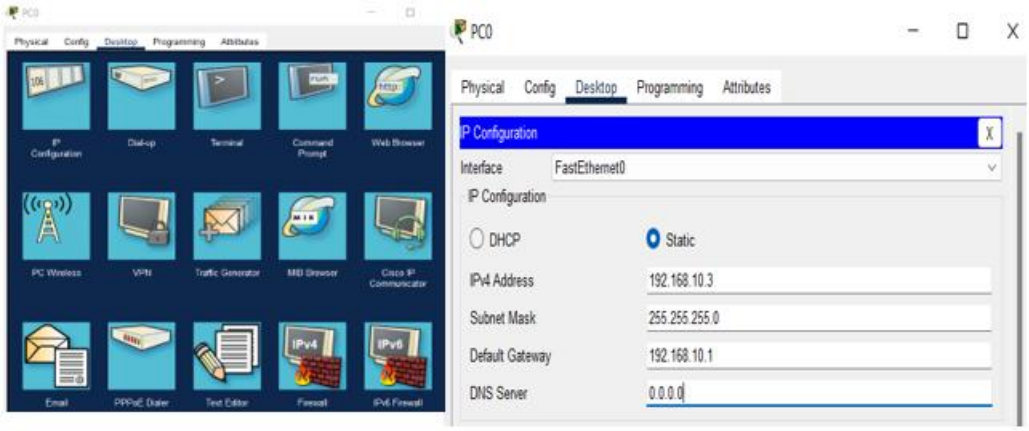
- *Subnet Mask*: Se debe colocar la máscara de subred a la cual parece nuestra dirección *IP*, en el siguiente capítulo se detallarán estos conceptos.

- *Gateway default*: Ingresamos la dirección IP de nuestro *Router* al cual está ligado nuestra *PC*.

- *DNS server*: Si contamos con esta dirección la colocamos ya que para el simulador no es muy necesaria.

Ingresando estos datos nuestra *PC* ya cuenta con su dirección *IP* para realizar envió de paquetes, la otra opción que podemos seleccionar es por *DHCP*, en la cual colocará de manera automática la dirección *IP*.

Figura 58. **Configuración de dirección IP en simulador**

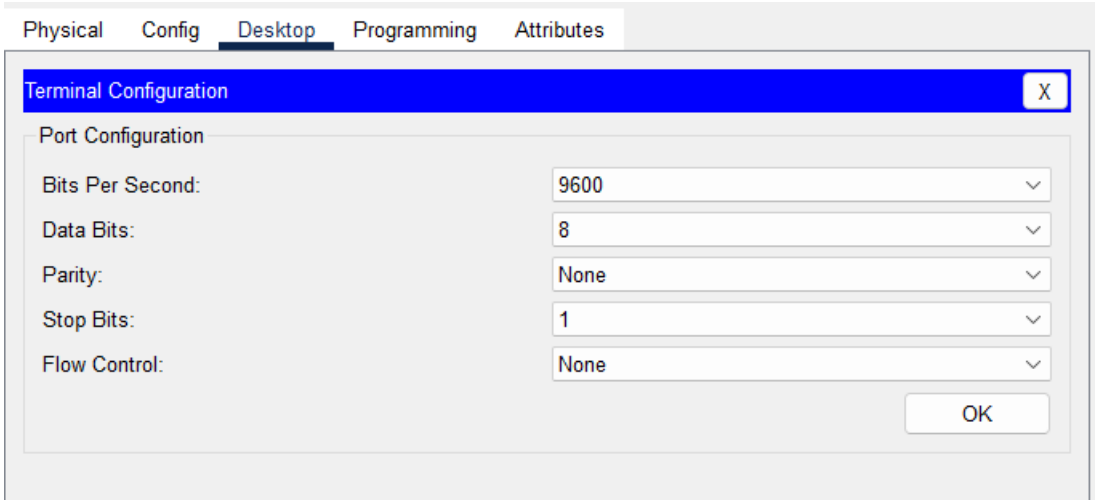


Fuente: elaboración propia, realizado con cisco packet tracert.

Configuración de equipos por medio de cable de consola: Como se demostró en el inciso anterior podemos ingresar desde nuestra *PC* hacia los dispositivos de red para lograr configurarlos, esto ya que al realizar la configuración en la vida real es de esta manera como se debe realizar.

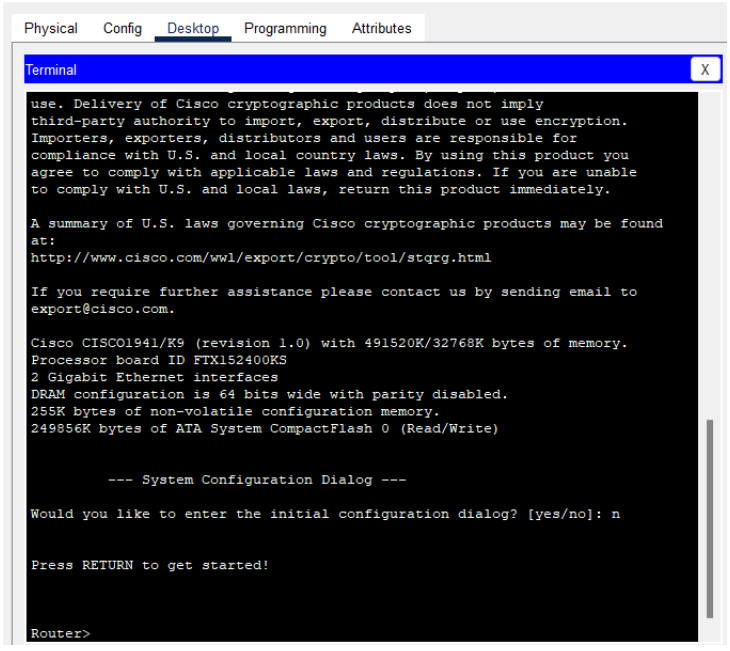
En nuestro simulador debe estar conectada la PC con el dispositivo de red a configurar e ingresaremos en la opción *DESKTOP*, seguido nos posicionaremos en el apartado *TERMINAL*, en este caso ya estará configurado por defecto los datos, estos son los mismos datos que utilizaríamos en una conexión con equipos reales ya sea por medio de una aplicación como por ejemplo PuttY entre otras. Por último, presionamos *OK* para tener acceso a nuestro dispositivo.

Figura 59. **Configuración por cable de consola**



Fuente elaboración propia, realizado con cisco packet tracert.

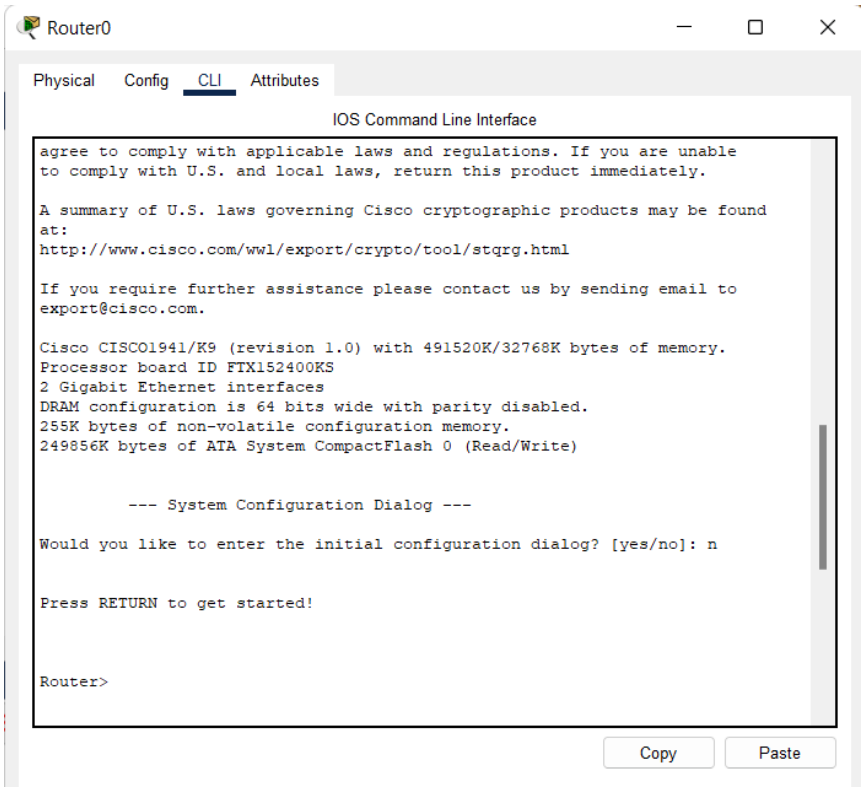
Figura 60. **Página principal de configuración de dispositivos de red**



Fuente: elaboración propia, realizado con cisco packet tracert.

Configuración por medio de *CLI*: Otra forma en la cual podemos configurar nuestros dispositivos es directamente en ellos sin necesidad de utilizar el cabe de consola y una *PC* (esto solo para el simulador), esto es posible por la configuración en *CLI*, para ello debemos dar un *click* sobre el dispositivo a configurar y dirigirnos a esta opción y ya tendremos acceso para realizar las configuraciones necesarias.

Figura 61. **Configuración por medio de CLI**



Fuente: elaboración propia, realizado con cisco packet tracert.

3. CONFIGURACIONES BÁSICAS DE DISPOSITIVOS CISCO

3.1. Modos y métodos de programación

Ya que tenemos el conocimiento, de cómo funciona la plataforma que utilizaremos para realizar prácticas sobre las configuraciones veremos los modos de configuración para los dispositivos los cuales se dividen en dos ramas: comandos directos y subcomandos, de los cuales cada uno admite sus propias configuraciones las cuales son:

- Modo EXEC de usuario
- Modo EXEC privilegiado
- Modo de configuración de línea
- Modo de configuración de interfaz

Para realizar estas configuraciones, existen varios métodos de ingreso al dispositivo, siendo esto los siguientes:

- Consola
- *Secure Shell* (SSH)
- Telnet

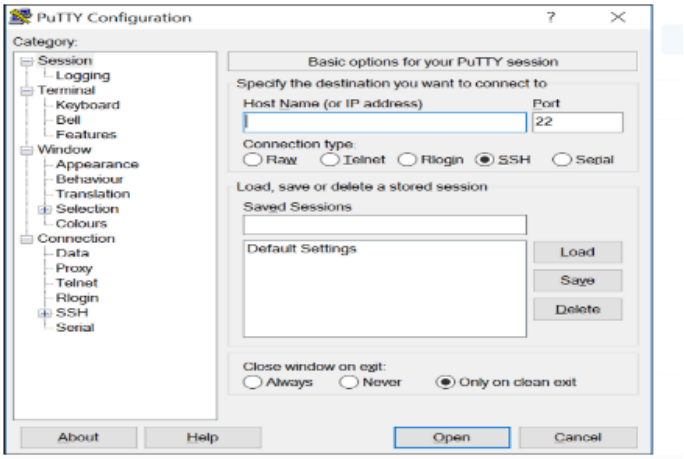
Existen también variedad de programas de emulación, con los cuales podemos realizar las configuraciones requeridas por cualquier medio, como ejemplo podemos mostrar las siguientes:

- PuTTY

- Tera Term
- SecureCRT

Entre otras, con estas podemos acceder de cualquiera de los tres métodos mencionados anteriormente, cabe destacar que para el método de consola es el único en el cual se utilizara cableado externo ya que este se realizará en conexión directa con el equipo, pero esto se detallara más adelante.

Figura 62. **Programa de emulación PuttY**



Fuente: elaboración propia, realizado con cisco packet tracert.

3.1.1. Métodos de programación

Como ya hemos mencionado se contará con tres métodos para la programación de los dispositivos cisco en este manual, sin embargo, el que más utilizaremos es por medio de consola, no obstante, se enseñara como se realizara la configuración para el acceso por medio de *Telnet y SSH*.

3.1.1.1. Consola

Este es el método más simple para la configuración de equipos, ya que solamente utiliza un puerto de administración físico, el cual proporciona acceso desde nuestra *PC* hacia el dispositivo a configurar. El canal utilizado es exclusivo que se utilizará con fines de mantenimiento o programación.

La ventaja sobresaliente de este método es que no necesitamos de servicios de red previamente configurados, ya que para ello solamente necesitaremos nuestro cable serial y un dispositivo con software para la emulación del terminal.

3.1.1.2. Secure Shell (SSH)

Este método se refiere a una conexión remota de manera segura a través de una interfaz virtual por medio de una red. Una diferencia de este método es que necesita servicios de red activos y una interfaz con una dirección ya configurada.

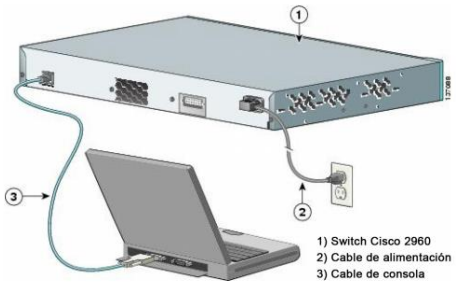
La mayoría de versiones de CISCO *IOS* incluyen un servidos *SSH* y un cliente *SSH* que son de utilidad para conexión hacia otros dispositivos.

3.1.1.3. Telnet

Al igual que el método *SSH*, este es un método de conexión remota sin embargo no es muy seguro en comparación al método anterior, esto se debe a que *TELNET* no proporciona conexión segura y encriptada y su forma de utilización es entorno a laboratorio.

Las contraseñas autenticación de usuario y los comandos se envían por medio de la red en forma de texto simple. CISCO *IOS* incluye un servidor *TELNET* y un cliente *TELNET*.

Figura 63. **Método de conexión por consola**



Fuente: Practicasuptxabraham. Acceso a un switch Cisco a través del puerto serie de consola. Consultado el 26 de septiembre de 2022. Recuperado de https://sites.google.com/site/practicasuptxabraham/2-1-establecimiento-de-una-sesion-de-consola-con-tera-term.

3.1.2. Modos de programación

Ya que sabemos cómo ingresaremos a nuestro dispositivo, es momento de saber en qué modo debemos realizar las configuraciones y sub-configuraciones para no tener errores en nuestros dispositivos o bien que no realicemos la configuración correcta.

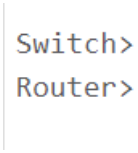
Cabe mencionar que para estas configuraciones se utilizara el *CLI*, para los modos principales se cuenta con dos formas o maneras.

3.1.2.1. Modos de comandos principales

Modo EXEC de usuario: Este cuenta con capacidades limitadas, su forma de uso es para configuraciones básicas, de igual forma utiliza una lista limitada de comandos de monitoreo, como nota importante en este modo no podremos realizar configuraciones de cambio para el dispositivo. A este modo se le conoce como un modo simplemente de visualización.

La forma de reconocer este modo es por el símbolo con que termina el nombre del dispositivo mostrado en el CLI >.

Figura 64. **Modo EXEC usuario**



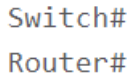
Fuente: elaboración propia, realizado con cisco packet tracert.

Modo EXEC privilegiado: Para la ejecución de comandos de configuración el técnico de redes debe acceder a este modo, ya que solamente se puede acceder a los modos de configuración global y modos más altos por medio de la ejecución privilegiada.

Con este modo podemos acceder a cualquier comando de monitoreo, ejecutar configuraciones y comandos de administrador.

Para reconocer que estemos en este modo lo podemos hacer por medio del símbolo que se encuentra seguido del nombre del dispositivo el cual es #.

Figura 65. **Modo EXEC privilegiado**



Fuente: elaboración propia, realizado con cisco packet tracert.

3.1.2.2. Modos de configuración y sub-configuración

Para la realización de las configuraciones de nuestro dispositivo debemos estar en el modo de EXEC privilegiado y de este punto acceder al modo de configuración global.

Modo de configuración global: Al ingresar en este modo podremos realizar configuraciones en el *CLI*, las cuales realizan cambios totales en la programación de nuestros dispositivos.

La forma de validar que nos encontramos en este modo es por la frase encerrada entre paréntesis *config*, seguido del símbolo de numeral que nos indica estar en el modo EXEC privilegiado. *Router*(config)#.

En este modo de configuración podemos acceder las sub-configuraciones, las cuales permiten la configuración de partes o funciones específicas del dispositivo IOS, los modos más comunes son:

Modo de configuración de línea: Es el modo utilizado para la realización de cambios en consola, *SSH, Telnet* o el acceso auxiliar, y su forma de visualización es la siguiente: Router(config-line) #.

Modo de configuración de interfaz: Es el modo que utilizamos para realizar las configuraciones de los puertos de nuestros dispositivos, la forma de visualización es la siguiente: *Router(config-if)*#.

Como podemos observar para cada configuración siempre se tiene en primer puesto el nombre de nuestro dispositivo, seguido la petición que realizaremos y por último el modo EXEC en el que nos encontramos

Tabla III. **Modos de configuración y sub-configuración**

Modo de configuración	**Ejemplo**
EXEC usuario	Router>
EXEC privilegiado	Router#
Global	Router(config)#
Configuración de línea	Switch(Config-line) #
Configuración de interfaz	Switch(config-if)#

Fuente: elaboración propia, realizado con Excel.

3.2. Navegación entre modos y estructura de comandos

Ya que conocemos los modos para la configuración de nuestros dispositivos debemos saber también como saltar de un modo a otro y viceversa, de igual manera conocer las estructuras para cada comando, teclas de acceso rápido, teclas para finalizar operaciones entre otros.

En este capítulo nos adentraremos en la estructura básica para posteriormente iniciar con las configuraciones básicas de nuestros dispositivos,

así también veremos las ayudas que nos brinda nuestro simulador, para el ingreso de comandos y comprobación de sintaxis.

3.2.1. Navegación entre modos IOS

Para poder realizar la configuración de los dispositivos debemos pasar entre modos y para ello se cuenta con una gama de comandos los cuales nos permiten ingresar y salir de los modos, cabe mencionar que se cuenta con un proceso de pasos para llegar a los modos de configuración más altos, ya que estos están de forma escalonada, siendo de la siguiente forma.

- Modo EXEC usuario.
- Modo EXEC privilegiado.
- Modo de configuración global.
- Modo de configuración de línea.
- Modo de configuración de interfaz.

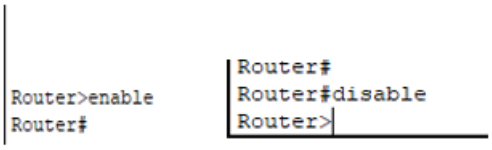
Para los modos de configuración de line y de interfaz se tienen en el mismo peldaño por lo que podemos acceder a cualquiera de ellos estando en el modo de c configuración global.

Nota: Para los comandos el simulador le es indiferente si la escritura es en mayúsculas o en minúsculas, exceptuando nombres de dispositivos o bien contraseñas.

También al inicio de nuestra configuración el equipo enviara un mensaje el cual debemos colocar la palaba no o en su defecto la letra n, con esto avanzaremos a las configuraciones.

Al ingresar a nuestro dispositivo siempre iniciaremos la configuración desde el modo EXEC usuario para pasar al siguiente modo utilizamos el comando *enable* y para regresar al modo EXEC usuario usamos el comando *disable.*

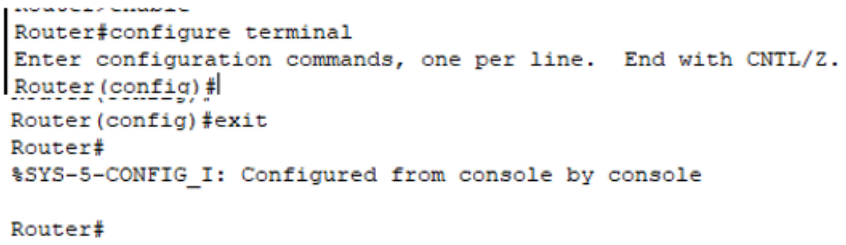
Figura 66. **Comandos de acceso y salida de modo EXEC usuario**



Fuente: elaboración propia, realizado con cisco packet tracert.

Estando en el Modo EXEC privilegiado podremos ingresar al modo de configuración global, para el ingreso utilizaremos el comando terminal, y para volver a nuestro modo de configuración EXEC privilegiado colocamos el comando *exit*.

Figura 67. **Comandos de acceso y salida de modo EXEC privilegiado**



Fuente: elaboración propia, realizado con cisco packet tracert.

Estando en el modo de configuración podremos ingresar a los modos de configuración de línea o interfaz.

Para los comandos de línea contamos con los accesos por medio de consola o bien las entradas virtuales (*VTY*), estas dependen de cada dispositivo con el número de entradas, las líneas virtuales son las que utilizaremos para el ingreso por medio de una dirección *IP* ya sea por telnet o bien por *SSH*.

Para acceder del modo de configuración global al modo configuración de línea, debemos colocare la frase line seguido si será consola *consol* o si será virtual *vty* y el número de la entrada, y para volver al modo de configuración global colocamos la palabra *exit*.

Figura 68. **Comandos de acceso y salida de configuración global a configuración de línea**

```
Router(config)#
Router(config)#line consol 0
Router(config-line)#
Router(config-line)#
Router(config-line)#exit
Router(config)#
Router(config)#
Router(config)#line vty 2
Router(config-line)#
Router(config-line)#
Router(config-line)#exit
Router(config)#
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Para los medios de configuración de interfaz se realizará de manera similar, ya que cada dispositivo cuenta con entradas distintas, las cuales pueden ser *FASTETHERNET, SERIAL, GIGABITETHERNET*, entre otras, por lo que los comandos a utilizar serían la frase interface seguido del nombre de la entrada seguido del numeral de la entrada, y para regresar al modo de configuración global se debe colocar la palabra *exit*.

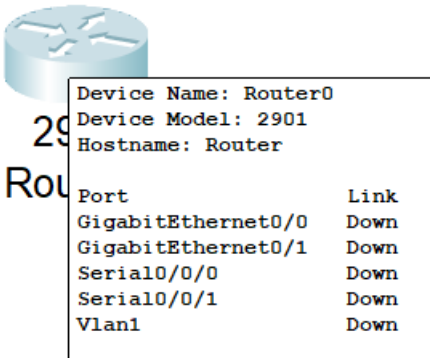
Figura 69. **Comando de acceso y salida de configuración de interfaz**

```
Router(config)#
Router(config)#interface gigabitethernet 0/1
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#exit
Router(config)#s
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Para saber que entradas posee nuestro dispositivo una manera fácil de verlo es posicionando nuestro mouse sobre el componente y nos dará un listado de las entradas que posee.

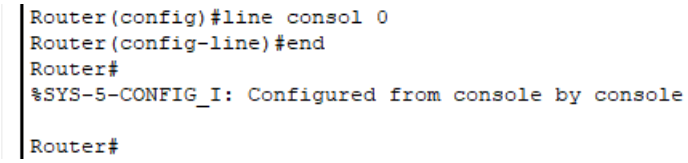
Figura 70. **Listado de entradas otorgado por el simulador**



Fuente elaboración propia, realizado con cisco packet tracert.

Si lo que queremos realizar es pasar de los sub-modos de configuración de línea o interfaz al modo EXEC privilegiado, solo debemos colocar la palabra *end* o presionando la combinación CTRL+Z

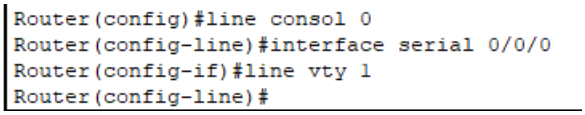
Figura 71. **Comando para salir de sub-modos de configuración a modo EXEC privilegiado**



Fuente: elaboración propia, realizado con cisco packet tracert.

Otro privilegio que podemos observar en estos sub-modos es que podemos pasar de un sub-modo a otro sin necesidad de salir de ellos solo colocando los comandos anteriormente mencionados

Figura 72. **Navegación entre sub-modos de configuración**



Fuente: elaboración propia, realizado con cisco packet tracert.

Tabla IV. **Comandos de navegación entre modos y sub-modos de configuración**

MODO DE CONFIGURACIÓN	ACCEDER	MODO ANTERIOR
EXEC usuario a EXEC privilegiado	enable	disable
EXEC privilegiado a configuración global	configure terminal	exit
configuración global a configuración de línea o interfaz	line consol # line vty # interface (tipo de entrada) #	exit
configuración de línea o interfaz a EXEC privilegiado		end ctrl+Z

Fuente: elaboración propia, realizado con Exel.

3.2.2. Estructura de comandos IOS

Para la configuración de nuestros dispositivos debemos conocer como está conformado nuestro comando en su sintaxis, con el fin de no tener problemas en nuestra configuración o que nuestro simulador nos genere advertencia de mala escritura, ya que contamos con esta ventaja puesto que al tener un error en nuestra sintaxis el simulador mostrara el siguiente mensaje.

Figura 73. **Mensaje de error en sintaxis**

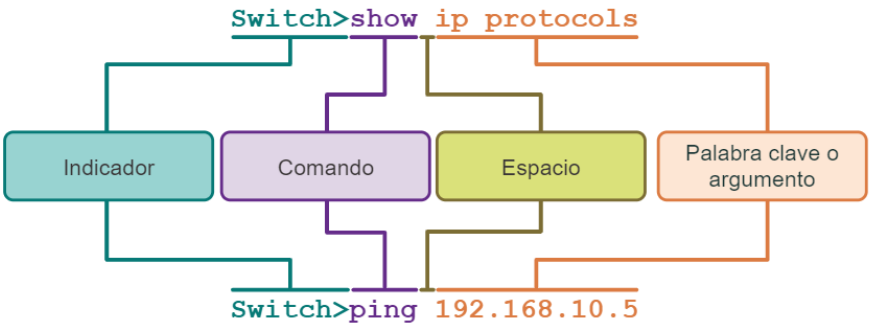
```
Router(config)#intrfce gigabitethernet 0/1
                 ^
% Invalid input detected at '^' marker.

Router(config)#
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Como podemos apreciar en el ejemplo, nos indica donde tenemos nuestro error marcado por el símbolo ^.

En la siguiente figura 74 se muestra cómo se conforma un comando en el simulador.

Figura 74. **Estructura de comandos**



Fuente: Cruz Kevin (2017). *La estructura de los comandos.* Consultado el 3 de octubre de 2022. Recuperado de https://kevin-linares.blogspot.com/2017/05/Configuracion-de-un-sistema-operativo-de-red-Entrenamiento-intensivo-sobre-IOS-La-estructura-de-los-comandos.html.

Como se puede apreciar se inicia siempre con el indicador este es el nombre de nuestro dispositivo a configurar y nos muestra el símbolo para reconocer en qué modo o sub-modo nos encontramos luego vine el comando

principal o el acceso que estemos solicitando y por último el argumento que deseamos en específico o la configuración especifica que estamos necesitando.

3.2.2.1. Sintaxis de comandos

En un mismo comando puede solicitar uno o más argumentos, sin embargo, estos cuentan con palabras claves las cueles se verán reflejadas por un patrón de formato único, Cisco otorga la siguiente tabla para verificar esta sintaxis de una manera más sencilla.

Tabla V. **Sintaxis de comandos**

Convención	Descripción
negrita	El texto en negrita indica los comandos y las palabras clave que ingresa literalmente como se muestra.
Cursiva	El texto en cursiva indica los argumentos para los cuales el usuario proporciona el valor.
[x]	Los corchetes indican un elemento opcional (palabra clave o argumento).
{x}	Las llaves indican un elemento obligatorio (palabra clave o argumento).
[x {y | z }]	Las llaves y las líneas verticales entre corchetes indican que se requiere dentro de un elemento opcional. Los espacios se utilizan para delinear claramente partes del comando.

Fuente: *Cisco. Comprobación de la sintaxis del comando de IOS.* Consultado el 5 de octubre de 2022. Recuperado de https://contenthub.netacad.com/itn-dl/2.3.2.

Como podemos observar se cuenta con varios tipos de formato los cuales especifican una acción diferente al momento de realizar nuestra programación.

Figura 75. **Ejemplo de sintaxis en simulador**

```
Switch(config-if)# switchport port-security aging { static | time time | type
{absolute | inactivity}}
```

Fuente: Cisco. *Comprobación de la sintaxis del comando de IOS.* Consultado el 5 de octubre de 2022. Recuperado de https://contenthub.netacad.com/itn-dl/2.3.2.

Adicional a ello cisco brinda en sus dispositivos una ayuda al momento que no tengamos claro algún comando o bien queramos visualizar las opciones de un comando, ¿esto lo podemos realizar colocando el inicio del comando que deseamos conocer seguido del símbolo ?, presionamos *enter* y nos dará una lista de los posibles argumentos a utilizar.

Figura 76. **Función de ayuda para configuraciones**

```
Router#show ?
  aaa                 Show AAA values
  access-lists        List access lists
  arp                 Arp table
  cdp                 CDP information
  class-map           Show QoS Class Map
  clock               Display the system clock
  controllers         Interface controllers status
  crypto              Encryption module
  debugging           State of each debugging option
  dhcp                Dynamic Host Configuration Protocol status
  dot11               IEEE 802.11 show information
  file                Show filesystem information
  flash:              display information about flash: file system
  flow                Flow information
  frame-relay         Frame-Relay information
  history             Display the session command history
  hosts               IP domain-name, lookup style, nameservers, and host
table
  interfaces          Interface status and configuration
  ip                  IP information
  ipv6                IPv6 information
  license             Show license information
  line                TTY line information
```

Fuente: elaboración propia, realizado con cisco packet tracert.

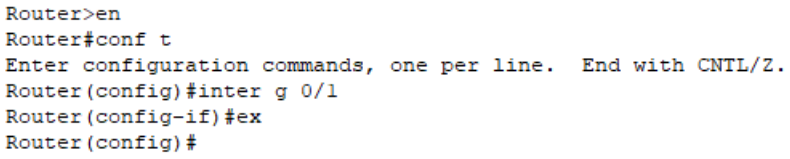
3.2.2.2. Teclas de acceso rápido y métodos de abreviación

El *CLI* no proporciona formas fáciles o accesos rápidos para la configuración de nuestros dispositivos.

Para la escritura nos permite colocar palabras abreviadas para que el IOS reconozca un comando complejo, como ejemplo podemos iniciar con el comando configure de forma abreviada podemos colocar *conf* que sería la abreviación de configure, sin embargo, se usan palabras claves ya que si la palabra con no sería reconocida ya que podrían existir otros comandos con esas iniciales.

De la misma forma para comandos con más de una frase ambas se pueden abreviarse como por ejemplo configure terminal, como ya se explicó anteriormente la abreviación de la primer palabra no es necesario escribir toda la segunda frase ya que ese comando es reconocido podemos colocar simplemente la letra t, otro ejemplo puede ser para las entradas de nuestros dispositivos, como sabemos los nombres de las entradas no se repiten, se puede colocar para *fastethernet* la letra f, para la entrada *gigabitethernet* la letra g, entre otros.

Figura 77. **Comandos abreviados**



Fuente: elaboración propia, realizado con cisco packet tracert.

Cisco otorga una tabla con las teclas que podemos utilizar para mejorar la sintaxis de nuestros comandos.

Tabla VI. **Teclas para mejorar la edición de línea de comandos**

Pulsación de teclas	Descripción
Tabulación	Completa una entrada de nombre de comando parcial.
Retroceso	Borra el carácter a la izquierda del cursor.
Ctrl+D	Borra el carácter donde está el cursor.
Ctrl+K	Borra todos los caracteres desde el cursor hasta el final de la línea de comandos.
Esc D	Borra todos los caracteres desde el cursor hasta el final de la palabra.
Ctrl+U o Ctrl+X	Borra todos los caracteres desde el cursor hasta el comienzo de la línea de comando
Ctrl+W	Borra la palabra a la izquierda del cursor.
Ctrl+A	Desplaza el cursor hacia el principio de la línea.
Flecha izquierda o Ctrl+B	Desplaza el cursor un carácter hacia la izquierda.
Esc B	Desplaza el cursor una palabra hacia la izquierda.
Esc F	Desplaza el cursor una palabra hacia la derecha.
Flecha derecha o Ctrl+F	Desplaza el cursor un carácter hacia la derecha.
Ctrl+E	Desplaza el cursor hasta el final de la línea de comandos.
Flecha arriba o Ctrl+P	Recupera los comandos en el búfer de historial, comenzando con la mayoría comandos recientes
Ctrl+R o Ctrl+I o Ctrl+L	Vuelve a mostrar el indicador del sistema y la línea de comando después de que se muestra un mensaje de consola recibido.

Continuación de tabla VI.

Ctrl-Shift-6	Secuencia de interrupción multipropósito utilizada para anular búsquedas DNS, traceroutes, pings, entre otros.

Fuente: Cisco. *Teclas de acceso rápido y métodos abreviados.* Consultado el 10 de octubre de 2022.Recuperado de https://contenthub.netacad.com/itn-dl/2.3.5.

Nota: Para devolver una configuración a su forma predeterminada solo debemos colocar no + comando normal.

3.3. Configuraciones básicas

Ya que tenemos conocimiento de la estructura de los comandos, navegación entre modos y sub-modos de configuración, estamos listos para iniciar con las configuraciones de nuestros dispositivos, las configuraciones básicas se pueden realizar en cualquier dispositivo y estas son las siguientes:

- Nombre de dispositivos.
- Contraseñas.
- Encriptación de contraseñas.
- *Banners*.
- Guardar configuraciones.

3.3.1. Nombre de dispositivo

Esta configuración es importante ya que al contar con demasiados dispositivos podremos darle una etiqueta especial a cada uno o bien especificar a que red pertenece, por ejemplo, un switch que pertenezca a la red de informática, podremos colocar el nombre SW-INFORMATICA, o bien si es el

cuarto *router* de la red de finanza se puede colocar R6_finanzas, entre otra opción es esto queda a discreción del técnico en redes.

- Para este nombre se debe seguir ciertas normas:

    - Comenzar con letra.
    - No debe contener espacios.
    - Finalizar con letra o en su defecto con número.
    - Se restringe el uso a solo letras, números y guiones.
    - La longitud no debe superar los 64 caracteres.

Esta configuración se realiza en el modo de configuración global, y el comando a utilizar es *hostname* + nombre que desee él técnico en redes.

Figura 78. **Cambio de nombre de dispositivos**

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-PRUEBA-1
SW-PRUEBA-1(config)#
```

Fuente: elaboración propia, realizado con cisco packet tracert.

3.3.2. Configuración de contraseñas

La seguridad es importante en redes, por tal razón debemos limitar el acceso a nuestros dispositivos, solamente a personal calificado.

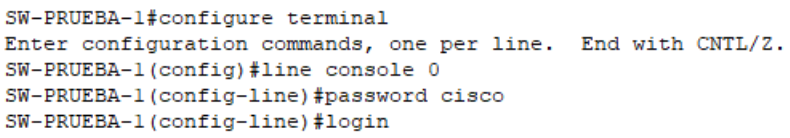
En nuestros dispositivos podemos restringir el acceso a los modos EXEC usuario y privilegiado de la misma forma a los accesos remotos. Para que nuestra contraseña sea efectiva debemos considerar los siguientes puntos:

- Contraseñas de 8 caracteres en adelante de longitud.
- Combinaciones entre mayúsculas y minúsculas, símbolos, números.
- Evitar utilizar la misma contraseña en los dispositivos.

Para la configuración de contraseña del modo EXEC usuario debemos seguir los siguientes pasos:

- Ingresar al modo de configuración global.
- Ingresar a sub-modo de configuración de línea.
- Colocar comando *password* + contraseña.
- Habilitar la contraseña con comando *login*.

Figura 79. **Configuración de contraseña para modo EXEC usuario**



Fuente: elaboración propia, realizado con cisco packet tracert.

Al momento de querer ingresar a nuestro dispositivo este solicitará la contraseña, cabe mencionar que al momento de escribirla en el *CLI* no aparecerá la contraseña que estamos escribiendo, pero si colocamos la contraseña correcta al presionar *enter* nos dará acceso

Para las líneas virtuales se realizan de la misma manera, ya que estas darán el acceso al modo EXEC usuario de manera remota, ya sea por acceso *telnet o ssh*.

Figura 80. **Configuración de contraseña líneas VTY**

```
SW-PRUEBA-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-PRUEBA-1(config)#line vty 0
SW-PRUEBA-1(config-line)#password cisco-vty
SW-PRUEBA-1(config-line)#login
SW-PRUEBA-1(config-line)#exit
```

Fuente: elaboración propia, realizado con cisco packet tracert.

En el aseguramiento de acceso al modo EXEC privilegiado se realiza de manera distinta por lo que se tiene los siguientes pasos:

- Ingresar al modo de configuración global.
- Colocar el comando *enable secret* + contraseña.

Como podemos ver en este no es necesario habilitar la contraseña, simplemente con escribir el comando ya quedara registrada

Figura 81. **Configuración de contraseña para modo EXEC privilegiado**

```
SW-PRUEBA-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-PRUEBA-1(config)#enable secret class
SW-PRUEBA-1(config)#

SW-PRUEBA-1>enable
Password:
Password:
SW-PRUEBA-1#
```

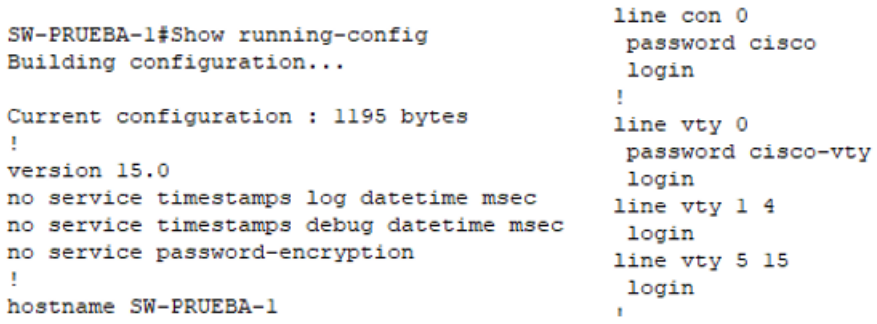
Fuente: elaboración propia, realizado con cisco packet tracert.

3.3.3. Encriptación de contraseñas

Ya que sabemos cómo ingresar contraseñas en nuestro dispositivo, debemos asegurarnos que no puedan ser descubiertas puesto que están en formato de texto, ya que de esta manera pueden ser descubiertas desde las memorias de nuestro dispositivo (memoria *RAM* o memoria *NVRAM*). Para comprobar que aún no hemos cifrado las contraseñas podemos verlo de la siguiente manera.

- Ingresar a modo EXEC privilegiado.
- Podemos acceder a la memoria volátil o a la memoria rom si ya hemos copiado los archivos (se verá en el inciso 3.3.5).
- Colocamos comando *show* + memoria.
    - Memoria RAM *running-config*.
    - Memoria NVRAM *startup*-config**.**
- Verificamos contraseñas.

Figura 82. **Revisión de estado de contraseñas**

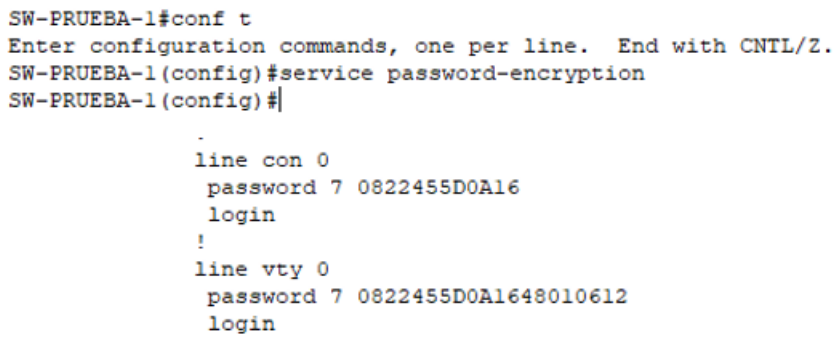


Fuente: elaboración propia, realizado con cisco packet tracert.

Esta encriptación aplica un cifrado débil a todas las contraseñas que no estén encriptadas, para este proceso se debe realizar:

- Ingreso a modo de configuración global.
- Colocar comando *service password-encription*.

Figura 83. **Configuración y verificación de contraseñas encriptadas**



Fuente: elaboración propia, realizado con cisco packet tracert.

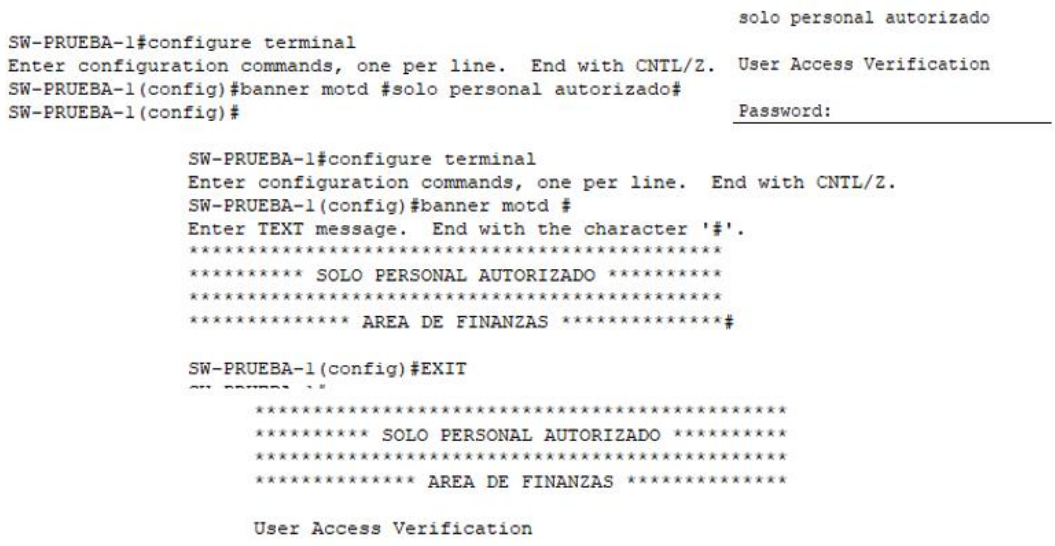
3.3.4. Banners o mensajes de aviso

Una forma de que solo el personal calificado realice cambios en los dispositivos son las contraseñas, pero cisco nos ofrece la opción de colocar un mensaje de aviso al tratar de acceder a nuestro dispositivo.

- Para la creación de este mensaje se debe seguir los pasos siguientes:

    - Ingresar al modo de configuración global.
    - Colocar comando *banner* motd.
    - El mensaje debe estar encerrado entre el símbolo de numeral #.

Figura 84. **Configuración de mensaje de aviso**



Fuente: elaboración propia, realizado con cisco packet tracert.

Nota: existe variedad de tipos de banners, ya sea para líneas *VTY*, para los modos EXEC, pero en este documento nos basaremos solamente al banner básico que nos dará el acceso por consola, *SSH o telnet.*

3.3.5. Guardar configuraciones

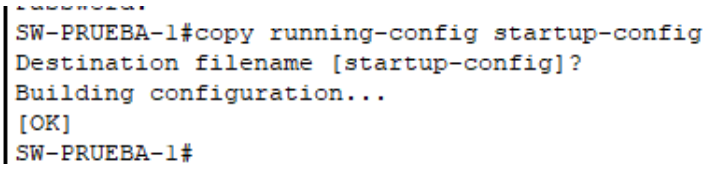
Ya que hemos realizado las configuraciones básicas de nuestro dispositivo es necesario guardar las configuraciones ya que de momento solo se han guardado en la memoria *RAM*, lo que significa que si apagamos el dispositivo estas configuraciones se perderán, por lo que debemos guardarlas en la memoria *NVRAM*.

Para el procedo de copiar la información de la memoria *RAM* a la memoria *NVRAM* es sencillo solo debemos seguir los siguientes pasos:

- Acceder al modo EXEC privilegiado.
- Colocar el comando *copy running*-config *startup*-config.
- Presionamos *enter* dos veces.

Con esto se ha copiado de manera exitosa nuestra información y estará segura, aunque se pierda la conexión eléctrica o bien apaguemos el dispositivo.

Figura 85. **Guardar información en memoria RAM**



Fuente: elaboración propia, realizado con cisco packet tracert.

Existe también una forma de borrar los datos de la *NVRAM*, si fuese necesario debemos realizarlo de la siguiente manera:

- Ingresar a modo EXEC privilegiado.
- Colocar el comando erase *startup*-config.
- Aceptamos presionando *enter* en el mensaje que nos brinda.
- Colocamos el comando *reload*.
- Aceptamos presionando *enter* en el mensaje que nos brinda.

Esto hará que se pierda la conexión del dispositivo por unos instantes, sin embargo, borrara por completo lo que este en la *NVRAM* hasta el momento.

3.4. Configuración de interfaces

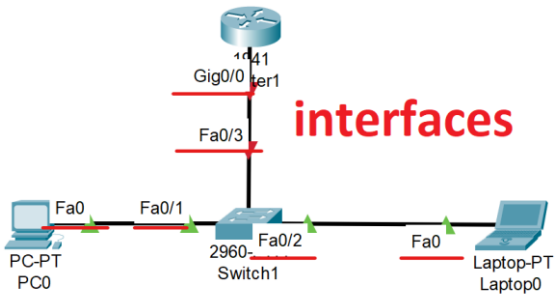
En este capítulo se iniciará con la configuración de las interfaces de nuestros dispositivos, como ya hemos aprendido como realizar las configuraciones básicas este sería el siguiente paso.

Las interfaces nos permiten conectar nuestros dispositivos ya sea *router*, switch, pc entre otros, mediante una dirección IP, cabe mencionar que al contar con esta dirección también se contara con una dirección MAC (dirección fisca). Contamos con diferentes interfaces como son:

- *GigabitEthernet*.
- *FastEthernet*.
- Seriales.

Para los switches se realizará en su interfaz virtual SVI se realizará de la misma manera que en un router como se detallará más adelante.

Figura 86. **Interfaces de una conexión LAN**



Fuente: elaboración propia, realizado con cisco packet tracert.

Cabe mencionar que las interfaces cambian dependiendo del modelo de nuestro dispositivo ya que algunos cuentan con interfaces Gigabit otros por el contrario pueden tener interfaces *Fast*, o en su defecto podemos cambial la tarjeta o añadirle una tarjeta que contenga interfaces seriales.

3.4.1. Configuración de interfaces de un Router

Para habilitar una interfaz debemos contar con la dirección *IP* que vamos a asignarle a nuestro componente, esta puede ser proporcionada por nuestro proveedor de red, asignarla de forma manual ya sea por división de subredes o bien por *VLSM*.

Es necesario seguir los siguientes pasos para la realización correcta de este tipo de configuraciones:

- Ingresar a modo de configuración global.
- Ingresar al tipo de interfaz a configurar.
- Colocar descripción de la interfaz (opcional), con el comando *description*.
- Agregamos el comando ip *address* + ip +mascara de subred (ipv4), ipv6 *address* + ip/prefix (ipv6).
- Activamos la interfaz con el comando no *shutdown*.

Figura 87. **Configuración de dirección IP en interfaz de router**

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g 0/0
Router(config-if)#description red-1
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Nota: En este documento se realizarán las configuraciones solamente con direccionamiento *IP* versión 4.

La parte de descripción es opcional, pero nos apoya cuando contamos con redes demasiado grandes, así también es una buena práctica para que el técnico de redes identifique cada red.

Como podemos observar al presionar *enter* esta configuración, si se ha realizado de manera correcta, nos brindara un mensaje indicándonos que la interfaz se encuentra operativa.

Con el comando show *ip* interface *brief*, podremos ver el estado de nuestras interfaces, es necesario encontrarnos en el modo EXEC privilegiado para colocar este comando.

Figura 88. **Visualización de estados de interfaces**

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     192.168.10.1    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Fuente: elaboración propia, realizado con cisco packet tracert.

La dirección que se ha colocado en el *router* servirá como puerta de enlace hacia otros componentes ya que por medio de él se podrán comunicar con redes distintas a esta dirección se lo conoce como *GATEWAY* PREDETERMINADO.

En el dispositivo siguiente se debe colocar esta dirección para que reconozca la red en la cual se encuentra y poder realizar el enrutamiento de paquetes, esto se detallara más adelante cuando se configura una red de más de una dirección de subred.

3.4.2. Configuración de dirección en Switch y host

Como se explicó en capitulo anterior al switch también se le puede otorgar una dirección IP, sin embargo, esto se realiza en las interfaces virtuales del dispositivo, ya que con ello podremos acceder al mismo de manera *Telnet o SSH*.

Para el ingreso de una dirección *IP* es similar que en un *router* solamente se agrega un paso extra que es colocar la *IP* del *Gateway* predeterminado, por lo tanto, esto se realiza de la siguiente manera:

- Ingresamos al modo de configuración global.
- Ingresamos a la *SVI* a configurar.

- Ingresamos el comando *description* (opcional).
- Ingresamos la ip con el comando ip *address* + ip + mascara de subred.
- Activamos nuestra interfaz con el comando no *shutdowm*.
- Regresamos al modo de configuración global.
- Ingresamos la dirección del *Gateway* predeterminado con el comando *ip defaul-gateway* + ip de *router*.

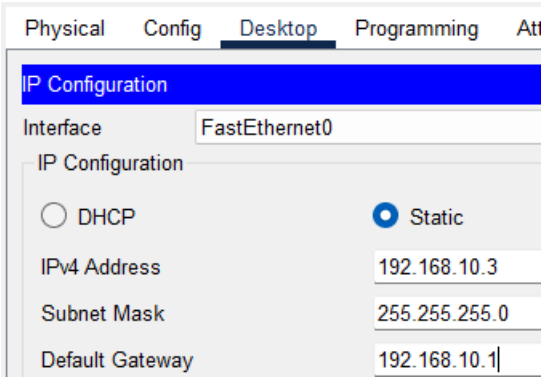
Figura 89. **Configuración de dirección IP en Switch**

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#description sw-1
Switch(config-if)#ip address 192.168.10.2 255.255.255.0
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.10.1
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Para el dispositivo final se puede agregar como se explica en el capítulo 1, ingresado los datos requeridos por nuestra tabla esto de ser ingreso de forma manual ya que esto se puede realizar de forma automática por medio de *DHCP*.

Figura 90. **Configuración de IP de forma manual en Host**



Fuente: elaboración propia, realizado con cisco packet tracert.

3.4.3. Comprobación de comunicación de red LAN

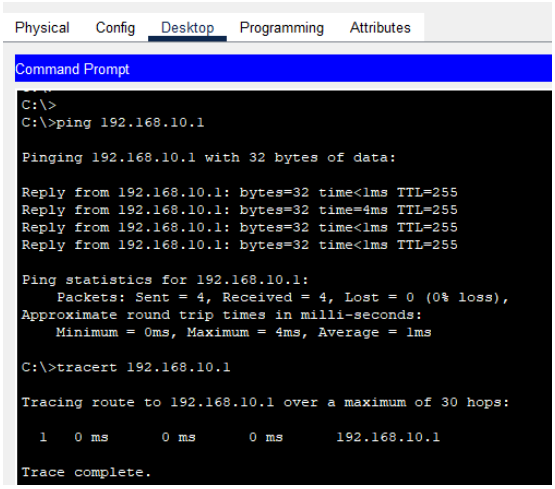
Una vez asignadas las direcciones *IP* en cada dispositivo podremos comprobar su conectividad, de una manera muy sencilla y con ello verificar que hemos realizado de manera correcta el direccionamiento *IP*.

Para la comprobación contamos con dos maneras de realizarlo esto siempre desde la terminal de nuestro host o en el modo EXEC privilegiado. Las pruebas son:

- *Ping*
- *Traceroute*

Ambas funcionan para comprobar la conectividad de nuestros dispositivos, sin embargo, la prueba *Traceroute*, nos muestra la serie de saltos hasta llegar a su destino, por lo cual esta es mejor al momento de contar en qué punto se pierde la conexión.

Figura 91. **Comprobación de conectividad**



Fuente: elaboración propia, realizado con cisco packet tracert.

Nota: Existen diferentes formas de realizar un ping, ya sea que nosotros propongamos el número de paquetes enviados, pings infinitos, entre otros. Esto varia de cada dispositivo que utilizamos es de validar cual es el comando ya sea servidor Windows, Linux o Mac. Lo mismo sucede con la prueba *traceroute.*

3.5. Segmentación de la red

Ya teniendo claros los fundamentos para configurar una dirección *IP*, debemos aprender a como realizar divisiones de una misma red, con el fin de optimizar al máximo la red que estemos configurando, puesto que esto nos puede ayudar al momento que necesitemos dividir un a red, siendo algunos casos: Fraccionamiento de host en un departamento, ampliaciones de redes entre otros.

Para la realización de esta segmentación debemos conocer los siguientes puntos:

- Estructura de la dirección IPv4.
- División por subredes de igual tamaño.
- División por *VLSM*.

3.5.1. Estructura de direcciones IPv4

Es la dirección que consta de 32 bits de la cual se compone la porción de red y una porción de *host*, esto se visualiza los bits del frente que no cambian son la porción de red y los bits finales los cuales cambian son la porción de red (*HOST*).

Esta red se divide en cuatro octetos (8 bits).

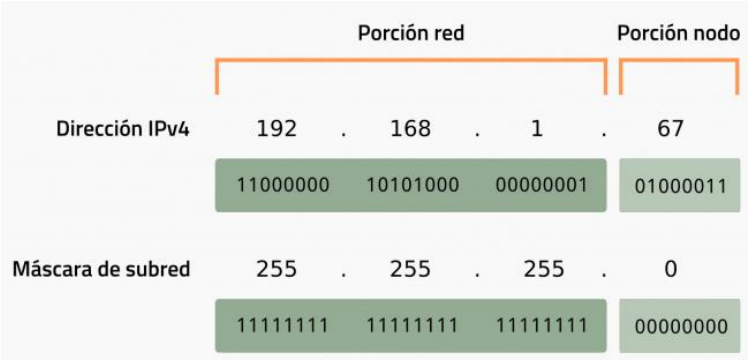
Figura 92. **Posiciones de red y Host IPv4**

Fuente: SilderPlayer. *Direccionamiento de la red IPv4.* Consultado el 28 de octubre de 2022. Recuperado de https://slideplayer.es/slide/5389710/.

Otra característica de estas redes es las máscaras de subred, que es la encargada de identificar la parte que será utilizada para la red y la porción

utilizada para los *host*, las cuales se dividen en cuatro espacios que van desde 0 a 255.

Figura 93. **Máscara de subred**

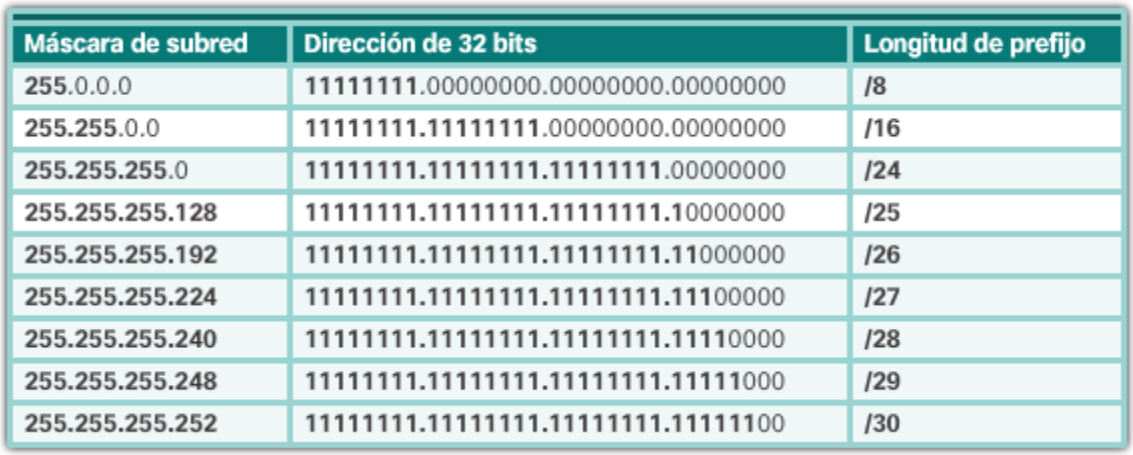


Fuente: AZadslZone. *Qué es y cómo conocer la máscara de subred en Windows.* Consultado el 20 de noviembre de 2022. Recuperado de https://www.adslzone.net/reportajes/internet/que-es-mascara-de-subred/.

Con lo que nos lleva al siguiente punto que es la longitud del prefijo, siendo este el número que se le otorga dependiendo de la máscara de subred y este podemos identificar fácilmente, puesto que es el número que sigue después del símbolo /.

Este número nos indica cuantos bits están llenos en la dirección de 32 bits y los que quedan con 0 son los que podremos utilizar para nuestros hosts.

Figura 94. **Tabla de prefijos de red**



Máscara de subred	Dirección de 32 bits	Longitud de prefijo
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Fuente: wordpress (2017). *La longiuitd de prefijo.* Consultado el 20 de noviembre de 2023. Recuperado de https://interpolados.wordpress.com/2017/03/26/la-longitud-de-prefijo/.

Ejemplo 3.5.1

Teniendo la siguiente red 192.168.10.0/29 identifique:

- Porción de red
- Porción de host
- Mascara de subred

Tabla VII. **Ejemplo de porciones de red**

	RED		**HOST**	
192	168	10	0	
11111111	11111111	11111111	11111000	/29

Fuente: elaboración propia, realizado con Excel.

Es importante aclara que en la elaboración de redes se cuenta con:

- Dirección de red.
- Dirección de broadcast.
- Primera dirección de host utilizable.
- Ultima dirección de host utilizable.

Dirección de red: Es la dirección que representa una red específica, si un dispositivo cumple los parámetros de esta red es considerado como perteneciente a la red

Por ejemplo, la dirección de red es 192.168.10.0/24 si un dispositivo conectado en su mismo dominio contiene la dirección 192.168.10.3/24 es considerado como parte de esa red ya que cumple con lo siguiente:

- Tiene la misma máscara de subred.
- Contiene la misma porción de red.
- Se encuentra en el dominio de la red.

Dirección de *Broadcast*: También conocido como dirección de difusión, es la que utilizamos cuando deseamos llegar a todos los dispositivos de una red IPv4, por lo regular es la última dirección de una red.

Por ejemplo, para la red 192.168.10.0/24 la dirección de *broadcast* es 192.168.10.255/24, esta no es necesario configurarla en los dispositivos ya que ellos lo toman por defecto, pero si debemos saber que no podremos asignarla a un *host*.

Direcciones de *Host*: Son las direccione que podemos colocar en los distintos dispositivos finales, para ello solamente debemos de quitar 2 direcciones de la red otorgará, la cual la primera será la dirección de red y la última para la dirección de broadcast.

Por ejemplo, para la red 192.168.10.0/24 sabemos que:

- Gracias al prefijo caemos en cuenta que contamos con el ultimo octeto como porción de host lo que significa que $2^8 = 256\,\text{direcciones}$ de las cuales inicia de 0 a 255.

- Quitamos la dirección de red y la dirección de *broadcast* 256 - 2 = 254 redes disponibles.

- Primera red utilizable 192.168.10.1/24 y la última dirección de red 192.168.10.254/24.

Ejemplo 3.5.2

Teniendo la red 192.168.20.0/29 encontrar*:*

- Dirección de *broadcast*.
- Dirección de red.
- Primera y última red utilizable.

Por el prefijo sabemos que tenemos 29 bits utilizados de red por lo que nos quedan 3 bits de host esto usando la fórmula de

$$32 - prefijo = \#\ de\ bits\ de\ host$$

Por lo tanto

$2^3 = 8\, redes$ de las cuales debemos quitar 2 nos quedarían 6 redes utilizables par hosts

Entonces:

- La dirección de red es 192.168.20.0/29
- La dirección de broadcast 192.168.20.7/29
- Primera red utilizable 192.168.20.1/29
- Ultima red utilizable 192.168.20.6/29

3.5.2. División por subredes de igual tamaño

Ahora realizaremos divisiones de una red otorgada por el proveedor, esto puede servir para redes simples donde queramos particionar nuestra red en redes más pequeñas para crear subdivisiones de nuestra red *LAN.*

Para la realización de este método debemos realizar los siguientes pasos:

- Conocer la dirección de red.
- Saber la cantidad de host en cada red o en su defecto saber el número de subredes que el cliente necesita.

Como sabemos cada octeto representa 8 bits los cuales se leen de la siguiente manera en forma decimal.

Tabla VIII. **Lectura de Bits en octeto**

OCTETO							
128	64	32	16	8	4	2	1
ULTIMO BIT							PRIMER BIT

Fuente: elaboración propia, realizado con Excel.

Si al momento de realizar nuestras redes leemos los bits de derecha a izquierda, estaremos realizando la subdivisión por el número de host que necesitamos, si lo leemos de izquierda a derecha estaremos realizando nuestra subdivisión por el número de subredes que no ha solicitado.

Por ejemplo, si necesitamos 8 subredes tomamos 3 bits ya que $2^3 = 8,$ y realizamos la lectura de izquierda a derecha

Tabla IX. **Ejemplo de subredes**

	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
1er subred	0	0	0					
2da subred	0	0	1					
3er subred	0	1	0					
4ta subred	0	1	1					
5ta subred	1	0	0					
6ta subred	1	0	1					
7ma subred	1	0	0					
8va subred	1	0	1					

Fuente: elaboración propia, realizado con Excel.

Si queremos saber cuántas direcciones tendrá nuestra subred debemos leer de derecha a izquierda hasta donde se encuentra el cambio de color, en este caso cada red tiene 32 direcciones.

Nota: A cada subred debemos de apartar la dirección de red y la dirección de *broadcast*.

Ejemplo 3.5.3:

Dada la dirección 192.168.10.0/24 solicitamos:

- 13 subredes
- Detallar dirección de red y *broadcast*

Iniciamos validando cuantos bits necesitaremos, $2^3 = 8$ y $2^4 = 16$ por lo que logramos apreciar la que más se acerca a nuestro requerimiento es la de 4 bits.

Por lo tanto, la máscara de subred cambiara ya que el sufijo ha cambiado puesto que antes teníamos

Tabla X. **Ejemplo de mascara de subred**

antigua mascara	**255**	**255**	**255**	**0**
	11111111	11111111	11111111	0
nueva mascara	255	255	255	240
	11111111	11111111	11111111	11110000

Fuente: elaboración propia, realizado con Excel.

Esta máscara se encuentra sumando los bits utilizados para la subred los cuales se encuentran de color amarillo

Tabla XI. **División de subredes**

bits	128	64	32	16	8	4	2	1
1er subred	192.168.10.0/28		192.168.10.15/28					
2da subred	192.168.10.16/28		192.168.10.31/28					
3er subred	192.168.10.32/28		192.168.10.47/28					
4ta subred	192.168.10.48/28		192.168.10.65/28					
5ta subred	192.168.10.64/28		192.168.10.79/28					
6ta subred	192.168.10.80/28		192.168.10.95/28					
7ma subred	192.168.10.96/28		192.168.10.111/28					
8va subred	192.168.10.112/28		192.168.10.127/28					
9na subred	192.168.10.128/28		192.168.10.143/28					
10ma subred	192.168.10.144/28		192.168.10.159/28					
11va subred	192.168.10.160/28		192.168.10.175/28					
12va subred	192.168.10.176/28		192.168.10.191/28					
13ra subred	192.168.10.192/28		192.168.10.207/28					
14ta subred	192.168.10.208/28		192.168.10.223/28					
15ta subred	192.168.10.224/28		192.168.10.239/28					
16ta subred	192.168.10.240/28		192.168.10.255/28					

Fuente: elaboración propia, realizado con Excel.

3.5.3. División de red por medio de VLSM

Conocida como máscara de subred de longitud variable, es una manera más eficiente de fraccionar nuestra red, puesto que en este caso se realizará en

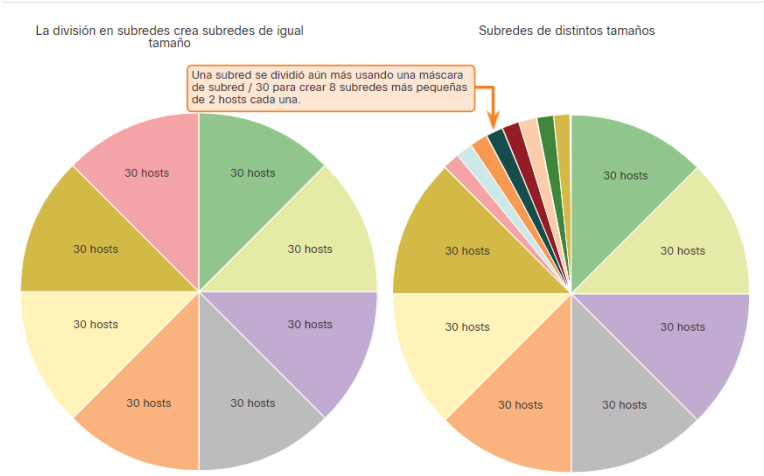
base al número de host, que el usuario solicite, por lo que no habrá desperdicio de direcciones en cada subred.

Para realizar este tipo de subredes debemos de saber con exactitud el número de host ya que no se podrá expandir la red una vez se realicen las sub divisiones.

Esto ocasionara que cada partición de la red tenga su propia máscara de subred. Para realizar esta configuración debemos realizar los siguientes pasos:

- Ordenar los hosts solicitados de mayor a menor.
- Validar con la formula $2^{n} - 2 \geq \#\ \text{de}\ host$.
- Generar las redes de mayor a menor dando continuidad a las redes ya usadas.

Figura 95. **Diferencia de división por subredes de igual tamaño y VLSM**



Fuente: CCNA 200-301. *VLSM.* Consultado el 28 de noviembre de 2022. Recuperado de https://ccnadesdecero.es/vlsm-mascaras-subred-longitud-variable/.

Ejemplo 3.5.4

Dada la red 192.168.50.0/24 una empresa desea particionar su red en:

- 100 host para el área administrativa.
- 30 host para el área comercial.
- 24 host para el área financiera.
- host para el área de comunicación.
- 2 host para el área de transporte.
- 2 host para el área de limpieza.

Encontrar por medio de división *VLSM* cuál es la dirección de red y la dirección de *broadcast* y cuantos hosts tendrán disponibles en cada red.

Ya que contamos con los hosts de manera ordenada vemos que necesitamos

- Una red de 100 *host*
- Una red de 30 *host*
- Una red de 24 *host*
- Tres redes de 2 *host*

Por lo tanto, usando la formula $2^{n} - 2 \geq \#\ \text{de host}$ sabemos que

- $2^{7} - 2 = 128 - 2 = 126 \geq 100$
- $2^{5} - 2 = 32 - 2 = 30 \geq 30$
- $2^{5} - 2 = 32 - 2 = 30 \geq 24$
- $2^{2} - 2 = 4 - 2 = 2 \geq 24$

Tabla XII. **Bits utilizados en división VLSM**

bits	128	64	32	16	8	4	2	1
	red de 100 host							
			red de 32 host					
			red de 24 host					
						red de 2 host		
						red de 2 host		
						red de 2 host		

Fuente: elaboración propia, realizado con Excel.

Entonces siguiendo la secuencia de estos bits usados contaríamos con los siguientes datos:

Tabla XIII. **División VLSM de ejemplo 3.5.4**

RED	IP DE RED	IP BROADCAST	HOST DISPONIBLES
Administrativa	192.168.50.0/25	192.168.50.127/25	1 - 126
Comercial	192.168.50.128/27	192.168.50.159/27	129 - 158
Financiera	192.168.50.160/27	192.168.50.191/27	161 - 190
Comunicación	192.168.50.192/30	192.168.50.195/30	193 - 194
Transporte	192.168.50.196/30	192.168.50.199/30	197 - 198
Limpieza	192.168.50.200/30	192.168.50.203/30	201 -202

Fuente: elaboración propia, realizado con Excel.

Como se puede apreciar en el ejemplo anterior este método es simple, sin embargo, debemos de ser cuidadosos en su cálculo, ya que como se indica anteriormente para revertir o ingresar una nueva red se debe de recalcular nuevamente todo el segmento.

Es por ello que su cálculo se realiza del host más alto hacia el *host* más pequeño, ya que una vez echo el cálculo no se podrán agregar *host* en la subred.

3.6. Configuración de SSH y Telnet

En este punto ya tenemos el conocimiento necesario para gestionar la conexión de manera virtual o remota, como se mencionó la configuración *SSH* es la más segura para este tipo de conexión, ya que telnet no es muy confiable en cuestiones de seguridad. Cabe mencionar que para que esta configuración funcione el *host* que utilicemos debe encontrarse en la red.

3.6.1. Configuración SSH

La configuración *Secure Shell* es una forma de conexión remota segura que utiliza el puerto TCP 22, otorga una conexión de administración encriptada, *SSH* se crea en remplazo de Telnet.

Debemos de realizar los siguientes pasos para la configuración de SSH en nuestro equipo.

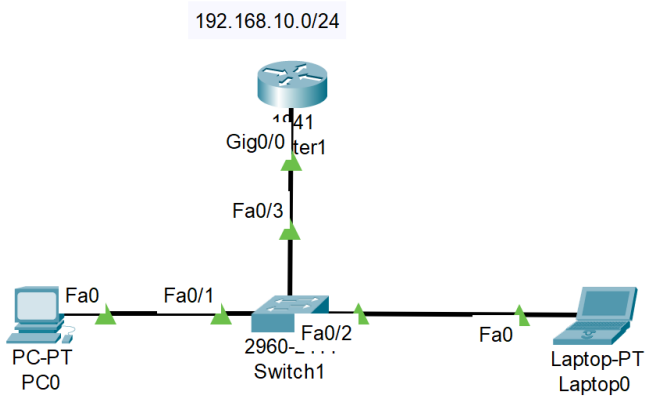
- Ingresar a modo EXEC privilegiado.
- Verificar que el dispositivo sea compatible con *SSH*, usando el comando *show ip ssh*.
- Ingresar a modo de configuración global.

- Cambiar *hostname* a dispositivo.
- Agregar *ip* al dispositivo.
- Configurar el nombre del dominio con el comando *ip domain-name*.
- Para habilitar el servidor *SSH* y claves rsa, se debe usar el comando *crypto key generate rsa.*
- Ingresar la longitud de bits entre más grande esta longitud más segura.
- Configurar usuario y contraseña con los comandos *username* y secret.
- Configurar las líneas *VTY* a utilizar los siguientes comandos:

    - *Transport input ssh*, limita que las conexiones sean por *SSH*.
    - *Login local, activa ssh*

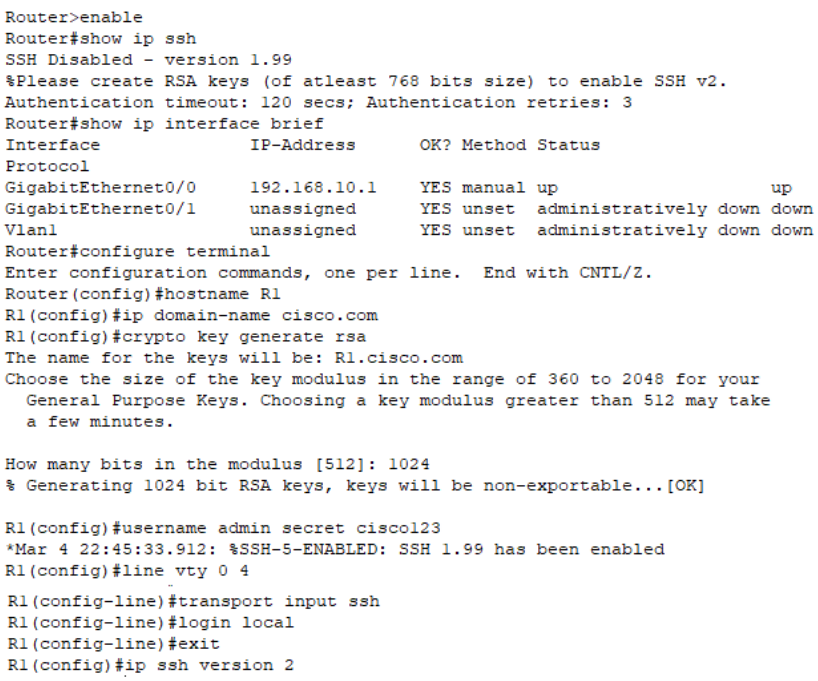
- Configurar la versión 2 con el comando *ip sshversion* 2, esta es más segura.
- Ingresar contraseña para modo EXEC privilegiado.

Figura 96. **Red LAN para configuración SSH**



Fuente: elaboración propia, realizado con cisco packet tracert.

Figura 97. **Configuración SSH**



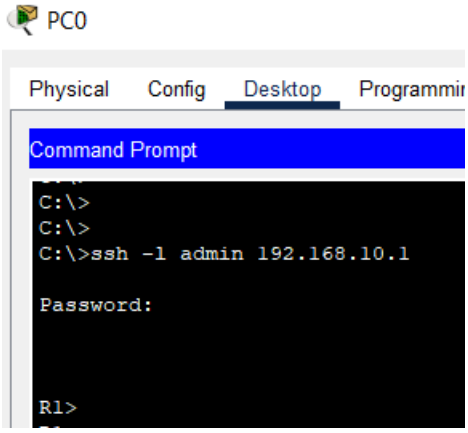
```
Router>enable
Router#show ip ssh
SSH Disabled - version 1.99
%Please create RSA keys (of atleast 768 bits size) to enable SSH v2.
Authentication timeout: 120 secs; Authentication retries: 3
Router#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     192.168.10.1    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#ip domain-name cisco.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#username admin secret cisco123
*Mar 4 22:45:33.912: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#ip ssh version 2
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Para comprobar que hemos realizado de manera correcta la configuración debemos ingresar a un host de la red e ingresar el comando *ssh* -l + nombre de usuario + dirección *ip*.

En la imagen anterior vemos que el nombre de usuario de nuestro dispositivo es *admin*, y la *ip* del *router* es 192.168.10.1, estos son los datos que debemos ingresar.

Figura 98. **Ingreso por medio de SSH**



Fuente: elaboración propia, realizado con cisco packet tracert.

Nota: Para configurar SSH en un switch debemos de agregar un paso más, el cual es agregar la *ip default Gateway.*

3.6.2. Configuración Telnet

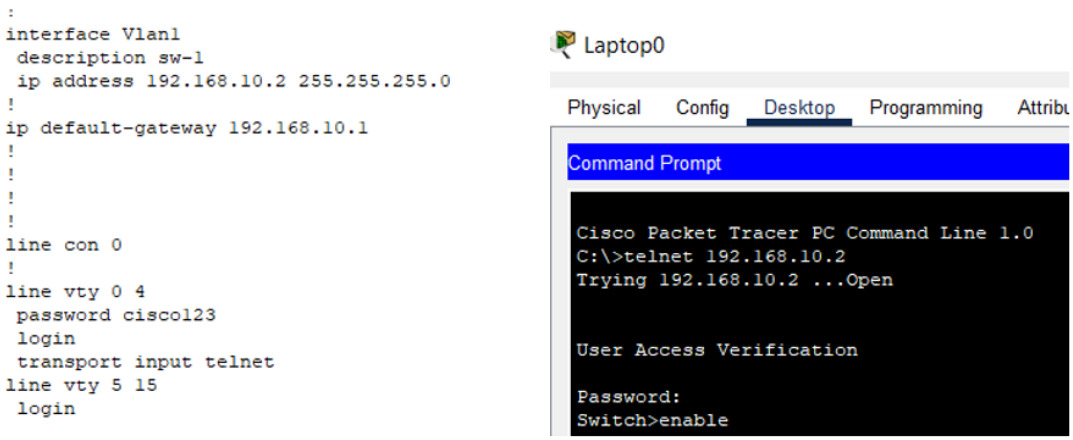
Esta configuración utiliza el puerto TCP23, no es seguro ya que utiliza un formato de texto, los equipos ya cuentan con esta configuración por defecto.

Para configurarlo debemos seguir los siguientes pasos:

- Ingresar a modo de configuración global.
- Asignar una dirección IP.
- Ingresar a subcomando de línea VTY.
- Agregar contraseña.
- Indicar por cómo será el acceso por medio de comando *transport input* telnet.

- Ingresar contraseña para modo EXEC privilegiado.

Figura 99. **Configuración y verificación de modo de acceso por medio de Telnet**



Fuente: elaboración propia, realizado con cisco packet tracert.

4. CONFIGURACIONES DE ENRUTAMIENTO ESTÁTICO EN DISPOSITIVOS CISCO

4.1. VLAN

Ya que contamos con las herramientas básicas de configuraciones, en los distintos dispositivos cisco es momento de ampliar nuestros conocimientos, para formar redes de mayor magnitud, utilizando redes *LAN* de forma virtual, para particionar una red de gran tamaño en subredes de menor tamaño, con el fin de dividir nuestra red *LAN*, de los sectores que no tengamos la necesidad de intercambian información entre sí.

Lo que nos lleva a una mayor eficiencia en la red ya que el tráfico de datos será sectorizado.

4.1.1. Descripción de red VLAN

Las *VLAN* otorgan segmentación y flexibilidad organizativa, su forma de comunicación es como si todos los dispositivos de la red estén conectados a un mismo cable, son conexiones de forma lógica y no de forma física.

Es una red conmutada, que permite a los segmentos de dicha red a un solo enlace independientemente del dispositivo físico que se esté utilizando, la forma de división la decide cada técnico y estas pueden ser por la función, la aplicación o simplemente la ubicación. Cada dispositivo que se encuentre en una *VLAN*, funcionara como si este tuviera su propia red independiente.

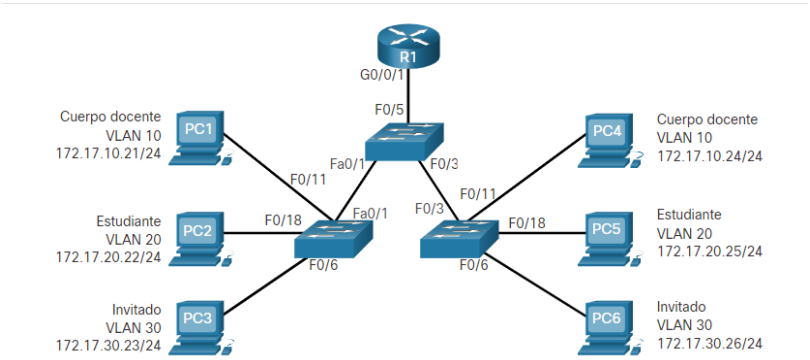
Los paquetes se reenviarán solamente a las terminales dentro de la *VLAN*, y los paquetes que sea necesario enviarlos fuera de la *VLAN* deben ser trasmitidos por dispositivos que admitan *routing*.

Las *VLAN* mejoran el rendimiento de la red mediante divisiones de grandes dominios de difusión, cabe mencionar que cada *VLAN* puede admitir políticas de acceso y seguridad como lo consideren los técnicos o el cliente, cada puerto del Switch se puede asignar a una *VLAN*, sin embargo, esto no se puede realizar con los puertos que estén conectados otro *Switch* o bien a un teléfono *IP*.

Así también se cuenta con una serie de ventajas al momento de su aplicación:

- Seguridad mejorada.
- Reducción de costos.
- Mejor rendimiento.

Figura 100. **Diseño de red VLAN**



Fuente: Cisco. *Ventajas de un diseño de VLAN.* Consultado el 28 de noviembre de 2022. Recuperado de https://contenthub.netacad.com/srwe-dl/3.1.2.

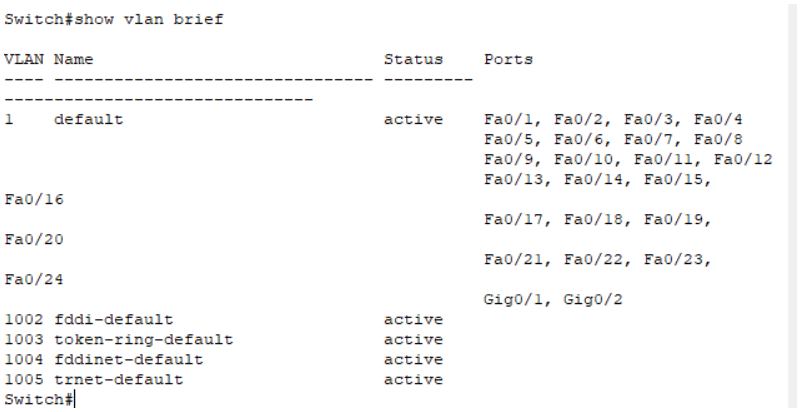
Existen varios tipos de redes *VLAN*, las cuales son:

- Predeterminada.
- De datos.
- Nativa.
- Administración.
- De voz.

4.1.1.1. VLAN predeterminada

Esta es la *VLAN* que contienen por defecto nuestros dispositivos, para los *Switches* es la *VLAN* 1 y todo el tráfico de control se asocia en esta *VLAN*, para esta no se puede realizar el cambio de nombre ya que por defecto todos los puertos están asignados a esta *VLAN*, lo cual podemos comprobar colocando el comando *show vlan brief* en el modo EXEC privilegiado.

Figura 101. **Verificación de puertos VLAN en Switch**



Fuente: elaboración propia, realizado con cisco packet tracert.

4.1.1.2. VLAN de datos

Estas son las generadas para separar el tráfico que se genera por el usuario, es la utilizada para subdividir las redes ya sea en grupos de usuarios o bien en cantidad de dispositivos, hay que tomar en cuenta que para este tipo de redes no se debe tener acceso el tráfico de administración de voz y red, es por ello que también se le conoce como *VLAN* de usuario.

4.1.1.3. VLAN nativa

Es la asignación de una *VLAN* a un puerto troncal 802.1Q también conocido como dot1Q, es un trabajo de la IEEE que permite a múltiples redes compartir el mismo medio físico, sin problemas de interferencia, ya que esta coloca una etiqueta de 4 bytes en el inicio de la trama para identificar de que *VLAN* proviene el mensaje; este puerto troncal admite el tráfico generado por las *VLAN*, de la misma manera que acepta el tráfico que no proviene de una *VLAN*, por defecto que se configura es la *VLAN* nativa es la VLAN99.

La función principal de ella es un identificador común en extremos opuestos de un enlace troncal, ya que es tráfico sin etiquetar, por lo cual se recomienda configurar una *VLAN* distinta a la *VLAN* 1, es normal configurar una *VLAN* fija para todos los puertos del enlace troncal.

4.1.1.4. VLAN de administración

Como su nombre lo indica es la encargada de administrar la red incluyendo *SSH, Telnet, SNMP y HHTP*. De igual forma la *VLAN* 1 se configura como la *VLAN* de administración de un Switch, esto como ejemplo de la configuración que hemos realizado en el capítulo 3 en el apartado de Telnet, ya que en el podemos

ver como al asignarle una dirección *IP*, le otorgamos accesos de administración para nuestro equipo.

4.1.1.5. VLAN de voz

Como ya se explicó, se necesita una VLAN aparte para la admisión de tecnología de voz sobre IP o mejor conocida como VoIP, ya que para esta se requieren de los siguientes elementos:

- Ancho de banda garantizado para el aseguramiento de la calidad de voz.
- Prioridad ante los tipos de tráfico de la red.
- Capacidad de envió en redes congestionadas.
- Demora no mayor 150 ms por medio de la red.

Es por ello que es necesario gestionar una VLAN aparte para este modo de trasmisión ya que de no ser así se contaría con interferencia cada vez que se emitan datos y voz al mismo destino.

4.1.2. Configuración de VLAN

Como ya conocemos los tipos de redes *VLAN* que existen, es momento de aprender a configurarlas, en los distinto switches Cisco admiten diversas cantidades de *VLAN*, como ejemplo los switches de series 2960 y 3550 aceptan más de 4000 *VLAN*, el rango normal se enumera iniciando con la *VLAN* 1 hasta la *VLAN* 1005, y las *VLAN* de rango extendido van desde la 1006 al 4094.

VLAN de rango normal: Este tipo de uso de *VLAN* es para redes pequeñas o medianas, se tienen las *VLAN* 1, 1002, 1003, 1004 y 1005 creadas por defecto y estas no se pueden eliminar.

Las configuraciones realizadas en ellas se almacenan en una base de datos llamado *vlan*.*data*, la cual se guardan en la memoria *flash.*

VLAN de rango extendido. Estas se utilizan para otorgar servicios a varios clientes y empresas globales, su configuración se almacena en el archivo de configuración de ejecución.

4.1.3. Configuración de VLAN en switch

Para la creación de redes *VLAN* se deben de seguir los siguientes pasos:

- Ingresar al modo de configuración global.
- Ingresar con el comando *vlan* + el número de *vlan* deseado (*vlan*-id).
- Especificar el nombre de la *VLAN* con el comando *name*.
- Salir de la configuración.

Figura 102. **Configuración de VLAN en Switch**

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Guatemala
Switch(config-vlan)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15,
Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19,
Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23,
Fa0/24
                                                Gig0/1, Gig0/2
10   Guatemala                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Como podemos observar en la figura anterior ya hemos creado la *VLAN* 10, sin embargo, no tiene asignado ninguna terminal, ya que por defecto todos los puertos se encuentran cargados a la *VLAN* 1.

Para asignar puertos en nuestra *VLAN* debemos realizar la siguiente configuración:

- Ingresar en modo de configuración global.
- Ingresar a la interfaz deseada ya sea con el comando *interface* o con el comando *inteface range* para configurar varias interfaces.
- Establecer el puerto como modo de acceso con el comando switchport *mode access*.
- Asignar el puerto a la *VLAN* con el comando switchport *Access vlan + vlan id*.
- Salir de la configuración.

Figura 103. **Asignación de puertos a VLAN**

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range f 0/1 - 5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,
Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,
Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,
Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24,
Gig0/1
                                                 Gig0/2
10   Guatemala                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Si lo que requerimos es establecer una *VLAN* de voz se debe configurar de la siguiente manera:

- Ingresar en modo de configuración global.
- Ingresar a la interfaz a configurar.
- Establecer el puerto como modo de acceso.
- Habilitar la calidad del servicio (*QoS*), mediante el comando mls qos trust**,** podemos usar [cos | *device* cisco-*phone* | *dscp* |*ip-precedence*].
- Asignar el puerto a la *VLAN* con el comando *switchport voice vlan* + *vlan-id***.**
- Salir de la configuración.

Figura 104. **Configuración de VLAN de voz**

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name voz
Switch(config-vlan)#exit
Switch(config)#interface f 0/6
Switch(config-if)#switchport mode access
Switch(config-if)#mls qos trust cos
Switch(config-if)#switchport voice vlan 20
Switch(config-if)#exit
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Si deseamos saber la *VLAN* que se ha configurado en un puerto lo podemos realizar con el comando *show interface* + *interface-id* + *switchport*.

Figura 105. **Información de interfaces asociado a una VLAN**

```
Switch#show interface f0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 20
```

Fuente: elaboración propia, realizado con cisco packet tracert.

De igual forma para eliminar una *VLAN* solo debemos de colocar el comando no *vlan* + *vlan-id*, y con ello se borrará la *VLAN* configurada.

4.1.4. Configuración de VLAN troncal en Switch

Esta configuración nos permite trasportar el tráfico entre dos *Switches* hacia todas las *VLAN* configuradas en ellos. Para lo cual se debe seguir los siguientes pasos:

- Ingresar al modo de configuración global.
- Ingresar a la interfaz a configura el trocal.
- Configurar el puerto como troncal con el comando *switchport mode* trunk.
- Cambiar la configuración de la *VLAN* nativa a la *VLAN* deseada con el comando *switchport trunk native vlan* + *vlan-id*.
- Especificar un listado de las VLAN que admitirá el enlace con el comando *switchport trunk allowed vlan* (opcional).
- Salir.

Figura 106. **Configuración modo troncal de una interfaz VLAN**

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface f 0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down

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

Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#switchport trunk native vlan 99
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (99), with Switch FastEthernet0/24 (1).

Switch(config-if)#switchport trunk allowed vlan 10,20
Switch(config-if)#end
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Como podemos observar al asignar el modo troncal al puerto este nos envía un mensaje indicándonos que el puerto se encuentra operativo, luego podemos observar que al cambiar la *VLAN* nativa nos muestra otro mensaje indicándonos a que puerto del siguiente switch estamos conectados.

Esto se debe realizar en ambos extremos de la conexión. Para evitar que se realice una negoción de enlaces troncales de manera dinámica (*DTP*), algunos dispositivos pueden enviar tramas *DTP* de manera incorrecta por lo que es aconsejable desactivar el *DTP*. El comando para deshabilitar el *DTP* es *switchport nonegotiate*, y lo colocamos después de activar el modo troncal.

Para activarlo nuevamente se debe colocar el comando *switchport mode dynamic auto*.

4.2. inter-VLAN routing

Una vez ya hemos aprendidos a segmentar la red *VLAN*, es momento de ponernos a pensar, que pasaría si nuestros dispositivos finales se quieren comunicar con otro *host* de otra *VLAN* distinta. Pues es el momento de agregar a nuestros dispositivos un dispositivo de capa 3 (*router*).

Para esto existen tres opciones de inter-VLAN:

- *Inter-VLAN routing* heredado.
- *Router-on-a-stick*.
- Switch capa 3 con interfaces virtuales (*SVIs*).

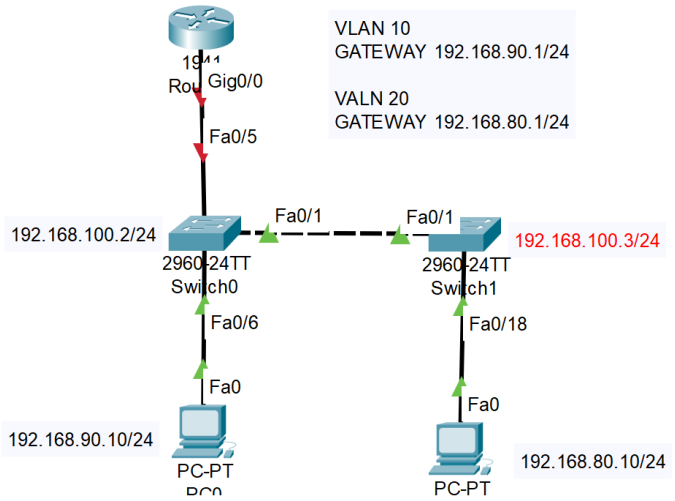
Nota: En este documento no se realizará configuración de *inter-VLAN routing* heredado ya que es muy antiguo y no es escalable.

4.2.1. Router-on-a-stick

Este tipo de configuración solo requiere una interfaz, para realizar el enrutamiento de las tramas de una red *VLAN*, ya que en el *router* se debe configurar al interfaz como troncal 802.1Q y se debe conectar al enlace troncal del switch capa 2.

En el *router* se crean interfaces virtuales para cada *VLAN*, para configuración del *router* previamente debemos de configurar los switches a utilizar con los comandos explicados en el inciso 4.1 de este documento.

Figura 107. **Ejemplo de configuración de Router-on-a-stick**



Fuente: elaboración propia, realizado con cisco packet tracert.

La configuración que se debe realizar en este ejemplo como se ve en la figura 107 se cuenta con 3 *VLAN*, las cuales son 99, 10 y 20, para el switch0 tenemos dos enlaces troncales uno que va hacia el switch1 y otro que va hacia el *router*, por lo cual debemos realizar los siguientes pasos:

- Ingresar al modo de configuración global.
- Ingresar a la interfaz del *router* conectado hacia el switch de esta manera *interface +interface-id.vlan-id*.
- Ingresar descripción.
- Realizar la encapsulación 802.1Q con el comando *encapsulation* dot1Q + *vlan-id*.
- Agregar la dirección *IP*.
- Salir.
- Se repite este paso con cada *VLAN* a configurar.
- Ingresar a la interfaz conectada al *switch* y activarla.

- Salir.

Figura 108. **Configuración de Router-on-a-stick**

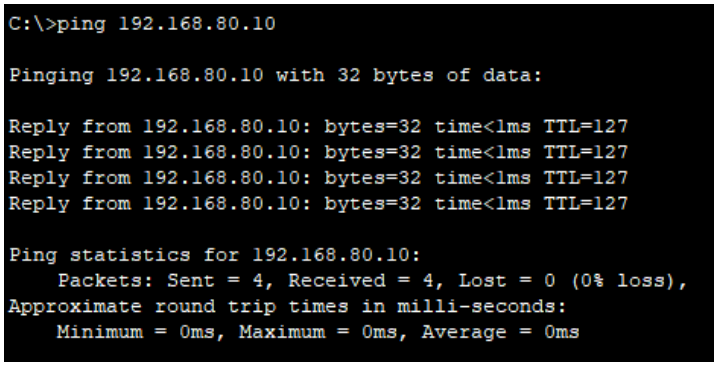
```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g 0/0.10
Router(config-subif)#description gateway vlan 10
Router(config-subif)#encapsulation  dot1Q 10
Router(config-subif)#ip address 192.168.90.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
Router(config)#interface g 0/0.20
Router(config-subif)#description gateway vlan 20
Router(config-subif)#encapsulation  dot1Q 20
Router(config-subif)#ip address 192.168.80.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
Router(config)#interface g 0/0.99
Router(config-subif)#description gateway vlan 99
Router(config-subif)#encapsulation  dot1Q 99
Router(config-subif)#ip address 192.168.100.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
Router(config)#interface g 0/0
Router(config-if)#description enlace troncal a switch
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.99,
changed state to up

Router(config-if)#exit
Router(config)#
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Como podemos observar al momento que activamos la interfaz principal del *router* esta activa todas las subinterfaces que se hayan configurado en el dispositivo.

Al completar esta configuración podremos realizar una prueba de conectividad entre ambos dispositivos, para validar que si exista comunicación entre ambas *VLAN*.

Figura 109. **Prueba PING entre VLAN**



Fuente: elaboración propia, realizado con cisco packet tracert.

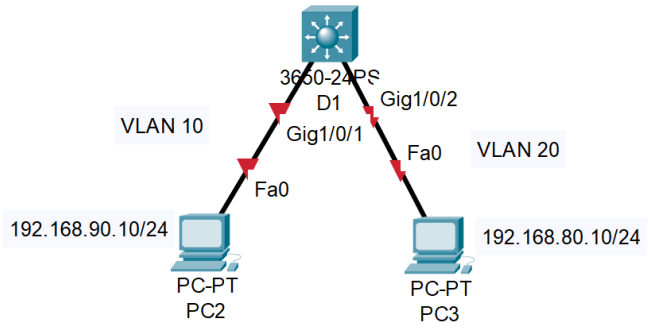
4.2.2. Routing en switch capa 3

Para redes pequeñas está bien utilizar la configuración de *router-on- a-stick*, sin embargo, para redes grandes no es muy factible el usar esta configuración, por lo que los técnicos en redes utilizan los switches de capa 3 esto por su escalabilidad.

Esta configuración se basan hardware para realizar el *switching* de manera más veloz que un *router*, también otorgan la facilidad de configurar los puertos ya sea para capa 2 o bien para lo que estaremos observando en este módulo un puerto enrutado ya que estos utilizan *SVIs*.

Realizar las configuraciones utilizaremos las mismas *VLAN* que en el ejemplo anterior, simplemente cambiaremos el modo de configuración.

Figura 110. **Diseño inter-VLAN con switch capa 3 o multilayer**



Fuente: elaboración propia, realizado con cisco packet tracert.

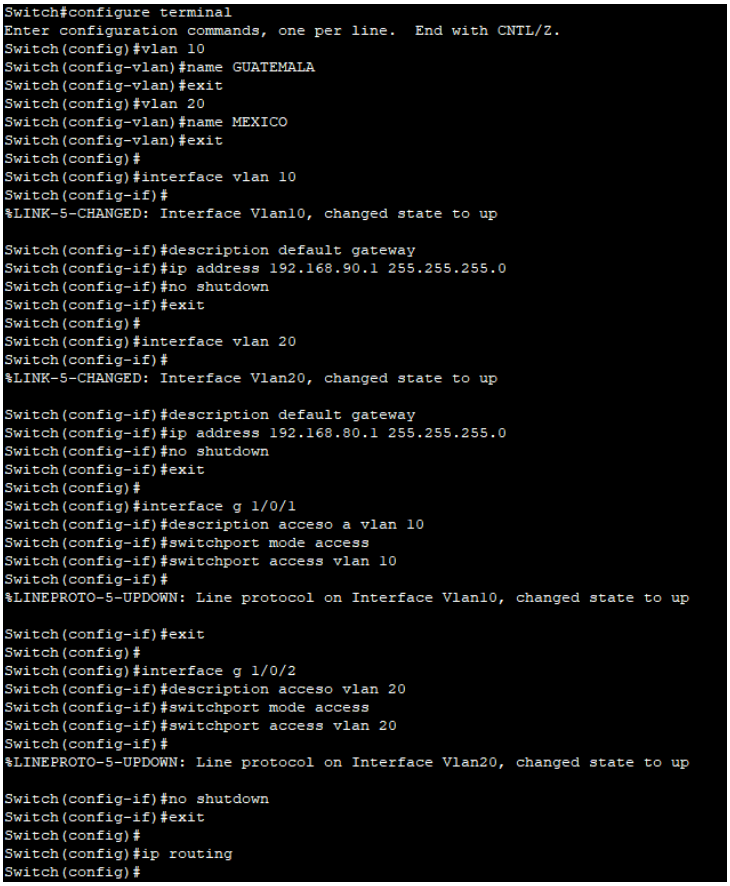
Para realizar la configuración del equipo se debe realizar de la siguiente manera:

- Ingresar al modo de configuración global.
- Creación de las *VLAN*.
- Crear las interfaces *VLAN SVIs*.
    - Ingresar a la interfaz de las *VLAN* a configurar.
    - Colocar descripción e ingresar *IP default Gateway*.
    - Activarla y salir.

- Configurar los puertos del *switch* capa 3.
    - Ingresar al puerto a configurar.
    - Colocar descripción.
    - Activar le modo de acceso.
    - Asignar el acceso a la VLAN deseada.
    - Salir.

- Habilitar el enrutamiento IPv4 con el comando ip routing.

Figura 111. **Configuración inter-VLAN con switch capa 3 o multilayer**



Fuente: elaboración propia, realizado con cisco packet tracert.

Como podemos observar en esta imagen se facilita en gran magnitud la manera de configurar los dispositivos ya que se realiza de manera más simple, así también, se reducen componentes en el diseño de nuestra red.

Es por ello que esta es la opción más factible al momento de configuración *inter-VLAN*, ya que para su escalabilidad es más simple, por lo tanto, para configuraciones grandes esta es la mejor opción.

4.2.3. Resolución de problemas en inter-VLAN Routing

Puede que se tengan problemas al momento de configurar una red *VLAN*, estos en su mayoría se deben a problemas de conectividad, por lo que siempre es importante hacer la revisión física de nuestros equipos.

Para comprobar que las *VLAN* estén bien configurada podemos verlas por medio de los comandos de verificación:

- *Show vlan brief*: Muestra las *VLAN* creadas, con sus nombres y puertos asignados.
- *Show interfaces switchport*: Muestra el estado de los puertos, modos de accesos y a que *VLAN* pertenecen.
- *Show interfaces trunk*: Muestra las interfaces que son troncales, así también el tráfico de las *VLAN* que tienen a su cargo.

Al detectar que la falla está en la creación lo más aconsejable es volver a crear la *VLAN*. Estos comandos mencionados anteriormente se aplican solamente para los *switches*.

Para un *router* los comandos a utilizar son:

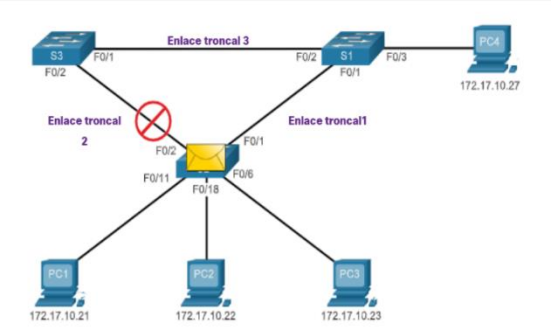
- *Show ip interface brief*: Muestra las direcciones *IP* cargadas en cada interfaz y sus subinterfaces, y su estado operativo.
- *Show interfaces*: Brinda información detallada de la interfaz, tanto como dirección *IP* como a que *VLAN* pertenece y el modo de encapsulamiento.

4.3. Conceptos STP

Para redes que cuentan con rutas redundantes, los cuales ayudan en los enlaces para no tener perdidas de información o en tramas de datos es muy bueno, pero esto puede ocasionará que se tenga un problema conocido como bucle de capa 2.

Este bucle causa una distorsión del mensaje ya que este mismo mensaje es enviado en repetidas ocasiones por el mismo canal, afectando así la comunicación, es por ello que se tiene la necesidad de crear el protocolo de árbol de expansión (*STP*).

Figura 112. **Modelo STP**



Fuente: Cisco. *STP Normal Operation.* Consultado el 10 de diciembre de 2022. Recuperado de https://contenthub.netacad.com/srwe-dl/5.1.2.

Como se indica se basa en la creación de una red redundante que permita mantener el tráfico de datos aun cuando se tenga alguna falla en el enlace principal, buscando así otra ruta para entregar el mensaje por medio de los dispositivos ce capa 2.

Como podemos ver en la figura 112, el mensaje debe ser enviado a la PC4, por lo tanto, si no contáramos con el modelo *STP*, solamente se contaría con un *Switch* por lo que tendríamos una falla ya que nuestro mensaje no podría ser enviado, sin embargo, con este modelo vemos que el mensaje puede tomar una ruta alterna para llegar a su destino.

Pero qué pasaría si ambas rutas están bien, el mensaje generaría un bucle ya que tendería a reenviar el mensaje hacia el mismo punto, la respuesta es no ya que, si ambas líneas se encuentran bien el modelo *STP*, bloqueara una, hablando en otras palabras realiza un falso fallo indicando que por esa ruta no le es permitido pasar el mensaje.

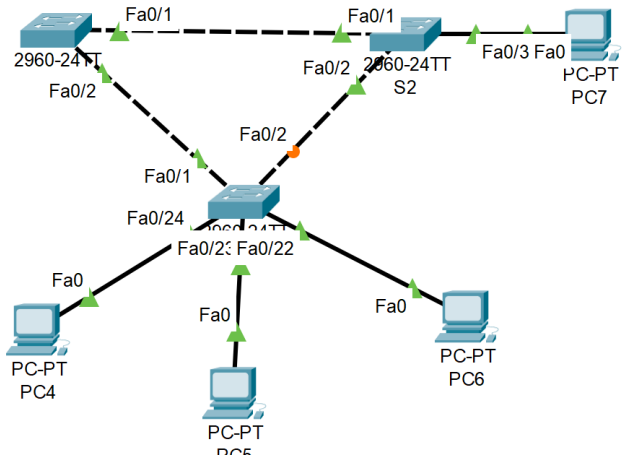
4.3.1. Funcionamiento de STP

Esta configuración se realiza de forma automática, en los dispositivos para ello toma los siguientes datos:

- Mac *address*
- Prioridad del puerto (4096 - 32769)

Esto nos dice quién será el *root bridge*, o el *switch* principal ya que primero valida la prioridad de los puertos si todos son iguale la MAC *address* más pequeña será el *root bridge* y el puerto con el coste más alto será el que se bloqueara para no dar paso al bucle de capa 2, esto lo podemos observar en los dispositivos pues el puerto tendrá una luz de color naranja indicando que bloqueara ese acceso.

Figura 113. **Modelo STP en packet tracet**

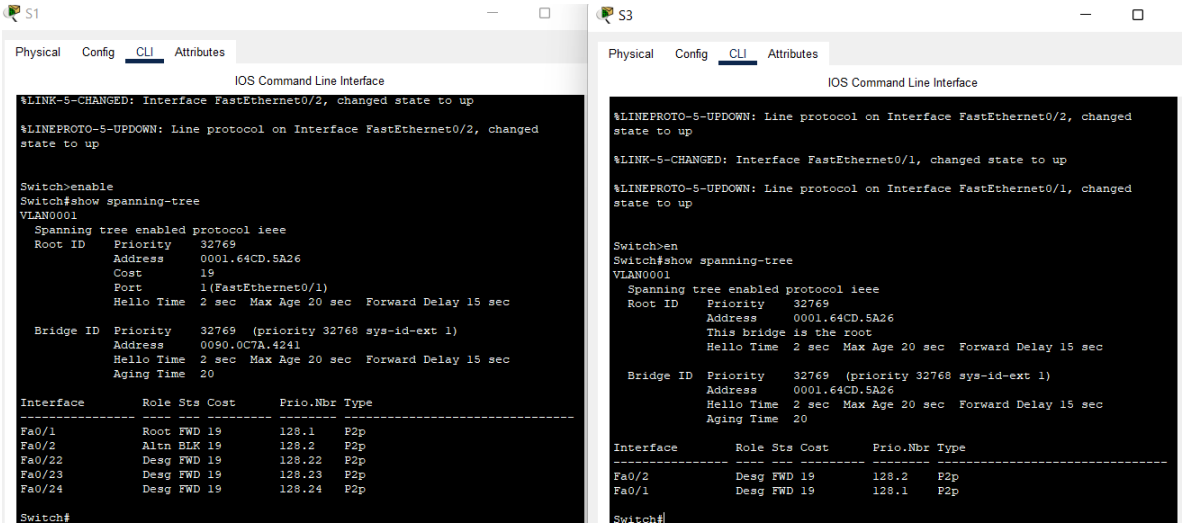


Fuente: elaboración propia, realizado con cisco packet tracert.

Y para verificar la configuración de *STP* en nuestros dispositivos podemos hacerlo ingresando el comando *show spanning-tree*, con lo cual nos otorgará una tabla detallada de nuestro componente, como ejemplo:

- Mac *address*.
- Prioridad y si es el *root bridge*.
- Puertos activos e inactivos.
- Coste de trasferencia de datos.

Figura 114. **Visualización de configuración STP**



Fuente: elaboración propia, realizado con cisco packet tracert.

Como podemos observar en la imagen anterior podemos destacar:

- S3 es el switch principal ya que nos indica que es el *root bridge*
    - Nos indica la prioridad
    - La MAC del dispositivo, observemos que es la misma tanto en la información de *Root ID* como en Bridge *ID*
    - Nos indica que los puertos son designados, lo cual nos indica que habrá tráfico de datos ya que tiene el estatus *forwarding* (reenvió)
- S2 es un *switch routing*
    - Nos indica la prioridad
    - El costo para el tráfico de datos

- En *Root ID* no dará la MAC de switch principal y en *Bridge ID* la MAC de nuestro dispositivo
- Nos indica los puertos que se están utilizando, pero vemos que los puertos conectados hacia los switches tenemos uno que indica *root* el cual está en *status FWD* (*forwarding*), y otro puerto que es *Altn* (alterno), el cual se encuentra bloqueado o por sus siglas en inglés (*BLK*).

Por lo tanto, el puerto que tiene estatus *BLK*, no permitirá el paso de tramas, resolviendo así el bucle de capa dos.

Pero que pasaría el técnico desea asignar de forma manual un *switch* como *root bride*; pues esto es posible ya que como vemos en la imagen anterior, por contar con la misma prioridad, la configuración *STP* se basó en la dirección MAC más baja, por lo cual si queremos asignar de forma manual el *switch* primario solo debemos cambiar la prioridad que sea más baja que los demás switches.

Para realizar esta configuración debemos de seguir los siguientes pasos:

- Ingresamos a configuración global.
- Cambiar la prioridad de la *VLAN* por defecto con el comando *spanning-tree vlan 1 priority*+ prioridad entre (4096 - 32769)**.**

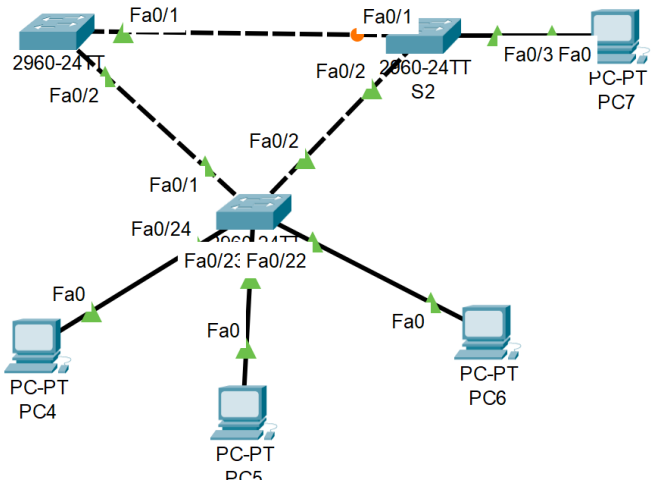
Figura 115. **Configuración manual de STP**

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spanning-tree vlan 1 priority 4096
Switch(config)#
```

Fuente elaboración propia, realizado con cisco packet tracert.

Por lo que la topología cambiara y lo veremos en la imagen 4 – 17 que ahora el punto naranja ha cambiado de puesto ya que este en la imagen 4 – 14 se encontraba en los puertos del *Switch* 1.

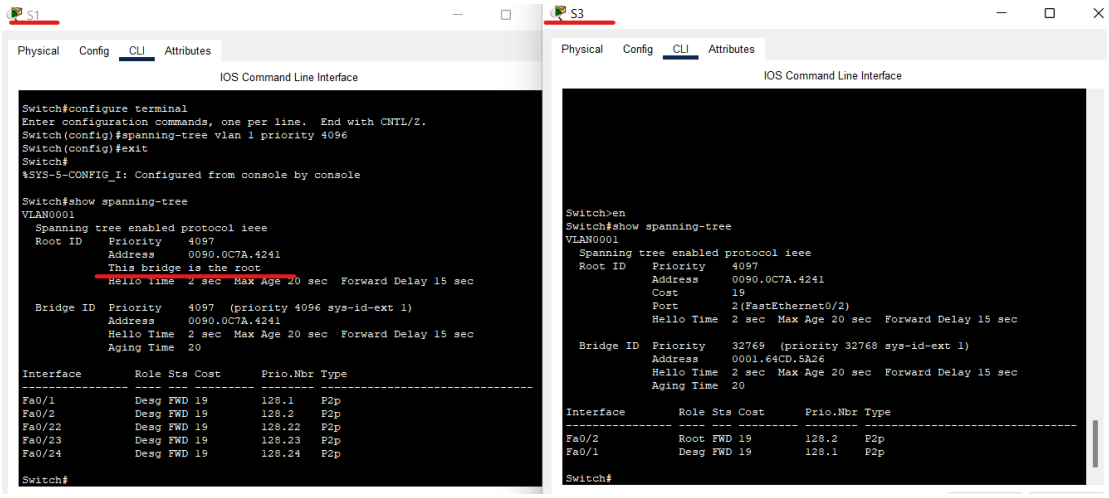
Figura 116. **Reconfiguración STP**



Fuente: elaboración propia, realizado con cisco packet tracert.

Observemos que ahora el puerto bloqueado es el puerto Fa 0/1 del *Switch* 2, con lo cual hemos cambiado la configuración del *STP*. Si observamos las configuraciones de los dispositivos podremos darnos cuenta que se han cambiado el *root bridge* y el rol de los puertos de ambos dispositivos.

Figura 117. **Visualización de STP después de cambio de prioridad**



Fuente: elaboración propia, realizado con cisco packet tracert.

4.4. Conceptos de enrutamiento

Ya contamos con conceptos de enrutamiento los cuales hemos visto en los incisos anteriores, debemos conocer cómo trabaja el *router* para lograr la conectividad y envío de paquete.

El *router* debe determinar la mejor ruta para el envío de las tramas, por lo que seleccionara una interfaz por la cual enviar la paquetería, a esto se le conoce como enrutamiento, lo cual para elegir esta interfaz se basa en su tabla de enrutamiento o bien llamada tabla *routing*.

Esta tabla funciona con la dirección *IP*, pues el *router* utiliza la coincidencia entre las direcciones *IP* que contiene con la dirección de destino. La tabla cuenta con las direcciones *IP* y sus prefijos, como se menciona esta deben coincidir para que se escoja la interfaz de envío.

Pero para que nuestro *router* conozca estas redes lo puede hacer de tres maneras:

- Redes conectadas directamente: Esas son las redes que se encuentran configuradas en las interfaces activas de nuestro *router*.
- Redes remotas: Estas son las redes que nuestro dispositivo no tiene configuradas directamente en su interfaz por lo cual el las descubre remotamente, y estas pueden ser de dos formas.

    - Rutas estáticas.
    - Rutas dinámicas.

- Ruta predeterminada: Esta es el siguiente salto que el *router* debe tomar cuando no se tiene en su tabla de enrutamiento una ruta especifica que coincida con la *IP* de destino.

4.4.1. Reenvío de paquetes

Ya que el *router* ha decidido la mejor ruta para el envío de nuestro mensaje, debe de encapsular dicho mensaje y enviarlo por la interfaz correcta.

Reenvía el paquete a un dispositivo conectado directamente. Si al enviar un mensaje se valida que la interfaz está conectada directamente con dicho dispositivo final, se sabe que este dispositivo pertenece a la misma red, por lo cual el paquete se envía con encapsulación *Ethernet*, ya que estos por lo regular suelen ser dispositivos de una *LAN ETHERNET*.

Para encapsular este paquete, el *router* debe determinar la dirección MAC de destino con la cual se encuentra asociada la dirección *IP*. La comprobación lo hace mediante su tabla *ARP*.

Reenviar el paquete a un *router* de salto siguiente. Si el *router* valida que la dirección de destino se encuentra en una red remota, lo cual indicaría que la red de destino no se encuentra conectada directamente a ninguna de sus interfaces, lo que se hará será enviar el mensaje a otro enrutador, el salto que realizara nuestro mensaje se indica en la entrada de ruta, esto hasta que se encuentre el *router* que esté conectado directamente con la dirección de destino correcta.

Nota: Si en la tabla *routing* no se encuentra ninguna conciencia el paquete se descartará.

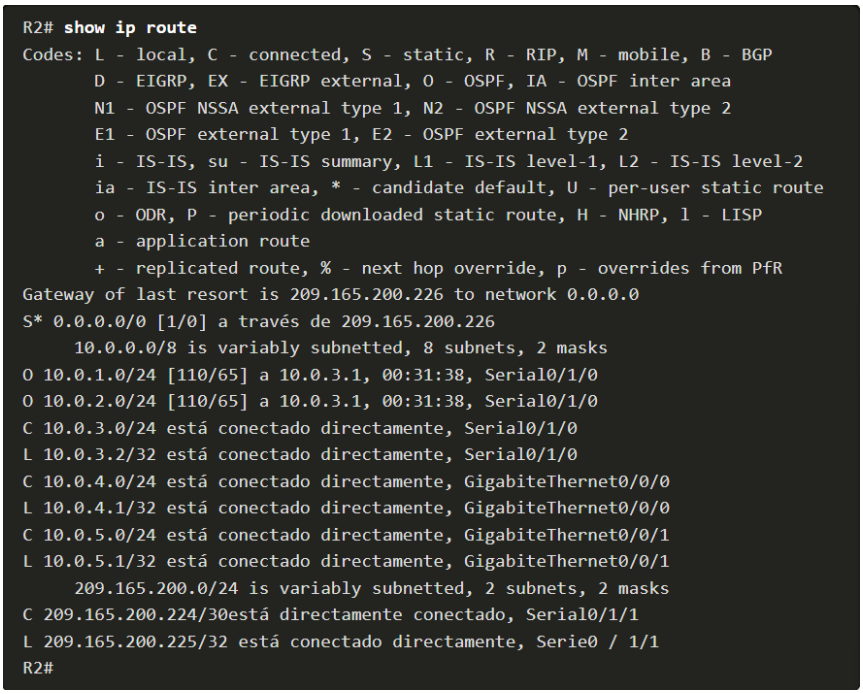
4.4.2. Tablas de routing IP

Esta tabla contiene la lista de rutas las cuales son conocidas por el dispositivo *router* (Prefijos y longitudes del prefijo), esta tabla contara con algunas iniciales las cuales son:

- L: Es la dirección asignada en la interfaz del *router*.
- C: Es la red conectada directamente en el *router*.
- S: Es la ruta estática que se crea para llegar a una red especifica.
- O: Es la red que es descubierta de manera dinámica con el protocolo *OSPF*.
- *-: La ruta que es candidata para ser una ruta predeterminada.

Para poder visualizar esta tabla en el enrutador debemos colocar el comando *show* ip *route*, en el modo de configuración privilegiado.

Figura 118. **Tabla de enrutamiento**



Fuente: elaboración propia, realizado con cisco packet tracert.

4.5. Rutas IP estáticas

Estas rutas se configuran de forma manual, por lo cual no se actualizan automáticamente ya que si se realiza un cambio se deberá cambiar la configuración de forma manual, se cuenta con algunos veneficios al utilizar este método y a que se cuenta con mayor seguridad y con la eficacia de los recursos, también consumen menor ancho de banda.

El enrutamiento estático tiene tres funciones principales:

- Facilita el mantenimiento en redes pequeñas.
- Utiliza solamente una ruta predeterminada para conectar el dispositivo hacia otra red, con la cual no se encuentre coincidencia en la tabla *routing*.
- Realiza enrutamiento entre sus redes internas.
- Para las rutas estáticas existen los siguientes tipos:

    - Ruta estática estándar.
    - Ruta estática predeterminada.
    - Ruta estática flotante.
    - Ruta estática resumida.

De igual forma se puede designar una opción para el siguiente salto esto con una dirección IP, una interfaz de salida o si se desea se puede realizar de ambas maneras, por lo que es siguiente salto puede ser:

- Ruta de siguiente salto: En esta forma solo especifica la dirección IP por la cual dará le salto nuestro paquete.
- Ruta estática conectada directamente: Es la que solamente indica la interfaz del router por la cual saldrá nuestro mensaje.
- Ruta estática totalmente especificada: Es la que brinda tanto la dirección IP y la interfaz del router por la cual será enviado el mensaje.

4.5.1. Configuración de enrutamiento estático

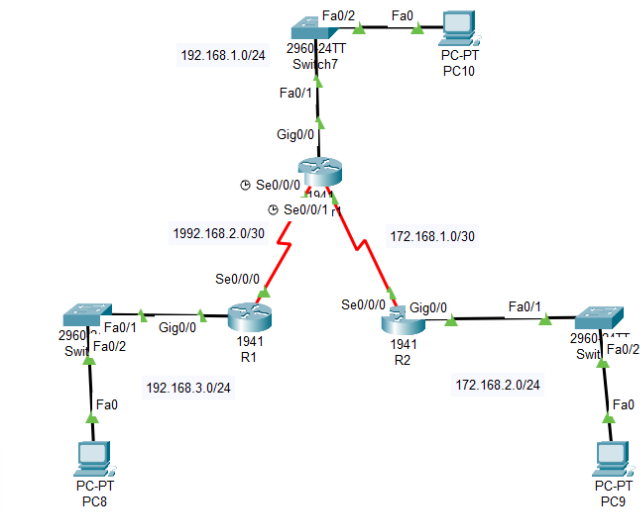
Para la realización de esta configuración debemos estar en la configuración global del dispositivo seguido se debe colocar el comando *IP route*

+ dirección *IP* destino + mascara de subred + dirección *IP* del siguiente salto. Con esto tendremos un enrutamiento por ruta del siguiente salto.

Si lo que deseamos es un enrutamiento por ruta estática conectada directamente debemos cambiar el comandado por el siguiente *IP route* + dirección *IP* destino + mascara de subred + interfaz de salida del *router*.

Por último, podemos contar con ambas opciones, con el siguiente comando *IP route* + dirección IP destino + mascara de subred + interfaz de salida del *router* + *IP* del siguiente salto.

Figura 119. **Red configurada por redes estáticas**



Fuente: elaboración propia, realizado con cisco packet tracert.

Teniendo en cuenta la red de la imagen 4-20, la configuraremos de las 3 formas posibles, para el R1 realizaremos una configuración de ruta de siguiente salto:

- Esta red cuenta con tres redes desconocidas las cuales son 192.168.1.0/24, la red 172.168.2.0/24 y la red 172.168.1.0/30 para todas las redes el siguiente salto es la dirección conocida con R3 192.168.2.2, por tal modo la configuración será la siguiente.

Figura 120. **Configuración R1 Ruta de siguiente salto**

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.2
R1(config)#ip route 172.168.2.0 255.255.255.0 192.168.2.2
R1(config)#ip route 172.168.1.0 255.255.255.252 192.168.2.2
R1(config)#
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Ya que hemos configurado R1 configuraremos R2, pero en esta ocasión lo realizaremos por medio de Rutas estáticas conectadas directamente.

- Esta red cuenta con tres redes desconocidas, la red 179.168.3.0/24, la red 192.168.2.0/30 y la red 192.168.1.0/30 y su salida será por la interfaz del *router* Serial 0/0/0, por lo que su configuración se realizará de la siguiente manera:

Figura 121. **Configuración de R2, ruta estática conectada directamente**

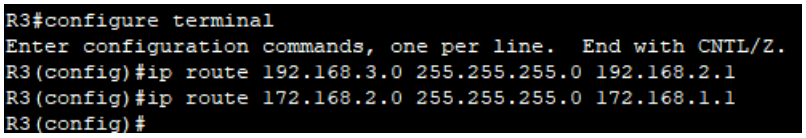
```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 192.168.3.0 255.255.255.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R2(config)#ip route 192.168.2.0 255.255.255.252 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R2(config)#ip route 192.168.1.0 255.255.255.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R2(config)#
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Por último, contamos con R3 el cual, se realizará configuración por medio de ruta de siguiente salto.

- Este router desconoce solamente dos redes las cuales son: la red 192.168.3.0/24 para la cual el siguiente salto es 192.168.2.1, y la red 172.168.2.0/24 el siguiente salto es 172.168.1.2.

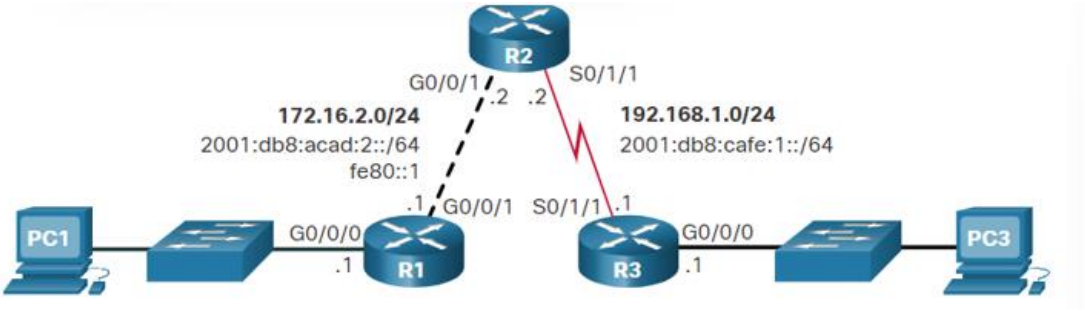
Figura 122. **Configuración de R3, por medio de ruta de siguiente salto**



Fuente: elaboración propia, realizado con cisco packet tracert.

Nota: Para las redes que estén conectadas por medio de cable serial no será posible realizar la configuración de ruta estática totalmente especificada, ya que esta admite solamente un dispositivo *router* en ambos extremos, por lo cual si queremos realizar este tipo de configuración se debe realizar en un puerto Ethernet de acceso múltiple ya que es posible que el existan distintos dispositivos.

Figura 123. **Configuración de Ruta estática totalmente especificada**




```
R1(config)# ip route 172.16.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
```

Fuente: Cisco. *Configuración de rutas estáticas IP*. Consultado el 12 de diciembre de 2022. Recuperado de https://contenthub.netacad.com/srwe-dl/15.2.1.

Terminadas las configuraciones podremos probar la conectividad por medio de los comandos *ping* o *treacert* en cada host, así también podremos ver que la tabla de configuración de cada dispositivo al cual se le antepone una letra S, la cual especifica que es una ruta estática.

Figura 124. **Tabla de enrutamiento IP**

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.168.0.0/16 is variably subnetted, 3 subnets, 3 masks
C       172.168.1.0/30 is directly connected, Serial0/0/1
L       172.168.1.2/32 is directly connected, Serial0/0/1
S       172.168.2.0/24 [1/0] via 172.168.1.1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/30 is directly connected, Serial0/0/0
L       192.168.2.2/32 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.1
```

Fuente: elaboración propia, realizado con cisco packet tracert.

4.5.2. Configuración de ruta estática por defecto

Esta es una manera más fácil de realizar la configuración estática para que coincida con todos los paquetes ya que el *router* puede tener solamente una ruta para el envío de la paquetería hacia cualquier red que no esté contemplada en la tabla *routing*.

Esta ruta se utiliza cuando ninguna de las rutas conocidas por el *router* coincide, opta por utilizar la ruta predeterminada como última opción. Su utilización es para la conexión del *router* hacia proveedores de servicio entre otros.

Su configuración es simple ya que es similar al comando normal para la configuración estática, con el cambio que no se coloca la dirección *IP* de la red desconocida ni tampoco su mascara, en cambio se coloca 0.0.0.0 en la dirección *IP* y 0.0.0.0 en la máscara de subred luego se debe colocar ya sea la *IP* del siguiente salto o bien la interfaz de salida.

Figura 125. **Configuración de ruta estática predeterminada**

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip route static
     172.168.0.0/16 is variably subnetted, 2 subnets, 2 masks
S       172.168.1.0/30 [1/0] via 192.168.2.2
S       172.168.2.0/24 [1/0] via 192.168.2.2
S    192.168.1.0/24 [1/0] via 192.168.2.2
S*   0.0.0.0/0 [1/0] via 192.168.2.2
```

Fuente: elaboración propia, realizado con cisco packet tracert.

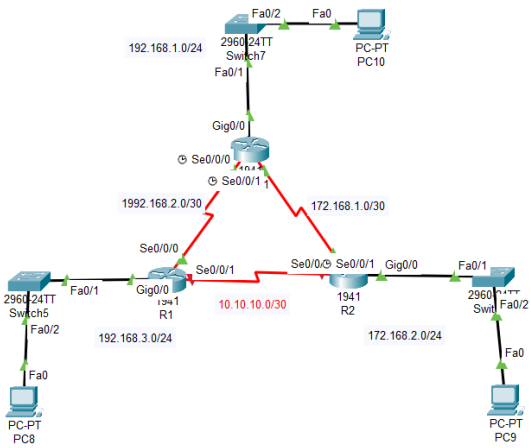
Como podemos ver en la figura 125, la ruta estática por predeterminada se crea y su símbolo es distinto a las rutas estáticas conocidas por el dispositivo ya que su símbolo es S*****, y como se detalló anteriormente el único cambio realizado es la colocación de colorar 0 en la dirección IP y la máscara de subred.

4.5.3. Rutas estáticas flotantes

Estas son las rutas de respaldo ante una ruta principal ya esa estática o dinámica, la cual entre en falla, y esto se logra colocando una distancia administrativa mayor a la asignada a la ruta principal, en términos simples esta distancia administrativa es la confiabilidad de la ruta, de manera que si existe más de una ruta el *router* elegirá la ruta con menor distancia administrativa.

La distancia administrativa puede ir de 1 a 255, este número se coloca al final del comando después de especificar porque medio saldrá el mensaje.

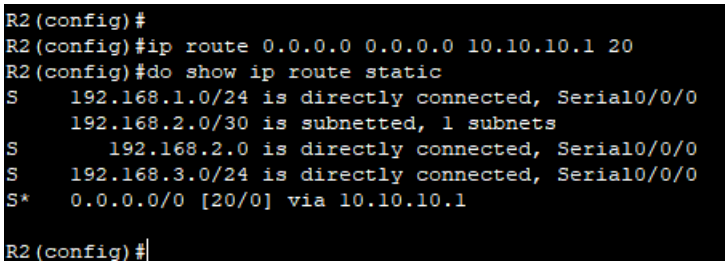
Figura 126. **Modificación para configuración de ruta flotante**



Fuente: elaboración propia, realizado con cisco packet tracert.

Como podemos observar en la figura 126, es similar a la figura 119, con el cambio que se configurará el R2 con su interfaz *Serial* 0/0/1 como ruta flotante.

Figura 127. **Configuración de ruta flotante**



Fuente: elaboración propia, realizado con cisco packet tracert.

5. CONFIGURACIÓN DE ENRUTAMIENTO DINÁMICO EN DISPOSITIVOS CISCO

5.1. DHCP

En los capítulos anteriores hemos podido realizar las configuraciones de direccionamiento *IP* de manera manual o estática, sin embargo, se cuenta con un método que realizará la asignación de esta dirección de manera dinámica la cual es conocida como protocolo de configuración dinámica de *host* y más conocido por sus siglas en inglés (*DHCP*).

Este servidor es fácil de administrar y es escalable, su funcionalidad se basa en asignar o prestar una dirección *IP* de un grupo de direcciones por un tiempo limitado o bien hasta que el host ya no necesite dicha dirección.

Dicho proceso se realiza de manera cliente / servidor, lo que significa que el cliente se comunica con el servidor, y este a su vez le presta una dirección IP al cliente, esto lo debe realizar periódicamente como se menciona anteriormente la dirección IP es por tiempo limitado.

5.1.1. Configuración de servidor DHCP

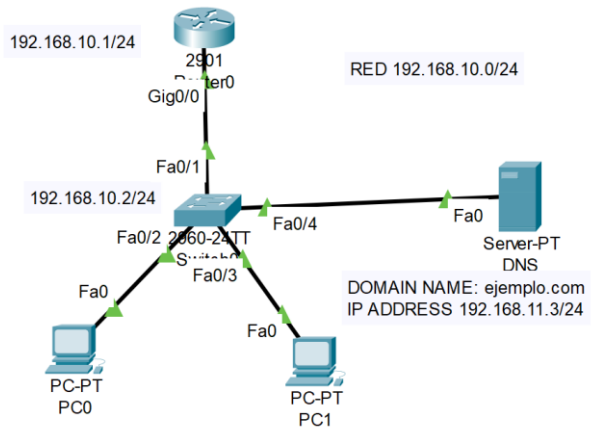
Este proceso se realiza desde un servidos, pero para fines de explicación en este manual se realizará desde el enrutador, ya que los dispositivos cisco cuentan con la configuración IOS para que puedan funcionar como servidores DHCP.

Para la configuración se deben seguir los siguientes pasos

- Ingresar a modo configuración global.
- Excluir las direcciones *IP* que no se deseen en *POOL DHCP* con el comando *ip dhcp excluded-addresss* + *ip* inicial + *ip* final.
- Configurar el nombre del *POOL DHCP* con el comando *ip dhcp pool* + nombre.
- Configurar el grupo de direcciones a utilizar con el comando *network* + direcciones *ip* + mascara de subred.
- Ingresar la direccione de *router* predeterminado con el comando default *router* + dirección *IP*.
- Configurar el servidor *DNS* con el comando *dns-server* + dirección *IP*.
- Colocar el nombre del dominio con el comando *domain-name* + dominio.

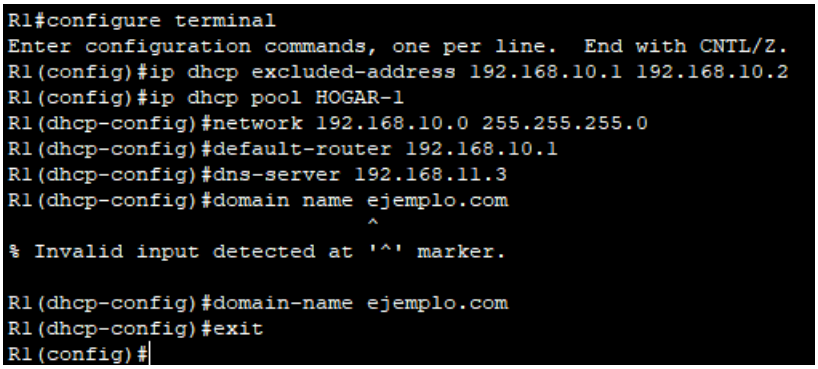
Nota: Se configura *DNS* solamente si se tiene servidor de no contar con *DNS* no se configura.

Figura 128. **Ejemplo de red para configuración DHCP**



Fuente: elaboración propia, realizado con cisco packet tracert.

Figura 129. **Configuración DHCP en router**

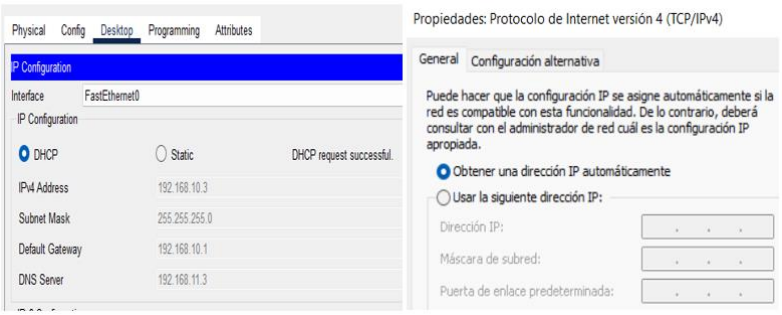


Fuente: elaboración propia, realizado con cisco packet tracert.

Como podemos observar en la figura 129, ya contamos con la información necesaria para la configuración ya que como se ha visto en capítulos anteriores las configuraciones de los dispositivos se saltó este paso.

Una vez configurado nuestro *router* podemos proceder a realizar la verificación en nuestros dispositivos finales (*HOST*), para lo cual debemos de ingresar a las configuraciones IP de la PC y cambiar de estático a *DHCP* si es el caso del simulador, si lo realizaremos de forma real, se configurará en las propiedades del protocolo de internet versión 4.

Figura 130. **Configuración DHCP en host**



Fuente: elaboración propia, realizado con cisco packet tracert.

5.1.2. Configuración de Cliente DHCP

Si en nuestros equipos contamos con un dispositivo al cual necesitamos que su dirección IP sea otorgada por medio de *DHCP*, en la cual una interfaz debe realizar esta petición, se debe realizar de la siguiente manera:

- Ingresar al método de configuración global.
- Ingresar a la interfaz a configurar.
- Colocar descripción a la interfaz.
- Ingresar el comando *ip address* dhcp.
- Activar la entrada con el comando no *shutdown*.

Figura 131. **Configuración DHCP en cliente**

```
SOHO(config)# interface G0/0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
Sep 12 10:01:25.773: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/0/1
assigned DHCP address 209.165.201.12, mask 255.255.255.224, hostname SOHO
```

Fuente: elaboración propia, realizado con cisco packet tracert.

Podemos observar que, al configurar el *DHCP* en una interfaz, esta al activar la misma otorgara la información de la conexión al servidor *DHCP*, con lo que podemos constatar que la configuración ha sido realizada de forma correcta.

Sin embargo, se cuenta con algunos dispositivos como por ejemplo routers inalámbricos los cuales contienen la opción de recibir la dirección de forma automática sin necesidad de realizar esta configuración.

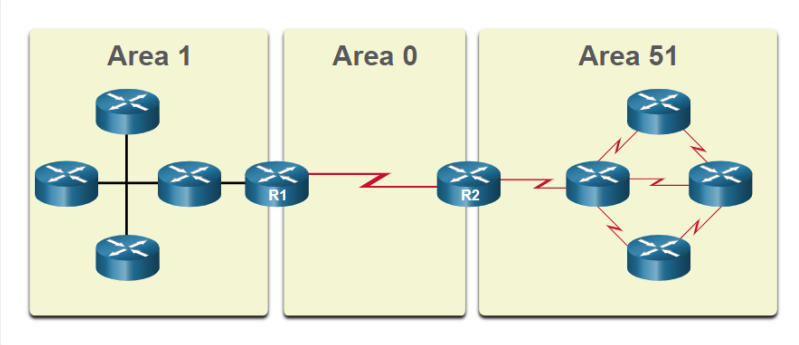
5.2. OSPF Versión 2

Este es un protocolo de direccionamiento conocido por sus siglas en ingles *Open Shortest Path First*, el cual se basa en envió de datos por el camino más corto, su forma de operar es por medio de áreas, ya que el técnico de redes puede segmentar el dominio en diferentes áreas.

El área *OSPF* es un conjunto de *routers* que comparten la información, por lo cual se puede realizar de dos maneras:

- *OSPF* de área única: Es la red en la cual todos los *routes* convergen en una misma área.
- *OSPF* Multiarea: Se implementa cuando se cuenta con distintas áreas, las cuales deben de contar con comunicación mediante un área troncal.

Figura 132. **Ejemplo de OSPF multiarea**



Fuente: Cisco. *Redes empresariales, Seguridad y Automatización*. Consultado el 20 de diciembre de 2022 recuperado de https://contenthub.netacad.com/ensa-dl/1.1.1.

5.2.1. Funcionamiento de OSPF

El protocolo envía una serie de paquetes para determinar cuál es la ruta más rápida, a esos se les conoce como paquetes de enlace de estado (*LSP*) y su función es mantener las adyacencias con los vecinos e intercambiar actualizaciones de enrutamiento. Los paquetes son:

- *Hello*: Encuentra vecino y genera adyacencias entre ellos.
- *DBR*: Los descriptores de base de datos sincronizan las bases de datos de los routers.
- *LSR*: La solicitud de estado de enlace, consulta el estado de router a router.
- *LSU*: La actualización de estado de enlace, envía solamente los registros del enlace que se solicita.
- *LSAck*: El acuse de recibo, reconoce todos los tipos de paqueres.

Por lo cual al activar el *OSPF* el *router* automáticamente verifica si encuentra otro vecino *OSPF*, esto lo realiza enviando el paquete *HELLO* por todas sus interfaces, al encontrar un *router* con *OSPF* este intentara crear una adyacencia con el *router* que genero el paquete *HELLO*.

Sincronización de *DB* (bases de datos). Una vez ya se han asignado en las listas de vecinos ambos *routers*, proceden a realizar los estados de sincronización.

Primero deciden quien será el *router* que envié primero los paquetes *DBD*, esto dependerá quien tenga el *ID* más alto, como segundo paso intercambiarán paquetes *DBD*, para finalizar envían un paquete *LSR*.

5.2.2. Configuración de OSPF

Como ya conocemos el funcionamiento del protocolo *OSPF*, es momento de aprender a configurarlo para realizar redes punto a punto. Para lo cual primeramente debemos habilitar este protocolo usando el comando *router* ospf + *id* de proceso, esto es para identificar nuestro *router* y el número de proceso puede ir del 1 hasta 65,535.

El ID toma acción para crear las adyacencias entre nuestros *router* conectados a *ospf*, por lo que se recomienda utilizar el mismo *process ID* para los *routers* de una misma área, aunque no es muy necesario que sean iguales.

De no configurar este *process ID* el router tomará la dirección más alta *IP* versión 4 de las interfaces de *loopback*, y la asignará como *process ID*. Si por otra parte no se configura una interfaz *loopback*, entonces se tomará la dirección *IPv4* activa que sea más alta, pero este método es el menos recomendado, ya que es difícil para el administrador *diferenciar* los *routers* específicos.

Para configurar la interfaz *loopback* debemos de crearla con una máscara de subred de 32 bits la cual seria 255.255.255.255 y se utilizará el comando interface *loopback* + número de *loopback*, luego seguimos el proceso para asignar una dirección IP en una interfaz.

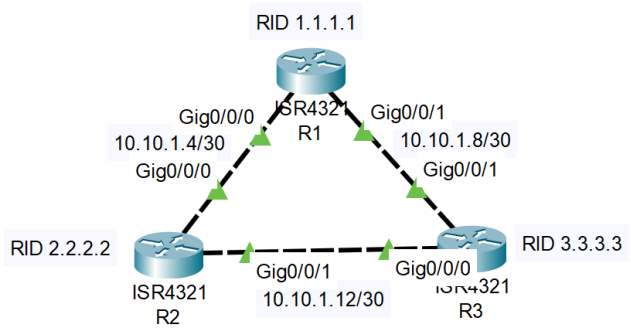
Como último paso para la identificación de un *router* debemos de asignarle una dirección *ID* para lo cual ingresaremos de la siguiente manera:

- Ingresamos a modo de configuración global.
- Habilitamos el protocolo *OSPF router* ospf + *id* de proceso.

- Asignamos la dirección ID con el comando *router-id* + octeto.

Si por alguna razón deseamos cambiar o modificar el *router ID* debemos de limpiar el proceso *OSPFv2*, esto se realiza para eliminar las adyacencias que se hayan realizado por lo cual debemos utilizar el comando *clear ip* ospf *process*.

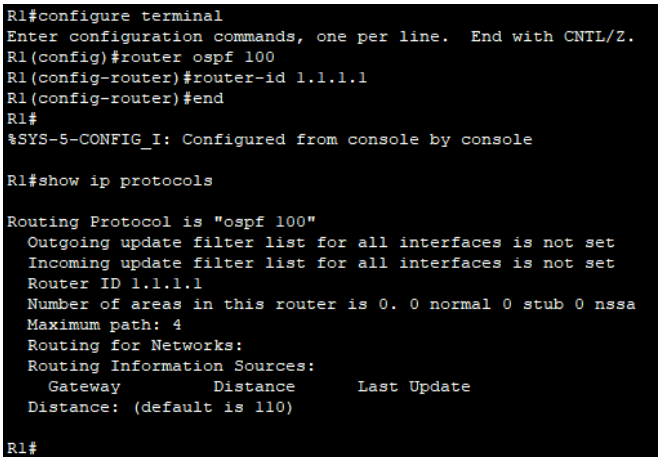
Figura 133. **Diagrama de routers OSPF**



Fuente: elaboración propia, realizado con cisco packet tracert.

Según la figura 132, se realizará la configuración de *ID* de los *router*, tomando en cuenta que para ello ya se realizaron las configuraciones básicas, así también asignación de *IP* en interfaces. Para dicho ejemplo utilizaremos el *process id* con numero 100 para todos los *router* ya que estarán en la misma área.

Figura 134. **Configuración de ID de router**



Fuente: elaboración propia, realizado con cisco packet tracert.

Como se puede apreciar en la imagen anterior con el comando *show ip protocols*, podemos la información de nuestra configuración indicándonos el ID de nuestro *router* así también el protocolo y el proceso que se está utilizando.

Con los *router* ya identificados es momento de realizar la configuración punto a punto, esto lo podemos realizar de dos maneras:

- Por comando *network*.
- Por comando *ip* ospf.

5.2.2.1. Configuración por comando network

Antes de adentrarnos en esta configuración debemos tener en cuenta el uso de la *wildcard mask,* la cual es la inversa de la máscara de subred de nuestro direccionamiento *IP*, por lo que para conocer la *wildcard mask* para nuestro

enrutamiento solo debemos realizar una resta entre una máscara de 32 bits y la máscara de nuestra subred.

Ejemplo 5.1

Se desea conocer la *wildcard* de las siguientes direcciones IP

- 192.168.19.0/24
- 10.10.10.2/30

Sabemos que los prefijos 24 y 30 son:

- 255.255.255.0 = prefijo 24
- 255.255.255.252 = prefijo 30

Por lo que la resta seria:

$$\begin{array}{r} 255.255.255.255 \\ -\ 255.255.255.0 \\ \hline 0.0.0.255 \end{array} \qquad \begin{array}{r} 255.255.255.255 \\ -255.255.255.252 \\ \hline 0.0.0.3 \end{array}$$

Entonces el resultado sería:

- Para el prefijo 24 / 0.0.0.255
- Para el prefijo 30 / 0.0.0.3

Ahora que ya sabemos calcular la *wildcard* podremos configurar nuestra red, sin embargo, hay otro tema a considerar puesto que se solicitará un número de área, este número indicará a que sector pertenece nuestra red ya que esta

red puede ser MULTI-AREA, pero en nuestro ejemplo por ser una red pequeña todas las redes pertenecerán a una misma red.

Para realizar la configuración *network* se deben seguir los siguientes pasos:

- Ingresar a modo de configuración global.
- Ingresar al protocolo *OSPF* ya habilitado.
- Ingresar las redes conocidas por nuestro *router* con el siguiente comando *network* + dirección *IP* de la red + *wildcard* + área + *id* de área.
- Repetimos el paso anterior las veces necesarias para gestionar todas las redes conocidas por el *router*.

Para el ejemplo seguiremos utilizando la imagen 5 – 6, pero a esta le agregaremos a cada *router* una red LAN:

- R1 192.168.10.0/24
- R2 192.168.20.0/24
- R3 192.168.30.0/24

Figura 135. **Configuración de OSPF por comando network**

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 100
R1(config-router)#network 10.10.1.4 0.0.0.3 area 0
R1(config-router)#network 10.10.1.8 0.0.0.3 area 0
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#exit
```

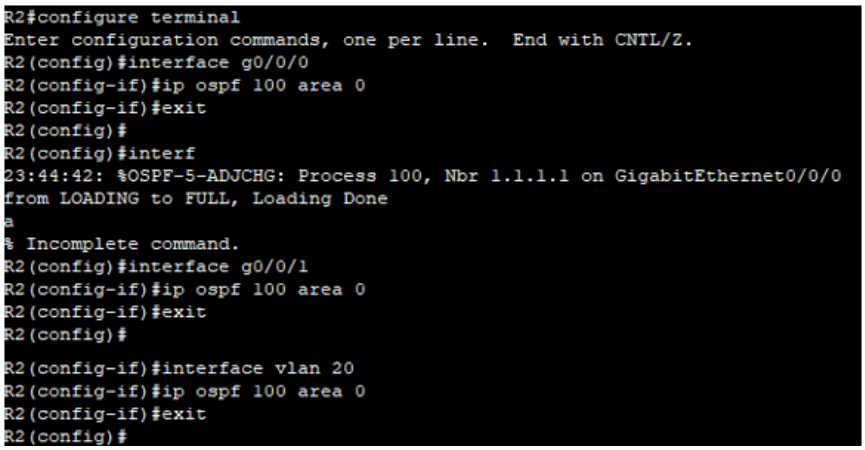
Fuente: elaboración propia, realizado con cisco packet tracert.

5.2.2.2. Configuración OSPF por comando IP OSPF

Podemos realizar la configuración de *OSPF* desde la interfaz, sin la necesidad de conocer la dirección *IP* y la *wildcard*, esto mediante el comando *ip ospf*. Para lo cual se deben seguir los siguientes pasos:

- Ingresar a modo de configuración global.
- Ingresamos a la interfaz deseada.
- Ingresamos el comando *ip* ospf + *process id* + área + número de área.
- Repetimos el paso anterior para todas las *interfaces* a configurar.

Figura 136. **Configuración OSPF por comando IP OSPF**

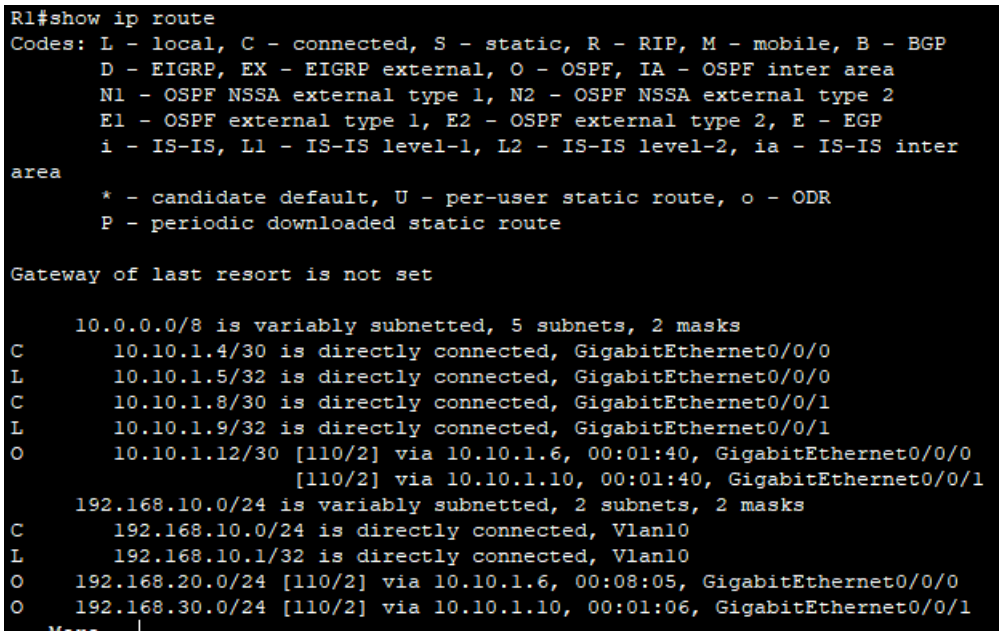


Fuente: elaboración propia, realizado con cisco packet tracert.

Como podemos observar en la imagen al conectar con otro dispositivo con protocolo *OSPF* configurado, este se sincroniza de manera automático con el *ID* del *router*, por lo que significa que la conexión ha sido exitosa.

También se puede visualizar la tabla de enrutamiento, en la cual veremos que se cuentan con nuevas redes conocidas las cuales como ya se ha mencionado anteriormente por ser reconocidas bajo el protocolo *OSPF* se verán reflejadas con la letra O.

Figura 137. **Tabla de enrutamiento de R1**



Fuente: elaboración propia, realizado con cisco packet tracert.

5.3. Lista de control de acceso

Ya conocemos como generar tráfico de datos entre dispositivos enrutados pero que sucede si necesitamos restringir el acceso a cierto tipo de datos, o bien necesitemos que no todos los datos sean permitidos en una red *LAN*, la solución es la lista de control de acceso (*ACL*), mediante el encabezado del paquete el *router* tomara la decisión si permite el acceso o lo niega.

La *ACL* controla si un *router* reenvía o descarta un paquete y esta lista se basa en las entradas de control de acceso (*ACE*), a las cuales se les conoce como instrucciones de *ACL*, por lo que este realiza una filtración de paquetes.

Estas listas pueden ser de dos modos:

- *ACL* estándar: La forma de filtración la realiza mediante la dirección *IPv4* de origen.
- *ACL* extendida: Puede realizar la filtración por medio de la dirección IPv4 ya sea de origen o destino, pero cuenta con una segunda opción la cual es por medio de la capa 4 ya sea por medio de los puertos *UDP* o *TCP*.

Algunas funciones con las que cuentan las *ACL* son:

- Limitación de tráfico.
- Aumento de rendimiento en la red.
- Mejor control del flujo de tráfico.
- Brindan prioridad a ciertos tipos de trafico de red.

5.3.1. Funcionamiento de ACL

Como primer paso el *router* toma la dirección de origen, esto mediante el encabezado del paquete, luego se compara la dirección *IPv4* tomada con cada entrada de control de acceso, esto de forma secuencial, a continuación, si se encuentra alguna conciencia se tomará la decisión establecida para ese paquete ya sea permitiendo su acceso o rechazándolo.

Cabe mencionar que siempre se tomará la primera *ACE* encontrada por el *router*, de existir alguna otra *ACE* que pudiera coincidir con esta se descartará automáticamente.

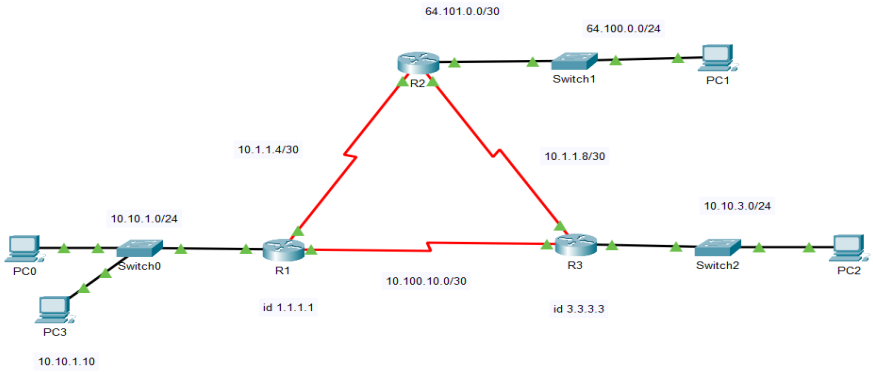
Por último, si la dirección IPv4 no tiene ninguna coincidencia con alguna *ACE*, el paquete será descartado ya que en esta configuración existe una *ACE* de negación ya implícita la cual se aplica de forma automática a todas las *ACL*.

5.3.2. Configuración de ACL

Ya que entendimos el funcionamiento de la *ACL*, podemos iniciar el proceso de configuración, para esta configuración se requiere de entradas de control de acceso (*ACE*). Por lo que el comando a utilizar es *Access-list* + número de lista + {*deny* | *permit*}, entonces se deben seguir los siguientes pasos:

- Ingresar a modo de configuración global.
- Crear la *ACL* con comando ya establecido *acces-list* + # de lista + {*deny* | *permit*} + dirección *IP* + *wildcard*.
- Se deben crear primero las direcciones que no tendrán acceso al *router* y luego las direcciones que si contaran con acceso.
- Ubicar la *ACL* lo más en la interfaz más cercana al destino.
- Ingresar a la interfaz y activar la *ACL* con el comando *ip access-group* + # de lista + *out.*

Figura 138. **Ejemplo de configuración ACL**



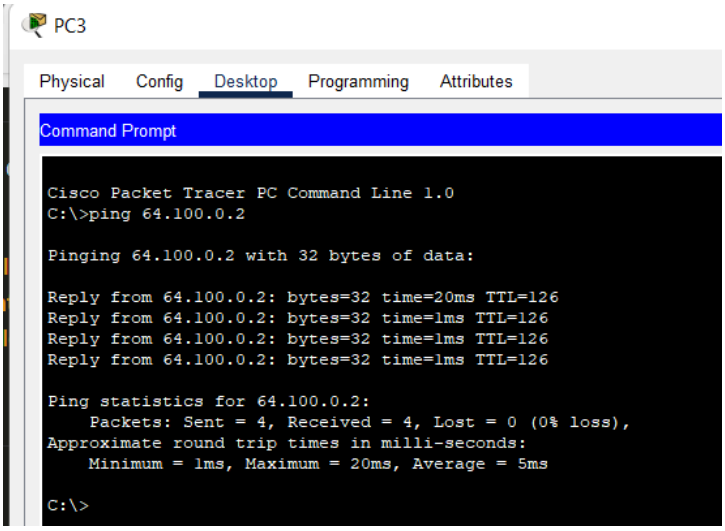
Fuente: elaboración propia, realizado con cisco packet tracert.

Para el siguiente ejemplo se usará la configuración de la figura 5 -11, en la cual se negará los paquetes enviados por medio del PC 3 con IP 10.10.1.10, y se permitirán las demás *IP*, esto hacia la PC1 con IP 64.100.0.2.

Entonces las configuraciones se deben realizar en R2.

Como primer paso verificaremos que se tenga conexión desde la PC3 hacia el destino PC1.

Figura 139. **Verificación de conexión de PC 3 a PC 1**

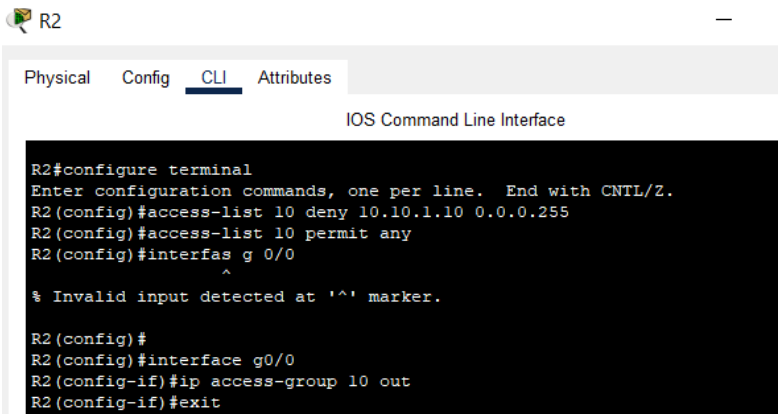


Fuente: elaboración propia, realizado con cisco packet tracert.

Como podemos observar, al realizar la prueba de *ping*, nuestro *host* logra la comunicación hacia el destino que es la PC1.

Como segundo paso realizaremos las configuraciones explicadas anteriormente en nuestro *router*

Figura 140. **Configuración de ACL en R2**

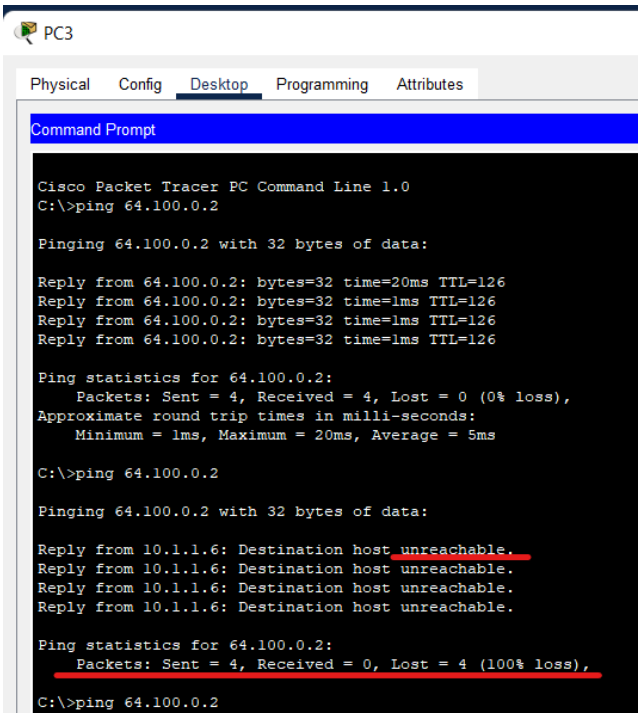


Fuente: elaboración propia, realizado con cisco packet tracert.

Observemos que la lista de acceso creada es una lista estándar ya que el numero de la lista se encuentra entre 1 y 99, adicional a ello la lectura de las listas de acceso es lineal, lo que significa que a la primera coincidencia realizará lo solicitado en la lista y saldrá de ella, es por ello que se colocan primero los accesos que negara.

Como último paso verificaremos que nuestra configuración funcione de manera correcta por lo que realizaremos un *ping* nuevamente desde la PC3 de la cual no se está permitiendo el acceso y veremos que mostrara un mensaje en él envió de datos.

Figura 141. **Prueba PING hacia PC1 con ACL**



Fuente: elaboración propia, realizado con cisco packet tracert,

Como podemos observar la PC3 no reconoce la dirección que anteriormente contaba con comunicación y en las especificaciones del *PING* se logra apreciar que de los 4 paquetes enviados los 4 se perdieron, por lo que podemos afirmar que nuestra *ACL*, se encuentra funcionando de manera correcta.

CONCLUSIONES

1. Por medio de la herramienta cisco packet tracert se otorga el apoyo necesario, para la configuración de manera física; ya sea por medio de conexión remota o conexión por consola, para la elaboración de una red a nivel LAN.

2. Se indica el proceso correcto de instalación y acceso a la herramienta de simulación para realizar configuraciones de los equipos, así también, se comenta de forma básica cómo funciona cada herramienta del simulador.

3. Se explica conceptos básicos necesarios para la realización de una red de manera completa, adicional a ello se detalla practicas necesarias para la buena sintaxis de programación en los equipos.

4. En el presente trabajo de graduación se detalla con ejemplos, los procesos necesarios para la configuración de los dispositivos, acompañados de su explicación teórica.

5. Se brinda por medio de ilustraciones las configuraciones necesarias para cada una de las configuraciones realizadas en el presente trabajo de graduación.

6. Para conexiones simples, de las cuales no se tenga contemplado ampliar la red, la forma de enrutamiento estático, es la que mejor se adecua, sin embargo, para redes en la que se contemple expansión, es mejor el enrutamiento dinámico.

RECOMENDACIONES

1. Para optar a una certificación en CCNA, ingresar al curso de redes en la página oficial de CISCO, ya que en el presente trabajo de graduación se realiza en base a enrutamientos.

2. El seguimiento constante de los temas explicados, puesto que CISCO puede renovar las versiones e información, este documento toma referencia de la versión 7.

3. Completar los conocimientos aprendidos, con métodos de conexión inalámbrica, seguridad de los equipos y ciberseguridad, en la página oficial de CISCO.

4. Tener extremo cuidado con las configuraciones de contraseñas en los dispositivos, en los modos de usuario y modo privilegiado, ya que de perder estas contraseñas se deberá restablecer a los parámetros de fábrica los equipos, por lo que en ocasiones puede ocasionar perdida de información en el mismo.

5. Para configuraciones de forma física el etiquetado de los cables, así también, en las configuraciones colocar descripciones a cada proceso que lo amerite, con el fin de contar con un sistema ordenado.

6. Al finalizar alguna configuración de manera correcta, copiar de la memoria running-config a la memoria startup-config, esto para mantener las configuraciones aun cuando se apague el equipo.

7. Crear sistemas redundantes para mantener la operación de manera óptima.

REFERENCIAS

1. Alcalá, Universidad (2017). *Protocolos de enrutamiento dinámico.* Recuperado de http://atc2.aut.uah.es/~rosa/LabRC/Prac_3/Prac_3.ProtocolosEnrutamientoDinamico_RIP_y_OSPF.pdf.

2. Ariganello Ernesto (2016). *Redes cisco, Guía de estudio para certificación*. Madrid, España: Editorial RA-MA, S.A. Recuperado de https://books.google.com.ec/books?id=tpBFDwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false.

3. Cisco. *Cisco Networking Academy*. Recuperado de https://www.netacad.com/es.

4. Cisco. *Cisco Packet Tracert.* Recuperado de https://www.netacad.com/es/courses/packet-tracer.

5. Corporation. Oracle. *Help Center*. Recuperado de https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html.

6. Huidobro, José Manuel (2014). *Telecomunicaciones tecnologías, redes y servicios*. Madrid, España: Editorial RA-MA, S.A.

7. Redesccna2cisco (2018). *Introducción al enrutamiento y envió de paquetes*. Recuperado de https://www.sites.google.com/site/redesccna2cisco/cap-1introduccion-al-enrutamiento-y-envio-de-paquetes.

8. Stallings, William (2004). *Comunicaciones y redes de computadores*. Madrid, España: Editorial Pearson educación, S.A.

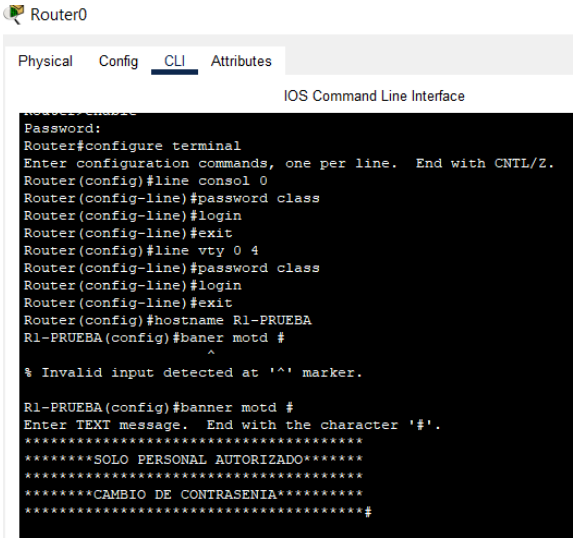
9. Veracruzana. Universidad (2014). *Enrutamiento estático*. Recuperado de https://www.uv.mx/personal/ocruz/files/2014/01/Enrutamientoestatico.pdf.

APÉNDICE

Apéndice 1. **Restablecimiento de contraseña de dispositivos ya configurados, de los cuales no tenemos acceso**

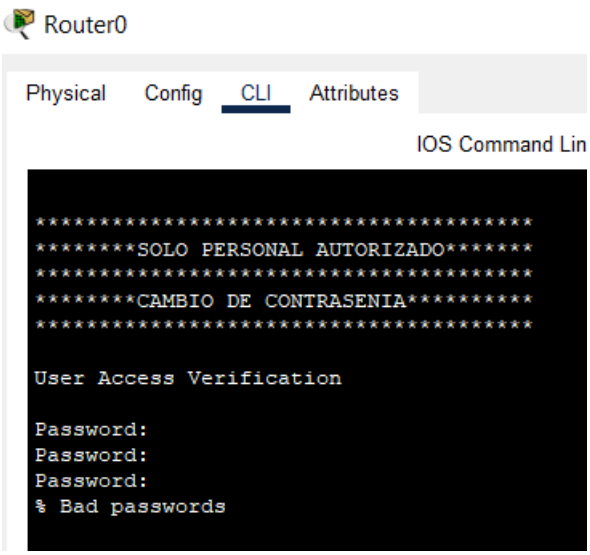
Un problema que podemos encontrar en los dispositivos en los cuales se trabaja es no conocer o que se olvide la contraseña que se le ha configurado anterior mente por lo cual se debe de realizar un proceso para ingresar al dispositivo de otra manera para poder cambiar la contraseña, sin afectar las configuraciones.

Apéndice 1. **Ingreso a Cll**



Fuente: elaboracion propia, realizado con cisco packet tracert.

Apéndice 2. **Contraseña invalida**



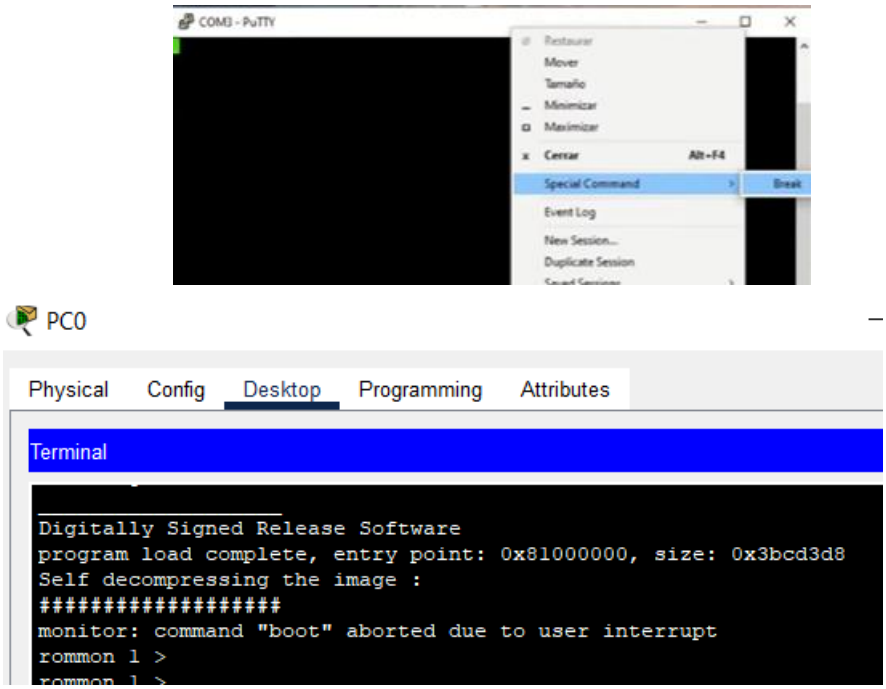
Fuente: elaboracion propia, realizado con cisco packet tracert.

Como observamos en la imagen anterior no conocemos la contraseña del router que queremos configurar. Por lo tanto, debemos cambiar las contraseñas, sin perder las configuraciones que ya posea nuestro dispositivo.

Primer paso a realizar es apagar el dispositivo de manera física, esperar como mínimo 5 segundos y vamos a encenderlo para entrar por medio del monitor de la ROM, para ello si lo estamos realizando en el simulador al entrar en consola debemos presionar Crtl+(*break*/*pause*), con el teclado, antes que termine de cargar la inicialización del dispositivo.

Si en cambio estamos usando un programa como por ejemplo PuTTy solo debemos dar *click* derecho, *Special Command* > *Break*.

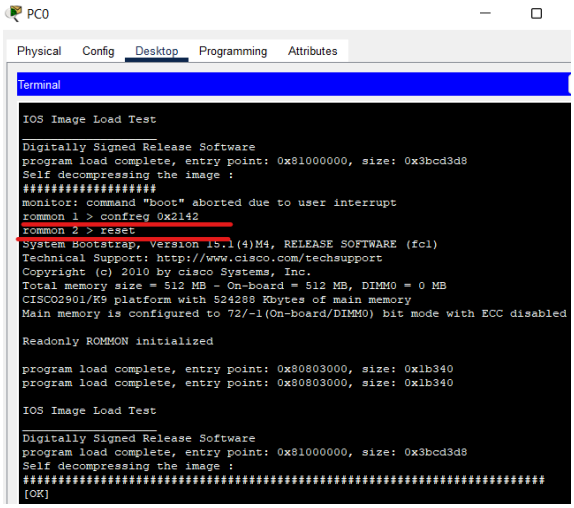
Apéndice 3. **Ingreso de forma segura por comandos**



Fuente: elaboracion propia, realizado con cisco packet tracert.

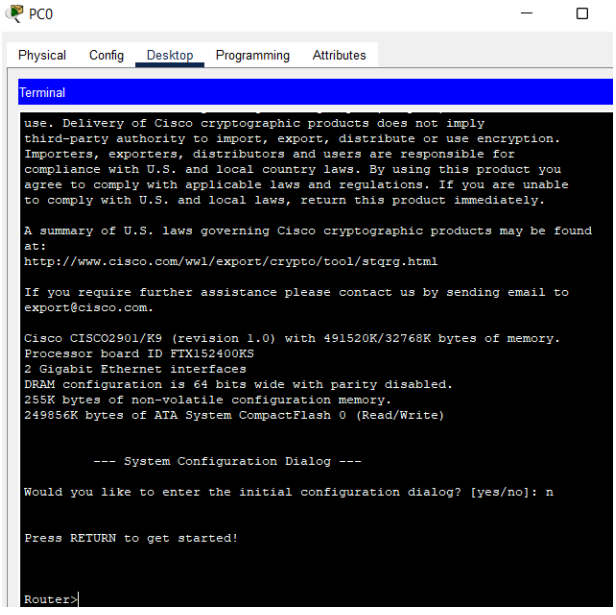
Una vez ingresamos colocaremos el comando de modo de recuperación confreg 0x2142, con este comando nos permitirá ingresar en un modo de arranque en el cual no tomará en cuenta los archivos de configuración existentes, y luego colocamos el comando *reset*.

Apéndice 4. **Reset en desde consola**



Fuente: elaboracion propia, realizado con cisco packet tracert.

Apéndice 5. **Reingreso normal en CLI**

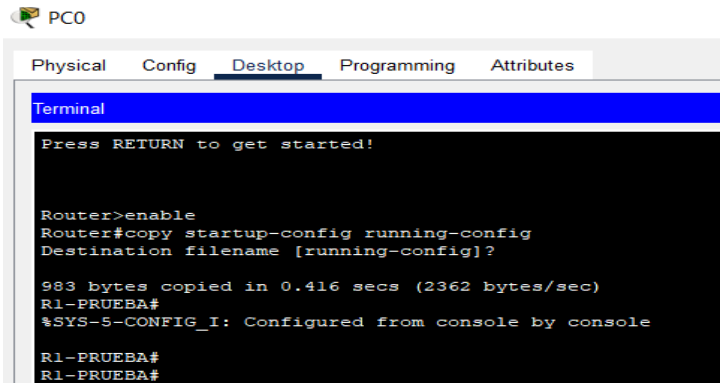


Fuente: elaboracion propia, realizado con cisco packet tracert.

Observemos que ingresamos al *router* que no tiene ninguna configuración, por lo tanto, debemos de pasar lo que se tiene configurado en la *NVRAM* (*startup-config*), a la *RAM* (*running-config*), y esto lo realizamos con el comando *copy*.

Una vez realizado lo anterior podemos corroborar que nos encontramos en la configuración del *router* puesto que el nombre ha cambiado al nombre configurado anteriormente.

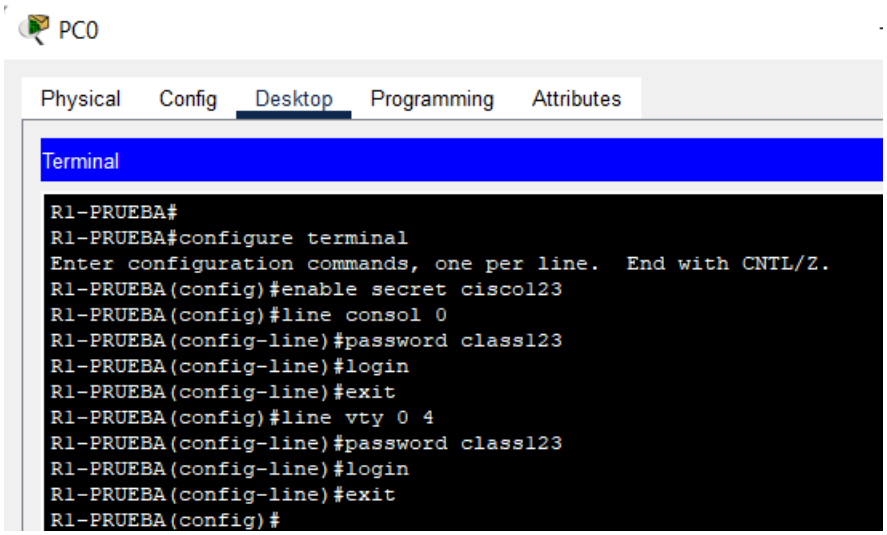
Apéndice 6. **Verificación de acceso**



Fuente: elaboracion propia, realizado con cisco packet tracert.

Desde este punto podemos realizar los cambios de contraseña, sin perder las configuraciones del equipo.

Apéndice 7. **Cambio de contraseña**

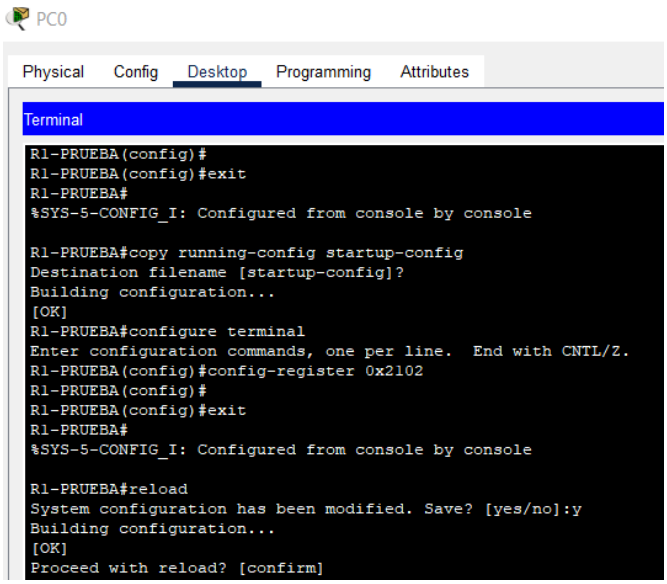


Fuente: elaboracion propia, realizado con cisco packet tracert.

Como último paso debemos pasar nuevamente lo configurado a la *NVRAM*, lo cual es con el comando *copy* y adicional a ello debemos cambiar el valor de registro de configuración lo cual se realiza con el comando *config-register* 0x2102, para que al apagar el equipo tenga en cuenta la configuración del equipo.

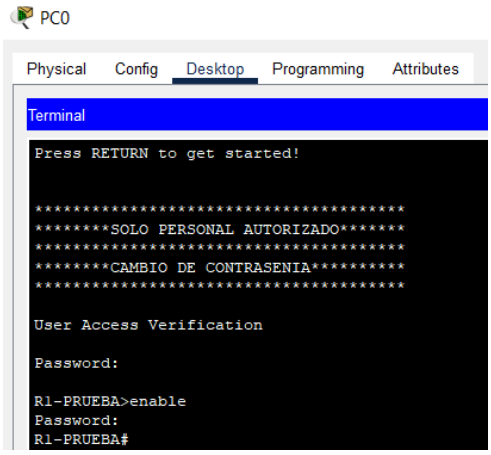
Por último, realizamos un reinicio con el comando *reload* y veremos que ya podremos ingresar con las contraseñas configuradas, esto sin haber perdido la configuración inicial que tenía nuestro equipo.

Apéndice 8. **Guardar cambios**



Fuente: elaboracion propia, realizado con cisco packet tracert.

Apéndice 9. **Prueba de nueva contraseña**



Fuente: elaboracion propia, realizado con cisco packet tracert.