



UNIVERSIDAD JOSÉ ANTONIO PÁEZ

**DESARROLLO DE PRÁCTICAS
ESTRUCTURADAS BAJO UN ENFOQUE CISCO
PARA EL LABORATORIO DE REDES DE
COMUNICACIONES DE LA UNIVERSIDAD JOSÉ
ANTONIO PÁEZ**

Autor: Genesis Theis
C.I. 25.009.134

Urb. Yuma II, Calle N° 3, Municipio San Diego
Teléfono: (0241) 8714240 (Máster) - Fax: (0241) 871239.



**REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES**

**DESARROLLO DE PRÁCTICAS ESTRUCTURADAS BAJO UN ENFOQUE
CISCO PARA EL LABORATORIO DE REDES DE COMUNICACIONES DE LA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ**

**Trabajo de grado presentado como requisito para optar al título de
INGENIERO DE TELECOMUNICACIONES**

Autor: Genesis N. Theis P.

C.I: 25.009.134

Tutor: Ing. Javier Clavo.

San Diego, Junio de 2017



Universidad José Antonio Páez
Facultad de Ingeniería

FI-TG-2017-1CR-009

Valencia, 13 de Enero de 2017.

Ciudadana:
Theis Genesis
C.I. 25.009.134
Presente.-

Cumplo con informarle que la Comisión de Trabajo de Grado y Pasantías de la Facultad de Ingeniería en su reunión N° 1-2017 de fecha 13/01/2017 aprobó el proyecto de trabajo de grado titulado **"DESARROLLO DE PRÁCTICAS ESTRUCTURADAS BAJO UN ENFOQUE CISCO PARA EL LABORATORIO DE REDES DE COMUNICACIONES DE LA UNIVERSIDAD JOSÉ ANTONIO PÁEZ."** Presentado por usted como requisito para optar al título de Ingeniero en Telecomunicaciones.

Se ratifica la designación del Ing. Javier Clavo, C.I. 15.627.432 y la Ing. Alicia Pizzella, C.I. 4.598.880 como Tutotes Académicos que lo asesorarán en el desarrollo de este proyecto.

Atentamente,

Prof. Marlene Zambrano
Decana (Encargada) de la Facultad de Ingeniería
(CU 502 de fecha 11/10/2016)



c. c. Coordinación de Pasantías y Trabajo de Grado (2).
Archivo.

MEZ/jp



REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUOLA DE INGENIERÍA DE TELECOMUNICACIONES

ACEPTACIÓN DEL TUTOR

Quien suscribe, **Ing. Javier Clavo**, portador de la cédula de identidad N°15.627.432, en mi carácter de tutor del trabajo de grado presentado por la ciudadana **Genesis Theis**, portadora de la cédula de identidad N° 25.009.134, titulado **DESARROLLO DE PRÁCTICAS ESTRUCTURADAS BAJO UN ENFOQUE CISCO PARA EL LABORATORIO DE REDES DE COMUNICACIÓN DE LA UNIVERSIDAD JOSÉ ANTONIO PÁEZ** presentado como requisito parcial para optar al título de Ingeniero de Telecomunicaciones, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del jurado examinador que se designe.

En San Diego, a los 09 días del mes de Junio del año dos mil diecisiete.

Ing. Javier Clavo C.I.: 15.627.432



AGRADECIMIENTOS.

A mis Padres.

Por el apoyo confianza y esfuerzo, por ser pilares fundamentales en mi formación como ser humano, por estar allí siempre a mi lado brindándome apoyo pacientemente, sin ustedes habría sido imposible recorrer este camino.

A los Profesores.

A todos aquellos maestros que en este andar por la vida, influyeron con sus lecciones y experiencias en formar personas de bien y preparadas para los retos que pone la vida, a todos y cada uno de ellos gracias por contribuir con el resultado de mi formación.

A la Universidad José Antonio Páez.

Por ser mi Alma Mater, lugar que me entrego la capacidad de desenvolverme en el mundo profesional. Y por último a todas aquellas personas que de alguna manera contribuyeron a la realización de este trabajo de grado.

A todos mi mayor y sincero agradecimiento.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS.....	viii
ÍNDICE DE CUADROS.....	viii
RESUMEN.....	ix
INTRODUCCION.....	1

CAPÍTULO

I EL PROBLEMA

1.1 Planteamiento del problema.....	3
1.2 Formulación del problema.....	4
1.3 Objetivos de la investigación.....	5
1.3.1 Objetivo general.....	5
1.3.2 Objetivos específicos.....	5
1.4 Justificación.....	5
1.5 Alcance.....	6
1.6 Limitaciones.....	6

II MARCO TEÓRICO

2.1 Antecedentes de la investigación.....	7
2.2 Bases teóricas.....	8
2.2.1 Redes de computadoras.....	8
2.2.2 Redes punto a punto.....	8
2.2.3 Redes multipunto.....	9
2.2.4 Redes de área local (LAN).....	9
2.2.5 Redes de área metropolitana (MAN).....	9
2.2.6 Redes de área amplia (WAN).....	9
2.2.7 Redes de área local inalámbrica (WLAN).....	10
2.2.8 Componentes de las redes.....	10
2.2.9 Topología de las redes.....	14
2.2.10 Protocolos.....	16
2.2.11 Protocolo TCP/IP.....	17
2.2.12 Modelo OSI.....	22
2.2.13 Switching.....	24
2.2.14 Habilitación IP en un Switch.....	27
2.2.15 Routing.....	27
2.2.16 Sistema Operativo OSI.....	30
2.2.17 Acceso mediante CLI.....	31
2.2.18 Programas de emulación terminal.....	33
2.2.19 Modos de funcionamiento de Cisco.....	33
2.2.20 Ayuda contextual del IOS bajo CLI.....	36

2.2.21 Verificación de comando.....	37
2.2.22 Teclas de acceso rápido.....	37
2.2.23 Fundamentos de Diseño de la Guía de Laboratorio.....	38
2.3 Definición de Términos Básicos.....	39
III MARCO METODOLÓGICO	
3.1 Tipo de investigación.....	40
3.2 Diseño de la investigación.....	40
3.3 Nivel de investigación.....	41
3.4 Población y muestra.....	41
3.5 Fuentes, Técnicas e instrumentos de recolección de datos.....	42
3.6 Fases metodológicas.....	42
IV RESULTADOS	
4.1 Fase I.....	45
4.1.1 Tabulación de Resultados.....	46
4.1.2 Interpretación de Resultados.....	53
4.2 Fase II.....	53
4.3 Fase III.....	54
4.4 Fase IV.....	56
Manual de Prácticas de Laboratorio enfocado en Tecnología Cisco Para la Materia Redes de Comunicaciones.....	57
CONCLUSIONES.....	95
RECOMENDACIONES.....	96
REFERENCIAS BIBLIOGRÁFICAS.....	97
REFERENCIAS ELECTRONICAS.....	98
ANEXOS.....	99
1. Instrumento de Investigación.....	100
2. Carta de Validación del Instrumento.....	103
3. Prueba de funcionalidad de la practica N°2.....	105
4. Prueba de funcionalidad de la practica N°4.....	110

ÍNDICE DE FIGURAS

Figura.	Pág.
1. Modem.....	11
2. Hub.....	12
3. Switch.....	13
4. Router.....	13
5. Topología anillo.....	15
6. Topología bus.....	15
7. Topología en árbol.....	16
8. Topología en estrella.....	16
9. Suite de protocolos TCP/IP.....	22
10. Estructura Jerárquica de los Modos del IOS.....	35
11. Grafico 1.....	47
12. Grafico 2.....	48
13. Grafico 3.....	49
14. Grafico 4.....	50
15. Grafico 5.....	51
16. Grafico 6.....	52

ÍNDICE DE CUADROS

Cuadros.	Pág.
1. Cuadro 1.....	46
2. Cuadro 2.....	47
3. Cuadro 3.....	48
4. Cuadro 4.....	49
5. Cuadro 5.....	50
6. Cuadro 6.....	51
7. Cuadro 7.....	52



**REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES**

**DESARROLLO DE PRÁCTICAS ESTRUCTURADAS BAJO UN ENFOQUE
CISCO PARA EL LABORATORIO DE REDES DE COMUNICACIÓN DE LA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ**

Autor: Theis P. Genesis N.

Tutor: Ing. Javier Clavo.

Fecha: Junio 2017

RESUMEN

La presente investigación se desarrolla en la Universidad José Antonio Páez en el laboratorio de redes de comunicaciones, en el cual existe una problemática con el uso de los equipos de tecnología Cisco que allí se encuentran ya que estos equipos no son usados en su totalidad por los alumnos que cursan dicha asignatura, por lo cual se plantea la elaboración de una serie de prácticas enfocadas en dicha tecnología, lo que hace necesario evaluar la situación actual de las prácticas existentes, identificar los equipos Cisco con que cuenta el laboratorio y por último estudiar los aspectos básicos de la tecnología Cisco que son necesarios para el aprendizaje profesional de los estudiantes que cursan dicha materia, este trabajo investigativo tiene como resultado el crecimiento del aprendizaje de los alumnos ya que podrán hacer uso los equipos de dicha tecnología a nivel profesional. El trabajo realizado se enmarca en la línea de investigación “Avances tecnológicos en tecnologías de información y comunicación”, bajo la modalidad de proyecto factible, de nivel descriptivo, con diseño de investigación de campo.

Descriptor: Práctica, redes de comunicación, telecomunicaciones.

INTRODUCCIÓN

Debido a los cambios y desarrollo de la sociedad, se considera hoy en día que la comunicación es un punto fundamental del crecimiento de la humanidad, desde tiempos inmemoriales el hombre ha buscado maneras de poder mantener comunicación con otros de su especie a través de las distancias de una forma eficaz, ingeniando sistemas pasando desde las ideas más rudimentarias hasta ideas más sofisticadas como las que se ven hoy en día, la necesidad de mantenerse en comunicación constante ha llevado al ser humano al desarrollo de una serie de tecnologías capaces de enviar datos a través de redes de comunicación a cualquier parte del mundo en una forma precisa y casi instantánea, tecnologías como la Internet manejada a través de redes de comunicación se han vuelto de tal importancia para la humanidad que hoy en día organismos tan importantes como las Naciones Unidas las consideran parte de los derechos humanos fundamentales del hombre, partiendo de estas razones es que se dice que hoy en día también es fundamental tener un recurso humano que sea capaz de diseñar y mantener toda la instalación necesaria para las comunicaciones.

El siguiente trabajo investigativo nace de una necesidad que se plantea en la Facultad de Ingeniería de la Universidad José Antonio Páez (UJAP), específicamente en la materia Redes de Comunicaciones de la escuela de Ingeniería de Telecomunicaciones, la ausencia del estudio y manejo de equipos de tecnología cisco, ha generado en mi como investigadora el estímulo para plantear una serie de prácticas estructuradas de manera que pueda contribuir en una mejor formación para el estudiante de la carrera de Ingeniería de Telecomunicaciones, dada la importancia que tiene para el futuro profesional en esta carrera el manejo de las redes de comunicación y la utilidad que representa para la sociedad la comunicación por medio de redes, es que se ha considerado un tema interesante de estudio en cuanto a la formación práctica del capital humano que egresará de esta casa de estudios.

Este proyecto de grado está enmarcado como un proyecto factible, está destinado a determinar soluciones a una problemática específica que se genera en la materia Redes de

Comunicaciones, para realizar la investigación ha sido necesaria la colaboración de la institución, de sus profesores y de personal capacitado en el área, se ha obtenido información importante de todos los estudiantes de la mencionada materia y se ha consultado con trabajos de grado semejantes a esta investigación. El objetivo fundamental de este proyecto es el de enseñar el manejo y configuración de los equipos de tecnología cisco, comotambién colaborar con la generación de conocimiento práctico, que sea de utilidad para la formación de los futuros profesionales de la carrera de Ingeniería de Telecomunicaciones, siendo esta investigación base para su desarrollo en el conocimiento de la materia Redes de Comunicaciones. Esta investigación se encuentra dividida en 4 capítulos, conformados de la siguiente manera:

Capítulo I: **El Problema** En él se realiza el planteamiento del problema, el propósito de la investigación, los objetivos que se buscan alcanzar en el desarrollo del proyecto, la justificación y finalmente el alcance.

Capitulo II: **Marco Teórico** este capítulo hará referencia a las investigaciones y proyectos de la misma índole que se hayan hecho con anterioridad, así como también las bases teóricas las cuales son un soporte en la realización del proyecto.

Capitulo III. **Marco metodológico.** Se planteó todo lo referente al proceso de investigación, definiendo el tipo, diseño y nivel de investigación, así como la población y la muestra para la recolección de datos. Igualmente se explican cada una de las fases a realizar durante el desarrollo del trabajo.

Capítulo IV. **Resultados.** Se presentan los recursos requeridos para cumplir con los objetivos específicos que se plantearon en el trabajo de grado.

CAPÍTULO I

EL PROBLEMA.

1.1 Planteamiento del problema.

En la actualidad el intercambio de información es algo que está presente en el día a día, que se necesita obligatoriamente y con lo que no podríamos subsistir, se puede hablar de intercambio de información a todos los niveles, desde la comunicación básica basada en un emisor y un receptor, hasta la comunicación basada entre un emisor y múltiples receptores.

Para poder realizar estos intercambios de información de la manera más óptima y eficaz se debe seguir una serie de procedimientos, normativas y estándares que sean los adecuados para obtener el mayor rendimiento ya que en una red no solo el cableado es importante, si no que se debe tener una distribución lógica y planificada, ya que las redes sin diseño abundan en la realidad y la misión de los ingenieros en telecomunicaciones es mejorarlas, para ello es fundamental conocer los principios básicos del diseño de redes y configuración de equipos tales como switches y routers.

Es muy importante para la formación del estudiante de telecomunicaciones el conocer a fondo la tecnología Cisco, puesto que esto le permite estar capacitado para la realización del diseño, instalación, configuración y mantenimiento de redes, además de adquirir las habilidades para visualizar la localización y aislamiento de problemas que puedan existir en la red. Los estudiantes de ingeniería en telecomunicaciones deben ser capaces de adaptarse a los cambios acelerados y continuos que la tecnología enfrenta diariamente, para ello las soluciones de switching y routing ofrecen una ventaja estratégica a la redes de cualquier tamaño y en cualquier sector ya que sus avances tecnológicos impulsan a la productividad de los usuarios, fomentan la excelencia operativa y aumentan el valor comercial de la

red y de los recursos conectados. Las plataformas extensibles y los servicios de switching y routing inteligentes hacen realidad toda la promesa de las redes sin fronteras en forma escalable, segura, confiable y transparente.

Actualmente los estudiantes de ingeniería en telecomunicaciones durante su pensum curricular deben obligatoriamente cursar en el noveno semestre la asignatura teórico-práctico redes de comunicaciones, la cual tiene como objetivo principal el aprendizaje continuo de las redes de computadoras y todo lo referente a lo que el área se refiere. Esta asignatura también cuenta con un laboratorio de redes que se encuentra ubicado en la Universidad José Antonio Páez donde los estudiantes pueden realizar el montaje de sus prácticas y exponer los conocimientos teóricos adquiridos en aplicaciones de prácticas de laboratorio. El mencionado laboratorio se encuentra ahora mismo en la dicha de disponer equipos de tecnología Cisco, pero con la desdicha de que actualmente estos equipos no están siendo integrados completamente a las prácticas regulares que los estudiantes allí realizan.

Considerando que en el mercado y la industria la tecnología Cisco es la que predomina en el área de redes, se hace necesario incluir dentro de las prácticas del laboratorio de redes de comunicaciones, un área dedicada a la configuración y programación de estos equipos, ya que no han sido tomados en cuenta como herramienta para la formación académica de los alumnos, siendo indispensable que el alumno tenga la experiencia de trabajar con estos dispositivos. En base a lo expuesto anteriormente nace la necesidad de desarrollar una serie de prácticas estructuradas para el laboratorio de redes de comunicaciones bajo un enfoque cisco, las cuales serán una forma de profundizar los conocimientos del estudiante, y a su vez optimizar y dinamizar la interrelación entre el conocimiento teórico y la aplicación práctica.

1.2 Formulación del problema.

En este sentido, se presenta la siguiente interrogante, ¿De qué manera se podrá impartir de una forma más sistemática y organizada las prácticas de laboratorio de la materia Redes de Comunicaciones, de forma que pueda mejorar la experiencia de aprendizaje del alumno?

1.3 Objetivos de la investigación.

1.3.1 Objetivo general.

Desarrollar prácticas estructuradas bajo un enfoque Cisco para el laboratorio de redes de comunicaciones de la Universidad José Antonio Páez.

1.3.2 Objetivos específicos

- Evaluar la situación actual de las prácticas existentes en el laboratorio de redes de comunicaciones.
- Identificar los equipos Cisco con que cuenta el laboratorio de redes de comunicaciones.
- Estudiar, organizar y seleccionar los aspectos básicos de la tecnología Cisco, que son necesarios para el aprendizaje y desempeño profesional de los estudiantes.
- Elaboración de un manual de trabajo con prácticas de laboratorio desarrolladas paso a paso y enfocadas en tecnología Cisco para los estudiantes de ingeniería en telecomunicaciones, de manera que permita al estudiantado de la materia Redes de Comunicaciones desarrollar de una forma eficaz el conocimiento académico en el laboratorio de acuerdo a las necesidades actuales y a las condiciones del Laboratorio de Redes.

1.4 Justificación

El uso de manuales académicos en las clases prácticas es en la actualidad ampliamente aceptado como una forma óptima de aprovechar el tiempo y adquirir conocimientos de manera eficiente, es por ello que la elaboración de las practicas destinadas a la programación y configuración de tecnología Cisco sería una forma de optimizar y dinamizar la interrelación entre el conocimiento teórico y la aplicación práctica.

El diseño de estas prácticas capacitara y preparara a los estudiantes para que puedan configurar y programar a nivel de software y hardware el equipamiento que se necesita para la creación de redes confiables y escalables, así como también comprobar físicamente el desarrollo funcional de una red.

Contar con un manual de laboratorio destinado a las prácticas de configuración Cisco en el laboratorio de Redes de Comunicaciones permitiría además al estudiante enriquecer el tiempo empleado en el laboratorio para obtener los conocimientos prácticos y la experiencia adecuada de la materia, puesto a que dicho manual le permite estar capacitado para la realización del diseño, instalación, configuración y mantenimiento de redes, además de adquirir las habilidades para enfrentarse a los retos tecnológicos que se encuentran en el mercado ya que cuando hablamos de routing, switching, aplicaciones de red, protocolos y servicios, Cisco es privilegiadamente la marca número uno a nivel mundial.

1.5 Alcance

Con la realización de este trabajo de grado se pretende llegar hasta el diseño de prácticas de laboratorio enfocadas en tecnología Cisco, permitiendo al estudiante ser parte activa de la generación del conocimiento mediante la elaboración de prácticas sistemáticamente organizadas en un manual de laboratorio, tomando en cuenta que se respeten las unidades descritas por el cronograma de actividades de la materia redes de comunicaciones.

Este proyecto buscará también mejorar, organizar y simplificar de forma eficiente la adquisición de conocimientos académicos tanto teóricos como prácticos en cuanto a tecnología Cisco se refiera en el Laboratorio de la materia Redes de Comunicaciones y de esta forma los estudiantes se encontraran capacitados para manejar a nivel profesional la tecnología que prevalece en el mercado de las redes de comunicaciones Cisco.

1.6 Limitaciones

Algunas de las limitaciones en este trabajo de investigación se encuentran dadas por la falta de tiempo requerido a lo largo del semestre para el cumplimiento de las prácticas en su totalidad ya que en el amplio mundo de las redes existe un gran campo de información y por ende se pueden realizar un sin fin de prácticas enfocadas en tecnología Cisco, Otra de sus limitaciones es debido a que la tecnología de los equipos con que cuenta el laboratorio no es muy nueva y por ende esto representa una gran limitación al momento de salir al mercado profesional ya que estos equipos no son con los que frecuentemente el profesional se encuentra en la industria de las telecomunicaciones.

CAPÍTULO II

MARCO TEORICO

2.1 Antecedentes

La transmisión de datos se ha convertido en parte fundamental de la comunicación, y del desarrollo de las Redes de Telecomunicaciones, mediante la incorporación de innovaciones tecnológicas que han acortado las distancias, facilitando las comunicaciones y modificando los estilos de vida, a continuación se muestran algunos estudios que guardan similitud con la investigación seleccionada.

Tejedor, J. (2014), en su trabajo de grado titulado, “**Diseño, Implementación, Administración y Enrutamiento Avanzado bajo el núcleo IOS CLI (CISCO)**”, proyecto de trabajo de grado presentado en la Universitat Politècnica de València, que tuvo como objetivo el diseño, implementación y administración de una red de área local con conexiones externas a nivel de campus en la Universitat Politècnica de València, e implementado mediante una simulación con el programa Cisco Packet Tracer. El mencionado trabajo de grado, es una guía de los conceptos que se necesitan para la creación de redes confiables y escalables, mediante el uso de equipamiento de tecnología Cisco.

Así mismo, Clavo, J. y Barrientos, G. (2013), en su trabajo de grado titulado “**Desarrollo de un manual de prácticas para el laboratorio de redes de comunicación**”, proyecto de trabajo de grado presentado en la Universidad José Antonio Páez, que tuvo como finalidad el desarrollo de un manual de laboratorio el cual contiene un conjunto de prácticas que ayudan a contribuir en una mejor formación al estudiante de la carrera de Ingeniería de Telecomunicaciones, Este proyecto aporta a la investigación información tanto teórica como práctica la cual buscará mejorar de forma eficiente la adquisición de conocimientos académicos en el desarrollo del manual de las prácticas de laboratorio.

Por último, Bautista, M.(2013), en su trabajo de grado titulado “**Manual de prácticas de laboratorio de Redes de datos seguras**”, proyecto de trabajo de grado presentado en la Universidad Nacional Autónoma de México, este proyecto de grado se baso la elaboración de un manual de prácticas de redes de datos seguras, el cual ayuda a los alumnos a utilizar y manejar las herramientas necesarias para la administración adecuada de las redes de datos. El mencionado trabajo de grado, es una guía de la metodología que debe ser usada al momento de la elaboración de cada una de las prácticas estructuradas de laboratorio que conforma el manual.

2.2 Bases Teóricas

En esta etapa del proyecto se estudiarán y definirán los términos y teorías relacionadas con las redes, sus características, componentes, y conocimientos necesarios para comprender las redes de comunicaciones, así como los conceptos, aplicaciones, servicios y protocolos de red, enfocados en tecnología Cisco, para lograr un entendimiento más claro y preciso de lo que se explica en el proyecto.

2.2.1 Redes de Computadores

Las redes de computadores son un conjunto de computadores interconectados entre sí donde la conexión no necesita hacerse a través de un hilo de cobre, también puede hacerse mediante el uso de láser, microondas y satélites de comunicación con la finalidad de compartir recursos. Estos recursos comprenden desde una impresora hasta archivos, todo esto con la utilización de ciertas normas y dispositivos que con el avance tecnológico van facilitando el trabajo de los usuarios de forma transparente, que no imagina la complejidad que va por debajo de toda la interconexión.

2.2.2 Redes Punto a Punto

Las redes punto a punto abarca la conexión de dos equipos por medio de un canal, también son conocidas como peer to peer o entre iguales, en este tipo de redes ambos equipos prestan el recurso, es decir, ambas máquinas son el cliente y el servidor al mismo tiempo. Las redes entre iguales ofrecen la ventaja de que su velocidad, además de tener un costo bastante bajo, con una facilidad de uso pero solo requiere de dos equipos (numero de

usuario limitado) y su utilización es para redes caseras donde la utilización no es para grandes volúmenes de información.

2.2.3 Redes Multipunto

Las redes multipunto son redes en las cuales cada canal de datos se puede usar para comunicarse con diversos nodos. En este tipo de redes, las terminales compiten por el uso del medio (línea) de forma que el primero que lo encuentre disponible lo acapara, aunque también puede negociar su uso. Es decir, en términos más sencillos la información fluye de manera bidireccional y es discernible para todas las terminales de la red. Las ventajas dadas por este tipo de redes es que son muy flexibles al momento de ser administradas, aunque pueden perder velocidad y seguridad.

2.2.4 Redes de área local (LAN: Local Area Network)

Son redes de propiedad privada que operan dentro de un solo edificio, como una casa, oficina o fábrica. Las redes LAN se utilizan ampliamente para conectar computadoras personales y electrodomésticos con el fin de compartir recursos (por ejemplo, impresoras) e intercambiar información. La velocidad de transferencia de datos en una red de área local puede alcanzar hasta 10 Mbps y 1 Gbps.

2.2.5 Redes de área metropolitana (MAN: Metropolitan Area Network)

Una red de área metropolitana es un sistema de interconexión de equipos informáticos distribuidos en una zona que abarca diversos edificios, por medios pertenecientes a la misma organización propietaria de los equipos. Generalmente interconectan tanto a sistemas individuales como a otras LAN. Este tipo de redes representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas de una cobertura superior que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

2.2.6 Redes de rea amplia (WAN: Wide Area Network)

Este tipo de redes consisten en una colección de equipos y redes individuales conectadas a través de una infraestructura llamada subred, esta subred está formada por una serie de líneas retransmisión interconectadas por medio de routers. Su tamaño puede variar

entre los cien y mil kilómetros (Km.), lo que la diferencia de las demás es que proporciona un medio de transmisión a larga distancia de datos, voz, imágenes, videos, sobre grandes áreas geográficas que pueden llegar a extenderse hacia un país, un continente o el mundo entero. El ejemplo más actual y de mayor dimensión de éste tipo de red es Internet.

2.2.7 Redes de área local inalámbrica (WLAN: Wireless Local Area Network)

Es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre varias computadoras

2.2.8 Componentes de las redes

- **Servidores:** Es el encargado de gestionar los recursos y la información compartida, pudiendo ser un servidor físico, quien es el encargado de ejecutar el sistema operativo de red y ofrecer los servicios de red a las estaciones de trabajo, o simplemente un software (sistema operativo de red), donde básicamente su función es coordinar y manejar las actividades de los recursos del ordenador en una red.
- **Estaciones de Trabajo:** Las estaciones de trabajos pueden ser computadoras personales, se encargan de sus propias tareas de procesamiento, así que cuanto mayor y más rápido sea el equipo, mejor.
- **Clientes:** Equipos que acceden a los recursos compartidos de la red ofrecidos por los servidores.
- **Medio:** Mediante él se transmiten los datos y es el elemento encargado de la conexión física de los equipos, tanto los terminales entre sí (clientes) como con el servidor o con otros dispositivos de la red. Tradicionalmente, el medio más utilizado ha sido el cable (trenzado, coaxial o fibra óptica), aunque también se han utilizado los medios inalámbricos (ondas de radio, microondas o infrarrojos).

- **Datos compartidos:** Archivos suministrados a los clientes por parte de los servidores a través de la red.
- **Dispositivos de interconexión:** Entre los dispositivos denominados básicos que son utilizados para el diseño de redes, tenemos los siguientes:
 - Ø **Modem:** Dispositivo que tiene la importante función de comunicar los equipos informáticos que forman parte de una red con el mundo exterior, es decir, es el aparato en donde se conecta el cable principal de red y que recibe la información de la línea telefónica. Estos dispositivos pueden conectar varias redes entre sí.

El funcionamiento de los modem es simple. El ordenador o red emisora envía señales digitales que son convertidas a señales analógicas en el modem emisor y viajan a través de líneas telefónicas hasta su destino, donde el modem receptor convierte la señal analógica nuevamente en una señal digital que podrá ser interpretada por un ordenador. **(Ver figura 1).**



Figura 1: Modem

Fuente: <http://culturacion.com/dispositivos-basicos-para-conexion-de-redes/>

- Ø **Hub:** Un hub recibe una señal, la regenera y la envía a todos los puertos. El uso de hubs crea un buslógico. Esto significa que la LAN utiliza medios de acceso múltiple. Los puertos utilizan un método de ancho de banda compartido y a menudo

disminuyen su
(Ver figura 2).

la recuperación



Figura 2: Hub

Fuente:<http://www.omniseccu.com/basic-networking/>

- Ø **Switch:** Es un dispositivo similar al hub, con la diferencia de que en vez de retransmitir la señal a todos los puertos la envía solamente al puerto al que está conectado. Un switch reduce las colisiones en una LAN. Cada puerto del switch crea un dominio de colisiones individual. Esto crea una topología lógica punto a punto en el dispositivo de cada puerto. Además, un switch proporciona ancho de banda dedicado en cada puerto y así aumenta el rendimiento de la red. El switch de una LAN también puede utilizarse para interconectar segmentos de red de diferentes velocidades. Si bien un switch es más costoso que un hub, resulta económico al considerar su confiabilidad y rendimiento mejorado. (Ver figura 3)
- Ø **Repetidores:** Los repetidores son dispositivos que deben ser utilizados para unir segmentos alejados de una red LAN. Estos no realizan ningún tipo de filtrado o direccionamiento, sólo conectan segmentos de red y restauran señales degradadas.
- Ø **Routers:** Estos dispositivos generalmente son los dispositivos más conocidos de las redes ya que tienen la particularidad de determinar el camino más rápido para enviar datos a través de la red y por supuesto, realizar el filtrado de tráfico en un segmento de red determinado.



Figura 3: Switch

Fuente:<http://www.cisco.com/c/en/us/support/switches/>

Estos dispositivos (Routers) pueden conmutar y encaminar los paquetes de información que son transmitidos a través de la red de intercambio de información de protocolos de comunicación. Existen diferentes tipos de routers, los estáticos, dinámicos y de difusión y pueden trabajar con cables o de manera inalámbrica. (**Ver figura 4**).



Figura 4: Router

Fuente:<http://routercisco.com.mx/seguridad-cisco/>

Ø **Gateway:** Estos dispositivos activan la comunicación entre arquitecturas y entornos y realizan el empaquetado y conversión de paquetes de datos que se van a transmitir a través de una red, en otras palabras es un servidor dedicado que tiene el poder de intercomunicar dos redes diferentes.

Existen tres tipos de Gateway:

De direcciones: conecta redes con directorios estructurados de manera diferente y con técnicas diferentes para el manejo de archivos.

De protocolo: conecta redes que utilizan diferentes protocolos.

De formato: conecta redes que utilizan diferentes formatos.

2.2.9 Topología de las redes

La disposición física de los equipos de comunicación en una red es llamada **topología**. Hay cuatro tipos principales topologías:

- 1. Topología Anillo:** Topología de red en la que cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación de trabajo tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación. La ventaja de esta red es que se puede operar a grandes velocidades, los mecanismos para evitar colisiones (choques entre paquetes de datos viajando por los conductores) son sencillos, además de poseer una simplicidad de arquitectura y facilidad de crecimiento, sin embargo tiene como desventaja que si algún nodo de la red deja de funcionar, la comunicación en todo el anillo se pierde. **(Ver figura 5).**
- 2. Topología de bus:** Esta topología se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos, de esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí. La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre sí. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente.

Los sistemas de bus, como Ethernet o la mayoría de los sistemas de banda ancha, emplean un cable bidireccional con trayectorias de avance y regreso sobre el mismo medio, o bien emplean un sistema de cable doble (o dual) para lograr la bidireccionalidad. En los

extremos del bus es necesario colocar “terminadores” que evitan que la señal se refleje y produzca colisiones. (Ver figura 6).

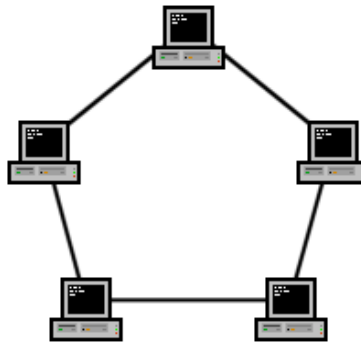


Figura 5: Topología Anillo

Fuente: <http://redestipostopologias.blogspot.com/2009/03/topologia-de-redes.html>

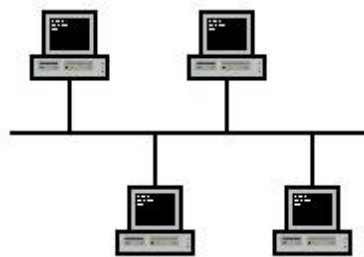


Figura 6: Topología de bus

Fuente: <http://redestipostopologias.blogspot.com/2009/03/topologia-de-redes.html>

3. **Topología en árbol:** Es una generalización de la topología en bus. Esta topología comienza en un punto denominado cabezal o raíz (headend). Uno ó más cables pueden salir de este punto y cada uno de ellos puede tener ramificaciones en cualquier otro punto. Una ramificación puede volver a ramificarse. En una topología en árbol no se deben formar ciclos.(Ver figura 7).
4. **Topología en estrella:** Una red en estrella es una red en la cual las estaciones están conectadas directamente a un nodo central y todas las comunicaciones que han de hacer necesariamente a través de este. Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un conmutador

(switch) o un concentrador (hub) siguen esta topología. El nodo central en estas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes.(Ver figura8).

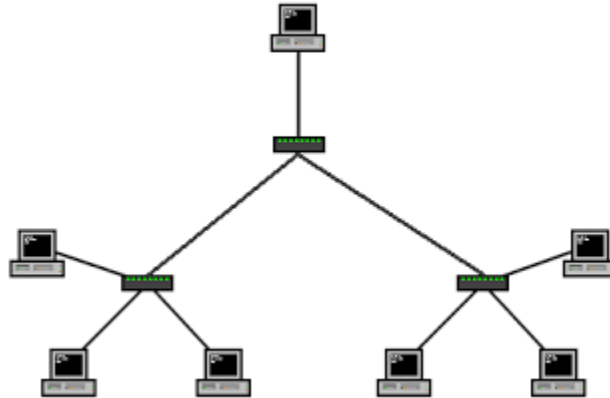


Figura 7: Topología en árbol

Fuente: <http://redestipostopologias.blogspot.com/2009/03/topologia-de-redes.html>

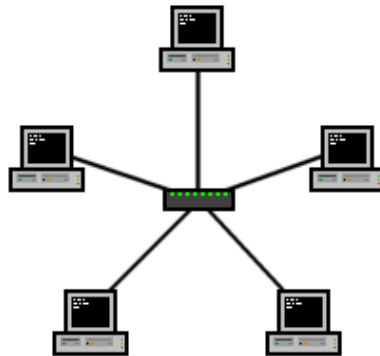


Figura 8: Topología en estrella

Fuente: <http://redestipostopologias.blogspot.com/2009/03/topologia-de-redes.html>

2.2.10 Protocolos

Los protocolos en una red enmarcan las reglas y pasos para la transmisión de datos, incluyendo el método de acceso y las regulaciones relacionadas con la topología, el

cableado y la velocidad de transferencia de datos. Enviar datos sobre la red involucra varios pasos que deben ser seguidos de manera consistente a fin de que la comunicación tenga lugar. La computadora que envía y la que recibe usan protocolos para:

- Cortar los datos en paquetes.
- Agregar información de direccionamiento a los paquetes.
- Preparar los paquetes para la transmisión.
- Tomar los paquetes del cable.
- Copiar los datos de los paquetes para ensamblarlos.
- Pasar los datos ensamblados a la computadora.

2.2.11 Protocolo TCP/IP (Transmisión Control Protocol / Internet Protocol)

El protocolo TCP/IP, es un conjunto de reglas o normas que determinan cómo se realiza el intercambio de datos entre dos ordenadores. Es quien se encarga de que los equipos puedan “hablar” en un lenguaje común, independientemente del tipo que sea o del sistema operativo que utilice. **(Ver figura 9)**.

El protocolo TCP se encarga de dividir las informaciones en paquetes de tamaño adecuado, numerar estos paquetes para que puedan volver a unirse en el lugar correcto y añadir cierta información para la transmisión y posterior decodificación del paquete y detectar posibles errores en la transmisión. El modelo TCP/IP consta de cuatro capas, las cuales son las siguientes:

- 1. Capa de Acceso al Medio:** Es la encargada de utilizar el medio de transmisión de datos para realizar un enlace físico real con otros dispositivos conectados a la red. Especifica la forma en la que los datos deben enrutarse, sea cual sea el tipo de red utilizado.

La capa de acceso al medio del modelo TCP/IP consta de una suite de protocolos:

- Ø **ARP (Address Resolution Protocol):** ARP (Protocolo de Resolución de Direcciones) es un protocolo cuyo principal objetivo es conocer la dirección física (MAC) de una tarjeta de interfaz de red correspondiente a una dirección IP.

- Ø **PPP (Point-to-Point Protocol):** PPP (Protocolo Punto a Punto) es un protocolo donde su función es la de proporcionar un medio de encapsulación de paquetes para transmitirlos a través de un enlace serial.
- Ø **Ethernet:** También conocido como estándar IEEE 802.3, es un estándar de transmisión de datos para redes de área local que define las reglas para establecer los estándares de cableado y señalización de la capa de acceso a la red.
- 2. Capa de Red:** La capa de red o también llamada Internet es la capa más importante (si bien todas son importantes a su manera), ya que es la que define los datagramas y administra las nociones de direcciones IP permitiendo el enrutamiento de datagramas IP hacia su destino, determinando la mejor ruta a través de varias redes. La capa de Red del modelo TCP/IP consta de una suite de protocolos:
 - Ø **IP (Internet Protocol):** el protocolo IP (Protocolo de Internet) es un protocolo que atiende todas las operaciones relacionadas con el encaminamiento de los paquetes del origen al destino, encargándose de etiquetar cada paquete de información con la dirección apropiada.
 - Ø **NAT (Network Address Translation):** NAT (Traducción de Direcciones de Red) es un protocolo que traduce las direcciones IP desde una red privada a direcciones IP públicas únicas de forma global.
 - Ø **ICMP (Internet Control Message Protocol):** ICMP (Protocolo de mensajes de control de Internet) es un protocolo que proporciona comentarios desde un host de destino a un host de origen con respecto a los errores en la entrega de paquetes, en otras palabras permite administrar información relacionada con errores de los equipos en red.
 - Ø **RIP (Routing information protocol):** RIP (protocolo de información de encaminamiento) es un protocolo de enrutamiento interior por vector distancia, es decir para la parte interna de la red. Es muy usado en sistemas de conexión en los que muchos usuarios se conectan a una red y pueden acceder por lugares distintos. Cuando uno de los usuarios se conecta el servidor de terminales avisa con un mensaje RIP al router más cercano advirtiéndole de la dirección IP que ahora le pertenece. Así podemos ver que RIP es un protocolo usado por distintos routers

para intercambiar información y así conocer por donde deberían enrutar un paquete para hacer que éste llegue a su destino.

Ø **EIGRP (Enhanced Interior Gateway Routing Protocol):** EIGRP (Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español) es un protocolo de gateway interior apropiado para muchos tipos diferentes de topologías y dispositivos. En una red correctamente diseñada, EIGRP escala de forma óptima y ofrece tiempos de convergencia extremadamente rápidos con un mínimo tráfico de red. Algunas de las varias ventajas de EIGRP son:

- Uso mínimo de los recursos de la red durante su funcionamiento normal; sólo se transmiten paquetes de saludo en una red estable.
- Cuando se produce un cambio, sólo se propagan los cambios en la tabla de ruteo, y no toda la tabla; con esto se consigue reducir la carga que el propio protocolo de ruteo deposita en la red.
- Tiempos de convergencia rápidos en la topología de la red (en determinadas situaciones, la convergencia puede llegar a ser casi instantánea).

EIGRP es un protocolo propietario de Cisco y de vector de distancia mejorado basado en el Algoritmo de actualización difuso (DUAL) para calcular el trayecto más corto hasta un destino dentro de la red.

Ø **OSPF (Open Shortest Path First):** OSPF (Camino más Corto Primero), es un protocolo de routing de estado de enlace desarrollado como reemplazo del protocolo de routing vector distancia RIP. OSPF es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad. OSPF se caracteriza por ser un protocolo:

- **Sin clase:** Por su diseño, es un protocolo sin clase, de modo que admite VLSM (máscara de subred de tamaño variable).
- **Eficaz:** Los cambios de routing dirigen actualizaciones de routing (no hay actualizaciones periódicas). Usa el algoritmo SPF (algoritmo que encuentra el mejor camino entre dos puntos)
- **Convergencia rápida:** Propaga rápidamente los cambios que se realizan a la red.

- **Escalable:** Funciona bien en tamaños de redes pequeños y grandes. Se pueden agrupar los routers en áreas para admitir un sistema jerárquico.
 - **Seguro:** Cuando están habilitados, los routers OSPF solo aceptan actualizaciones de routing cifradas de pares con la misma contraseña compartida previamente.
- 3. Capa de transporte:** Está diseñada para permitir que las entidades pares, en los nodos de origen y de destino, lleven a cabo una conversación. Aquí se definieron dos protocolos de transporte de extremo a extremo (TCP Y UDP).
- Ø **TCP (Transmission Control Protocol):** TCP (Protocolo de control de transmisión), Permite la comunicación confiable entre los procesos que se ejecutan en hosts independientes y sus transmisiones son confiables ya que entregan acuse de recibo lo que confirma el envío correcto.
 - Ø **UDP (User Datagram Protocol):** UDP (Protocolo de datagramas del usuario), protocolo que tiene como objetivo principal habilitar un proceso que se debe ejecutar en un host para enviar paquetes a un proceso que se ejecutara en otro host. Es un protocolo que no confirma la transmisión correcta de datagramas.
- 4. Capa de aplicación:** Contiene la lógica necesaria para llevar a cabo las aplicaciones de usuario, la capa de aplicación en TCP/IP incluye los detalles de las capas de presentación y de sesión del modelo OSI. También determina la presentación de los datos, y la codificación y control del dialogo. En esta capa de aplicación se encuentran los siguientes protocolos:
- Ø **DNS (Domain Name System):** DNS (Sistema o Servicio de Nombres de Dominio), es un servidor que traduce nombres de dominio a IPs y viceversa. En las redes TCP/IP, cada host dispone de una dirección IP para poder comunicarse con el resto de hosts, en palabras más sencillas, es un servidor que permite averiguar la IP de una PC a partir de su nombre. Para ello, el servidor DNS dispone de una base de datos en la cual se almacenan todas las direcciones IP y todos los nombres de los PCs pertenecientes a su dominio.

Los servidores DNS están dispuestos jerárquicamente de forma que cuando nuestro servidor más inmediato no puede atender nuestra petición, éste la traslada al DNS superior.

Ø **DHCP (Dynamic Host Configuration Protocol):** DHCP (Protocolo de Configuración Dinámica de Host), Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

El protocolo DHCP sirve principalmente para distribuir direcciones IP en una red. Cada equipo de una red TCP/IP debe tener una dirección IP única. La dirección IP (junto con su máscara de subred relacionada) identifica al equipo host y a la subred a la que está conectado. Al mover un equipo a una subred diferente se debe cambiar la dirección IP. DHCP permite asignar dinámicamente una dirección IP a un cliente a partir de la base de datos de direcciones IP del servidor DHCP de la red local.

Ventajas del uso de DHCP:

- Asignación automática de direcciones IP a los equipos, después de arrancar el ordenador.
- Con la configuración manual errónea se pueden tener problemas de red como por ejemplo la asignación de una misma dirección IP, lo que trae como consecuencia que la red no funcione correctamente. Con un servidor DHCP estos problemas dejan de existir ya que no existe la posibilidad de que se cometan errores humanos, por lo tanto la asignación de direcciones IPs siempre será correcta.
- La utilización de servidores DHCP puede reducir significativamente el tiempo necesario para configurar y modificar la configuración de los equipos de la red, trayendo como ventaja la reducción de personal capacitado para la configuración de los diferentes equipos que necesiten direcciones ip para su interconexión.

- Ø **SMTP (Simple Mail Transfer Protocol):** SMTP (Protocolo Simple de Transferencia de correo), es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos
- Ø **TFTP (Trivial File Transfer Protocol):** TFTP (Protocolo de Transferencia de Archivos Trivial), Es un protocolo que tiene como objetivo principal la transferencia de archivos simple, sin conexión y se caracteriza por ser un protocolo de entrega de archivos de máximo esfuerzo, sin confirmación.
- Ø **HTTP ():** HTTP (Protocolo de Transferencia de Hipertexto), básicamente se define como un conjunto de reglas para intercambiar texto, imágenes gráficas, sonido, video y otros archivos multimedia en la World Wide Web (WWW)

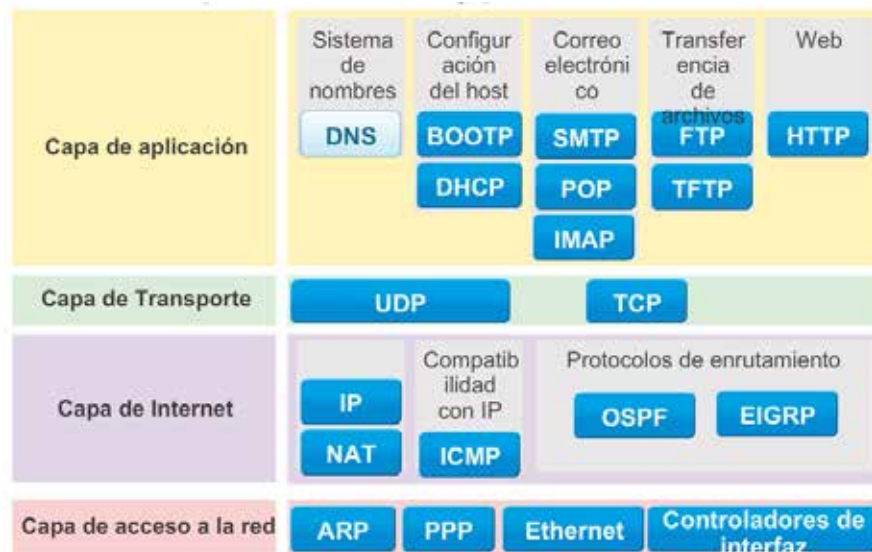


Figura 9: Suite de protocolos TCP/IP

Fuente: <https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html#3.2.2.3>

2.2.12 Modelo OSI

El modelo de referencia OSI es un modelo de los protocolos propuestos por ISO (Organización Internacional de Normalización) como protocolos abiertos interconectables en cualquier sistema.

El modelo OSI, Open System Interconnect (Interconexión de Sistemas Abiertos), es básicamente una estructura de normas comunes dentro de las redes y una referencia para todos los sistemas de comunicación, donde se define un modelo de capas en un entorno de sistemas abiertos. Tiene como finalidad permitir la comunicación entre distintos procesos en computadoras diferentes, independientemente de la arquitectura del hardware. Está estructurado en 7 capas:

- **Capa física(Physical):**Se encarga de los procedimientos necesarios para transmitir un flujo de datos a través de un medio físico, en esta capa los protocolos de capa física describen los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para la transmisión de bits hacia un dispositivo de red y desde él.
- **Capa de Enlace (Data Link):**En esta capa del modelo OSI los protocolos pertenecientes a la misma es decir los protocolos de enlace de datos describen los métodos para intercambiar tramas de datos entre dispositivos en un medio común,convirtiéndose de esta manera el flujo de bits proveniente de la capa física en una serie de tramas que puedan ser usadas por la capa de red. Se llevan a cabo funciones de control de flujo, y detección y corrección de errores para en caso de ser necesario retransmitir tramas dañadas o pérdidas.
- **Capa de Red (Network):**Proporciona servicios para intercambiar los datos individuales en la red entre dispositivos finales identificados, de la misma manera es la encargada de establecer caminos a través de la red, para hacer llegar la información agrupada en paquetes desde el origen hasta el destino. Para lo cual puede ser necesario pasar por varias máquinas intermedias. En esta capa residen los protocolos de enrutamiento.
- **Capa de Transporte (Transport):** La capa de transporte define los servicios para segmentar, transferir y rearmar los datos para las comunicaciones individuales entre dispositivos finales. La función principal es de aceptar los datos de la capa superior (sesión) y fragmentarlos de forma adecuada en unidades más pequeñas, para

posteriormente pasarlos a la capa de red, asegurando que todos los segmentos lleguen correctamente a su destino. Realiza el control de extremo a extremo de la comunicación, proporciona control de flujo y control de errores. Los protocolos que residen en ella al igual que el modelo TCP/IP son los protocolos UDP y TCP.

- **Capa de Sesión (Session):** La capa de sesión proporciona servicios a la capa de presentación para organizar su diálogo y administrar el intercambio de datos, es decir establece, administra y termina sesiones entre host.
- **Capa de Presentación (Presentation):** La capa de presentación proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación. Por lo general forma parte del sistema operativo y su función es dar formato los datos. Opcionalmente puede encriptar o comprimir la información.
- **Capa de Aplicación (Application):** En esta capa se encuentran las aplicaciones que los usuarios usan habitualmente, a estas aplicaciones se le denominan servicios, en otras palabras la capa de aplicación es quien proporciona los medios para la conectividad de extremo a extremo entre individuos de la red humana mediante redes de datos. Hay tantos protocolos diferentes como aplicaciones distintas, y en la misma medida en que surgen nuevas aplicaciones, así también crece el número de nuevos protocolos. El objetivo de las demás capas es proveer un transporte confiable a los datos usados por las aplicaciones residentes en esta capa.

2.2.13 Switching

El concepto de switching y reenvío de tramas es universal en la tecnología de redes y en las telecomunicaciones. En las redes LAN, WAN y en la red pública de telefonía conmutada (PSTN), se usan diversos tipos de switches. El concepto fundamental de switching hace referencia a un dispositivo que toma una decisión según dos criterios:

- Puerto de entrada
- Dirección de destino

La decisión sobre cómo un switch reenvía el tráfico se toma en relación con el flujo de ese tráfico. El término “entrada” se usa para describir el lugar de un puerto por donde

ingresa una trama al dispositivo. El término “salida” se usa para describir las tramas que salen del dispositivo desde un puerto determinado. Así mismo, los switches usan direcciones MAC para dirigir las comunicaciones de red a través de ellos mismos. Para definir qué puerto usar para transmitir una trama, el switch primero debe saber qué dispositivos existen en cada puerto y a medida que el switch descubre la relación entre puertos y dispositivos, crea una tabla denominada “tabla de direcciones MAC”, que a su vez usa para direccionar el paquete recibido a su destino final.

El rendimiento de una red es un factor importante en la productividad de una organización y la mejor forma de contribuir a mejorar el rendimiento de una red es realizando una división de los grandes dominios de difusión en dominios más pequeños, lo cual le da inicio a una nueva tecnología conocida como VLAN (Red de Área Local Virtual). Si bien las VLAN se utilizan principalmente dentro de las redes de área local conmutadas, las implementaciones modernas de las VLAN les permiten abarcar redes MAN y WAN.

Las VLAN permiten que el administrador divida las redes en segmentos según factores como la función, el equipo del proyecto o la aplicación, sin tener en cuenta la ubicación física del usuario o del dispositivo. Los dispositivos dentro de una VLAN funcionan como si estuvieran en su propia red independiente, aunque compartan una misma infraestructura con otras VLAN. Cualquier puerto de switch puede pertenecer a una VLAN diferente y cada VLAN se considera una red lógica independiente.

Los principales beneficios de utilizar las VLAN se mencionan a continuación:

- **Seguridad:** los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial. por ejemplo: las computadoras del cuerpo docente se encuentran en la VLAN 10 y están completamente separadas del tráfico de datos del invitado y de los estudiantes

- **Reducción de costos:** el ahorro de costos se debe a la poca necesidad de actualizaciones de red costosas y al uso más eficaz de los enlaces y del ancho de banda existentes.
- **Mejor rendimiento:** la división de las redes planas de capa 2 en varios grupos de trabajo lógicos (dominios de difusión) reduce el tráfico innecesario en la red y mejora el rendimiento.

Existen diferentes tipos de redes VLAN, los cuales se utilizan en las redes modernas. Algunos tipos de VLAN se definen según las clases de tráfico. Otros tipos de VLAN se definen según la función específica que cumplen.

- **VLAN de datos:** Una VLAN de datos es una VLAN configurada para transportar tráfico generado por usuarios. Las VLAN de datos generalmente se usan para dividir la red en grupos de usuarios o dispositivos.
- **VLAN predeterminada:** es la encargada de que el switch admita cualquier dispositivo conectado a cualquier puerto del mismo y así se pueda establecer una comunicación con otros dispositivos en otros puertos del switch. La VLAN predeterminada para los switches Cisco es la VLAN 1 y en consecuencia tiene todas las características de cualquier VLAN, excepto que no se le puede cambiar el nombre ni se puede eliminar.
- **VLAN nativa:** Una VLAN nativa está asignada a un puerto troncal 802.1Q. Los puertos de enlace troncal son los enlaces entre switches que admiten la transmisión de tráfico asociado a más de una VLAN. Los puertos de enlace troncal 802.1Q admiten el tráfico proveniente de muchas VLAN así como también el tráfico que no proviene de una VLAN. El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa, que es la VLAN 1 de manera predeterminada.
- **VLAN de administración:** Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch.

2.2.14 Habilitación de IP en un switch

Los dispositivos de infraestructura de red requieren direcciones IP para habilitar la administración remota. Con la dirección IP del dispositivo, el administrador de red puede conectarse al dispositivo de forma remota mediante Telnet, SSH, HTTP o HTTPS. Los switches no tienen una interfaz dedicada a la que se pueda asignar una dirección IP. Más sin embargo la información de dirección IP se configura en una interfaz virtual denominada “interfaz virtual conmutada” (SVI), donde más adelante se mostrara detalladamente su programación.

2.2.15 Routing

La comunicación entre redes no sería posible sin un router que determine la mejor ruta hacia el destino y que reenvíe el tráfico al router siguiente en esa ruta. El router es responsable del routing del tráfico entre redes y esto se debe porque cuando el router recibe un paquete, analiza la dirección de destino del paquete y usa la tabla de routing para buscar la mejor ruta hacia esa red. La tabla de routing también incluye la interfaz que se debe usar para reenviar los paquetes a cada red conocida. Cuando se encuentra una coincidencia, el router encapsula el paquete en la trama de enlace de datos de la interfaz de salida, y el paquete se reenvía hacia el destino.

Para habilitar el acceso a la red, se deben configurar los dispositivos con la información de dirección IP para identificar los elementos correspondientes ya que en cualquier internetwork, las direcciones IP son fundamentales para que los dispositivos se comuniquen de origen a destino y viceversa. Algunos ejemplos de estos dispositivos finales son: Computadoras, Impresoras de red, Teléfonos VoIP, Cámaras de seguridad, Smartphones, Dispositivos portátiles móviles (como los escáneres inalámbricos para códigos de barras)

La estructura de una **dirección IP** se denomina “notación decimal punteada” y se representa con cuatro números decimales entre 0 y 255. Las direcciones IPv4 son números asignados a los dispositivos individuales conectados a una red. Son de naturaleza lógica, ya que proporcionan información sobre la ubicación del dispositivo. Las direcciones IP se

pueden asignar tanto a los puertos físicos como a las interfaces virtuales de los dispositivos. Una interfaz virtual significa que no hay hardware físico en el dispositivo asociado a ella.

Ahora bien, no solo basta la **dirección IP** en un dispositivo para lograr correctamente su interconexión si que además también se necesitan la configuración de otros parámetros como, **máscaras de subred y gateway predeterminado**, donde las mencionadas máscaras de subred son un tipo especial de direcciones IPv4 que, combinadas con las direcciones IP determinan con qué subred de la red se puede comunicar el host, mientras que a su vez el gateway predeterminado es quien identifica el router al que se debe enviar un paquete cuando el destino no está en la misma subred de la red local. Estos parámetros ya mencionados se pueden asignar de dos formas:

- **Forma Estática:** se asigna la dirección IP, la máscara de subred y el gateway predeterminado correctos al host de forma manual. También se puede configurar la dirección IP del servidor DNS.
- **Forma Dinámica:** un servidor proporciona la información de dirección IP mediante el protocolo de configuración dinámica de host (DHCP). El servidor de DHCP proporciona una dirección IP, una máscara de subred y un gateway predeterminado válidos para las terminales.

El enrutamiento o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad, es allí donde entran los diferentes tipos de enrutamiento dado a que el concepto de **routing** trata de encontrar la mejor ruta posible, por lo tanto al momento de elegir cuál es la mejor opción cuando se tiene que instalar una red de interconexión lo primero será definir la mejor ruta y en consecuencia cuál es la métrica que se debe utilizar para medirla, lo cual da paso para definir los diferentes tipos de enrutamiento:

- **Enrutamiento estático:** Las rutas estáticas se configuran de forma manual. Estas definen una ruta explícita entre dos dispositivos de red, a diferencia de los protocolos de routing dinámico, las rutas estáticas no se actualizan automáticamente y se deben reconfigurar de forma manual si se modifica la topología de la red. Los

beneficios de utilizar rutas estáticas incluyen la mejora de la seguridad y la eficacia de los recursos. Las rutas estáticas consumen menos ancho de banda que los protocolos de routing dinámico. La principal desventaja de usar rutas estáticas es que no se vuelven a configurar de manera automática si se modifica la topología de la red

- **Enrutamiento dinámico:** Los routers usan protocolos de enrutamiento dinámico para compartir información sobre el estado y la posibilidad de conexión de redes remotas. Los protocolos de routing dinámico realizan diversas actividades, como la detección de redes y el mantenimiento de las tablas de routing un ejemplo de ellos son:
 - Ø **EIGRP:** protocolo de routing de gateway interior mejorado
 - Ø **OSPF:** Open Shortest Path First
 - Ø **RIP:** protocolo de información de routing

El descubrimiento de redes es la capacidad de un protocolo de enrutamiento de compartir información sobre las redes que conoce con otros routers que también están usando el mismo protocolo de enrutamiento. En lugar de depender de las rutas estáticas configuradas manualmente en cada router, los protocolos de routing dinámico permiten que los routers descubran estas redes de forma automática. Estas redes y la mejor ruta hacia cada una se agregan a la tabla de routing del router y se identifican como redes descubiertas por algún protocolo de routing dinámico específico. Los protocolos de routing dinámico funcionan bien en cualquier tipo de red conformada por varios routers. Este tipo de enrutamiento dinámico hace que las redes sean escalables y determinan automáticamente las mejores rutas si se produce un cambio en la topología, representando de esa manera su ventaja. Si bien existen otros aspectos para tener en cuenta respecto de la configuración de los protocolos de routing dinámico, son más simples de configurar en redes grandes, pero en desventaja el routing dinámico es menos seguro que el routing estático, porque las interfaces identificadas por el protocolo de routing envían actualizaciones de routing fuera de la red.

2.2.16 Sistema Operativo IOS (Internetwork Operating System)

Todos los dispositivos finales y de red conectados a Internet requieren un sistema operativo (SO) que los ayude a realizar sus funciones, al encender una computadora por ejemplo se carga el SO, la parte del código del SO que interactúa directamente con el hardware de la computadora se conoce como núcleo y la porción que interactúa con las aplicaciones y el usuario se conoce como “shell” y en esta parte es donde el usuario finalmente puede interactuar de manera profesional con el dispositivo mediante la interfaz de línea de comandos (CLI, command-line interface), una interface donde el usuario interactúa directamente introduciendo comandos con el teclado en una ventana de petición de entrada de comandos o la interface gráfica de usuario (GUI, graphical user interface), una interface que permite al usuario interactuar con el sistema en un entorno que utiliza imágenes gráficas, formatos multimedia y texto, lo que da como resultado de que la GUI sea más fácil de usar y requiera un menor conocimiento de la estructura de comandos para utilizar el sistema. Por este motivo, la mayoría de los sistemas operativos de los dispositivos finales, incluidos MS Windows, MAC OS X, Linux, Apple iOS y Android, entre otros, se accede mediante una GUI, sin embargo muchos sistemas operativos ofrecen tanto una GUI como una CLI.

El sistema operativo de red que se utiliza en los dispositivos Cisco se denomina Sistema operativo Internetwork (IOS, Internetwork Operating System). “Cisco IOS” es un término genérico para la colección de sistemas operativos de red que se utilizan en los dispositivos de red Cisco. Cisco IOS se utiliza en la mayoría de los dispositivos Cisco, independientemente del tamaño o el tipo del dispositivo. El método más frecuente para acceder a estos dispositivos consiste en utilizar una CLI.

Los routers y switches en los que se utiliza Cisco IOS realizan funciones de las cuales dependen los profesionales de red para hacer que sus redes funcionen de la forma esperada. Las funciones principales que realizan o habilitan los routers y switches Cisco incluyen las siguientes:

- Prestación de seguridad de la red
- Direccionamiento IP de interfaces virtuales y físicas

- Habilitación de configuraciones específicas de la interfaz para optimizar la conectividad de los respectivos medios
- Enrutamiento
- Habilitación de tecnologías de calidad de servicio (QoS)
- Compatibilidad con tecnologías de administración de red

Cada característica o servicio tiene asociado un conjunto de comandos de configuración que permite su implementación por parte de los técnicos de red. Por lo general, se accede a los servicios que proporciona Cisco IOS mediante una CLI.

2.2.17 Acceso Mediante CLI

Existen varias formas de acceder a un dispositivo Cisco a través del entorno de la CLI. Los métodos más comunes son los siguientes: Consola, Telnet o SSH y Puerto auxiliar

- **Consola**

El puerto de consola es un puerto de administración que proporciona acceso fuera de banda a los dispositivos. El acceso fuera de banda se refiere al acceso mediante un canal de administración dedicado que se utiliza únicamente para el mantenimiento del dispositivo. La ventaja de utilizar un puerto de consola es que es posible acceder al dispositivo incluso si no se configuró ningún servicio de red, por ejemplo, cuando se realiza la configuración inicial del dispositivo de red. Al realizar la configuración inicial, una PC con software de emulación de terminal se conecta al puerto de consola del dispositivo mediante un cable especial y de esta manera los comandos de configuración para el switch o el router se pueden introducir en la PC conectada.

El puerto de consola también puede utilizarse cuando fallan los servicios de red y no es posible acceder al dispositivo de manera remota. Si esto ocurre, una conexión a la consola puede habilitar a una PC para determinar el estado del dispositivo. En forma predeterminada, la consola comunica el inicio del dispositivo, la depuración y los mensajes de error, permitiendo al profesional conectarse con el equipo y así poder ejecutar cualquier comando de configuración necesario mediante la sesión de consola. Para muchos dispositivos, el acceso de consola no requiere ningún tipo de seguridad, en forma predeterminada. Sin embargo, la consola debe estar configurada con contraseñas para evitar

el acceso no autorizado al dispositivo. En caso de que se pierda una contraseña, existe un conjunto especial de procedimientos para eludir la contraseña y acceder al dispositivo.

- **Telnet**

Telnet es un método para establecer una sesión de CLI de un dispositivo en forma remota, mediante una interfaz virtual, a través de una red. A diferencia de la conexión de consola, las sesiones de Telnet requieren servicios de redes activos en el dispositivo. El dispositivo de red debe tener, por lo menos, una interfaz activa configurada con una dirección de Internet, por ejemplo una dirección IPv4. Los dispositivos Cisco IOS incluyen un proceso de servidor Telnet que permite a los usuarios introducir comandos de configuración desde un cliente Telnet. Esto permite que los administradores de red accedan mediante Telnet a cualquier otro dispositivo que admita un proceso de servidor Telnet desde la CLI del dispositivo Cisco.

- **SSH**

El protocolo de Shell seguro (SSH) proporciona un inicio de sesión remoto similar al de Telnet, excepto que utiliza servicios de red más seguros. El SSH proporciona autenticación de contraseña más potente que Telnet y usa encriptación cuando transporta datos de la sesión. De esta manera se mantienen en privado la ID del usuario, la contraseña y los detalles de la sesión de administración. Se recomienda utilizar el protocolo SSH en lugar de Telnet, siempre que sea posible.

- **Puerto Auxiliar**

Una antigua forma de establecer una sesión de CLI de manera remota era mediante una conexión telefónica de dial-up con un módem conectado al puerto auxiliar (AUX) de un router. Al igual que la conexión de consola, el método de puerto auxiliar también es una conexión fuera de banda y no requiere la configuración ni la disponibilidad de ningún servicio de red en el dispositivo. En caso de que los servicios de red fallen, es posible que un administrador remoto acceda al switch o al router mediante una línea telefónica.

El puerto auxiliar también puede usarse en forma local, como el puerto de consola, con una conexión directa a una computadora que ejecute un programa de emulación de terminal. No obstante, se prefiere el puerto de consola al puerto auxiliar para la resolución

de problemas, ya que el primero muestra mensajes de inicio, depuración y error de manera predeterminada, muchos de los switches actuales ya no admiten conexiones auxiliares

2.2.18 Programas de Emulación Terminal

Existen varios programas excelentes de emulación de terminales disponibles para conectarse a un dispositivo de red mediante una conexión serial por un puerto de consola o mediante una conexión Telnet o SSH. Algunos de estos programas incluyen los siguientes:

- PuTTY
- Tera Term
- SecureCRT
- HyperTerminal
- OS X Terminal

Estos programas le permiten aumentar la productividad mediante ajustes del tamaño de la ventana, modificaciones de los tamaños de fuente y cambios en los esquemas de colores.

2.2.19 Modos de Funcionamiento de Cisco IOS

Una vez que se establezca mediante un programa de emulación terminal la conectividad con los dispositivos de red bien sea (switches o routers) se pueden configurar dichos dispositivos en los diferentes modos del IOS. La CLI utiliza una estructura jerárquica para los diferentes modos de funcionamiento. **(Ver figura 10).**

En orden jerárquico desde el más básico hasta el más especializado, los modos principales son los siguientes:

- Modo de usuario (EXEC de usuario)
- Modo de ejecución privilegiado (EXEC privilegiado)
- Modo de configuración global
- Otros modos de configuración específicos, como el modo de configuración de interfaz

Cada modo tiene una petición de entrada distinta y se utiliza para realizar tareas determinadas con un conjunto específico de comandos que están disponibles solo para el modo en cuestión. Por ejemplo, el modo de configuración global permite que el personal capacitado configure los parámetros del dispositivo que lo afectan en su conjunto, como la

configuración del nombre de dispositivo. Sin embargo, se requiere un modo diferente si el profesional de red desea configurar los parámetros de seguridad en un puerto específico de un switch, por ejemplo. En ese caso, se debe ingresar al modo de configuración de interfaz para ese puerto específico. Todas las configuraciones que se introducen en el modo de configuración de interfaz se aplican solo a ese puerto.

- **Modo EXEC del usuario**

El modo EXEC del usuario tiene capacidades limitadas, pero es útil para algunas operaciones básicas. El modo EXEC del usuario se encuentra en el nivel más básico de la estructura jerárquica modal. Este es el primer modo que se encuentra al entrar a la CLI de un dispositivo IOS. El modo EXEC del usuario permite sólo una cantidad limitada de comandos de monitoreo básicos. A menudo se le describe como un modo de visualización solamente ya que no permite la ejecución de ningún comando que podría cambiar la configuración del dispositivo.

En forma predeterminada, no se requiere autenticación para acceder al modo EXEC del usuario desde la consola. Sin embargo, siempre conviene asegurarse de que se configure la autenticación durante la configuración inicial. El modo EXEC del usuario se puede reconocer por la petición de entrada de la CLI que termina con el símbolo >. Este es un ejemplo que muestra el símbolo > en la petición de entrada:

```
Switch>
```

- **Modo EXEC privilegiado**

La ejecución de los comandos de configuración y administración requiere que el administrador de red utilice el modo EXEC privilegiado o un modo más específico en la jerarquía. Esto significa que los usuarios deben ingresar primero al modo EXEC del usuario y, desde allí, acceder al modo EXEC privilegiado. Para ingresar al modo de configuración global y a todos los demás modos de configuración más específicos, es necesario entrar al modo EXEC privilegiado y se puede reconocer por la petición de entrada que termina con el símbolo #.

```
Switch#
```

- **Modo de configuración global**

El modo de configuración principal recibe el nombre de configuración global o global config. En el modo de configuración global, se realizan cambios en la configuración de la CLI que afectan el funcionamiento del dispositivo en su totalidad. Antes de acceder a los modos de configuración específicos, se accede al modo de configuración global. El siguiente comando de la CLI se usa para cambiar el dispositivo del modo EXEC privilegiado al modo de configuración global y para permitir la entrada de comandos de configuración desde una terminal:

Switch# **configure terminal**

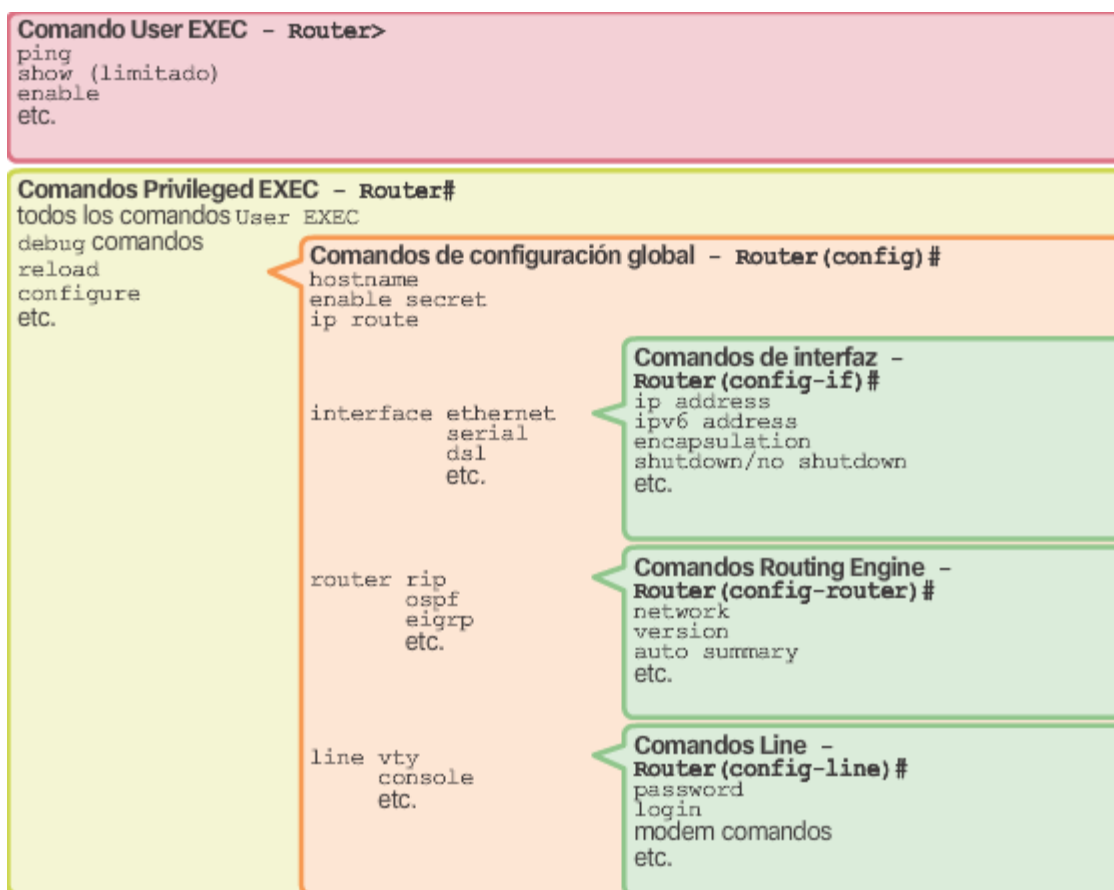


Figura 10: Estructura Jerárquica de lo Modos del IOS

Fuente : <https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html#2.1.3.1>

- **Modos de configuración específico**

En el modo de configuración global, el usuario puede ingresar a diferentes modos de subconfiguración. Cada uno de estos modos permite la configuración de una parte o función específica del dispositivo IOS. La lista que se presenta a continuación muestra algunos de ellos:

- Modo de interfaz: Para configurar una de las interfaces de red (Fa0/0, S0/0/0).
- Modo de línea: Para configurar una de las líneas físicas o virtuales (consola, auxiliar, VTY).

Para salir de un modo de configuración específico y volver al modo de configuración global, escriba **exit** (salir) en la petición de entrada. Para salir completamente del modo de configuración y volver al modo EXEC privilegiado, ingrese **end** o use la secuencia de teclas **Ctrl-Z**

2.2.20 Ayuda Contextual del ISO bajo CLI

La ayuda contextual proporciona una lista de comandos y los argumentos asociados con esos comandos dentro del contexto del modo actual. Para acceder a la ayuda contextual, introduzca un signo de interrogación, **?**, en cualquier petición de entrada. Aparece una respuesta inmediata sin necesidad de utilizar la tecla Entrar. Uno de los usos de la ayuda contextual es para la obtención de una lista de los comandos disponibles. Dicha lista puede utilizarse cuando existen dudas sobre el nombre de un comando o se desea verificar si el IOS admite un comando específico en un modo determinado. Por ejemplo, para obtener una lista de los comandos disponibles en el nivel EXEC del usuario, introduzca un signo de interrogación, **?**, en la petición de entrada Switch>.

En el mismo orden de ideas, otro de los usos de la ayuda contextual es visualizar una lista de los comandos o palabras clave que empiezan con uno o varios caracteres específicos. Si se introduce un signo de interrogación, sin espacio, inmediatamente después de introducir una secuencia de caracteres, el IOS muestra una lista de comandos o palabras clave para el contexto que comienzan con los caracteres introducidos. Por ejemplo, introduzca **sh?** para obtener una lista de los comandos que comienzan con la secuencia de caracteres **sh**.

Un último tipo de ayuda contextual se utiliza para determinar qué opciones, palabras clave o argumentos coinciden con un comando específico. Al introducir un comando, introduzca un espacio seguido de un ? para determinar qué puede o debe introducirse a continuación.

2.2.21 Verificación de comando

Cuando se emite un comando presionando la tecla Entrar, el intérprete de la línea de comandos analiza la sintaxis del comando de izquierda a derecha para determinar qué acción se solicitó, si el intérprete comprende el comando, la acción requerida se ejecuta y la CLI vuelve a la petición de entrada correspondiente. Sin embargo, si el intérprete no puede comprender el comando que se ingres mostrará un comentario que describe el error del comando. Tipos de mensajes de error:

- Ambiguous command (comando ambiguo)
- Incomplete command (comando incompleto)
- Incorrect command (comando incorrecto)

2.2.22 Teclas de acceso rápido

La interfaz de línea de comandos IOS proporciona teclas de acceso rápido y métodos abreviados que facilitan la configuración, el monitoreo y la resolución de problemas.

- **Flecha abajo:** permite al usuario desplazarse hacia delante a través de los comandos anteriores.
- **Flecha arriba:** permite al usuario desplazarse hacia atrás a través de los comandos anteriores.
- **Tabulación:** completa el resto de un comando o de una palabra clave que se escribió parcialmente.
- **Ctrl-A:** se traslada al comienzo de la línea.
- **Ctrl-E:** se traslada al final de la línea.
- **Ctrl-R:** vuelve a mostrar una línea
- **Ctrl-Z:** sale del modo de configuración y vuelve al modo EXEC del usuario.
- **Ctrl-C:** sale del modo de configuración o cancela el comando actual.

- **Ctrl-Mayús-6:** permite al usuario interrumpir un proceso de IOS, como ping o traceroute.

2.2.23 Fundamentos de Diseño de la Guía de Laboratorio

En la metodología de la educación no todos los métodos son los indicados para el desarrollo intelectual del estudiante, ya que en algunas ramas de la educación se hace necesaria una herramienta práctica que permita al estudiante afianzar sus conocimientos teóricos por medio de la práctica. Unas de estas herramientas son las guías prácticas de laboratorio de la materia de redes de comunicaciones, que le permitirán al estudiante una relación entre sus conocimientos y la forma de cómo llevarlos a la práctica. Las guías son una herramienta práctica de enseñanza que se puede aplicar de forma activa, propiciando ejercicios que permitan analizar y desarrollar el conocimiento.

En otras palabras las guías se basan en el término aprender haciendo donde las clases se apegan a la tradicional metodología presencial. A pesar de las ventajas de las guías prácticas, solo son una herramienta que le permiten al estudiante regirse para alcanzar un beneficio específico, por lo que su elaboración debe ser bien definida y no dejarse en un estado de simplicidad o realizadas de impremeditación ya que son base fundamental de la educación abriendo un camino para el trabajo entre el docente y el estudiante. Existen diferentes tipos de guías, según la necesidad o las metas que quieran alcanzar estas pueden ser:

- **Guías directivas:** Que indican al estudiante lo que debe hacer, lo remiten al material o a otros libros de consulta que más le puedan ayudar. Son guías base e indispensables en todo trabajo individualizado.
- **Guías de Información:** Que contienen una exposición o información; textos para estudiar datos y documentos. Suelen ser más amplias en el contenido. Las guías deben ser concisas, deben tener la información estrictamente necesaria, para que estas no se den a conocer a los estudiantes como un interrogatorio. Si no como de una herramienta que le permite desarrollar de una forma confiable e interactiva su habilidad cognoscitiva, para el desarrollo de las clases.

2.3 Definición de Términos Básicos

Red: Una red (en general) es un conjunto de dispositivos (de red) interconectados físicamente (ya sea vía alámbrica o vía inalámbrica) que comparten recursos y que se comunican entre sí a través de reglas (protocolos) de comunicación.

Hardware: Se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Software: Equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Host: Se refiere a las computadoras conectadas a una red, que proveen y utilizan servicios de ella.

Datagrama: Forma de encaminar los paquetes en una red.

Enrutamiento: permite determinar la ruta óptima para que un paquete llegue su destino.

Ping: es una utilidad diagnóstica en redes de computadoras que comprueba el estado de la comunicación del host local con uno o varios equipos remotos de una red IP por medio del envío de paquetes ICMP de solicitud y de respuesta.

Traceroute: es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host (punto de red).

IP: es un número que identifica, de manera lógica y jerárquica, a una Interfaz de red de un dispositivo (computadora, tableta, portátil) que utilice el protocolo IP. Corresponde al nivel de red del modelo TCP/IP

Interfaz: es una conexión entre dos máquinas de cualquier tipo, a las cuales les brinda un soporte para la comunicación a diferentes estratos, en otras palabras Se conoce como interfaz de usuario al medio que permite a una persona comunicarse con una máquina.

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Tipo de Investigación

La metodología de esta investigación está concebida dentro de la modalidad de proyecto factible, según clasificación expuesta por Hurtado (2008), porque

Consiste en la elaboración de una propuesta, plan, desarrollo o un modelo, como solución a un problema o necesidad de tipo práctico, ya sea de un grupo social, o de una institución, o de una región geográfica, en un área particular del conocimiento, a partir de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generados involucrados y de las tendencias futuras, es decir, con base en los resultados de un proceso investigativo”.

Los proyectos factibles corresponden a la producción de tecnología blanda siendo estos generadores de solución viable para la situación que se plantea, este tipo de proyectos se suelen traducir en propuestas, procesos y diseños instruccionales fundamentados en la planificación consultiva, desarrollados en medios impresos o virtuales.

Según Balestrini, (2002), Los proyectos factibles son aquellos proyectos o investigaciones que proponen la formulación de modelos, sistemas entre otros, que dan soluciones a una realidad o problemática real planteada, la cual fue sometida con anterioridad o estudios de las necesidades a satisfacer.

Los proyectos factibles son consecuencia de un diagnóstico realizado previa y sistemáticamente, no necesariamente de campo, estos están asociados a un estudio de factibilidad funcional con disposición a cambios y de disponibilidad de recursos con la participación de los entes involucrados, todo esto con la finalidad de encontrar una serie de soluciones de carácter inteligente para resolver una necesidad planteada.

3.2 Diseño de la Investigación

Para la realización de esta investigación se elaboraron una serie de procesos de forma sistemática y racional de recolección, evaluación, tratamiento, análisis y

presentación de datos, basado en una estrategia de obtención aplicada directamente en el lugar de los acontecimientos, siendo partícipes de la observación directa de las realidades que generan el problema, para así poder obtener las informaciones necesarias para el desarrollo de la ya mencionada investigación.

Según Arias, (2006), una investigación de campo “consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna”. Por lo tanto, este estudio se enmarcó en una investigación de campo, ya que los datos fueron extraídos en forma directa de la realidad y por la propia investigadora, dentro de la misma escuela de Ingeniería de Telecomunicaciones de la UJAP, obteniendo los datos dentro del mismo escenario donde ocurre el problema.

3.3 Nivel de la Investigación

El presente trabajo se ubica en la modalidad de proyecto descriptivo, ya que se desarrolla una metodología para el aprendizaje de nuevas tecnologías en el laboratorio de redes de comunicaciones de la UJAP. Este tipo de investigación consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables con respecto a esto Arias (2006), dice que la investigación descriptiva “consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento” Este tipo de investigación permite no solo aplicar elementos de recolección de datos si no también hacer un análisis descriptivo del problema planteado en la institución.

3.4 Población y muestra

Tamayo y Tamayo, (2001), una población está definida por sus características definitorias, por tanto el conjunto de elementos que posea esta característica se denomina población o universo.

Al respecto Hernández, FernándezBaptista, (2001), establecen que la población es todo aquello a ser estudiada y sobre la cual se pretende generalizar los resultados. Así, la

población es un conjunto de todos los casos que concuerdan con una serie de especificaciones. En cuanto a este trabajo investigativo es importante mencionar que la población es igual a la muestra y esto se debe a que la muestra es tan pequeña que se considera igual a la población, haciendo así que todos los estudiantes de la materia Redes de Comunicaciones de la carrera Ingeniería de Telecomunicaciones de la Universidad José Antonio Páez, sean la población estudiada para este trabajo grado realizado.

3.5 Fuentes, Técnicas e Instrumentos de recolección de datos

Según Hurtado, (2008), “las técnicas tienen que ver con los procedimientos utilizados para la recolección de datos”, es decir el cómo estas pueden ser de revisión documental. Además, según el mismo autor (2006), “la selección de técnicas e instrumentos de recolección de datos implica determinar por cuales medios o procedimientos el investigador obtendrá la información necesaria para alcanzar los objetivos de la investigación”.

Para la realización de esta investigación fue necesario realizar una encuesta de tipo cerrada aplicada a cada uno de los elementos que conforman la muestra estudiada, que para el caso está representada por la totalidad de los estudiantes de la materia redes de comunicaciones de la carrera Ingeniería de Telecomunicaciones en la UJAP, además se utilizó la entrevista directa con los profesores y expertos en el área para tratar de obtener datos técnicos sobre la enseñanza de la mencionada materia. En lo que concierne a las fuentes la web oficial de Cisco proporciono la gran parte de la información de manera abierta, sobre el funcionamiento, aplicaciones y recomendaciones de dicha tecnología lo que en consecuencia ayudo de manera fundamental en el desarrollo del trabajo investigativo.

3.6 Fases Metodológicas

A continuación se describen por medio de fases, el procedimiento seguido para el cumplimiento los objetivos específicos planteados en el Capítulo I de este trabajo de grado, a través de los cuales se alcanzó el objetivo general de investigación propuesto.

Fase I: Evaluación de la situación actual de las prácticas existentes en el laboratorio de redes de comunicaciones.

Para poder evaluar la problemática se utilizó una serie de instrumentos para la recolección de datos como por ejemplo: las entrevistas y las encuestas para así poder determinar con certeza la situación actual y poder concretar la evaluación de los datos necesarios para el enfoque de las posibles soluciones al problema.

Fase II: Identificación de los equipos Cisco con que cuenta el laboratorio de redes de comunicaciones.

En esta fase del proyecto se identificó con ayuda del personal capacitado con que cuenta la UJAP, es decir el personal técnico de laboratorio y los profesores el equipamiento de tecnología Cisco con que cuenta el laboratorio de redes de comunicaciones y el cual tendrá como finalidad ser involucrado en las practicas realizadas por los estudiantes que cursan dicha materia.

Fase III: Estudio, organización y selección de los aspectos básicos de la tecnología Cisco, que son necesarios para el aprendizaje y desempeño profesional de los estudiantes.

Basados en lo obtenido en cuanto a las necesidades planteadas por el problema se procede a buscar información sobre los aspectos básicos y necesarios de la tecnología Cisco, que son de suma importancia para el aprendizaje y desempeño profesional de los estudiantes, consultando material bibliográfico, material web, entrevistando a personal capacitado en el área y ordenando en una serie de opciones para escoger la que mejor se adapte al programa académico de la materia Redes de Comunicaciones.

Fase V: Elaboración de un manual de trabajo con prácticas de laboratorio desarrolladas paso a paso y enfocadas en tecnología Cisco para los estudiantes de ingeniería en telecomunicaciones, de manera que permita al estudiantado de la materia Redes de Comunicaciones desarrollar de una forma eficaz el conocimiento académico en el laboratorio de acuerdo a las necesidades actuales y a las condiciones del Laboratorio de Redes.

En esta fase se elabora el manual de prácticas de laboratorio que permita a todos los estudiantes que cursen la materia Redes de Comunicaciones obtener una formación práctica adecuada y sistematizada sobre el manejo, programación y configuración de la tecnología

Cisco de acuerdo a los estándares modernos en cuanto al tema , permitiendo así tener una mejor experiencia en la adquisición de destrezas que posteriormente podrán ser aplicadas por ellos en el campo laboral y mejorando también la experiencia del profesor en cuanto a la facilitación de conocimiento en el laboratorio.

CAPÍTULO IV

RESULTADOS

El presente trabajo tuvo como objetivo desarrollar un manual de prácticas estructuradas bajo un enfoque Cisco para el laboratorio de Redes de Comunicaciones.

Los resultados arrojados en cada una de las fases, se presentan a continuación:

4.1) FASE I: Evaluar la situación actual de las prácticas existentes en el laboratorio de redes de comunicaciones.

En esta fase se realizaron encuestas a cada uno de los estudiantes cursantes de la materia Redes de Comunicaciones al igual que al profesor encargado de impartir dicha materia, para así conocer y determinar la situación actual y establecer los requerimientos necesarios para la optimización de este proceso.

La encuesta realizada a los estudiantes y al profesor de la materia Redes de Comunicaciones, se presenta a continuación:

A. *“¿Está Ud. de acuerdo y conforme con las prácticas realizadas en el laboratorio de la materia Redes de Comunicaciones?”.*

SI___ NO___

B. *“¿Considera Ud. que la implementación de dichas prácticas son lo suficientemente complementarias para el máximo aprendizaje de la materia?”.*

SI___ NO___

C. *“¿En la actualidad los equipos de tecnología Cisco con que cuenta el laboratorio de redes de comunicaciones están siendo utilizados e incluidos en su totalidad en la practicas que se realizan en dicho laboratorio?”.*

SI___ NO___

D. “¿Le Gustaría que los equipos de tecnología Cisco se incluyeran con más frecuencia en las practicas regulares realizadas en el laboratorio de Redes de Comunicaciones?”.

SI___ NO___

E. “¿Considera Ud. Que la falta de un sistema estructurado de prácticas de laboratorio enfocado en tecnología Cisco impide al estudiante obtener la experiencia adecuada para enfrentarse a los retos tecnológicos que atraviesan diariamente las redes de comunicaciones?”.

SI___ NO___

F. “¿Estaría Ud. de acuerdo con el desarrollo de un nuevo, didáctico y actual manual de prácticas enfocado en tecnología Cisco para el laboratorio de Redes de Comunicaciones?”.

SI___ NO___

4.1.1 Tabulación de Resultados

Cuadro 1.

Tabulación de Resultados de la encuesta

ITEMS	FRECUENCIAS		PORCENTAJES (%)	
	SI	NO	SI	NO
A	3	5	37.5	62.5
B	2	6	25	75
C	2	6	25	75
D	8	0	100	0
E	7	1	87.5	12.5
F	100	0	100	0

Fuente: Theis Genesis (2016).

Ítem. A.

¿Está Ud. de acuerdo y conforme con las prácticas realizadas en el laboratorio de la materia Redes de Comunicaciones?

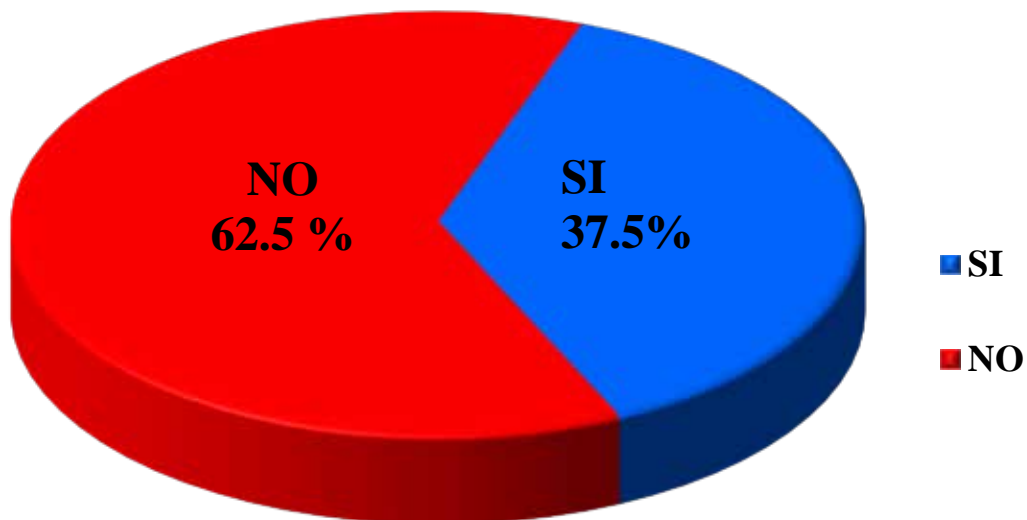
Cuadro 2.

Resultados Ítem A. de la Encuesta.

Alternativas	Frecuencia	Porcentaje (%)
SI	3	37.5
NO	5	62.5

Fuente: Theis Genesis (2016).

GRAFICO 1.



Fuente: Theis Genesis (2016).

INTERPRETACION:

La encuesta arrojó que el 62,5% de los consultados no está conforme con las prácticas realizadas en el laboratorio de Redes de Comunicaciones.

Ítem. B.

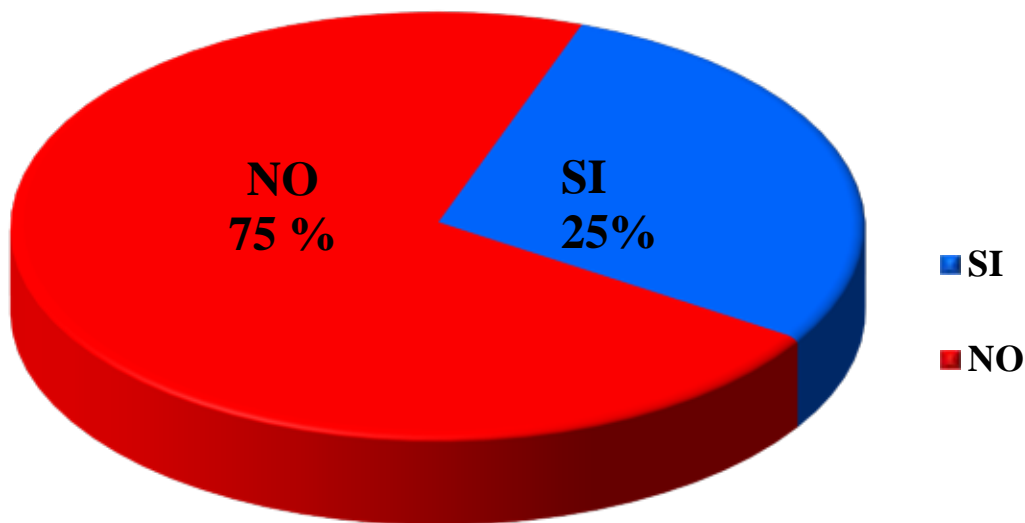
¿Considera Ud. que la implementación de dichas prácticas son lo suficientemente complementarias para el máximo aprendizaje de la materia?

Cuadro 3.
Resultados Ítem B. de la Encuesta.

Alternativas	Frecuencia	Porcentaje (%)
SI	2	25
NO	6	75

Fuente: Theis Genesis (2016).

GRAFICO 2.



Fuente: Theis Genesis (2016).

INTERPRETACION:

El 87.5% considera que las practicas no complementan suficientemente el aprendizaje recibido en las clases regulares.

Ítem. C.

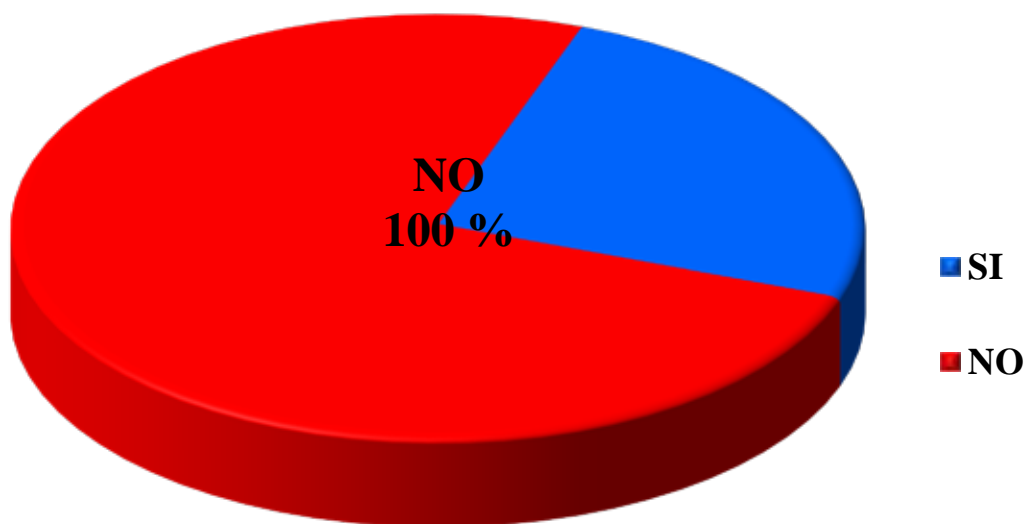
¿En la actualidad los equipos de tecnología Cisco con que cuenta el laboratorio de redes de comunicaciones están siendo utilizados e incluidos en su totalidad en la practicas que se realizan en dicho laboratorio?

Cuadro 4.
Resultados Ítem C. de la Encuesta.

Alternativas	Frecuencia	Porcentaje (%)
SI	2	25
NO	6	75

Fuente: Theis Genesis (2016).

GRAFICO 3.



Fuente: Theis Genesis (2016).

INTERPRETACION:

El ítem arrojo como resultado que los equipos Cisco que existen en el laboratorio de Redes de Comunicaciones, no están siendo utilizados en su totalidad por los alumnos que cursos dicha materia.

Ítem. D.

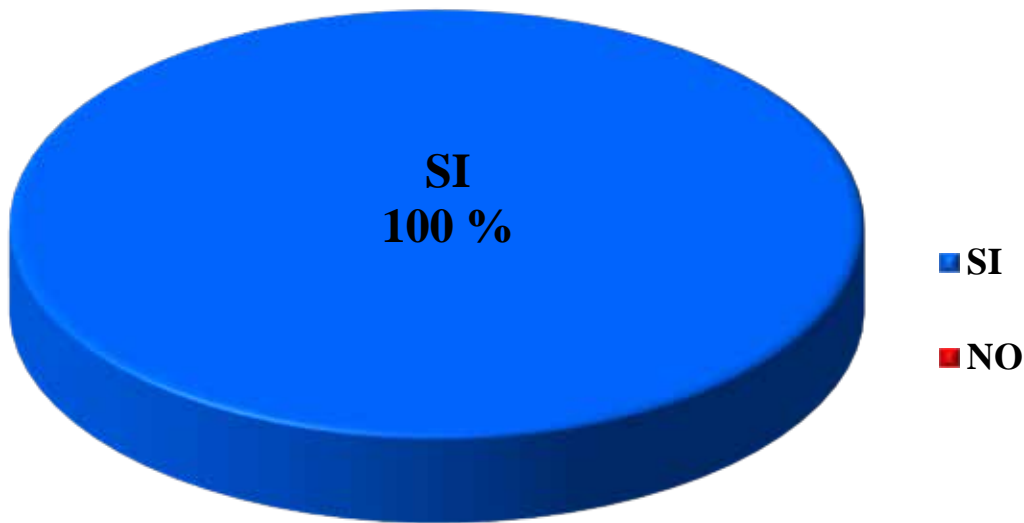
¿Le Gustaría que los equipos de tecnología Cisco se incluyeran con mas frecuencia en las practicas regulares realizadas en el laboratorio de Redes de Comunicaciones?

Cuadro 5.
Resultados Ítem D. de la Encuesta.

Alternativas	Frecuencia	Porcentaje (%)
SI	8	100
NO	0	0

Fuente: Theis Genesis (2016).

GRAFICO 4.



Fuente: Theis Genesis (2016).

INTERPRETACION:

El ítem arrojó como resultado que la mayoría absoluta le gustaría manejar con más frecuencia los equipos de tecnología Cisco y así a su vez aprender a utilizar profesionalmente estos equipos.

Ítem. E.

¿Considera Ud. Que la falta de un sistema estructurado de prácticas de laboratorio enfocado en tecnología Cisco impide al estudiante obtener la experiencia adecuada para enfrentarse a los retos tecnológicos que atraviesan diariamente las redes de comunicaciones?

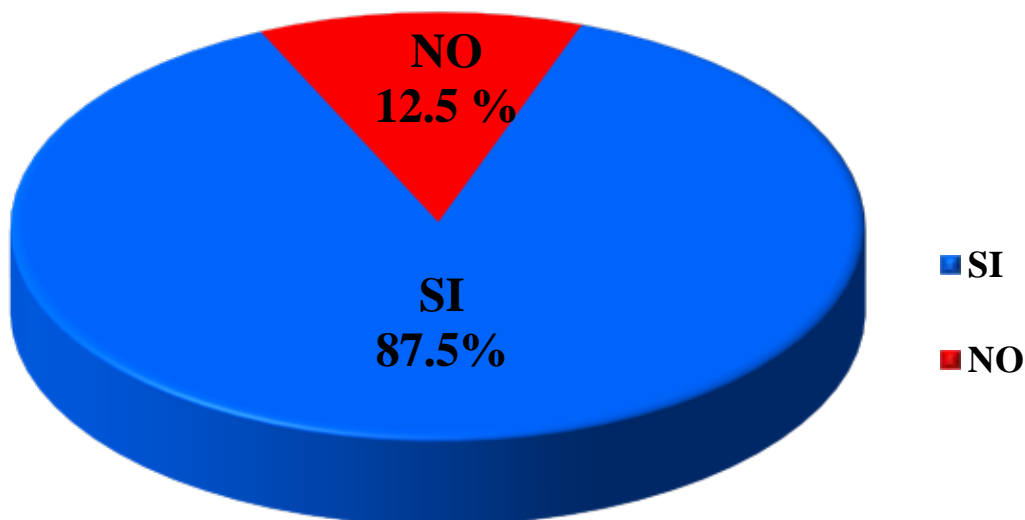
Cuadro 6.

Resultados Ítem D. de la Encuesta.

Alternativas	Frecuencia	Porcentaje (%)
SI	7	87.5
NO	1	12.5

Fuente: Theis Genesis (2016).

GRAFICO 5.



Fuente: Theis Genesis (2016).

INTERPRETACION:

El 87.5% expreso la necesidad de un sistema estructurado bajo un enfoque Cisco, que le permitirá guiar sus prácticas para enfrentarse a los retos tecnológicos que atraviesan diariamente las redes de comunicaciones.

Ítem. F.

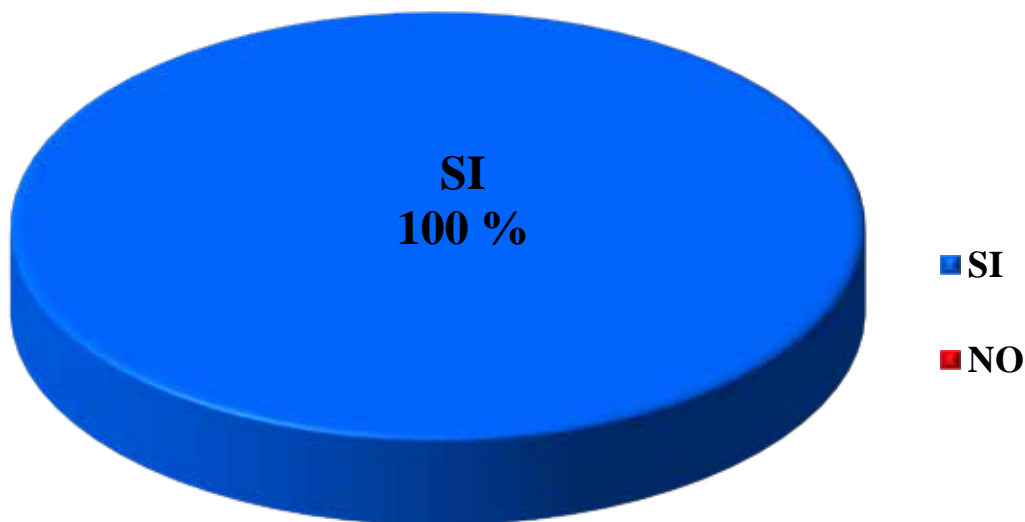
¿Estaría Ud. de acuerdo con el desarrollo de un nuevo, didáctico y actual manual de prácticas enfocado en tecnología Cisco para el laboratorio de Redes de Comunicaciones?

Cuadro 7.
Resultados Ítem F. de la Encuesta.

Alternativas	Frecuencia	Porcentaje (%)
SI	8	100
NO	0	0

Fuente: Theis Genesis (2016).

GRAFICO 6.



Fuente: Theis Genesis (2016).

INTERPRETACION:

El ítem arroja como resultado que todos los encuestados están a favor de la realización de un manual enfocado en tecnología Cisco para las prácticas de laboratorio.

4.1.2 Interpretación de Resultados:

Con la entrevista realizada se pudo deducir, que actualmente en el laboratorio de la materia Redes de Comunicaciones se realizan una serie de prácticas a lo largo del semestre cursado, estas son realizadas por el profesor y los estudiantes pero las mismas no cuentan con el uso de los equipos de tecnología Cisco que posee el laboratorio, lo cual se transforma en una desventaja para el aprendizaje de los estudiantes, las practicas que allí se realizan se basan en el contenido académico dictado por el profesor durante el semestre académico, también se pudo concluir del resultado de estas encuestas, que existen ciertos factores que impiden que el aprendizaje aportado por dichas prácticas se efectuó de una manera óptima para la enseñanza de los estudiantes, factores como la falta de tiempo requerido a lo largo del semestre para el cumplimiento de las prácticas en su totalidad así como falta de claridad en cuanto al material requerido para la realización de estas prácticas.

Las personas encuestadas estuvieron de acuerdo en una totalidad de apoyar unánimemente el desarrollo de un nuevo manual de prácticas enfocado en tecnología Cisco para ser impartidas en el laboratorio, con un aporte y mejora que les permita realizar paso a paso, de forma sistemática, controlada y con claridad las prácticas para así ampliar y reforzar los conocimientos adquiridos en la materia de Redes de Comunicaciones.

4.2) FASE II. Identificar los equipos Cisco con que cuenta el laboratorio de redes de comunicaciones.

Para obtener la información de los equipos Cisco con que cuenta actualmente el laboratorio de Redes de Comunicaciones, fue necesario dirigirse personalmente a dicho laboratorio y poder verificar los equipos con la ayuda del personal técnico encargado del mismo y profesores. Como resultado se encontraron 3 Switches Cisco Catalyst 2950 y 5 Routers Cisco 1700.

· Características generales del Switches Cisco Catalyst 2950

Numero de puertos utilizables:	24 x Ethernet 10/100 Mbit/s
Interna de ancho de banda:	13.6 Gbps
Tamaño de la tabla de direcciones MAC:	8192
Tamaño de memoria FLASH:	16Mb

Tamaño de memoria RAM: 32Mb

- **Características generales del Router Cisco 1700**

Los routers Cisco de la serie 1700 proporcionan un rápido, fiable y seguro acceso a Internet y a redes remotas a través de diferentes tecnologías de acceso WAN de alta velocidad. La serie 1700 ofrece una extensa familia de características de seguridad integradas como protección por "firewall", túneles VPN y detección de intrusos o "IDS". También proporcionan una vía de acceso a servicios como la Voz por IP o "Voice-over-IP" y telefónica IP a través de la convergencia de las redes de voz y datos que ofrecen servicios de procesamiento de llamada y calidad de servicio o "QoS".

Puertos WAN: 1 Ethernet 10/100

Puertos Switch: 4 Ethernet 10/100

4.3) FASE III: Estudiar, organizar y seleccionar los aspectos básicos de la tecnología Cisco, que son necesarios para el aprendizaje y desempeño profesional de los estudiantes.

Para obtener la información de los aspectos básicos de la tecnología Cisco relacionada con las técnicas de análisis e información que cumplan con lo establecido en el programa académico de la materia redes de comunicaciones, se utilizó una serie de recolección y organización de datos.

Se definió como primer paso, por parte del Ingeniero Javier Clavo, profesor que imparte la materia, el programa académico de las actividades a realizar a lo largo del curso, para poder así realizar la búsqueda y recolección de toda la información relacionada con la tecnología Cisco necesaria, que cumpla con los requisitos y exigencias del programa académico. A su vez asesoró y proporcionó material informativo, el mismo por medio de entrevista ayudó a seleccionar el material de mayor importancia para la materia.

Se recurrió a diversas fuentes bibliográficas, haciendo usos de herramientas como internet, obteniendo muchos datos complementarios en cuanto al programa académico de la materia así como las técnicas requeridas para el proceso de elaboración de las prácticas. En el desarrollo de esta fase, se trataron temas de sumo interés, los cuales ayudaran a la consecución de los objetivos propuestos. Los temas son los mencionados a continuación:

- Redes de computadoras
- Redes punto a punto
- Redes multipunto
- Redes de área local
- Redes de área metropolitana
- Redes de área amplia
- Redes de área local inalámbrica
- Componentes de las redes
- Topología de las redes
- Protocolo TCP/IP
- Modelo OSI
- Switching
- Habilitación IP en un Switch
- Routing
- Sistema Operativo OSI
- Acceso mediante CLI
- Programas de emulación terminal
- Modos de funcionamiento de Cisco
- Ayuda contextual del IOS bajo CLI
- Verificación de comando
- Teclas de acceso rápido

En un mundo tecnológicamente avanzado y conectado por redes, es muy fácil hacerse de un número de información muy alto, lo cual trajo consigo ventajas y desventajas, ventajas como un gran número de información al alcance de la mano y desventajas como un gran análisis en el momento de seleccionar la información que realmente era necesaria obtener.

En el amplio mundo de las redes existe un gran campo de información, lo cual permitió obtener todo el conocimiento necesario, herramientas tecnológicas como los simuladores de redes, elementos enteros como prácticas que se realizan en otros centros

educativos del mundo y mejor aún la experiencia, de asesores entrevistados personalmente y de personas que escriben en los foros a través de la web.

Todo lo mencionado anteriormente, en cuanto al material informativo recolectado durante el desarrollo de esta fase, permitió tener una amplia guía de conocimientos y seguimientos relacionados específicamente con la materia redes de comunicaciones.

4.3) FASE IV: Elaboración de un manual de trabajo con prácticas de laboratorio desarrolladas paso a paso y enfocadas en tecnología Cisco para los estudiantes de ingeniería en telecomunicaciones, de manera que permita al estudiantado de la materia Redes de Comunicaciones desarrollar de una forma eficaz el conocimiento académico

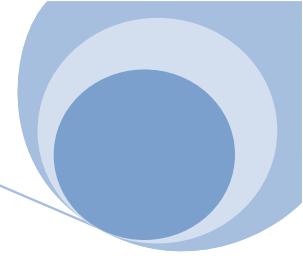
En este punto de la investigación se procedió a realizar un manual cuyo contenido está determinado por un conjunto de prácticas, adaptado al contenido de la materia, a los equipos Cisco con que cuenta el laboratorio y al tiempo disponible durante el semestre académico en el cual se imparte la materia Redes de Comunicaciones, este manual se diseñó de forma tal que cada practica pudiese ser realizada sistemáticamente por el estudiante y guiada de la misma manera por el profesor simplificando así el aprendizaje y el trabajo de evaluación del laboratorio de la materia antes mencionada.

El manual es el resultado de las fases anteriores de la investigación, entrevistas con expertos y recopilación de documentación fueron de vital importancia para su desarrollo, por lo cual se puede garantizar que es un elemento adaptado a las realidades actuales que cubren el campo de las redes de comunicaciones. A continuación se presenta el resultado de esta fase que es la elaboración del manual que contiene plasmado un número de prácticas de laboratorio para la materia Redes de Comunicaciones.

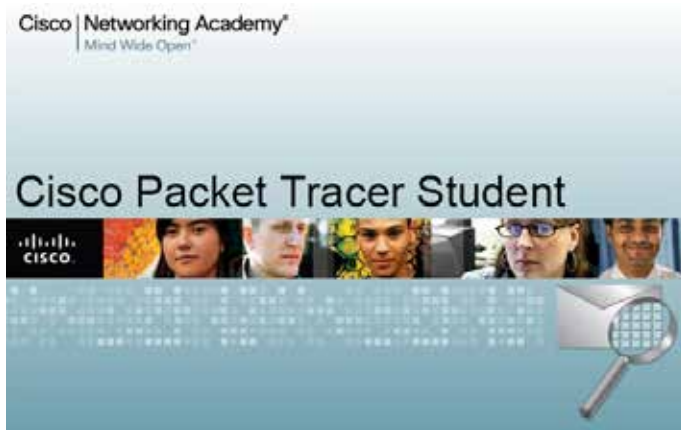


Universidad
José Antonio Páez

**Manual de Prácticas
de Laboratorio
enfocado en
Tecnología Cisco
Para la Materia
Redes de
Comunicaciones.**



Packet Tracer-1



Manejo de software de simulación de redes

Packet Tracer.

Una de las herramientas más utilizadas en el mundo orientadas a la simulación de redes de datos es Packet Tracer, el cual consiste en un

simulador gráfico de redes desarrollado y utilizado por Cisco como herramienta de entrenamiento para obtener la certificación CCNA. Packet Tracer, es un simulador de entorno de redes de comunicaciones de fidelidad media, que permite crear topologías de red mediante la selección de los dispositivos y su respectiva ubicación en un área de trabajo, utilizando una interfaz gráfica.

El software simulador, permite el diseño y planificación de redes, sin la necesidad de tener dispositivos de hardware o software adicionales a la máquina en la que se instala. Entrega funcionalidades de configuración real lo cual agrega un gran valor, pues el programa dispone de interfaces de hardware genéricas, así como interfaces diseñadas para equipos específicos de la empresa CISCO.

El manejo de este software permitirá al estudiante hacer diseño y pruebas de las redes utilizadas en los laboratorios de este manual previamente a su montaje real, para así tener una idea previa de lo que ocurrirá físicamente en la práctica.

Una vez modeladas las topologías de red deseadas, hay que seguir únicamente los pasos sistemáticos que se realizaron en la herramienta, para poder hacer funcionar la red designada en el laboratorio. Esta es una gran ventaja, pues no se necesita tener el espacio físico y todas las computadoras para saber si funciona la red.



Packet Tracer-2

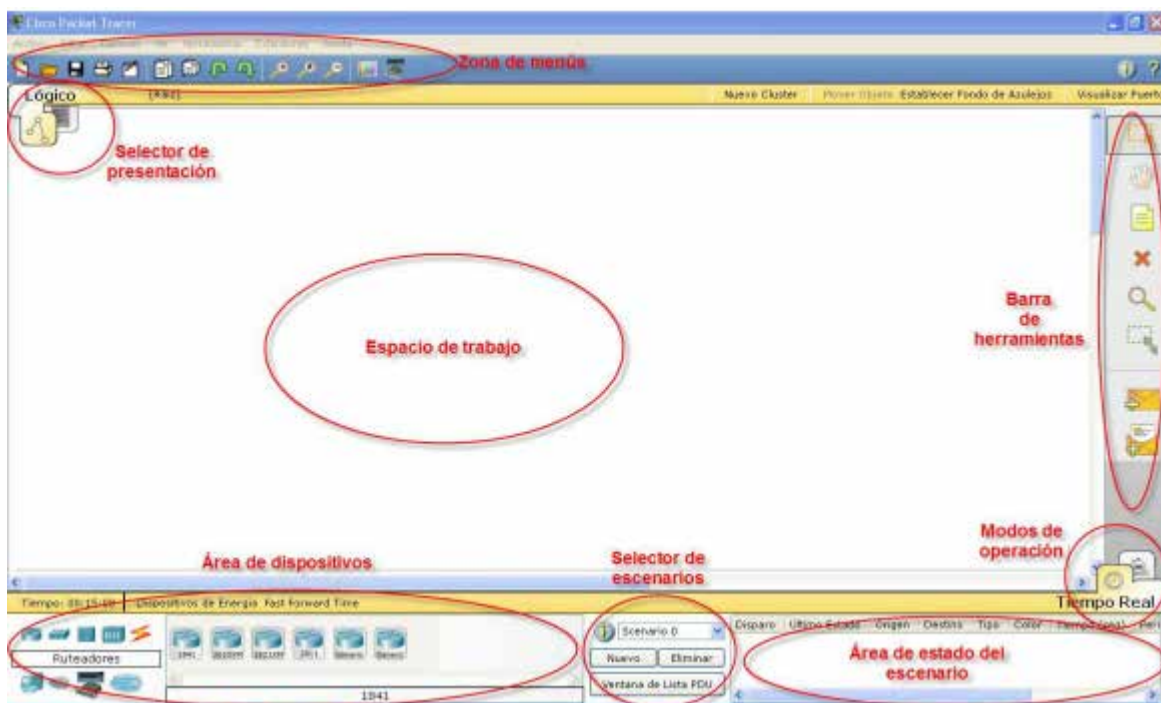
Es por eso que esta parte del manual está dedicada a explicar el funcionamiento del ya antes mencionado simulador, para así facilitar al estudiante su uso y aplicación durante el curso de las prácticas de Laboratorio de la asignatura redes de comunicación.

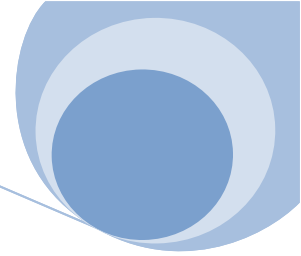
Objetivos:

- Aprender a configurar redes de computadores de forma teórica.
- Utilizar la herramienta Packet Tracer, para el posterior desarrollo de las experiencias en el laboratorio.
- Disposición de configuraciones reales de computadores a pequeña y gran escala

Explorar la interfaz del Packet Tracer (PT).

Cuando se inicia el Packet Tracer, éste presenta una vista lógica de la red en el modo de tiempo real. La parte principal de la interfaz del PT es el Área lógica de trabajo. Ésta es el área principal donde se colocan y conectan los dispositivos.





Packet Tracer-3

En el espacio de trabajo de Packet Tracer se encuentran diferentes zonas:

Zona de menús.

Es el área donde se encuentran las opciones típicas de todos los programas para la gestión y la configuración del software.

Selector de presentación.

Permite cambiar entre esquema lógico y esquema físico a la hora de presentar los dispositivos. Lo habitual es trabajar con el esquema lógico.

Espacio de trabajo.

El área de trabajo lógico permite colocar cada uno de los dispositivos de red para luego interconectarlos con el medio físico apropiado, de acuerdo a las topologías lógicas que requiere el diseño de la red.

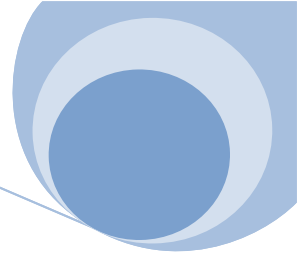
El espacio de trabajo físico permite dar las dimensiones físicas al diseño de la red. Usted define una escala y lugar (como su red se vería en un entorno real) para cada dispositivo utilizado en su diseño lógico de la red(es). Analiza la colocación y distribución de todos los dispositivos de la red en un “área física de trabajo”, para así evaluar: calidad/marca de los dispositivos seleccionados, eficiencia, problemas de cobertura, etc., los cuales no se observan en el diseño lógico de la red.

Barra de herramientas.

Proporciona herramientas para seleccionar dispositivos, mover el espacio de trabajo, analizar parámetros específicos de los dispositivos (la lupa), generar unidades de datos de protocolo (PDU) simples o complejas (sobre cerrado y sobre abierto, respectivamente).

Selector de modos de operación.

Los modos de operación de Packet Tracer reflejan el funcionamiento del esquema de red, los cuales pueden ser:



Packet Tracer-4

a) Modo tiempo real (Realtime Mode): El simulador ejecuta su topología en tiempo real, limitando los protocolos a probar. La red responde a sus acciones inmediatamente, como lo haría un medio de red en el momento que ocurra un suceso en la red.

b) Modo de Simulación (Simulation Mode): El creador de la topología puede evaluar los tipos, tiempos y secuencias de paquete 's generados en diversos "escenarios de prueba". Puede ver a su red, ya sea paso a paso o sino, evento por evento.

Selector de escenarios.

Sirve para realizar distintos análisis sobre una misma red.

Área de estado del escenario.

Muestra las UDP que han intervenido en el análisis realizado, ya sea en tiempo real o en modo simulación, para cada uno de los escenarios o situaciones en los que ha operado la red.

Área de dispositivos.

Es la zona que permite seleccionar los dispositivos que van a ser incluidos en el espacio de trabajo, así como la conexión entre estos. La zona izquierda recoge los dispositivos por grupos y la zona derecha del área ofrece los dispositivos incluidos, de acuerdo con la numeración utilizada por Cisco System.

Para iniciar a construir una topología de red, se debe realizar lo siguiente:

1. Seleccionar de las herramientas de categorías y modelos al primer dispositivo requerido de su diseño de red.

*Ejemplos: Para colocar una PC Host, dar clic en Categoría End Device y luego PC-PT
Para colocar un dispositivo repetidor: Categoría: Hubs y dispositivo Repeater-PT*

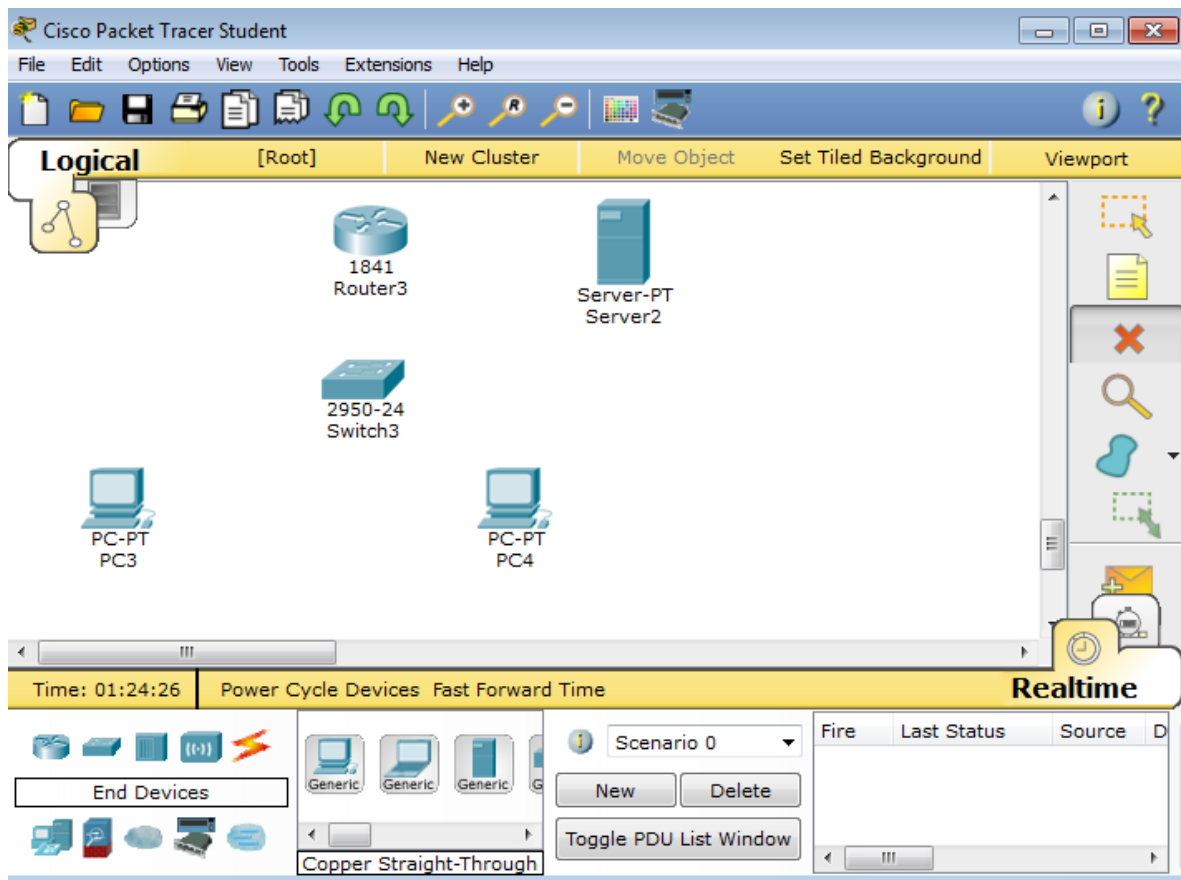
2. Desplazar el cursor hasta la posición final en el área de trabajo lógico donde se colocara dispositivo y dar un clic se mostrara una imagen, la cual representa una copia del dispositivo seleccionado.



Packet Tracer-5

3. Repetir los pasos anteriores para colocar el resto de dispositivos de la topología a simular.

Para elaborar la interconexión física entre los dispositivos, se localizan los medios físicos requeridos en la categoría de dispositivos (Connections).



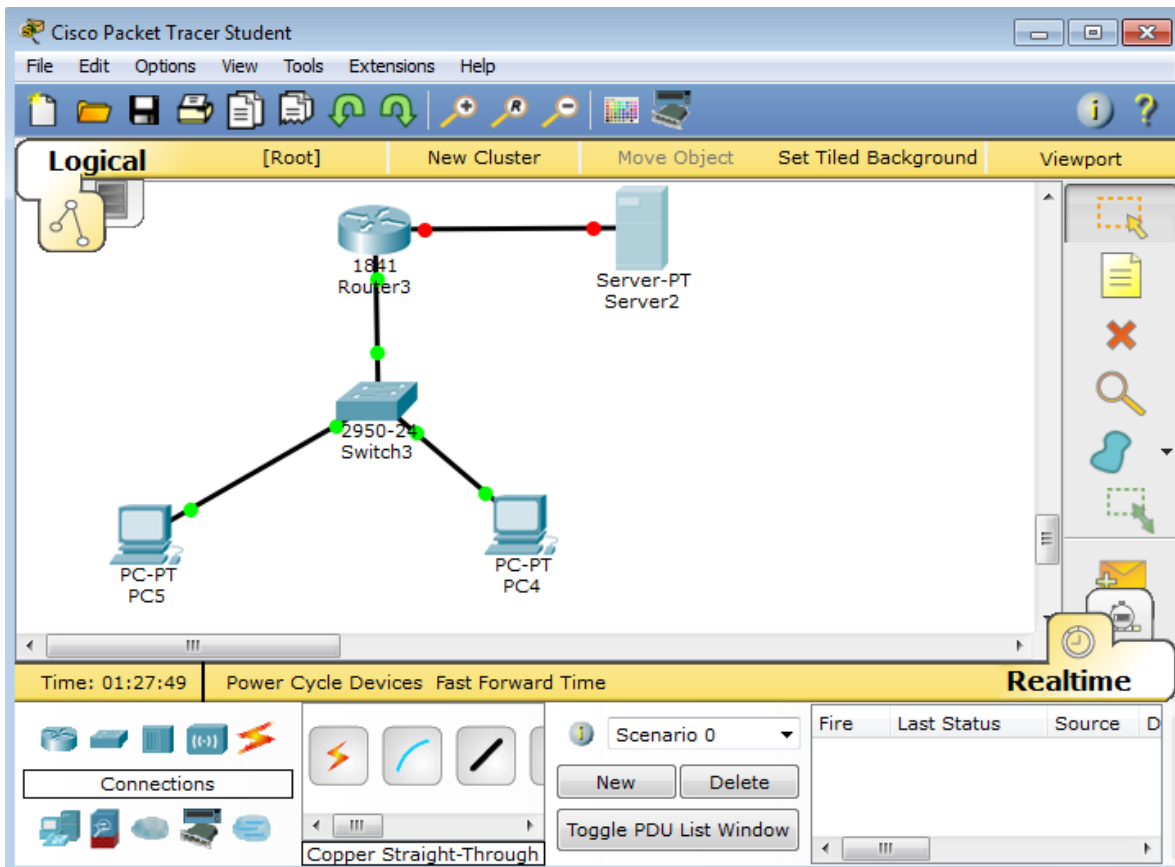
Interconexión de los dispositivos de la topología de la Red.

1. Se selecciona el medio apropiado (ya sea cable plano, cable cruzado, de consola, etc.), luego se selecciona cada dispositivo de la pareja a unir con el medio seleccionado. Por cada dispositivo debe seleccionar la conexión apropiada, por ejemplo: Fast Ethernet para cable UTP, RS232 para cable serial, etc.



Packet Tracer-6

2. Si ha realizado correctamente la conexión entre las interfaces de ambos dispositivos correctamente, podrá ver un punto verde en cada extremo del medio físico que hace la conexión, de lo contrario el punto se tornara rojo, se puede hacer uso de la herramienta Delete (cruz roja mostrada en cuadro de herramientas) para marcar y borrar el medio físico incorrecto.
3. Repita los 2 pasos anteriores para cada pareja de dispositivos a interconectar.

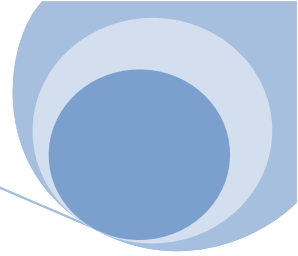


4. Una vez interconectados físicamente los dispositivos de la topología de red, se realiza la configuración del protocolo TCP/IP en los dispositivos que lo requieran.



Packet Tracer-7

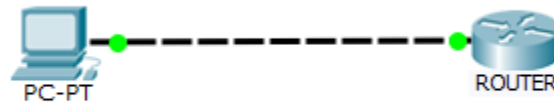
5. Se da clic en el dispositivo a configurar y selecciona la ficha Escritorio De las múltiples opciones, selecciona IP Configuration.
6. Ingresar el trío de parámetros básicos: IP del Host, mascara de subred e IP de Gateway.
7. Se repite los pasos anteriores por cada dispositivo que requiera TCP/IP.



Practica – 1

Práctica 1: Configuración básica del router

Diagrama de topología



Objetivos

1. Identificar correctamente los cables que se utilizan en la red.
2. Configuración básica de Router y Configuración PC.
3. Pruebas de Conectividad.

Recursos necesarios:

- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Putty)
- 1 cable de consola
- 1 adaptador RJ-45 a DB-9
- Software de emulación de terminal (Putty)
- 1 Router cisco 1700.

Tarea 1: Establecer una conexión de consola al router.

El puerto de consola es un puerto de administración que se utiliza para proveer acceso al router fuera de banda. Se utiliza para establecer y controlar la configuración inicial de un router. Para conectar una PC al puerto de consola se utiliza un cable de consola y un adaptador RJ-45 a DB-9, el software de emulación de terminal se utiliza para configurar el router sobre la conexión de consola el software a utilizar es el PUTTY.



Practica – 1

Paso 1: Conecte el cable de consola al router y la PC. Primero conecte el cable de consola al puerto de consola del router, un conector RJ-45. Luego conecte el extremo DB-9 del cable de consola al puerto serial de la PC1.

Paso 2: Pruebe la conexión del router.

1. Abra el software de emulación de terminal (PUTTY)
2. Configure los parámetros de software específicos para estas aplicaciones.
3. Una vez que la ventana terminal esté abierta, presione la tecla **Intro**. Deberá haber una respuesta del router. Si hay, esto significa que la conexión se ha realizado con éxito. Si no hay ninguna conexión, resuelva el problema según sea necesario. Por ejemplo, verifique que el router esté conectado. Compruebe la conexión al puerto serial en la PC y el puerto de la consola en el router.

¿Que tipo de cable se uso para establecer la conexión al router?

Tarea 2: Borrar y recargar los routers.

Paso 1: Por medio de la sesión HyperTerminal establecida en la Tarea 1, ingrese al modo EXEC privilegiado en el router.

```
Router>enable  
Router#
```

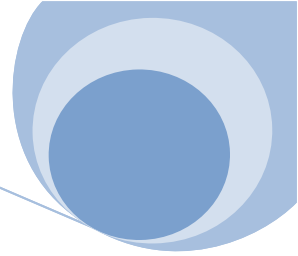
Paso 2: Borre la configuración. Para eliminar la configuración, ejecute el comando **erase startup-config**. Cuando se lo solicite, confirme el objetivo

Paso 3: Recargue la configuración. Al volver el indicador, ejecute el comando **reload**. Cuando se le solicite, confirme el objetivo.

Tarea 3: Realizar la configuración básica del router R1.

Paso 1: Entre al modo EXEC privilegiado.

```
Router> enable  
Router#
```



Practica – 1

¿Qué sucede si en vez de escribir comando **enable** coloca otro comando por ejemplo **configure terminal**? Justifique su respuesta.

Paso 2: Entre al modo de configuración global.

```
Router# configure terminal
Router(config)#
```

Paso 3: Configure el nombre del router como **R1**.

```
Router(config)# hostname R1
R1(config)#
```

Paso 4: Desactive la búsqueda de **DNS** con el comando: `no ip domain-lookup`.

```
R1(config)#no ip domain-lookup
R1(config)#
```

Salga del modo de configuración global y modo EXEC privilegiado con el comando **exit** y escriba **cisco.com** explique se sucede

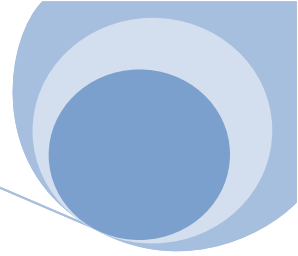
Paso 5: Configure una contraseña de modo EXEC.

Configure una contraseña de modo EXEC por medio del comando **enable secret** redes

```
R1(config)#enable secret redes
R1(config)#
```

Paso 6: Configure un título con el mensaje del día mediante el uso del comando **banner motd**.

```
R1(config)#banner motd &
*****
```



Practica – 1

```
!!!SOLO ACCESO AUTORIZADO!!!  
***** &  
R1(config)#
```

Paso 7: Configure la contraseña de consola en el router.

Utilice UJAP como contraseña. Cuando haya finalizado, salga del modo de configuración de línea.

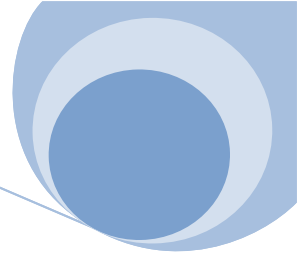
```
R1(config)#line console 0  
R1(config-line)#password ujab  
R1(config-line)#login  
R1(config-line)#exit  
R1(config)#
```

Paso 8: Configure la contraseña para las líneas de terminal virtual. Utilice REDES como contraseña. Cuando haya finalizado, salga del modo de configuración de línea.

```
R1(config)#line vty 0 4  
R1(config-line)#password telecom  
R1(config-line)#login  
R1(config-line)#exit  
R1(config)#
```

Salga del modo de configuración global con el comando **exit** y ejecute el comando **show running-config**, pulse la barra espaciadora y explique que sucede

¿Se muestran las contraseñas de modo EXEC y de acceso a consola? ¿De ser así cuáles son?



Practica – 1

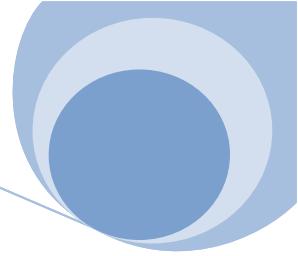
Paso 9: Encrypte todas las contraseñas con el comando **service password-encryption**

```
R1(config)#service password-encryption  
R1(config-line)#exit
```

Ejecute nuevamente el comando **show running-config**, y explique que encuentra diferente a cuando se ejecuto anteriormente

Paso 10: Guarde toda la configuración con el comando **copy running-config startup-config**

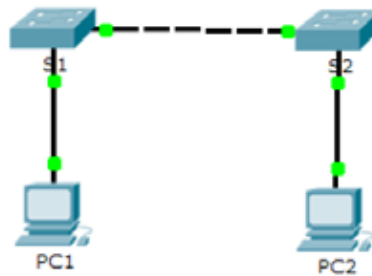
```
R1#copy running-config startup-config
```



Practica-2

Practica 2: Configuración de los parámetros iniciales del switch

Diagrama de Topología



Objetivos

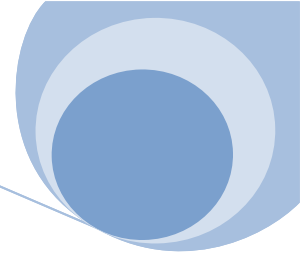
1. Realizar el cableado de una topología física de laboratorio.
2. Introducir la información de dirección IP estática en la interfaz LAN de los hosts
3. Verificar que las PC puedan comunicarse por medio de la utilidad ping.
4. Configurar y verificar los parámetros básicos del switch.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway Predeterminado
S1	VLAN 1	No Aplicable	No aplicable	No aplicable
S1	VLAN 1	No Aplicable	No aplicable	No aplicable
PC-A	NIC	192.168.1.10	255.255.255.0	No aplicable
PC-B	NIC	192.168.1.11	255.255.255.0	No aplicable

Recursos necesarios

- 2 switches (Cisco 2950)
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Putty)



Practica-2

- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet

Tarea 1: Configurar la topología de la red (Ethernet únicamente).

En la Tarea 1, se realizará el cableado para conectar los dispositivos según la topología de la red.

Paso 1: Encender los dispositivos

Encienda todos los dispositivos de la topología. Los switches no tienen un interruptor de corriente; se encienden en cuanto enchufa el cable de alimentación.

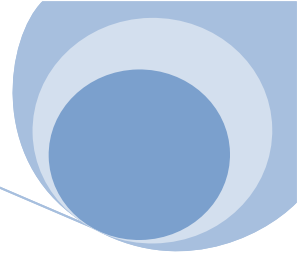
Paso 2: Conectar los dos switches

Conecte un extremo de un cable Ethernet a F0/1 en el S1 y el otro extremo del cable a F0/1 en el S2. Las luces de F0/1 en los dos switches deberían tornarse ámbar y, luego, verde. Esto indica que los switches se conectaron correctamente.

Paso 3: Conectar las PC a sus respectivos switches

a. Conecte un extremo del segundo cable Ethernet al puerto NIC en la PC-A. Conecte el otro extremo del cable a F0/6 en el S1. Después de conectar la PC al switch, la luz de F0/6 debería tornarse ámbar y luego verde, lo que indica que la PC-A se conectó correctamente.

b. Conecte un extremo del último cable Ethernet al puerto NIC en la PC-B. Conecte el otro extremo del cable a F0/18 en el S2. Después de conectar la PC al switch, la luz de F0/18 debería tornarse ámbar y luego verde, lo que indica que la PC-B se conectó correctamente.

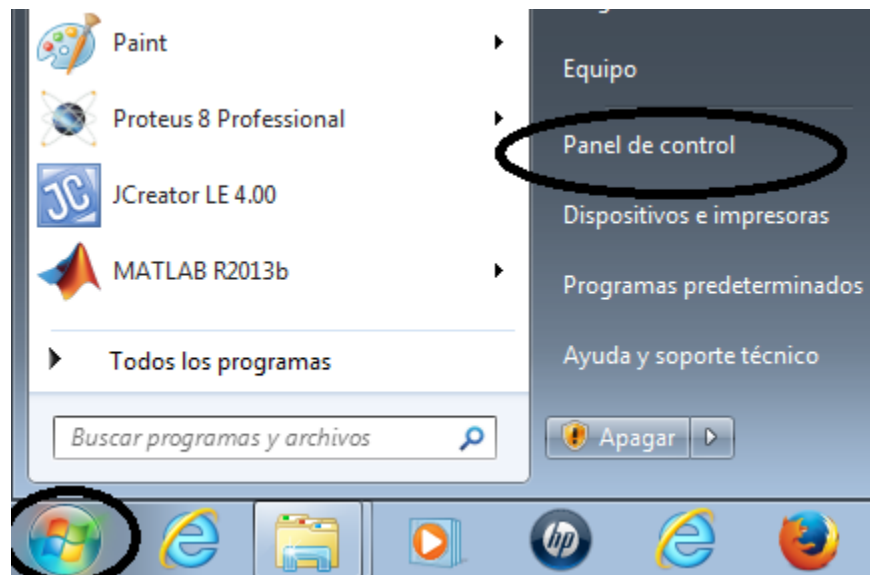


Practica-2

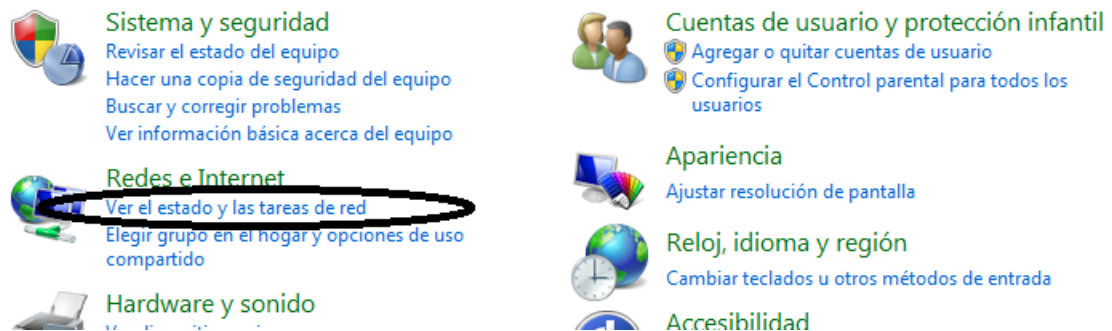
Tarea 2: Configurar hosts en las PC

Paso 1: Configurar la información de dirección IP estática en las PC

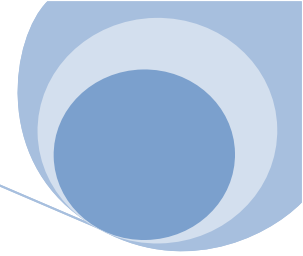
a. Haga clic en el ícono **Inicio de Windows** y, a continuación, seleccione **Panel de control**.



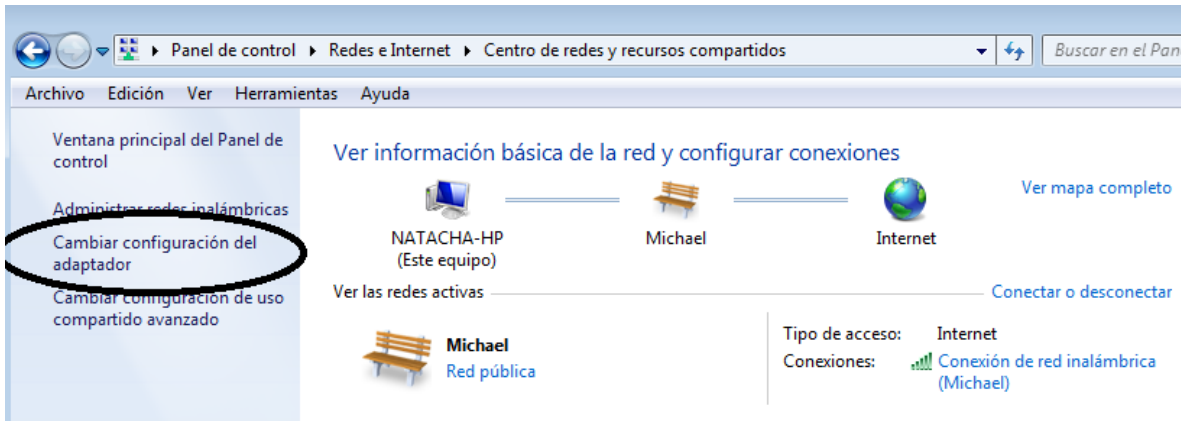
b. En la sección Redes e Internet, haga clic en el enlace **Ver el estado y las tareas de red**.



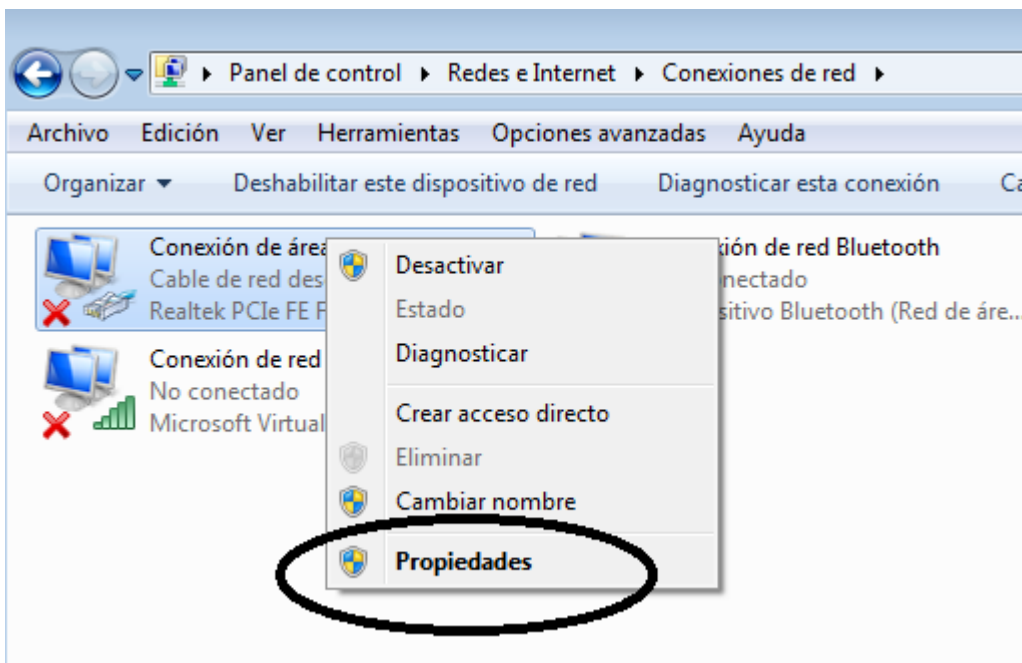
c. En el panel izquierdo de la ventana Centro de redes y recursos compartidos, haga clic en el enlace **Cambiar configuración del adaptador**.



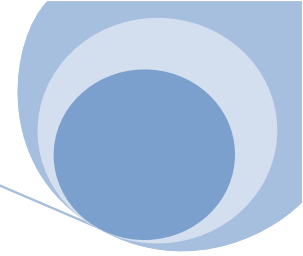
Practica-2



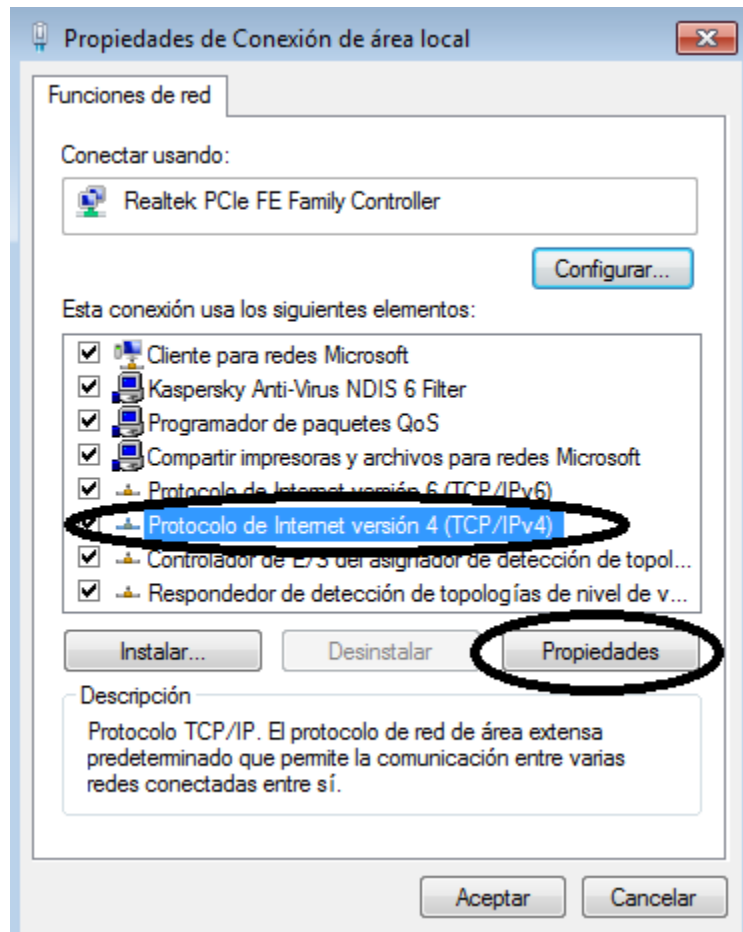
d. En la ventana Conexiones de red, se muestran las interfaces disponibles en la PC. Haga clic con el botón secundario en la interfaz **Conexión de área local** y seleccione **Propiedades**.



e. Seleccione la opción **Protocolo de Internet versión 4 (TCP/IPv4)** y, a continuación, haga clic en **Propiedades**.



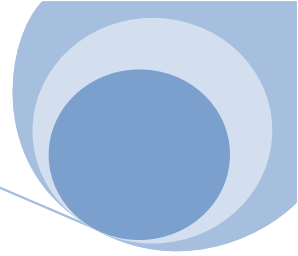
Practica-2



- f. Haga clic en el botón de opción **Usar la siguiente dirección IP** para introducir manualmente una dirección IP, la máscara de subred y el gateway predeterminado.
- g. Después de introducir toda la información IP, haga clic en **Aceptar**.
- h. Repita los pasos anteriores para introducir la información de dirección IP para la PC-B.

Tarea 3: Verificar la configuración y la conectividad de la PC

Utilice la ventana del símbolo del sistema (**cmd.exe**) para verificar la configuración y la conectividad de la PC.

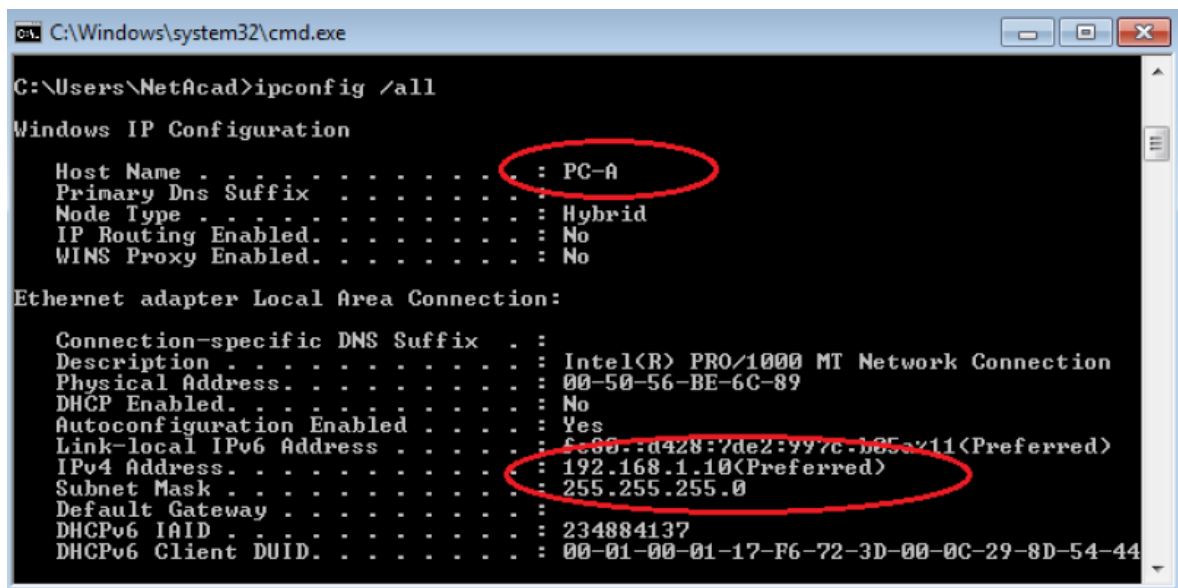


Practica-2

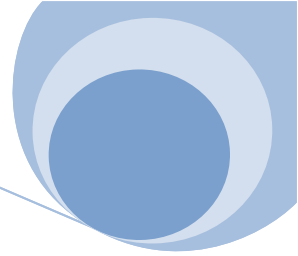
a. En la PC-A, haga clic en el ícono **Inicio de Windows**, escriba **cmd** en el cuadro de diálogo **Buscar programas y archivos** y, a continuación, presione Entrar.



b. En la ventana cmd.exe, puede introducir comandos directamente en la PC y ver los resultados de esos comandos. Verifique la configuración de la PC mediante el comando **ipconfig /all**. Este comando muestra el nombre de host de la PC y la información de la dirección IPv4.



c. Escriba **ping 192.168.1.11** y presione Entrar.



Practica-2

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time=1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\NetAcad>
```

¿Fueron correctos los resultados del ping?

Si no lo fueron, resuelva los problemas que haya presentes.

Tarea 4: Configurar y verificar los parámetros básicos del switch

Paso 1: Acceda al switch mediante el puerto de consola.

Utilice Putty para establecer una conexión de consola al switch desde la PC-A.

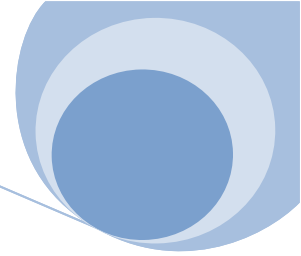
Paso 2: Ingrese al modo EXEC privilegiado.

```
Switch>enable
Switch#
```

Paso 3: Entre al modo de configuración.

Utilice el comando **configuración terminal** para ingresar al modo de configuración.

```
Switch# configure terminal
```



Practica-2

Paso 4: Asignar un nombre al switch

```
Switch(config)# hostname S1  
S1(config)#
```

Paso 5: Evitar búsquedas de DNS no deseadas

```
S1(config)# no ip domain-lookup  
S1(config)#
```

Paso 6: Introducir contraseñas locales.

```
S1(config)# enable secret class  
S1(config)# line con 0  
S1(config-line)# password cisco  
S1(config-line)# login  
S1(config-line)# exit
```

Paso 7: Encryptar las contraseñas

```
S1(config)# service password-encryption
```

Paso 8: Desactivar las Interfaces de los puertos del Switch que no se utilizan.

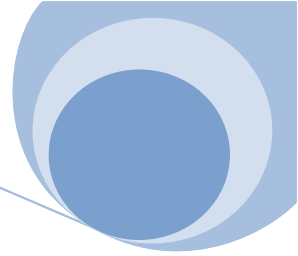
Utilice el comando interface FastEthernet 0/Nro. Del puerto, para desactivas los puertos del switch que desee ejemplo:

```
S1(config)# Interface FastEthernet 0/3  
S1(config)# shutdown
```

Paso 9: Guardar la Configuración

Utilice el comando copy para guardar la configuración en ejecución en el archivo de inicio de la memoria de acceso aleatorio no volátil (NVRAM).

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



Practica-2

Paso 10: Mostrar la configuración actual

El comando show running-config muestra toda la configuración en ejecución, de a una página por vez. Utilice la barra espaciadora para avanzar por las páginas.

```
S1# show running-config
```

Paso 11: Mostrar el estado de las interfaces conectadas en el switch

Para revisar el estado de las interfaces conectadas, utilice el comando show ip interface brief. Presione la barra espaciadora para avanzar hasta el final de la lista.

```
S1# show ip interface brief
```

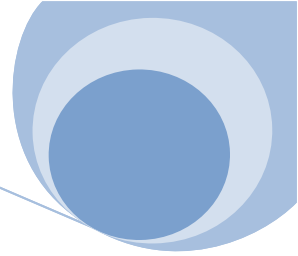
Paso 12: Repetir los pasos del 1 al 12 para configurar el switch S2

De acuerdo a los comandos Shows realizados en los pasos anteriores, registre el estado de las interfaces en la siguiente tabla

Interfaz	S1		S2	
	Estado	Protocolo	Estado	Protocolo
F0/1				
F0/6				
F0/18				
VLAN 1				

¿Por qué algunos puertos FastEthernet en los switches están activos y otros inactivos?

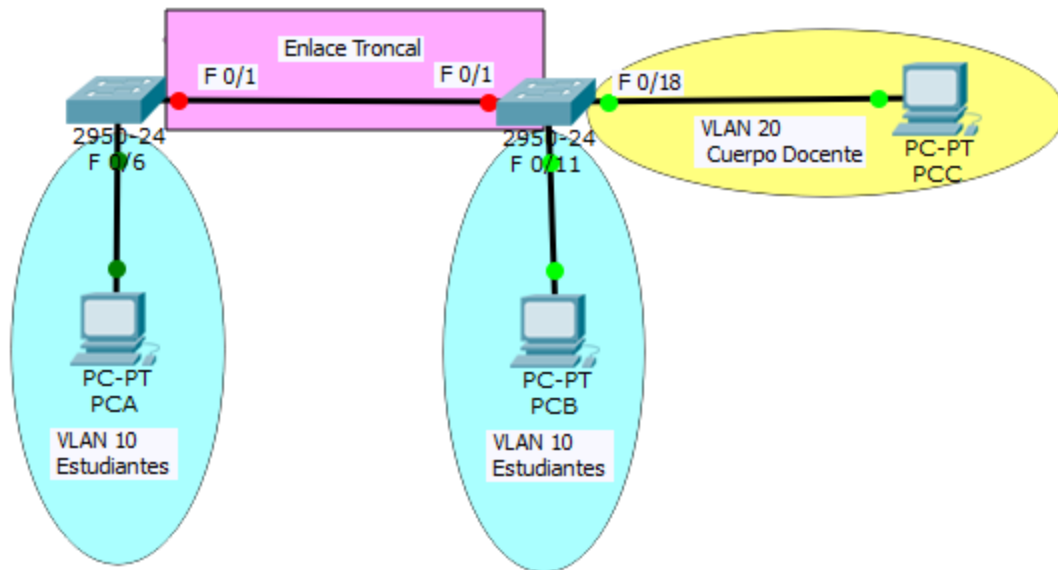
¿Qué podría evitar que se envíe un ping entre las PC?



Practica-3

Practica 3: configuración de redes VLAN y enlaces troncales

Diagrama de Topología

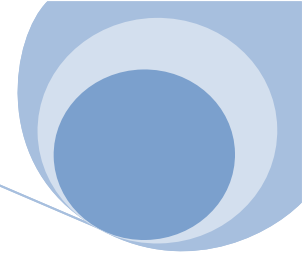


Objetivos

1. Armar la red y configurar los parámetros básicos de los dispositivos
2. Crear redes VLAN y asignar puertos de switch
3. Configurar un enlace troncal 802.1Q entre los switches

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway Predeterminado
S1	VLAN 1	192.168.1.11	255.255.255.0	No Aplica
S2	VLAN 1	192.168.1.12	255.255.255.0	No Aplica
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1



Practica-3

Recursos necesarios

- 2 switches (Cisco 2950 con IOS de Cisco)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Putty o Tera Tem)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Tarea 1: Armar la red y configurar los parámetros básicos de los dispositivos

En la tarea 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los switches.

Paso 1: Realizar el cableado de red tal como se muestra en la topología. Conecte los dispositivos tal como se muestra en el diagrama de la topología y realice el cableado según sea necesario.

Paso 2. Configurar los parámetros básicos para cada switch.

a. Desactive la búsqueda del DNS.

```
Switch>enable
```

```
Switch#configure terminal
```

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

```
Switch(config)# no ip domain-lookup
```

b. Configure el nombre del dispositivo como se muestra en la topología.

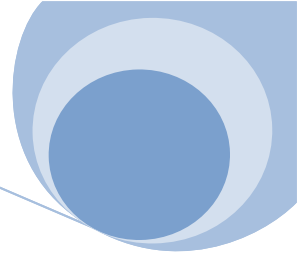
```
Switch(config)#hostname S1
```

```
S1(config)#
```

c. Asigne ujad como la contraseña del modo EXEC privilegiado.

```
S1(config)#enable secret ujad
```

```
S1(config)#
```



Practica-3

d. Asigne cisco como la contraseña de vty y la contraseña de consola.

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

e. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.

```
S1(config)#banner motd &
Enter TEXT message. End with the character '&'.

*****
!!! SOLO ACCESO AUTORIZADO !!!
*****
&

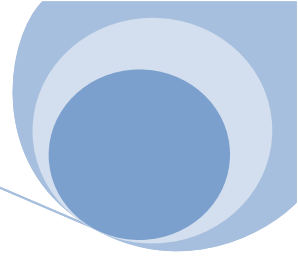
S1(config)#
```

f. Configure la dirección IP que se indica en la tabla de direccionamiento para la VLAN 1 en ambos switches.

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#
```

g. Desactive administrativamente todos los puertos que no se usen en el switch.

```
S1(config)#interface range fastEthernet 0/2-5
S1(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to
administratively down
```



Practica-3

```
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to  
administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to  
administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to  
administratively down
```

```
S1(config)#interface range fastEthernet 0/7-24  
S1(config-if-range)#shutdown
```

h. Copie la configuración en ejecución en la configuración de inicio

```
S1(config-if-range)#exit  
S1(config)#exit  
S1#copy running-config startup-config  
Destination filename [startup-config]?  
Building configuration...  
[OK]  
S1#
```

i. Repita los pasos anteriores para el Switch 2

Paso 3. Configurar los equipos host

Consulte la tabla de direccionamiento para que pueda obtener la información de las direcciones de los equipos host, y así poder asignar de manera correcta las ip de cada PC.

Paso 4. Probar la conectividad.

Verifique que los equipos host puedan hacer ping entre sí.

¿Se puede hacer ping de la PC-A a la PC-B? _____

¿Se puede hacer ping de la PC-A a la PC-C? _____

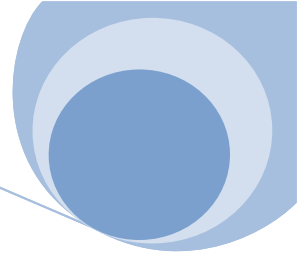
¿Se puede hacer ping de la PC-A al S1? _____

¿Se puede hacer ping de la PC-B a la PC-C? _____

¿Se puede hacer ping de la PC-B al S2? _____

¿Se puede hacer ping de la PC-C al S2? _____

¿Se puede hacer ping del S1 al S2? _____



Practica-3

Si la respuesta a cualquiera de las preguntas anteriores es no, ¿por qué fallaron los pings?

Tarea 2. Crear redes VLAN y asignar puertos de switch

En la parte 2, creará redes VLAN para los estudiantes, el cuerpo docente y la administración en ambos switches. A continuación, asignará las VLAN a la interfaz correspondiente. El comando **show vlan** se usa para verificar las opciones de configuración.

Paso 1. Crear las VLAN en los switches.

a. Cree las VLAN en S1.

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# end
```

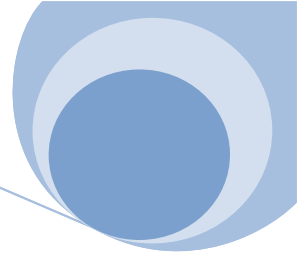
b. Cree las mismas VLAN en el S2.

c. Emita el comando show vlan para ver la lista de VLAN en el S1.

```
S1# show vlan
```

¿Cuál es la VLAN predeterminada? _____

¿Qué puertos se asignan a la VLAN predeterminada?



Practica-3

IOS Command Line Interface

```
S1(config-vlan)#exit
S1(config)#
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show vlan

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

10   student                active
20   Faculty                active
99   Management              active
1002 rddi-default          act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet     100001    1500  -     -     -     -     -     0     0
10   enet     100010    1500  -     -     -     -     -     0     0
20   enet     100020    1500  -     -     -     -     -     0     0
--More-- |
```

Paso 2. Asignar las VLAN a las interfaces del switch correctas.

a. Asigne las VLAN a las interfaces en el S1.

1) Asigne la PC-A a la VLAN Estudiantes.

```
S1(config)# interface f0/6
```

```
S1(config-if)# switchport mode access
```

```
S1(config-if)# switchport access vlan 10
```

2) Transfiera la dirección IP del switch a la VLAN 99.

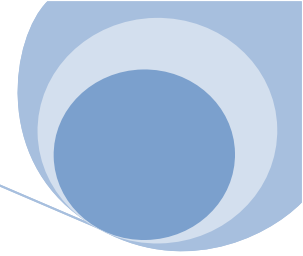
```
S1(config)# interface vlan 1
```

```
S1(config-if)# no ip address
```

```
S1(config-if)# interface vlan 99
```

```
S1(config-if)# ip address 192.168.1.11 255.255.255.0
```

```
S1(config-if)# end
```



Practica-3

b. Emita el comando `show vlan brief` y verifique que las VLAN se hayan asignado a las interfaces correctas.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, 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, Gi0/1 Gi0/2
10	Student	active	Fa0/6
20	Faculty	active	
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

c. Emita el comando `show ip interface brief`.

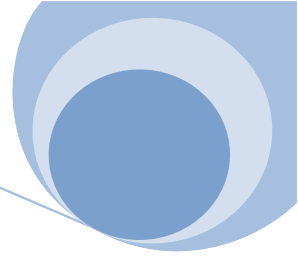
¿Cuál es el estado de la VLAN 99? ¿Por qué?

d. Use la topología para asignar las VLAN a los puertos correspondientes en el S2.

e. Configure una dirección IP para la VLAN 99 en el S2 según la tabla de direccionamiento.

f. Use el comando `show vlan brief` para verificar que las VLAN se hayan asignado a las interfaces correctas.

```
S2# show vlan brief
```



Practica-3

¿Es posible hacer ping de la PC-A a la PC-B? ¿Por qué?

¿Es posible hacer ping del S1 al S2? ¿Por qué?

Tarea 3. Configurar un enlace troncal 802.1Q entre los switches

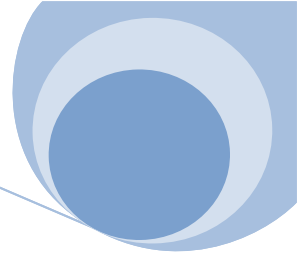
El comando **switchport mode trunk** se usa para configurar un puerto manualmente como enlace troncal. Este comando se debe emitir en ambos extremos del enlace.

Paso 1. Cambie el modo de switchport en la interfaz F0/1 para forzar el enlace troncal. Haga esto en ambos switch.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#switchport trunk allowed vlan 10
S1(config-if)#end
```

¿Qué se necesita para permitir que los hosts en la VLAN 10 se comuniquen con los hosts en la VLAN 20?

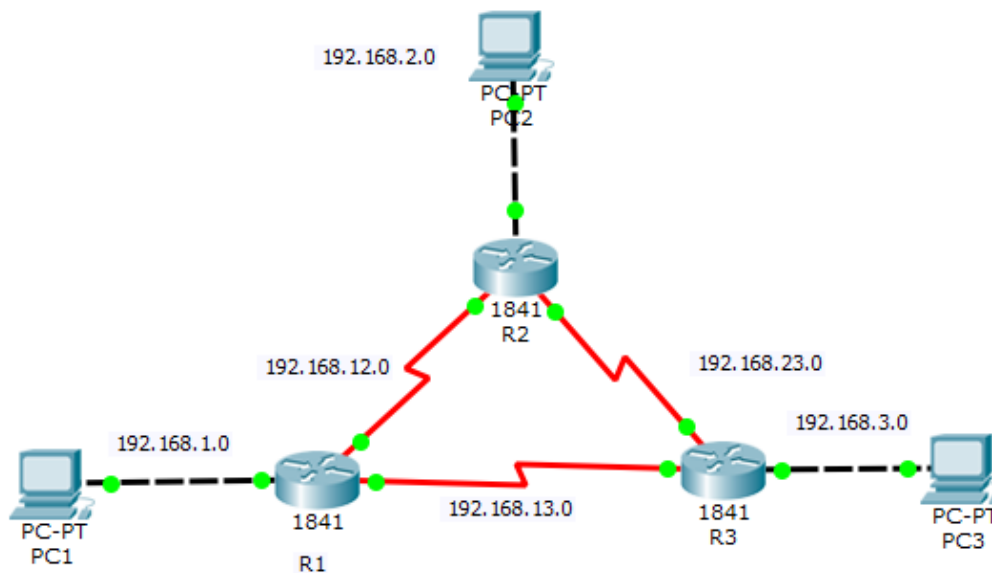
¿Cuáles son algunos de los beneficios principales que una organización puede obtener mediante el uso eficaz de las VLAN?



Practica-4

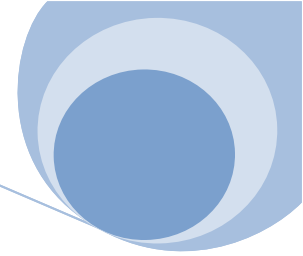
Practica 4: Configuración de enrutamiento estático y dinámico

Diagrama de Topología



Objetivos

1. Examinar la red y evaluar la necesidad de routing estático.
2. Armar la red y configurar los parámetros básicos de los dispositivos
3. Configurar rutas estáticas.
4. Configurar y verificar el routing OSPF.
5. Verificar la conectividad en ambos métodos de enrutamiento.



Practica-4

Recursos necesarios

- 3 routers (Cisco 1700 con IOS de Cisco)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Putty o Tera Tem)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

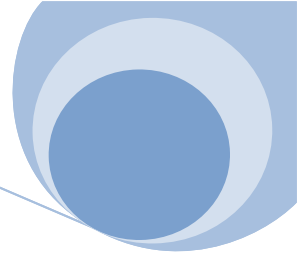
Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway Predeterminado
R1	F 0/0	192.168.1.1	255.255.255.0	N/A
	S0/1/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/1/1 (DCE)	192.168.13.1	255.255.255.252	N/A
R2	F 0/0	192.168.2.1	255.255.255.0	N/A
	S0/1/0	192.168.12.2	255.255.255.252	N/A
	S 0/1/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	F0/0	192.168.3.1	255.255.255.0	N/A
	S 0/1/0	192.168.23.2	255.255.255.252	N/A
	S 0/1/1	192.168.13.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Tarea 1: examinar la red y evaluar la necesidad de routing estático

a. Observe el diagrama de la topología. ¿Cuántas redes hay en total?

b. ¿Cuántas redes están conectadas directamente al R1, al R2 y al R3?



Practica-4

c. ¿Cuántas rutas estáticas requiere cada router para llegar a las redes que no están conectadas directamente?

d. Pruebe la conectividad a las LAN del R2 y el R3 haciendo ping de la PC1 a la PC2 y la PC3. ¿Por qué no logró hacerlo?

Tarea 2. Armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los routers.

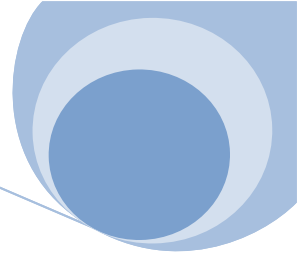
Paso 1: realizar el cableado de red tal como se muestra en la topología.

Paso 2: inicializar y volver a cargar los routers según sea necesario.

Paso 3: configurar los parámetros básicos para cada router.

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.
- c. Asigne UJAP como la contraseña del modo EXEC privilegiado.
- d. Asigne REDES como la contraseña de consola y la contraseña de vty.
- e. Configure un aviso de mensaje del día (MOTD) para advertir a los usuarios que el acceso no autorizado está prohibido.
- f. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config)#interface serial 0/1/0
Router(config-if)#ip address 192.168.12.1 255.255.255.252
Router(config-if)#clock rate 128000
```



Practica-4

```
Router(config-if)#no shutdown
Router#
Router#conf
Router(config)#interface serial 0/1/1
Router(config-if)#ip address 192.168.13.1 255.255.255.252
Router(config-if)#clock rate 128000
Router(config-if)#no shutdown
```

Nota: debe hacer la misma configuración para todas las demás interfaces fastEthernet y serial de los demás routers según indica la tabla de enrutamiento, se debe tener en cuenta que el **comando clock rate** es aplicable solo para las interfaces **DCE**.

h. Copie la configuración en ejecución en la configuración de inicio

Paso 4: configurar los equipos host.

Paso 5: Probar la conectividad.

Los routers deben poder hacerse ping entre sí, y cada computadora debe poder hacer ping a su gateway predeterminado.

¿Porque Las computadoras no pueden hacer ping a otras computadoras?

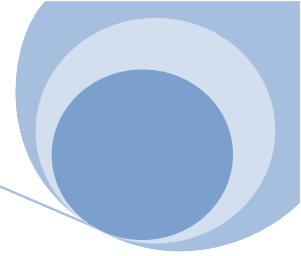
Tarea 3. Configurar rutas estáticas

El enrutamiento estático, es creado manualmente a diferencia de los protocolos dinámicos, que se intercambian las tablas de enrutamiento mediante actualizaciones periódicas. Para crear una ruta estática, es en modo configuración global, y el comando IOS es el siguiente:

```
Router(config)#ip route[ip red destino][mascara de subred][ip siguiente salto]
```

Paso 1: Configuración de Rutas estáticas en el Router 1

```
Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.12.2
```



Practica-4

```
Router(config)#ip route 192.168.23.0 255.255.255.252  
192.168.12.2  
Router(config)#ip route 192.168.3.0 255.255.255.0  
192.168.13.2  
Router(config)#exit
```

Paso 2: Configuración de rutas estáticas en el Router 2

```
Router(config)#ip route 192.168.1.0 255.255.255.0  
192.168.12.1  
Router(config)#ip route 192.168.13.0 255.255.255.252  
192.168.12.1  
Router(config)#ip route 192.168.3.0 255.255.255.0  
192.168.23.2  
Router(config)#exit
```

Paso 3: Configuración de Rutas estáticas en el Router 3

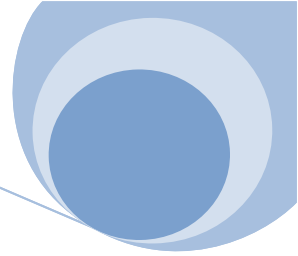
```
Router(config)#ip route 192.168.2.0 255.255.255.0  
192.168.23.1  
Router(config)#ip route 192.168.12.0 255.255.255.252  
192.168.13.1  
Router(config)#ip route 192.168.1.0 255.255.255.0  
192.168.13.1  
Router(config)#exit
```

OJO: No olvide ir guardando la configuración con el comando **copy running-config startup-config**

Tarea 4: Borrar la configuración de enrutamiento estático de los routers

Para eliminar las rutas estáticas ya creadas se debe emitir el mismo comando para su creación, pero con la diferencia de un **no** al principio del comando. Ejemplo:

```
Router(config)#no ip route 192.168.2.0 255.255.255.0  
192.168.12.2  
Router(config)#no ip route 192.168.23.0 255.255.255.252  
192.168.12.2  
Router(config)#no ip route 192.168.3.0 255.255.255.0  
192.168.13.2  
Router(config)#exit
```



Practica-4

De esta manera serán eliminadas las rutas estáticas, este proceso se debe hacer con cada una de las rutas estáticas creadas en la tarea anterior.

Tarea 5: Configurar y verificar el enrutamiento Dinámico

En la parte 5, se configurara el routing dinámico usando para esta caso el protocolo OSPFv2 en todos los routers de la red y, luego se verificará que las tablas de routing se hayan actualizado correctamente. Para crear una ruta OSPF, es en modo configuración global, y el comando IOS es el siguiente:

```
Router(config)#router ospf [ID DE PROCESO]
Router(config-router)#network [IP DE RED][WILDCARD DE LA RED]
area[ID DE AREA]
Router(config-router)#exit
```

Paso 1: Configure el protocolo OSPF en R1.

a.. Configure las instrucciones network para las redes en el R1. Utilice la ID de proceso 1 y la ID de área de área0.

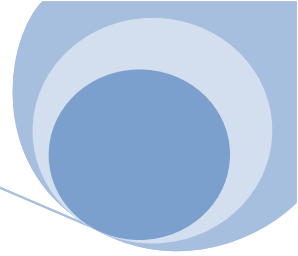
```
R1(config)# router ospf 1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 192.168.12.0 0.0.0.3 area 0
R1(config-router)# network 192.168.13.0 0.0.0.3 area 0
```

Paso 2: Configure OSPF en el R2 y el R3.

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0
R2(config-router)#network 192.168.23.0 0.0.0.3 area 0

R3(config)#router ospf 1
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 192.168.23.0 0.0.0.3 area 0
R3(config-router)#network 192.168.13.0 0.0.0.3 area 0
```

Paso 3: verificar que todos los routers y pc se comuniquen



Practica-4

En este paso, debe verificar haciendo ping, que todos los routers y PC se comuniquen de lo contrario, debe verificar y solucionar el error para poder continua.

Paso 4: verificar los vecinos OSPF y la información de routing.

a. Emita el comando **show ip ospf neighbor** para verificar que cada router indique a los demás routers en la red como vecinos.

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.23.1	0	FULL/ -	00:00:34	192.168.12.2	Serial0/1/0
192.168.23.2	0	FULL/ -	00:00:36	192.168.13.2	Serial0/1/1

¿Por qué aparecen la red 192.168.23.0 como red vecina y no las otras redes?

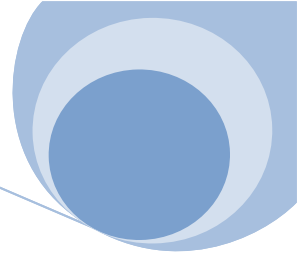
b. Emita el comando **show ip route** para verificar que todas las redes aparezcan en la tabla de routing de todos los routers.

```
R1# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF 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
```

```
C    192.168.1.0/24 is directly connected, FastEthernet0/0  
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:16:14, Serial0/1/0  
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:14:05, Serial0/1/1  
    192.168.12.0/30 is subnetted, 1 subnets  
C    192.168.12.0 is directly connected, Serial0/1/0  
    192.168.13.0/30 is subnetted, 1 subnets  
C    192.168.13.0 is directly connected, Serial0/1/1  
    192.168.23.0/30 is subnetted, 1 subnets  
O    192.168.23.0 [110/128] via 192.168.12.2, 00:14:05, Serial0/1/0  
    [110/128] via 192.168.13.2, 00:14:05, Serial0/1/1
```



Practica-4

Según la información mostrada por el comando **show ip route**. Indique que redes están conectadas, directamente y que redes están conectadas mediante el protocolo OSPF

¿En que se diferencia la configuración de enrutamiento estático a la configuración de de enrutamiento dinámico (OSPF)?

Nombre dos ventajas y desventajas de cada uno de los métodos de enrutamiento usados en la práctica.

CONCLUSIONES.

La realización del presente trabajo de grado tuvo como finalidad la búsqueda de un método eficiente y moderno para ejecutar un número de prácticas de laboratorio enfocadas en tecnología Cisco, que permita al estudiante afianzar sus conocimientos teóricos por medio de la ejecución práctica, con la intención de mejorar la experiencia del aprendizaje y del manejo de los equipos de tecnología Cisco con que cuenta el laboratorio de la materia Redes de Comunicaciones de la Universidad José Antonio Páez.

Durante la elaboración de este trabajo de grado fue necesario consultar y buscar conocimientos entre un amplio número de expertos en el área, experiencias plasmadas electrónicamente a través de la web y distintos libros de metodología abarcando hasta ciertos conceptos educativos para poder garantizar el manejo de las prácticas de forma pedagógica y lo más simple de ser captadas por el estudiante de forma tal de poder lograr un verdadero entendimiento de los conceptos que se buscan fijar en el participante.

En la búsqueda del material necesario para la realización del manual de prácticas de laboratorio se pudo entender que el mundo de las redes de comunicaciones tiene una extensa variedad de conocimientos, que el mismo es cambiante día a día porque está en constante expansión y reorganización, por lo cual fue extremadamente necesario seleccionar con precisión los recursos teóricos fundamentales para la formación académica del estudiante, basándose exclusivamente en la tecnología Cisco y en el contenido de la materia impartida para la carrera Ingeniería de Telecomunicaciones en la UJAP.

Finalmente la realización de este manual tiene como objetivo contribuir con la formación académica de los estudiantes de la carrera Ingeniería de Telecomunicaciones, reforzando los beneficios académicos que ofrece la tecnología Cisco y otorgando herramientas de fácil comprensión y manejo en el área práctica de la materia Redes de Comunicaciones.

RECOMENDACIONES.

A continuación se presentan una serie de recomendaciones a ser consideradas para la implementación de las prácticas.

- Û Es importante tener la cantidad de equipos activos para la realización de las prácticas.
- Û Las prácticas están diseñadas para el trabajo en equipo, por lo cual es importante la organización de los grupos por parte del profesor de forma tal que todos los estudiantes participen.
- Û Se pudo observar durante la ejecución de la realización de algunos de las practicas elaboradas en el manual, que el simulador Packet- Tracer con que cuentan las PC en el laboratorio esta desactualizado ya que la versión que actualmente se encuentra allí es la 3era versión, mientras que Cisco ya lleva la 7ma Versión, Por ende es importante recomendar la actualización del simulador, para que así se pueda usar esta herramienta que cisco ofrece.
- Û Se hace de suma importancia la organización del laboratorio, lo cual contribuye a la eficiencia de la elaboración de cada una de las practicadas mostradas en el manual, ya que existen prácticas en donde se requieren de varios equipos, cables, PC etc... y al no tener un orden en el laboratorio se genera un retardo de tiempo lo que no es favorable para los estudiantes, por ende se recomienda implementar las 5S de kaizen método que cumple con el objetivo de lograr lugares de trabajo más organizados, más ordenados y más limpios de forma permanente para lograr una mayor productividad.
- Û Durante la elaboración del estudio se pudo constatar que las universidades en el mundo de la enseñanza de las redes utilizan equipos especializados de última generación para la enseñanza practica de sus estudiantes, por este lado no está de más recomendar el estudio de la adquisición de equipos de este tipo para tratar de estar a la vanguardia en cuanto a la formación en el manejo de redes.

REFERENCIAS BIBLIOGRAFICAS

- Arias (2006). **El Proyecto de Investigación, introducción a la metodología científica**, Caracas: Editorial. Episteme, C.A.
- Andrew S. Tanenbaum. (2003). **Redes de Computadoras**, México: Editorial Prentice-Hall.
- Balestrini (2002). **Como se Elabora el Proyecto de Investigación**, Caracas: Ediorial Consultores Asociados.
- Cysco Systems (2002). **Academia de Networking de Cisco Systemas: Guía del primer año CCNA1 Y CCNA2**, Tercera Edición.
- Hernández, Fernández y Baptista (2001). **Metodología de la Investigación**, México: Editorial Mc Graw Hill.
- Hurtado de Barrera (2008). **El Proyecto de Investigación. Metodología de la Investigación Holística**, Caracas: Editorial Sypal-Quiron ediciones.
- Jorge Martínez (2002). **Redes de Comunicaciones**, España: Universidad Politécnica de Valencia.
- Tamayo y Tamayo M. (2001). **El Proceso de Investigación Científica**, México: Editorial Limusa.
- William Stallings. (2004). **Comunicaciones y redes de computadores**, España: Editorial PEARSON.

REFERENCIAS ELECTRONICAS

Conceptos básicos de redes:

<http://www.slideshare.net/CieloCarranco/5-definiciones-de-conceptos-bsicos-dredes>

Definiciones: Protocolo Telnet, Protocolo ICMP, Ethernet:

<http://es.kioskea.net/contents/283-protocolo-telnet>

Definiciones: suite de suite de protocolos para las capas de modelo tcp/ip):

<https://geekytheory.com/redes-el-protocolo-arp>

Manual para la Interconexión de Dispositivos de red Cisco

http://es.slideshare.net/JAV_999/manual-redes-routers-y-switches-cisco-18894228

Normas Para La Elaboración y Presentación de Los Anteproyectos, Proyectos y Trabajos de Grado de la UJAP, 2007

<http://w3.ujap.edu.ve/wpcontent/uploads/2013/10/NORMAStrabajodegrado>

Plataforma de aprendizaje **NETACAD**

<https://www.netacad.com/>

Unión Internacional de Telecomunicaciones, Manual sobre redes basadas en el Protocolo (IP) y asuntos conexos.

<http://www.itu.int/ITU-T/special-projects/ip-policy/final/IPPolicyHandbook-S.pdf>

ANEXOS

Instrumento de Investigación



*Universidad José Antonio Páez.
Facultad de Ingeniería.
Escuela de Ingeniería de Telecomunicaciones.*

Instrumento de Investigación (Encuesta).

La información suministrada será utilizada con fines académicos y estrictamente confidenciales, por lo tanto se agradece su valiosa colaboración y aportes que pueda brindar a fin de llevar esta investigación a feliz término.

A. *“¿Está Ud. de acuerdo y conforme con las prácticas realizadas en el laboratorio de la materia Redes de Comunicaciones?”.*

SI___ NO___

B. *“¿Considera Ud. que la implementación de dichas prácticas son lo suficientemente complementarias para el máximo aprendizaje de la materia?”.*

SI___ NO___

C. *“¿En la actualidad los equipos de tecnología Cisco con que cuenta el laboratorio de redes de comunicaciones están siendo utilizados en su totalidad e incluidos en la practicas que se realizan en dicho laboratorio?”.*

SI___ NO

D. *“¿Le Gustaría que los equipos de tecnología Cisco se incluyeran con más frecuencia en las practicas regulares realizadas en el laboratorio de Redes de Comunicaciones?”.*

SI___ NO___

E. *“¿Considera Ud. Que la falta de un sistema estructurado de prácticas de laboratorio enfocado en tecnología Cisco impide al estudiante obtener la experiencia adecuada para enfrentarse a los retos tecnológicos que atraviesan diariamente las redes de comunicaciones?”.*

SI___ NO___

F. “¿Estaría Ud. de acuerdo con el desarrollo de un nuevo, didáctico y actual manual de prácticas enfocado en tecnología Cisco para el laboratorio de Redes de Comunicaciones?”.

SI___ NO___

Carta de Validación del Instrumento



REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

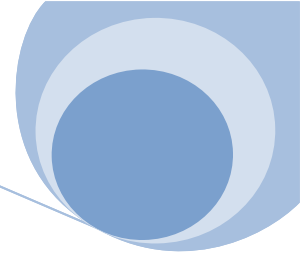
CARTA DE VALIDACIÓN DEL INSTRUMENTO

Quien suscribe , **Ing. Javier Clavo** , Portador de la cedula de identidad **Nro:15.627.432**, por medio de la presente hago constar que he leído y evaluado el instrumento de recolección de datos correspondiente al Proyecto: **DESARROLLO DE PRÁCTICAS ESTRUCTURADAS BAJO UN ENFOQUE CISCO PARA EL LABORATORIO DE REDES DE COMUNICACIONES DE LA UNIVERSIDAD JOSÉ ANTONIO PÁEZ.**, presentado por la ciudadana **Genesis Theis**, Portadora de la cedula de identidad **25.009.134** (Respectivamente), para optar al título Ingeniero de Telecomunicaciones, el cual apruebo en calidad de validador.

En San Diego, a los 24 días del mes de Mayo del año dos mil diecisiete.

Ing. Javier Clavo C.I.: 15.627.432

**Prueba de
Funcionalidad de la
Practica N°2**



Practica-2

Configuración de los parámetros iniciales del switch

Objetivo: Esta Prueba tuvo como objetivo la verificación de la funcionalidad de la práctica N° 2 desarrollada y enfocada en tecnología Cisco, dirigida a los estudiantes de la asignatura redes de comunicaciones, materia impartida en el 8°vo semestre de la carrera Ingeniería de Telecomunicaciones de la Universidad José Antonio Páez.

Topología Física

A continuación se muestra la topología física, realizada en el rack para la conectividad exitosa de los switch Cisco Catalyst 2950, Cabe de destacar que se tomo el puerto 24 de cada switch para la conectividad entre los mismos utilizando a su vez una conectividad en cascada con cable patch cord cruzado y el puerto 1 de cada switch para la conectividad a cada PC correspondiente, utilizando cables patch cord directo.



Figura 1: Conectividad Fisca de los Switch Catalyst 2950

Fuente:Theis Genesis (2017)



Practica-2

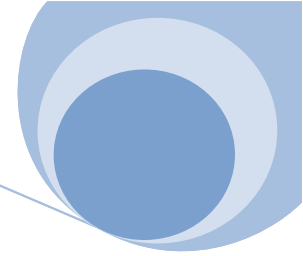
Es importante destacar que la configuración de dichos switches se hizo mediante la comunicación vía consola, utilizando a su vez un cable de consola, y un programa de emulación terminal como es el PUTTY.

Una vez ya armada la topología física, se procede a configurar las ip de las PC, como ya en la práctica se menciona detalladamente su procedimiento, como siguiente paso se procede a configurar los switches a través del programa de emulación terminal PUTTY, con los comandos que en la práctica se describen y en el orden como allí se mencionan. Un ejemplo de esta configuración se hace mostrar en las siguientes imágenes en donde se observa la configuración ya realizada tal cual como la práctica estructuradamente ya lo describe.

Figura 2: Configuración del switch 1 Cisco Catalyst 2950

Fuente: Theis Genesis (2017)

```
CDMI - PuTTY
Current configuration : 1569 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname S1
!
enable secret 5 $1$h6zZ$R0h1N74albdncveQPTJe00
!
ip subnet-zero
no ip domain-lookup
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
interface FastEthernet0/1
no ip address
--More--
```



Practica-2

```
COM1 - PuTTY
interface FastEthernet0/2
no ip address
!
interface FastEthernet0/3
no ip address
!
interface FastEthernet0/4
no ip address
!
interface FastEthernet0/5
no ip address
!
interface FastEthernet0/6
no ip address
!
interface FastEthernet0/7
no ip address
!
interface FastEthernet0/8
no ip address
!
interface FastEthernet0/9
--More--
```

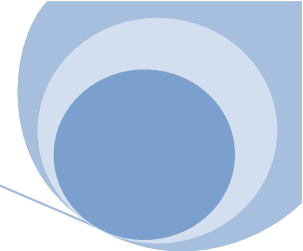
Figura 3: Configuración del switch 1 Cisco Catalyst 2950

Fuente: Theis Genesis (2017)

```
COM1 - PuTTY
interface FastEthernet0/17
no ip address
!
interface FastEthernet0/18
no ip address
!
interface FastEthernet0/19
no ip address
!
interface FastEthernet0/20
no ip address
!
interface FastEthernet0/21
no ip address
!
interface FastEthernet0/22
no ip address
!
interface FastEthernet0/23
no ip address
!
interface FastEthernet0/24
no ip address
--More--
```

Figura 4: Configuración del switch 1 Cisco Catalyst 2950

Fuente: Theis Genesis (2017)



Practica-2

```
COM1 - PuTTY
interface FastEthernet0/24
no ip address
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
ip http server
!
line con 0
password 7 0214015FOI15
login
line vty 0 4
password 7 070C285F4D06
login
line vty 5 15
login
end
#
```

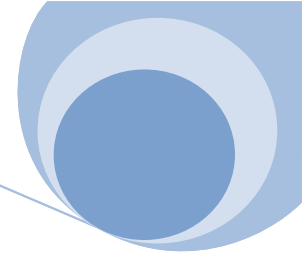
Figura 5: Configuración del switch 1 Cisco Catalyst 2950

Fuente: Theis Genesis (2017)

Nota: La configuración realizada en el Switch 1 de la red es la misma configuración que se debe realizar en el Switch 2.

Conclusión: Queda demostrada la configuración correcta entre los Switch Cisco, y la conectividad entre las PC y los switch que conforman la topología de la practica 2, dejando claro que la red cumple con los requisitos de conectividad que la practica de laboratorio quiere enseñar, en donde básicamente se quiere que el estudiante aprenda a configurar los parámetros iniciales de un Switch Cisco.

**Prueba de
Funcionalidad de la
Practica N°4**



Practica-4

Configuración de enrutamiento estático

Objetivo: Esta Prueba tuvo como objetivo la verificación de la funcionalidad de la práctica N° 4 desarrollada y enfocada en tecnología Cisco, dirigida a los estudiantes de la asignatura redes de comunicaciones, materia impartida en el 8°vo semestre de la carrera Ingeniería de Telecomunicaciones de la Universidad José Antonio Páez.

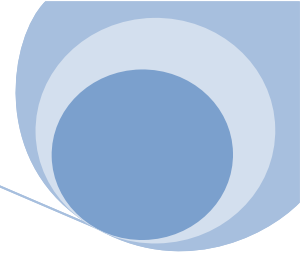
Topología Física

A continuación se muestra la topología física, realizada para la conectividad exitosa de los Router Cisco 1700, Cabe de destacar que se tomo el puerto serial de cada router para la comunicación serial entre los mismos, en donde el router 1 es el DCE (el reloj) y el router 2 es el DTE, cumpliendo así con los parámetros de comunicación para lograr la sincronización entre los mismos. Es importante mencionar que se utilizo a su vez un cable patch cord cruzado en los puertos Ethernet de cada Router para logra la conectividad a cada PC correspondiente.



Figura 3: Conectividad Física de los Routers Cisco 1700

Fuente: Theis Genesis (2017)



Practica-4

Es importante destacar que la configuración de dichos routers se hizo mediante la comunicación vía consola, utilizando a su vez un cable de consola, y un programa de emulación terminal como es el PUTTY.

Seguidamente de armar la topología física de la red, se procede a configurar las ip según la tabla de direccionamiento como se muestra en la práctica, y a su vez se configuran los router según los pasos y comandos que se mencionan en la misma, cabe de destacar que la configuración de estos router se basan en: seguridad de contraseña de acceso a la consola, modo privilegiado, acceso telnet y ssh, además de se realizó la configuración de ip tanto en el equipo como en los puertos serial y por último pero no menos importante configuro el enrutamiento mediante la creación de rutas estáticas para lograr la comunicación entre la PC.

Como verificación de la conectividad y comunicación exitosa de los equipos que conforman la red implementada en la practica N°4, se hacen mostrar imágenes a continuación donde se demuestra el ping de una PC a otra.

```
Símbolo del sistema
C:\Users\Ricardo>ping 192.168.1.3
Haciendo ping a 192.168.1.3 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.1.3:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

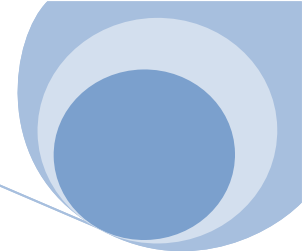
C:\Users\Ricardo>ping 192.168.12.1
Haciendo ping a 192.168.12.1 con 32 bytes de datos:
Respuesta desde 192.168.12.1: bytes=32 tiempo=10ms TTL=254
Respuesta desde 192.168.12.1: bytes=32 tiempo=9ms TTL=254
Respuesta desde 192.168.12.1: bytes=32 tiempo=9ms TTL=254
Respuesta desde 192.168.12.1: bytes=32 tiempo=9ms TTL=254

Estadísticas de ping para 192.168.12.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 9ms, Máximo = 10ms, Media = 9ms

C:\Users\Ricardo>
```

Figura 4: Ping de la PC-B a la PC-A

Fuente: Theis Genesis (2017)



Practica-4

```
Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Natacha>ping 192.168.12.2

Haciendo ping a 192.168.12.2 con 32 bytes de datos:
Respuesta desde 192.168.12.2: bytes=32 tiempo=1ms TTL=254
Respuesta desde 192.168.12.2: bytes=32 tiempo=9ms TTL=254
Respuesta desde 192.168.12.2: bytes=32 tiempo=9ms TTL=254
Respuesta desde 192.168.12.2: bytes=32 tiempo=9ms TTL=254

Estadísticas de ping para 192.168.12.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 9ms, Máximo = 1ms, Media = 9ms

C:\Users\Natacha>
```

Figura 5: Ping de la PC-A a la PC-B

Fuente: Theis Genesis (2017)

Conclusión: Queda demostrada la configuración correcta entre los Routers Cisco, y la conectividad entre las PC y los routers que conforman la topología de la practica 4, dejando claro que la red cumple con los requisitos de conectividad que la practica de laboratorio quiere enseñar, en donde básicamente se quiere que el estudiante aprenda a configurar los parámetros básicos del router, además de su configuración ip, aplicando los principios de enrutamiento entre routers y utilizando la creación de rutas estáticas en los mismos.